Maritime and Coastguard Agency

MARINE GUIDANCE NOTE

MGN 298 (M)

Measures to Counter Piracy, Armed Robbery and other Acts of Violence against Merchant Shipping

Note to all ship-owners and operators (companies), Masters etc.

This Marine Guidance Note supersedes Marine Guidance Note 241 (M) issued in November 2002.

SUMMARY

This Marine Guidance Note aims to assist all ship owners and operators (companies), Masters and seafarers in understanding the risk of piracy, armed robbery and other acts of violence against ships, and reminds them of the importance of taking action to deter such acts and advises on how to deal with them if they occur.

Key points:

• Be vigilant
• Reduce opportunities for theft
• Secure Restricted Areas at all times and establish safe secure area(s)
• Maintain, exercise and regularly review your Ship Counter-piracy Plan
• Report all incidents to the coastal and Flag State authorities (for UK flagged ships this is TRANSEC within the Department for Transport).

An index of this MGN, to assist readers find information on specific issues, is provided on page 28.

1. INTRODUCTION

1.1 This Marine Guidance Note (MGN) brings to the attention of ship owners and operators (referred to as companies in this document), Masters and crews, the risk of acts of piracy on the high seas or armed robbery against ships within the territorial sea of a State. It outlines steps that should be taken to **reduce the risk** of such attacks, possible responses to them and the need to report attacks, both successful and unsuccessful, to the authorities of the relevant Coastal State(s), to the IMB reporting centre and to the ship's own maritime administration. This MGN has been amended to take account of the International Ship and Port Facility Security Code Regulations, which were implemented on 1st July 2004 and their impact on the security requirements of UK ships and also on reporting procedures for incidents. The guidance has also been updated where the implementation of the Ship Security Alert System (SSAS) and Automatic Identification System (AIS) has had an impact on procedures.

1.2 In the United Kingdom, the Secretary of State for Transport is responsible for both maritime security and counter-piracy policy with regard to UK flagged ships. The Secretary of State's powers and responsibilities are designated to the Transport Security and Contingencies Directorate (TRANSEC) within the Department for Transport.

1.3 This Marine Guidance Note, which has been developed and written by TRANSEC, is principally aimed at UK seafarers on board UK flagged ships and refers in the first instance to UK maritime security/counter-piracy policy and procedures. However, TRANSEC acknowledges that the majority of readers will be UK nationals serving on board foreign owned/controlled and/or flagged ships. The text therefore makes it clear that the reader should also be aware of their own Flag State's maritime security/counter-piracy policies and procedures.

2. TRENDS IN PIRACY

2.1 The continuing high number and geographical spread of attacks clearly demonstrates that the issue of piracy and armed robbery at sea has not gone away since this Marine Guidance Note was last updated in 2002. However, there was a 27% reduction in piracy attacks between 2003 and 2004, bringing the total number of attacks down to 325 and the figures for the first 6 months of 2005 show that the overall number of attacks is on course to reduce again this year from 182 to 127, a 30% reduction. Although this reduction appears to be positive, in reality the devastating tsunami that occurred at the end of 2004 had a significant, albeit temporary, impact on the piracy figures for that area and this natural disaster is likely to account for a significant percentage of the reduction in attacks this year. Additionally, piracy attacks have seriously escalated this year in Somali and Iraqi waters, which reflects the general state of security in both of those countries. The current main hot spot areas where piracy attacks are prevalent are the Horn of Africa, including Somali waters and the Gulf of Aden; South East Asia including Indonesian waters, the Malacca Straits and the South China Sea; the Bay of Bengal; the Niger Delta in West Africa and also Iraqi/Persian Gulf waters. APPENDIX 1 provides more detail on the trends, figures and locations for piracy attacks.

2.2 While the overall reduction in piracy attacks since 2002 is welcome, there are still a number of locations around the world where increasingly violent attacks are taking place by well-organised groups. Masters and crew need to exercise extreme caution when transiting these areas. The updating and re-issue of this Guidance Note serves as an important reminder to seafarers about the measures that can be put in place to deter and deal with piracy and armed attacks. Details of such attacks are regularly reported in Lloyd's List and up to date information can be obtained from the Piracy Reporting Centre in Kuala Lumpur (see paragraph 11.1) and from the IMO in their monthly Maritime Security Committee Circulars (MSC.4/Circ.xx series). TRANSEC also issues advice to UK seafarers regarding specific countries or sea areas of concern as the need arises.

3. THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE

3.1 The ISPS Code is an internationally agreed protective security regime for the maritime sector and was adopted in a resolution on 12 December 2002 by a Diplomatic Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS) 1974. Another resolution was adopted which made necessary amendments to SOLAS Chapter V and the new Chapter XI-2 (the original chapter XI was amended and split into XI-1 and XI-2) of SOLAS by which compliance with the ISPS Code became mandatory on 1 July 2004. It contains measures aimed at improving the security of ships and port facilities by placing obligations on governments and the maritime industry, including the appointment of security officers, the preparation of security assessments, the implementation of security plans, the issue of mutually recognised security certificates and the setting of security levels. The changes that the amendments to SOLAS and the ISPS Code have brought and their impact on counter-piracy policy and procedures is explained in more detail in APPENDIX 2.

4. LOCATIONS AND METHODS OF ATTACK

4.1 Theft or Robbery from a Ship

4.1.1 The most common form of piracy and armed attack consists of boarding a ship, stealing cargo or ship's equipment and withdrawing (over 90% of successful attacks in 2003 fell into this category). Last year just over half of these robberies occurred when the ship was in port or at anchor with the remainder occurring when the ship was underway (both within territorial and international waters). The majority of incidents in port are opportunistic and a ship in port is particularly vulnerable since it is in a fixed position, will normally have a skeleton crew and the attacker has both more and easier escape routes than when the ship is at sea.

4.1.2 Most thefts of ships stores and equipment are carried out on an opportunity basis, particularly when crews appear to be complacent in their surroundings and less alert. More professional criminal gangs, including those in South East Asian waters, will target high value goods such as cash and valuables in the ship's safe, crew possessions and any portable ship's equipment. Such gangs have also stolen less valuable items in the past, including paint and mooring lines. Where there is evidence of tampering with containers it has been suggested that the raiders may initially have gained access when the ship was berthed in port and then gone over the side, with what they could carry or when the ship was underway to be picked up by their accomplices. In recent cases, when this was suggested, it had been found that compartments may not have been fully searched or secured before the ship left port.

4.2 Attacks at Anchor (Within Port Limits or at Anchorage)

4.2.1 A ship at anchor is usually boarded from a small boat under the cover of darkness. Most attacks occur between 2200 and 0600 hrs and the attackers primarily board the ship from the stern using grappling hooks attached to the ship's rail or by climbing the anchor chain. Often the raiders will try not to alert the crew, although they may take a crewmember hostage and threaten them either to gain information or to intimidate and gain control over the Master or other crewmembers, or to gain access to the crews' quarters. Communication equipment may be destroyed to prevent or delay the alarm being raised; crews' quarters may be raided for portable personal possessions; the Master's safe may be opened and any cash stolen and there may either alternatively or simultaneously be some opening of containers or holds. There is some evidence of selective opening of containers or holds with high value cargoes implying prior knowledge of the cargo manifest. The attackers may also steal any movable ship's stores. Having removed what they can carry, the raiders depart. There is some evidence that members of boarding parties have been recognised as previously having had access to the ship as employees of shore based cleaning or other contractors.

4.3 Attacks When Tied Alongside

4.3.1 A ship tied alongside either the quay wall or another ship is usually boarded by walking up an unmanned boarding ramp (gangway) between ship and shore/ship to ship, or by climbing mooring ropes and anchor chains or using grappling hooks to get on deck. Given the opportunistic nature of attacks when a ship is moored in port or at anchor, an attacker is statistically less likely to resort to violence and they may seek to escape empty-handed if challenged by crew. An exception to this is in the Caribbean where currently the favoured method of attack is for the attackers to rush on board a ship, brandishing knives to force the crew into handing over valuables.

4.4 Attacks When Underway

4.4.1 Attacks on ships whilst underway can often be more threatening and dangerous for a ship's crew than an attack taking place in port, as the attack is likely to be planned and the attackers will almost certainly be armed.

The majority of these attacks have taken place against ships in South East Asian waters and more recently around the Horn of Africa (refer to APPENDIX 1 for more detailed information on attacks). Recent evidence indicates that you should assume that they are carrying and prepared to use firearms (in 2003, the figure was 80% of attackers) and in a limited number of cases more powerful devices such as rocket-propelled grenades have been brandished or employed. Such incidents often involve the use of the tactics described in the following paragraphs.

4.4.2 Under cover of darkness, again most often between dusk and dawn, one or more high speed, low profile craft come alongside the intended target often utilising any blind spots such as approaching from the stern, but also the sides if the ship has a low freeboard. It should be noted that ships travelling at slow speeds, especially if this is combined with a low freeboard, are more vulnerable to attack. Access to the ship will often be by climbing up poles or by utilising grappling irons hooked on to the ship's rail. Attackers have shown considerable skill and daring and have boarded ships travelling in excess of 17 knots and with high freeboards. They have demonstrated knowledge of ship's procedures, often seeking to board when bridge and engine room personnel are fully engaged in navigating through congested or restricted waters, and knowledge of the general layout of the ships they have attacked. The small craft used by the attackers may come from adjacent coastlines (hiding behind headlands and islands until the ship is close enough to engage) or be launched from "mother" ships and there have been occasions where larger ships running without lights have been reported in the vicinity of ships which have been attacked.

4.4.3 Attackers have also been known to try to blend in with local fishing boats or to disguise themselves as Coast Guard or Naval personnel, or Pilots in order to board the ship. In the North Persian Gulf and particularly along the Iranian coast and waterways of Iraq, criminal gangs are operating from small high-speed craft and tend to conceal themselves among fishing fleets. When a target ship nears, the attackers' boats will break cover, approach the ship to allow the attackers to board the ship, stealing any valuables, particularly cash, or alternatively they may demand protection money. Another method is the stringing of fishing nets across the waterways to force the ships to slow and damage the nets. The ship is then boarded by the 'fishing crew' who demand compensation for the nets.

4.4.4 Attackers have boarded ships, made their way to the Master's cabin and intimidated crewmembers by threats or assault, into opening the safe. They have then departed taking what they can with them without alerting any other members of the crew. There have also been incidents of crewmembers being seized and threatened to secure the crew's compliance. In a number of hijack incidents the entire crew has been seized and locked up. This poses a serious threat to the safety of shipping because although the typical attack lasts for between 15 minutes and an hour, ships can be under the control of attackers for a much longer period with few, if any, qualified mariners manning the bridge. The ship could therefore be controlled by the attackers throughout this period and they themselves are likely to be under great stress. This can lead to a significant risk of collision or grounding with accompanying loss of life and if the ship is an oil tanker or chemical carrier, it can additionally result in major pollution.

4.4.5 Although the vast majority of attacks are to secure cash and steal crew possessions or portable equipment there are still cases of ships and their cargoes being seized and the entire cargo, and occasionally the ship, being disposed of by the attackers.

4.5 Hijacking of Ships

4.5.1 Such operations tend to be complex and require considerable expertise and resources, which usually puts them beyond the means of small opportunist groups. For example, in the late 1990's most hijacking incidents took place in the South China Sea and these were run by large organised crime syndicates until China launched a successful crackdown. Despite their complexity there has been an increase in the number of hijackings of ships to steal the cargo (usually transferring it to another ship) over the last decade.

A number of violent and well organised hijacking operations have taken place in the Malacca Straits this year following the initial lull in activity as a result of the tsunami. There have been a number of well documented cases such as the Alondra Rainbow or the recent case of the Natris/Paulijing where the ships have been physically altered and re-registered, in essence becoming 'phantom' ships. Similarly there is also a trend now towards the targeting of smaller tugs, barges and yachts which requires far less planning and resources. The ship's crew, particularly the most senior members are also now more likely to be taken captive and held to ransom, rather than have cargo or valuables stolen, particularly at the northern end of the Malacca Straits, in the Niger Delta and off the coast of Somalia. Several ransom demands have been met which may contribute to an increase in attacks of this type. Therefore, it is important that Masters and crew should be aware of the increased possibility of this type of attack when sailing in areas where ransom demands have previously been paid. If a ship is hijacked, crewmembers should adopt an acquiescent attitude and comply with the hijacker's demands and seek to avoid any actions that may antagonise further, what are likely to be already agitated attackers. Failure to do so is likely to endanger the lives of crewmembers.

5. FACTORS ENCOURAGING OR FAVOURING ATTACKERS

5.1 Cash in the Ship's Safe

5.1.1 The belief that large sums of cash are carried in the Master's safe attracts attackers. On several occasions this belief has been justified and substantial sums have been stolen. While carrying cash may sometimes be necessary to meet operational needs and crew requirements and to overcome exchange control restrictions in some States, it entices attackers, who in turn are likely to intimidate the Master or other crewmembers to open the safe. Even if the cash is dispersed throughout the ship the attackers may intimidate crewmembers until the locations have been revealed. Companies should consider ways of eliminating the need to carry large sums of cash on board ship. When this need arises because of exchange control restrictions imposed by States the matter should be referred to the ship's maritime administration to consider if representations should be made to encourage a more flexible approach as part of the international response to eliminate attacks by pirates and armed robbers. If large sums of money must be carried it is advisable to secrete safes in less obvious locations, i.e. not in the Master's cabin, or to have a number of safes each with a smaller amount of money. In either case it may be advantageous to limit the number of people with knowledge of the safes location(s) to the minimum required for operational purposes. Consideration could also be given to alarming the safes to indicate tampering.

5.1.2 Although the incidence of cruise ships being targeted is extremely low, these ships are attractive to those groups set on unlawful activity due to the money and valuables carried by their passengers. By virtue of their size (deck height) and the size of their crews, these ships are currently less susceptible to attack whilst underway than most other ships. As the attackers develop more sophisticated tactics and employ increasingly sophisticated equipment, so the threat of an attack on a cruise ship increases. Therefore, extra vigilance should be maintained when these ships are in port, and in particular when they are tied alongside.

5.2 Smaller Crews

5.2.1 The smaller crew numbers found on board most ships also favour the attacker. A small crew engaged in ensuring the safe navigation of their ship through congested or confined waters may also have the additional task of maintaining high levels of security surveillance and preparedness for prolonged periods. Companies should ensure that security watches are enhanced if their ship is in waters or ports, where attacks are known to occur.

Companies should also consider providing appropriate, i.e. designed for the marine environment, surveillance systems (e.g. portable or fixed CCTV) and intruder detection equipment (security systems incorporating robust sensors and alarms) to aid their crews and protect their ships.

The provision of piracy alarm systems on bridge wings and other vulnerable/ lookout positions should be seriously considered. Companies should also consider the need for additional security personnel to be carried (above the normal crewing level) in areas of high risk. If such a decision is taken, companies should seek to verify the bona fides of any security personnel they may engage locally.

6. RECOMMENDED PRACTICES

6.1 Recommended Practices Overview

6.1.1 The recommended practices outlined below are based on reports of incidents, advice published by commercial interests and organisations and measures developed to enhance ship security. The extent to which the recommendations are followed or applied are matters solely for the Company/Ship Security Officers or Masters of ships operating in areas where attacks may occur. The recommendations are not designed to replace or supersede the security measures recorded in the Ship Security Plan, but they may be operated in addition to the security measures required by the plan at each Security Level.

6.1.2 If possible appropriate risk assessments should be conducted by the Company/ Ship Security Officers or Master, prior to a ship entering areas with a high incidence of piracy. The aim of the assessment is to determine whether additional security personnel and/or measures are required over and above the mandatory security measures specified in the Ship Security Plan for the given Security Level.

6.2 The Counter-piracy Plan

6.2.1 All UK flagged ships operating in waters where piracy incidents occur should hold or develop a counter-piracy plan. This plan should be prepared having regard to the risks that may be faced, the crew numbers available, their capability and training, the ability to establish secure areas on board the ship (for crew to lock themselves into in the event that attackers are successful in boarding the ship) and should also cover the surveillance and detection equipment that has been provided. The plan should, among other things, cover:

- the need for enhanced watch keeping, and the use of lighting and surveillance, detection or perimeter protection equipment;
- crew responses if a potential attack is detected or an attack is underway;
- the radio and alarm procedures to be followed;
- the reports that should be made after an attack, or an attempted attack;
- training to ensure crew react consistently to an incident.

6.2.2 Counter-piracy Plans should ensure that Masters and crews are made fully aware of the risks involved during attacks by pirates or armed robbers. In particular it should address the dangers that may arise if a crew adopts an aggressive response to an attack. Early detection of a possible attack is the most effective deterrent. Aggressive responses once an attack is underway, and in particular once the attackers have boarded the ship, could significantly increase the risk to the ship and those on board. The counter-piracy plan can exist as a stand-alone document or be incorporated into the Ship Security Plan (see APPENDIX 2) for ease of reference for relevant members of the ship's crew. The important point is that the Counter-piracy Plan should supplement the Ship Security Plan but that the latter document must take precedence as a Government approved official document.

6.3 Routing and Delaying Anchoring

6.3.1 If at all possible ships should, at the Master's discretion, be routed away from areas where attacks are known to take place and in particular seek to avoid bottle necks.

If ships are approaching ports where attacks have taken place on ships at anchor, rather than on ships underway, and it is known that the ship will have to anchor off port for some time, consideration should be given to delaying anchoring by slow steaming or longer routing to remain well off shore thereby reducing the period during which the ship will be at risk. Charter party agreements should contain up to date War Clauses, which include piracy provisions and recognise that ships may need to delay arrival at ports where attacks occur, either when no berth is available for the ship, or off shore loading or unloading will be delayed for a protracted period.

6.4 Prior to Entering Areas where Attacks Occur

6.4.1 Prior to the ship entering an area where attacks have occurred the ship's crew should have practised and perfected the procedures set down in the Ship's Security Plan and/or counter piracy plan. Communication systems, alarm signals and procedures should have been thoroughly practised. If instructions are to be given over the ship's address systems or personal radios they must be clearly understood by those who may not have fully mastered the language in which the instructions will be given. To this end, code words could be employed to simplify the issuing of instructions, and the initiation of pre-rehearsed responses.

6.4.2 Access points to the ship and any secure restricted or controlled areas must be controlled through monitoring and patrolling in port and at anchor, and as far as practicable when the ship is underway (see paragraph 6.16.6 and APPENDIX 3 for further information). Crews should be trained in the use of any additional surveillance or detection equipment installed on the ship. Planning and training must be on the basis that an attack will take place and not in the belief that with some luck it will not happen. Indications to attackers that the ship has an alert and trained crew implementing an effective Counter-piracy Plan could help deter them from attacking the ship.

6.5 At Anchor or in Port

6.5.1 The ISPS Code and UK Government requires as a minimum that access to all UK flagged ships is controlled in order to prevent unauthorised access (measures to be put in place at each access point must be listed in the Ship Security Plan) and that an identification system (for example an ID Pass system incorporating a photograph of the pass holder) must be in place for visitors. The specific measures put in place will vary according to the Flag State and the ship itself. However extra precautions should be taken over certain groups of people who require access to the ship such as Stevedores. It would also be beneficial to site CCTV equipment and other electronic monitoring devices in such a way as to ensure coverage of areas vulnerable to infiltration e.g. the stern, low freeboards, the hawse pipe/ hole and the chain locker (see paragraph 6.10). It would also be wise to consider greasing or installing razor wire woven through and around the anchor chain (extending up to 2 metres down the hawse pipe) while the ship is at anchor to prevent climbing. Hawse pipe covers should be securely locked in place (attackers have been known to reach through covers and undo the traditional wing nut arrangement). A final and temporary measure while the ship is at anchor could be activate the ship’s fitted anchor cable wash-down system, or to aim a fire hose through the hawse pipe turned on at full pressure.

6.5.2 In high-risk areas, it is recommended that the Master organises a system of regular deck patrols and that they be conducted by a sufficient number of crew to ensure personal safety. The crewmembers conducting the patrol should be suitably equipped with two-way radios to ensure instant communication with the bridge, concentrating on vulnerable areas of the ship. The patrols and search patterns should be staggered at unpredictable and irregular intervals to prevent a potential attacker from establishing a routine which can then be exploited.

6.5.3 Given that attackers may use knowledge of cargo manifests to select their targets every effort should be made to limit the circulation of documents which give information on the cargoes on board or their location on the ship.

6.5.4 While it is acknowledged that there are considerable time pressures associated with the requirement for fast turnarounds in port, the security of the ship should not be compromised by poor procedures. Prior to leaving port/anchorage the ship should be thoroughly searched and all external doors or access points secured or controlled, with priority given to the bridge. Internally priority should be given to the engine room, steering space and other vulnerable areas. Doors and access points should be regularly checked thereafter. The means of controlling doors or access points which would need to be used in the event of an on board emergency will need careful consideration. Crew safety should not be compromised.

6.6 Watch-keeping and Vigilance

6.6.1 Maintaining vigilance is essential. All too often the first indication of an attack has been when the attackers appear on the bridge or in the Master's cabin. Advance warning of a possible attack will give the opportunity to sound alarms, alert other ships and the coastal authorities, illuminate the suspect craft, undertake evasive manoeuvring or initiate other response procedures. Signs that the ship is aware it is being approached can deter attackers.

6.6.2 When ships are in, or approaching, areas where attacks are known to have taken place, bridge watches and look outs should be significantly strengthened, manpower resources allowing. Additional watches on the stern or covering radar "blind spots" should also be considered if manpower allows. Companies should consider investing in low light binoculars for bridge staff and lookouts. Radar stations should be frequently manned, even though it may be difficult to detect low profile fast moving craft on a ship's radars. A Yacht or I-band radar mounted on the stern may provide additional monitoring capability to detect small craft approaching from astern. Use of an appropriately positioned radar system when the ship is at anchor may also provide warning of the close approach of small craft.

6.6.3 It is particularly important to maintain a radar and visual watch for craft which may be trailing the ship when underway, but which could close with the ship quickly when mounting an attack. Small craft, which appear to be matching the speed of the ship on a parallel or following course, should always be treated with suspicion. When a suspect craft has been noticed it is important that an effective all round watch is maintained in case the ‘obvious’ craft is a decoy. A decoy could be used to divert the attention of the ships’ crew away from a second craft on the other side of the ship, which could then be used to board the ship unobtrusively.

6.6.4 Companies with ships that frequently visit areas where attacks have occurred should consider the purchase and use of more sophisticated visual and electronic devices in order to augment both radar and visual watch capability against attackers' craft at night, thereby improving the prospects of obtaining an early warning of a possible attack. Additional advice on more sophisticated equipment appropriate for use on British ships will be provided on request from the Department for Transport (see section 14 for Transec contact details).

6.7 Ship Communications

6.7.1 Radio Procedures and Watch-keeping. There is detailed guidance on radio procedures, radio watch keeping advice and standard message formats contained in APPENDIX 3.

6.7.2 Ship Security Alert System. The amendments to SOLAS (Chapter X1-2) has required the installation of a new Ship Security Alert System (SSAS) on ships which are subject to the SOLAS Convention. The purpose of SSAS is to provide a covert means of alerting the ship's Flag State and company to the fact that a serious security incident is occurring on board the ship. (refer to APPENDIX 2 for more details).

6.7.3 Automatic Identification System (AIS) is required under Chapter V of SOLAS. AIS is a shipboard broadcast system that allows a ship's location and movements to be monitored within a certain range, both on shore and by other suitably equipped ships (see APPENDIX 2 for more details).

6.8 Lighting (When Underway)

6.8.1 Ships should use the maximum lighting available consistent with safe navigation, having regard in particular to the provisions of Rule 20(b) of the 1972 Collision Regulations. Bow, and overside lights should be left on if possible. Ships must not keep on deck lights when underway as it may lead other ships to assume the ship is at anchor. Wide beam floods could illuminate the area astern of the ship. Signal projector lights can be used systematically to probe for suspect craft illuminating radar contacts if possible. So far as is practicable crewmembers on duty outside the ship's secure areas when in port, or at anchor, should avail themselves of shadow and avoid being silhouetted by deck lights as this may make them targets for seizure by approaching attackers.

6.8.2 It has been suggested that ships underway should be blacked out except for mandatory navigation lights. This may prevent attackers establishing points of reference when approaching a ship. In addition turning on the ship's lights as attackers approach could alert them that they have been seen, dazzle them, and encourage them to desist. The fitting of passive infrared (PIR) activated floodlights to the periphery of the ship could be considered to ensure that the lights do come on, even if attackers are not observed in advance. It is difficult, however, to maintain full blackout on a merchant ship. The effectiveness of this approach will ultimately depend in part on the level of moonlight, but primarily on the vigilance and light discipline (the control of emitted light) of the ship's crew. While suddenly turning on the ship's lights may alarm or dazzle attackers it could also place the crew at a disadvantage at a crucial point through temporary loss of their night vision. To this end it is recommended that crews be instructed on how to preserve and enhance their night vision. Crewmembers can maximise their visual acuity by the simple expedient of not looking directly at the intended point. By focussing a few degrees (any direction) off the target, peripheral vision is utilised, and this is better suited to both motion detection and night sight. Ensuring that crews are adequately briefed and trained is essential and thought should be given on how to warn crewmembers that light is about to be employed, without forewarning the attackers.

6.9 Lighting (At Anchor)

6.9.1 The above lighting requirements under the Collision Regulations are not applicable when ships are at anchor or in port, and crews are at liberty to light their ships as they see fit (as long as they do not dazzle other mariners). However, many ships are not adequately fitted with deck lights and are thus poorly lit even when all of them are switched on. To reduce the number of areas vulnerable to night infiltration, it is recommended that the existing number, or at least the placement, of deck lights is reconsidered. Lighting of vulnerable areas could be linked to an alarm system or detection/surveillance equipment.

6.10 CCTV

6.10.1 As an additional deterrent, deck lighting directed on vulnerable areas of the ships superstructure, e.g. the stern, freeboards, the hawse pipe/hole and the chain locker could be augmented by effective CCTV coverage.

6.10.1 Companies should seek to provide closed-circuit television (CCTV) coverage, and recording of, the main access points to the ships secure areas (see paragraph 6.11), the corridors approaching the entrances to key areas and the bridge. If possible the recording equipment should be housed in a secure environment or at least in an unobtrusive place, so that there is an increased chance of it surviving any attack on the ship.

The ISPS Code requires that proper procedures are in place for the maintenance of CCTV systems including the documentation and reporting and fixing of defects.

6.11 Secure Areas

6.11.1 In accordance with the ship's Counter-piracy Plan, the Master and crew should ensure that they have a secure area(s) on the ship where they can safely retreat to in the event of attackers successfully boarding and hijacking the ship. This definition of a secure area should not be confused with the term Restricted Area as required by the ISPS Code, which requires access control measures to sensitive parts of a ship (refer to APPENDIX 2 for further details). However, it would make sense to place the secure area(s) of the ship within the ship's Restricted Areas because robust access control measures will already be in place.

6.11.2 All doors to a designated secure area(s) should be secured and/or controlled at all times and should be regularly inspected and monitored, for example by using CCTV. Consideration should be given to the installation of special access control systems to these areas. Ports, scuttles and windows, which could provide access should also be securely closed and have laminated glass installed if possible. Deadlights should be shut and clipped tightly. The internal doors within secure areas which give immediate access to key areas such as the bridge, radio office, engine room and Master's cabin should be strengthened and have special access control systems and automatic alarms. Certainly basic measures such as a spy-hole or an electronic door viewer should be considered for fitting to both the Master's cabin door and the internal Bridge door in order to establish who is on the other side before opening. Access control measures, surveillance and patrolling should all be stepped up in accordance with the Security Level that the ship is operating at.

6.11.3 Securing doors providing access to, and egress from, secure areas may give rise to concern over safety in the event of an accident. In any situation where there is a conflict between safety and security, the safety requirements should be paramount. Nevertheless, attempts should be made to incorporate appropriate safety provisions to ensure ease of egress and to permit access by rescue /emergency parties while allowing entries and exits to be secured or controlled.

6.11.4 To prevent the seizure of individual crewmembers by attackers (seizure and threatening a crewmember is one of the more common means of attackers gaining control over a ship), all crewmembers not engaged on essential outside duties should remain within a secure area during the hours of darkness. Those whose duties necessarily involve working outside such areas at night should remain in constant communication with the bridge and should have practised using alternative routes to return to a secure area in the event of an attack. Crewmembers who fear they may not be able to return to a secure area during an attack should select places in advance in which they can take temporary refuge. There should also be designated muster areas within the ship's secure areas where the crew can muster during an attack and communicate their location and numbers to the bridge.

6.12 Alarms

6.12.1 Alarm signals, including the ship's whistle, should be sounded on the approach of attackers. Alarms and signs of response can discourage attackers. Alarm signals or announcements which provide an indication at the point at which the attackers may board, or have boarded, may help crewmembers in exposed locations select the most appropriate route to return to a secure area.

6.13 Evasive Manoeuvring and Use of Hoses

6.13.1 Provided that navigational safety allows, Masters should consider "riding off" attackers craft by heavy wheel movements as they approach. The effect of the bow wave and wash may deter 'would be' attackers and make it difficult for them to attach poles or grappling irons to the ship.

Manoeuvres of this kind should not be used in confined or congested waters or close inshore or by ships constrained by their draught in the confined deep water routes found, for example in the Malacca and Singapore Straits.

6.13.2 The use of water hoses should also be considered, though the use of such equipment may be inappropriate and counter-productive in regions that have a high incidence of attackers employing firearms since the use of a water hose may antagonise the attackers causing them to start shooting at the ship and crew. It is at the Master's discretion as to whether such a defensive measure should be employed, and careful consideration must pre-empt any such order to crewmembers. Hoses may also be difficult to train on an approaching ship if evasive manoeuvring is taking place. However, water pressures of more than 550 kilopascals/ Kpa (80 lb psi) and above have deterred and repulsed attackers. Not only does the attacker have to fight against the jet of water, but the flow may swamp their boat and damage engines and electrical systems. Special fittings for training hoses could be considered which would also provide protection for the hose operator. A number of spare fire hoses could be rigged and tied down at vulnerable areas of the ship e.g. the stern whilst underway and anchor points/gangways whilst at anchor. These hoses could then be pressurised at short notice if a potential attack is detected.

6.13.3 Employing evasive manoeuvres and hoses must rest on a determination to successfully deter attackers or to delay their boarding long enough to allow all crewmembers to gain the sanctuary of secure areas. Continued heavy wheel movements with attackers on board may lessen their confidence that they will be able to return safely to their craft and may persuade them to disembark quickly. However, responses of this kind could lead to reprisals by the attackers if they seize crewmembers, and should not be undertaken unless the Master is confident that they can be used to advantage and without risk to those on board. They should not be used if the attackers have already seized crewmembers.

6.14 Use of Distress Flares

6.14.1 The only flares authorised for carriage on board ship are intended for use if the ship is in distress and is in need of immediate assistance. As with the unwarranted use of the Distress signal on the radio (see APPENDIX 3) use of distress flares simply to alert shipping rather than to indicate that the ship is in grave and imminent danger may reduce their effect in the situations in which they are intended to be used and responded to. Radio transmissions should be used to alert shipping of the risk of attacks rather than distress flares. Distress flares should only be used when the Master considers that the attacker's actions are putting the ship in grave and/or imminent danger.

6.15 Firearms

6.15.1 The carrying and use of firearms for personal protection or protection of a ship is strongly discouraged and will not be authorised by the British Government. Carriage of arms on board ship may escalate an already dangerous situation, and any firearms on board may themselves become an attractive target for an attacker. The use of firearms requires special training and aptitudes and the risk of accidents with firearms carried on board ship is great. In some jurisdictions killing a national may have unforeseen consequences even for a person who believes that they have acted in self-defence.

6.16 If Attackers Board

6.16.1 Early detection of potential attacks must be the first line of defence and action to prevent the attackers actually boarding the second, but there will be incidents when attackers succeed in boarding a ship. The majority of pirates and armed robbers are opportunists seeking an easy target and time may not be on their side, particularly if the crew are aware they are aboard and are raising the alarm. However, the attackers may seek to compensate for the pressure of time they face by escalating their threats or the violence they employ.

6.16.2 Once attackers have boarded, the actions of the Master and crew should be aimed at:

- securing the greatest level of safety for those on board the ship;
- seeking to ensure that the crew remain in control of the navigation of the ship;
- securing the earliest possible departure of the attackers from the ship.

6.16.3 If the crew is able to maintain control of the ship it is advisable, when navigating in confined waters, to reduce speed and/or head for open waters if possible. This recourse may reduce the risk of grounding or collision if the attackers were to gain control of the ship in the future.

6.16.4 The options available to the Master and crew will depend on the extent to which the attackers have secured control of the ship. If attackers gain access to the bridge or engine room, or seize crewmembers who they can threaten, the Master or crew may be coerced into complying with their wishes. However, even if the crew are all safely within secure areas, the Master will always have to consider the overall risk to the ship, and the damage the attackers could cause outside those secure areas, e.g. by using firebombs to start fires on a tanker or chemical carrier.

6.16.5 If the Master is certain that all crewmembers are within secure areas and that the attackers cannot gain access, or by their actions outside the secure areas place the entire ship at imminent risk, then consideration may be given to undertaking evasive manoeuvres of the type referred to in section 6.13, to encourage the attackers to return to their craft. The possibility of a sortie by a well organised crew has, in the past, successfully persuaded attackers to leave a ship but the use of this tactic is only appropriate if it can be undertaken at no risk to the crew.

6.16.6 For an action like this to be attempted the Master must have clear knowledge of where the attackers are on the ship, that they are not carrying firearms or other potentially lethal weapons and that the number of crew involved significantly outnumbers the attackers they will face. If a sortie party can use water hoses they stand an increased chance of success. The intention should be to encourage the attackers back to their craft. Crewmembers should not seek to come between the attackers and their craft nor should they seek to capture attackers as to do so may increase the resistance the attackers offer, which will in turn increase the risk faced by members of the sortie party. Once outside the secure area the sortie party should always stay together. Pursuit of an individual attacker by a lone crewmember should not be undertaken, as it may result in the crewmember being isolated and seized by the attackers giving them leverage over the rest of the crew. Crewmembers should operate together and remain in constant communication with the bridge and should be recalled if their line of withdrawal to a secure area is threatened.

6.16.7 All apprehended attackers should be placed in secure confinement and well cared for. Arrangements should be made to transfer the attacker to the custody of law enforcement officers or naval authorities of a port or Coastal State (depending on whether the attack occurred in territorial or international waters) at the earliest possible opportunity. Any evidence relating to the attacker's activities should also be handed over to the authorities taking custody.

6.17 If Attackers Gain Control

6.17.1 If the attackers have gained control of the engine room or bridge, have seized crewmembers or pose an imminent threat to the safety of the ship, the Master or officer in charge should remain calm and, if possible, seek to negotiate with the attackers with the intention of maintaining the crew's control over the navigation of the ship, the safe return of any hostages they may hold and the early departure of the attackers from the ship. There will be many circumstances when compliance with the attackers' demands will be the only safe alternative and when resistance or obstruction of any kind could be both futile and dangerous.

6.17.2 In the event of attackers gaining temporary control of the ship, crewmembers should, if it is safe and practicable, leave CCTV recorders running.

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

6.17.4 If ordered not to make any form of transmission informing shore authorities of the attack, any such order should be complied with as the attackers may carry equipment capable of detecting all radio signals, including satellite communication. All ships that fall within the scope of the ISPS Code are, or will be fitted (by end June 2007) with a Ship Security Alert System (see paragraph 6.7.2 and APPENDIX 2), which can be covertly and silently activated without attracting the attention of the attackers who may have overrun the ship. This will alert the ship's Company Security Officer and Flag State competent authority which in the case of the UK is MRCC Falmouth who will alert relevant UK authorities.

6.18 Action to Take After an Attack and Reporting Incidents

6.18.1 An immediate post attack report should be made to the relevant Rescue and Co-ordination Centre (RCC) and through them to the law enforcement agencies or naval authorities of the port or Coastal State. As well as information on the identity and location of the ship, any injuries to crewmembers or damage to the ship should be reported as should the direction in which the attackers departed together with brief details of their numbers and, if possible, a description of their craft. If the crew have apprehended an attacker, that should also be reported in this signal. (See APPENDIX 1 for more guidance).

6.18.2 If an attack has resulted in the death of, or serious injury to, any person on board the ship or serious damage to the ship itself, an immediate signal in line with statutory requirements should also be sent to the ship's maritime administration. A report of an attack is vital if follow up action is to be taken by the ship's maritime administration.

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

6.18.4 As soon as possible after the incident a fuller report should be transmitted to the authorities of the State in whose waters the attack occurred, or if on the high seas to the authorities of the nearest Coastal State. Due and serious consideration should be given to complying with any request made by the competent authorities of the Coastal State to allow law enforcement officers to board the ship, take statements from crewmembers and undertake forensic and other investigations. Copies of any CCTV recordings, photographs, etc should be provided if they are available.

6.18.5 Any report transmitted to a Coastal State should also be transmitted to the ship's maritime administration at the earliest opportunity. A complete report of the incident, including details of any follow up action that was taken or difficulties that may have been experienced, should eventually be submitted to the ship's maritime administration.

6.18.6 The reports received by maritime administrations may be used in any diplomatic approaches made by Her Majesty's Government of the United Kingdom to the Government of the port or Coastal State regarding the incident and will also provide the basis for the United Kingdom's report (through the Department for Transport in London) to the IMO, required under the relevant IMO Assembly Resolutions on piracy and armed robbery at sea.

The format required for reports to the IMO is attached at APPENDIX 4. Indeed, historically the lack of adequate and accurate reporting of attacks (although there has been a recent improvement) has directly affected the ability to secure governmental and international action. Reports may also contribute to future refining and updating of the advice in this Marine Guidance Note.

6.18.7 Reports to the RCC, port or Coastal State and the ship's maritime administration should also be made if an attack has been unsuccessful.

6.18.8 It is hoped that using RCCs as recommended by the IMO in MSC Circular 597 (contact details provided by Addendum 1 (May 1993) to the above Circular) will eliminate communication difficulties. However, if a British ship experiences difficulties in establishing, or has been unable to establish, contact with the authorities of the relevant port or Coastal State, then a signal, an email or fax should be sent to the Department for Transport outlining the difficulties experienced. (see TRANSEC contact details in section14).

7 SECURITY MEASURES

7.1 It is the responsibility of companies to ascertain the risk to the ship, its crew and its cargo and to then mitigate the risks by the introduction of appropriate security measures.

7.2 As well as the possibility of engaging additional crew to carry out specific security related duties mentioned in paragraph 5.2, companies could also consider equipping their ships with specialised passive security equipment, e.g. thermal imagers (cooled and uncooled types) which detect radiated thermal energy from a scene and can work in conditions from daylight to complete darkness and/or night vision devices which work in low light levels. This equipment should be both commensurate with the size and type of ship and the perceived level of risk.

8 SUMMARY OF GENERAL PRECAUTIONS

8.1 For ease of reference a summary of the general precautions that may be taken are given in APPENDIX 3.

9 JURISDICTION AND INTERVENTION

9.1 Criminal Jurisdiction

9.1.1 Piracy is an offence committed on the high seas, or in a place outside the jurisdiction (territorial sea) of any State. A pirate who has been apprehended on the high seas for committing an act of piracy against merchant shipping should therefore be dealt with under the laws of the Flag State of his/her captors by mutual agreement with any other substantially interested States. (See MSC Circular 622/Rev 1 for definitions and additional information/guidance).

9.1.2 Within territorial waters, jurisdiction over armed robbers rests solely with the Coastal State.

9.2 Naval Intervention

9.2.1 International law requires any warship or other government ship to repress piracy on the high seas. Such ships would be expected to take action if they encountered pirates, or come to the aid of any ship under attack by pirates, on the high seas. A naval ship of any State can pursue pirates on the high seas, but not into the territorial waters of another State without that State's prior consent.

9.2.2 Foreign naval ships on innocent passage within the territorial waters of another State cannot exercise any enforcement powers or pursue attackers without prior authorisation from the Coastal State. However, they may render humanitarian assistance to a ship in danger or distress.

9.2.3 Royal Navy ships will take all appropriate measures to respond to incidents of piracy on the high seas, and to provide humanitarian assistance to ships attacked in territorial waters, whenever they are on hand to do so. However, the likelihood of a Royal Navy ship being nearby when an incident occurs, particularly in distant waters, will not be great. British ships will therefore, need to rely on their own vigilance and resources to prevent attacks and on the capability of Coastal States to suppress piracy or armed robbery.

9.3 Role of the Port and Coastal State

9.3.1 The Government of the United Kingdom calls upon Coastal and Port States to ensure the safety and freedom from attack of ships exercising their rights of innocent passage in the territorial sea of a Coastal State and in their ports. The Government also requests and requires Coastal States to pursue, prosecute and punish pirates or armed robbers who may operate, reside or have their base of operations in their territory. The activities of pirates and armed robbers now pose a real threat not only to those on board ship, but also to the territory and interests of Coastal States through the threat of a major pollution incident following an attack. The Government urges Companies, Masters and crews to co-operate to the greatest possible extent with the authorities of Coastal States in their efforts to pursue and prosecute attackers.

10 CONCLUSION

10.1 Attacks by pirates and armed robbers are still occurring frequently. They pose a threat not only to those on board ships but also to the interests of Coastal States. Coastal States in whose waters armed robberies occur or in whose territory pirates are based are taking action. However, it is essential that the companies, Masters and crews of ships operating in waters where attacks occur also take appropriate measures themselves, such as those outlined in this Marine Guidance Note, to guard against attack, to minimise the risks if an attack takes place, to report attacks and to co-operate in criminal investigations if requested to do so.

10.2 Ships entering such areas must be aware of the risk of attack and should take appropriate measures to increase the level of surveillance and security on board and to devise means of responding to attacks if the opportunity arises. Adhering to the ISPS Code's Ship Security Plan, following a clearly drafted Counter-piracy Plan and training crews in security measures and response techniques are essential. Without clearly defined and rigorously practised procedures the risk of an uncoordinated response during the inevitable confusion of an attack increases the danger faced by those on board the ship. While a Counter-piracy Plan and crew training may not ultimately prevent an attack, they should help reduce the risks, variables and confusion when an attack is taking place by addressing vulnerabilities and preparing contingency arrangements.

10.3 By their nature, attacks by pirates or armed robbers can pose an immediate threat to the safety of a ship or to individual crewmembers. When preparing to respond, or when responding to attacks, Masters and crews should seek to minimise the risk to those on board and seek to maintain effective control over the safe navigation of the ship. In any balance that has to be struck between resistance and safety, actions which secure the greatest level of safety must take priority.

11 PIRACY REPORTING CENTRE

11.1 The latest information on piracy attacks and the regions of greatest risk may be obtained free of charge from the ICC International Maritime Bureau's Piracy reporting Centre at Kuala Lumpur. The centre operates 24 hours a day and can be contacted as follows:

24hr Anti-piracy Helpline ++ 60 3 2031 0014
Office hrs Tel ++ 60 3 2078 5763
Fax ++ 60 3 2078 5769
Telex MA34199 IMBPCI
E-mail: IMBKL@icc-ccs.org

11.2 The Centre issues status reports and warning messages on the SafetyNET service of Inmarsat C at 0001 UTC each day.

11.3 The Centre also posts a weekly update of attacks on the Internet at **www.icc-ccs.org**. This update posted every Tuesday is compiled from the Centre's daily status bulletins to ship at sea.

12 TRAVEL ADVICE NOTICES

12.1 Information on personal safety is available through the Foreign and Commonwealth Office (FCO) and can be obtained by contacting the FCO or British Embassies, High Commissions and Consulates in the area concerned.

12.2 The full range of notices are available on the FCO's World Wide Web server on the internet (http://www.fco.gov.uk). The email address is consular.fco@gtnet.gov.uk. The Travel Advice Unit can also be contacted direct on 0870 6060290. Alternatively it can be faxed on 020 7008 0155.

13 AMENDMENTS

13.1 An Addendum to this Marine Guidance Note will be issued, as required, advising of significant changes in the locations and/ or patterns or methods of attack. The text of this Marine Guidance Note may be amended to reflect experience based on the reports submitted to maritime administrations and also on reports submitted to the IMO by other flag or Coastal States.

14 FURTHER INFORMATION

Please use the following contact details for Transec if you require clarification or wish to raise an issue on any of the points made in this document:

Maritime Security Branch
Transport Security and Contingencies Directorate (TRANSEC)
Department for Transport
Zone 5/5 Southside
105 Victoria Street
London
SW1E 6DT

Maritime Helpdesk Telephone (Office Hours):	+44 (0) 20 7944 2844
DfT Duty Officer (Out of office hours):	+44 (0) 20 7944 5999
Fax (Office Hours):	+44 (0) 23 8032 9251
Fax (24 Hours):	+44 (0) 23 8032 9251
e-mail:	maritimesecurity@dft.dsi.gov.uk

This document is available to view and download on the Department for Transport website under Transport Security/ Maritime/ Piracy at: www.dft.gov.uk, File Ref: TRSEC 35/ 6/ 1

General Inquiries: 24 Hour Infoline
infoline@mcga.gov.uk
0870 600 6505

MCA Website Address: www.mcga.gov.uk

File Ref: TRSEC 35/6/1

Published: October 2005

Safer Lives, Safer Ships, Cleaner Seas

Printed on material containing minimum 75% post-consumer waste

An executive agency of the Department for Transport

APPENDIX 1

RECENT TRENDS IN PIRACY AND ARMED ROBBERY ATTACKS

A1.1. Since the last issue of this Guidance Note in **November 2002** there was an initial surge in the number of recorded incidents from the previous 2 years, with a total of 445 attacks in the whole of 2003 according to both the International Maritime Organisation and the International Maritime Bureau's Piracy Reporting Centre. This figure decreased considerably (a 27% reduction) in 2004 to 325 attacks and so far in 2005, the number of attacks in the first half of this year is the lowest since 2000. While this sounds encouraging, the tsunami that occurred on the 26th December 2004 and devastated many of the coastal regions of the countries within and bordering the Indian Ocean, undoubtedly impacted on piratical capability in the region. Many groups involved in piracy and armed robbery are likely to have been victims of the tsunami and/or had their equipment destroyed which in turn led to a two month lull in incidents. However, since March 2005 incidents of piracy and armed robbery have been on the increase again.

A1.2. The trend since the early 1990's when the IMB began recording incidents, has risen from an average of around 100 attacks per year to 300 plus since 1999 although much of this increase is probably attributable to an improvement in the reporting of incidents which was chronically low in the early 1990's. It is estimated that even today only about 80% of attacks are recorded **(all UK flagged ships are urged to report incidents to TRANSEC at the contact details in section 14)**. Taking the difference between actual and recorded attacks into account, the rise in overall attacks over the last 14 years is not as dramatic as media reporting suggests, although the trend is clearly upwards. However within the overall figure, there are various hotspots in the world where piracy and armed robbery is a prevalent and entrenched problem and attacks are rising, posing a serious problem to merchant shipping. The majority of recorded attacks now appear to be taking place within territorial waters and usually occur while a ship is in port or at anchor. Such acts are classed internationally as Maritime Armed Robbery and not true Piracy (on the high seas) which constitutes a smaller percentage of attacks.

A1.3. While the total number of attacks has dropped since 2002, there has been an overall 22% increase in the number of serious incidents with many acts of unprovoked and severe violence taking place. The majority of attacks continue to involve the use of knives and/or firearms resulting, in some cases, in death and injury to crewmembers. The majority of these violent attacks in recent years can be largely attributed to local gangs targeting indigenous ships and crews. The types of internationally trading ships that are most often attacked are bulk carrier and general cargo ships due to their low freeboard, followed by container ships and crude oil tankers.

A1.4. Piracy attacks against ships underway are particularly prevalent in South East Asian waters and a large proportion of attacks in this area have occurred in Indonesian territorial waters and particularly in the Malacca Straits (see A.1.5.) and adjoining channels such as the Selat Phillip (Phillip Channel) used by ships making passage via the Malacca Straits. Other attacks have taken place in the South China Sea and in waters adjacent to the Philippines. The Horn of East Africa has recently seen a dramatic increase in attacks on ships, especially off the coast of Somalia, in the Gulf of Aden and in the Red Sea. Until recently all attacks off the Somali coast were deemed to have been launched from the shore and advice up to now has been to stay at least 50 Nautical Miles from the shore. A recent hijacking of a number of ships beyond 100 NM from the eastern Somali coastline indicates that a mother ship was probably used and that the range of the attackers in this region has greatly increased. It is therefore in the interests of all ships transiting the Horn of Africa to be at a high state of alert and readiness for an attack. Attacks can take place in either international waters as piracy or, more commonly, as armed robbery in territorial waters of a Coastal State.

A1.5. The stretch of water where armed robbery has been most prevalent over the last decade is the Malacca Straits, which in the last four years has accounted for a fifth of all recorded attacks. The straits traverse the territorial waters of three sovereign nations, Malaysia, Indonesia and Singapore. All of the attack profiles previously listed, for example such as attacks while in port/harbour areas, especially on the Indonesian side, while in anchorages or against ships transiting through have been reported in this area. Due to the straits forming part of the territorial waters of three sovereign states, any solution or efforts to combat piracy here remains diplomatically complex. However, a number of initiatives have been launched in the last year which includes increased co-ordinated maritime patrols and a recent agreement to begin air patrols of the straits by the three states, a new intelligence centre in Singapore and a recent IMO sponsored conference in Jakarta focussing on the security and safety of the straits. In addition Singapore has started deploying new Accompanying Sea Security Teams (ASSET) Teams which will board and escort high-risk shipping within its waters. Malaysia set up a new Maritime Enforcement Agency to patrol its coastline from June this year, taking crew and support from the Navy, and is also deploying armed police on tugs and barges to enhance security. These measures are welcomed additions to the security of ships from piracy and armed robbery but crews should not become complacent and reduce the precautionary measures taken on board their ships.

A1.6. There has been a particular problem in the Niger Delta involving local rebel militia, who are fighting government forces and have been employing pirate style tactics, targeting and attacking ships for their valuables and cargo with oil tankers being the most popular. There have also been reports of hijackings and crew being kidnapped; therefore Masters and crew should be prepared for attacks as this area remains very dangerous. Although the number of recorded incidents in the first quarter of 2005 would appear to suggest a complete cessation of activity, it is likely that such incidents are simply not being recorded and heightened vigilance and preparedness is advisable.

A1.7. Attacks by pirates or armed robbers continue to take place outside of the geographical hotspot areas mentioned above and based on attacks in recent years, in areas of the Caribbean such as Jamaica and Haiti and along parts of the South American coastline, particularly Brazil, Venezuela and Guyana along the northern coast and Peru, Colombia and Ecuador along the western Pacific coast. Whilst the number of reported incidents are significantly lower than in the hotspot areas, Masters and crew should continue to err on the side of caution when transiting these areas.

APPENDIX 2

THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE & SOLAS AMENDMENTS 2002

A2.1. The ISPS Code covers all internationally trading passenger ships carrying 12 or more passengers; cargo ships of 500 gross tonnes and above (as measured by the International Convention on Tonnage Measurement of ships, 1969); mobile offshore drilling units and all port facilities (ship/port interfaces) serving these ships. With specific regard to UK ships, ISPS has required the preparation and subsequent agreement with TRANSEC or MCA of a Ship Security Plan (following the completion of a ship security assessment). The Ship Security Plan covers both the protective security measures required on the ship and the appropriate response to a security incident. Once the Ship Security Plan has been approved and a verification inspection has been conducted ships meeting UK requirements are issued with an International Ship Security Certificate. The Code also requires the appointment and training of a Ship Security Officer for each ship and a Company Security Officer for the shipping company who together are responsible for delivering against the Plan's security requirements. ISPS has also brought in a new 3 tier security level system, where Level 1 is the normal operating level, Level 2 is for a heightened alert and Level 3 is for a critical situation where there is an imminent and specific threat. While the security level is primarily based on counter-terrorism considerations, TRANSEC who sets the security level for all UK flagged ships, determines the appropriate security level that UK flagged ships must adopt when operating in a specific country or sea area taking into account other considerations such as the threat from piracy and armed robbery. However not all Flag States will set security levels for their ships in the same way.

A2.2. There is also now a much greater emphasis on Restricted Areas of a ship, the requirement for access control and pass systems, monitoring capabilities, visitor searching and in the UK, for Government approved training courses. The concept of a Declaration of Security (DoS) has been implemented which requires an agreement to be reached between two ships or between a ship and a port facility when they interface. It details the different security measures each will undertake and can be requested for example when a ship is at a higher security level than a port facility. The requirement to fit two new technological based systems, the Ship Security Alert System and the Automatic Identification System (see A2.6 for more details) were also agreed as part of the amendments to SOLAS and under the ISPS Code.

The Ship Security Plan

A2.3. It is now a requirement that all ships that fall within the scope of the ISPS Code must undergo a Ship Security Assessment, leading to a Ship Security Plan. This plan must be agreed with the relevant Flag State competent authority in order to receive an International Ship Security Certificate and thereby comply with the Code. The content of the plan will vary depending on the ship that it covers but must include details such as the organisational structure of security for the ship, the ship's communication systems and the security measures that will be in place at each of the three security levels. The plan is a living document and will need to be reviewed and updated as circumstances change.

Restricted Areas

A2.4. The Ship Security Assessment also requires the identification and establishment of Restricted Areas (RAs) onboard the ship, although certain Flag States such as the UK, determine the minimum baseline requirements which must then feature in the Ship Security Plan. The plan should specify the extent of the RA, the times of application, the security measures to be taken to control access to them and to control activity within them. The purpose of the RA is to demarcate certain areas of a ship to prevent unauthorised access; protect passengers and crew; protect sensitive security areas on the ship as appropriate and to protect the ship's cargo and stores from interference.

On UK flagged ships all RAs must be clearly marked to show that access is restricted and that unauthorised presence within the area constitutes a breach of security.

Ship Security Alert System

A2.5. The amendments to SOLAS under Chapter X1-2, Regulation 6 has required the installation of a new ship security alert system (SSAS) on board ships to which SOLAS applies (the roll-out is phased depending on the classification of the ship but will be completed during 2006). The purpose of the SSAS is to alert the ship's Flag State competent authority and also the Company Security Officer of the relevant shipping line to the fact that the security of the ship is under threat or has been compromised by terrorists. There are a minimum of two activation points for the SSAS which initiate the transmission of the alert and it is for the Master to decide on which crewmembers need to be aware of the location of the activation points. Once activated, a covert alert will be made to the relevant competent authority and each Flag State must have procedures in place to ensure quick and effective receipt and handling of the alert (the UK's own response procedure has been separately communicated to UK flagged shipping companies). The alert will continue until it is deactivated or reset. While the SSAS is primarily intended for counter-terrorism purposes, in the event of a pirate attack where the ship has been boarded or is very likely to be and when all other radio procedures have either failed or there is not enough time to use them, then the SSAS may be used as a last resort to alert the Flag State. Periodic testing (once a year as a minimum) of the SSAS to test the communication process is advisable although it is important to contact those who will be involved in the test in advance to ensure that no unnecessary response activity is implemented. For information, the UK's competent authority is the Maritime and Coastguard Agency and Ship Security Alerts are received at the MCA's Maritime Rescue and Co-ordination Centre in Falmouth.

Automatic Identification System (AIS)

A2.6. AIS is a shipboard broadcast system that acts like a transponder and operates on the VHF maritime band enabling the ship to communicate both with the shore and with other ships. Operation of AIS is a requirement under Chapter V of the amendments to SOLAS 2002. The system allows a ship's location and movements to be monitored on shore and by another suitably equipped ship up to a notional range of 35 miles. A ship with AIS installed is able to display information such as the size, speed and heading of similarly equipped ships within VHF range.

A2.7. Clearly the risk of having AIS turned on while a ship is transiting through an area known to have a high level of piracy attacks, is that the ship can easily be targeted and located. This is especially the case if 'would be' attackers in the vicinity have been able to obtain their own receiver. Additionally, the advent of open source on-line AIS information has also increased the 'visibility' of ships using AIS. While it is not recommended under ISPS Regulations to turn AIS off as this may affect the safety of the ship, if a situation arises where the Master of the Ship feels under threat by keeping AIS turned on, then UK flagged ships should conduct a risk assessment. If the assessment determines that the threat to the security of the ship is greater than the threat to safety, then the Master should turn AIS off while the threat remains present. This however may not be the position of other Flag States and Masters and crew of ships should establish their own policy on AIS use in such scenarios.

APPENDIX 3

SHIP COMMUNICATIONS

Radio Procedures

A3.1. The Navigational Officer on Watch (OOW) should be on duty at all times and should be extra vigilant when ships are in, or approaching, maritime transit chokepoints, potential ambush sites and areas where piracy is prevalent. The Master should not normally perform this duty, though on occasions, this may be unavoidable. Since the mandatory introduction of GMDSS in February 1999, the OOW now normally performs the radio watch, replacing the dedicated Radio Operator (RO) who used to carry out this function. To ensure that a ship's bridge is adequately manned when transiting potentially hazardous waters, it is advisable that a duly qualified, dedicated crewmember perform Radio Watch duty. This contingency allows the OOW and the Master to concentrate on navigational duties and maintaining the extra vigilance that is required when operating in high-risk areas.

A3.2. Prior to entering areas where attacks have occurred, OOWs should practice and perfect all appropriate radio operational procedures and ensure all transmitters, including satellite ship earth stations are fully operational and available for immediate use on distress and safety frequencies. Where a GMDSS installation is provided and "ship's position" data is not automatically updated from an associated electronic navigation aid, OOWs are strongly recommended to enter the ship's position at regular intervals into the appropriate communications equipment manually. Where an INMARSAT ship earth station is provided it may prove useful to draft and store "standard messages" (see paragraph A3.10) for ready use in an emergency in either the equipment's memory or on a computer disk. A special code for 'piracy/armed robbery attack' is now available for use on Digital Selective Calling (DSC) equipment. Where practicable and appropriate, DSC equipment should be modified to incorporate this facility. Masters should ensure that all procedures to generate a distress alert on any communications equipment are clearly marked on, or near, the equipment (with the exception of the Ship Security Alert System as this is a covert system and the obvious positioning of such procedures is likely to reduce the benefits of carrying the equipment). Masters should also ensure that all appropriate crewmembers are briefed on the operation of such equipment.

A3.3. Masters should bear in mind the possibility that attackers are monitoring both ship to ship and ship to shore communications and using intercepted information to select their targets. Caution should, therefore, be exercised when transmitting information on intended transit tracks and cargo or valuables on board by radio in areas where attacks occur. The implementation of the AIS broadcast system and the availability of online AIS information means that the location of ships, when they are sailing within close proximity of the shore (under 35 miles) is now more accessible to the public and Masters need to be aware of this when transiting high-risk areas.

Radio Watch-keeping and Responses

A3.4. A constant radio watch should be maintained with the appropriate shore or naval authorities when in areas where attacks have occurred. Continuous watch should also be maintained on all distress and safety frequencies, particularly VHF Channel 16 and 2182 kHz. Ships should also ensure all maritime safety information broadcasts for the area are monitored. As it is anticipated that INMARSAT's enhanced group calling system (EGC) will normally be used for such broadcasts using the SafetyNET(SM) service, companies should ensure a suitably configured EGC receiver is continuously available when in, or approaching, areas where there is a risk of attack. Companies should also consider fitting a dedicated receiver for this purpose, i.e. one that is not incorporated into a ship earth station used for commercial purposes, to ensure no urgent broadcasts are missed.

(Masters should note that as detailed in section 11 of this Marine Guidance Note, the IMB Piracy Reporting Centre broadcasts daily status reports to ships in Indian, Atlantic and Pacific Ocean Regions on the SafetyNET service of Inmarsat C at 0001 UTC each day).

A3.5. The International Maritime Organisation (IMO) recommends in MSC Circular 597, issued August 1992 and supplemented by an Addendum issued in May 1993, that reports concerning attacks by pirates or armed robbers should be made to the relevant Rescue Co-ordination Centre (RCC) for the area. Information on RCCs may be found in the Search and Rescue Section of volume 5 of the Admiralty List of Radio Signals. MSC Circular 597 also recommends that governments should arrange for the RCCs to be able to pass reports of attacks to the appropriate law enforcement agencies or naval authorities. The IMO subsequently published MSC Circular 622/Rev 1 in June 1999. This circular gives detailed recommendations to Governments to assist in the prevention and suppression of piracy and armed robbery against ships. In May 2002 the IMO published MSC Circular 623/Rev 3 as an equivalent guide to companies. Reports of attacks against UK flagged ships should also be made to the CSO and TRANSEC via MRCC Falmouth. Other Flag States will have their own reporting requirements which seafarers should make themselves aware of.

A3.6. In the event Masters are unable to contact the relevant RCC, it is recommended that they report the incident to the IMB Piracy Reporting Centre, which in turn, will pass the message to appropriate authorities (see section 11).

A3.7. If suspicious movements are identified which may result in an imminent attack, the ship is advised to contact the relevant RCC. Where the Master believes these movements could constitute a direct danger to navigation, consideration should be given to broadcasting an "All Stations" (CQ) "Danger Message" as a warning to other ships in the vicinity as well as advising the appropriate RCC. A danger message should be transmitted in plain language on a VHF working frequency following an announcement on VHF Channel 16, and/or transmission of a DSC call on VHF Channel 70 using the "safety" priority. All such messages shall be preceded by the safety signal (Securite). When, in his opinion, there is conclusive evidence that the safety of his ship is threatened, the Master should immediately contact the relevant RCC and, if considered appropriate, authorise broadcast of an "All Stations" "Urgency Message" on VHF Channel 16, 2182 kHz, or any other radio communications service considered to be appropriate; e.g. 500 kHz, INMARSAT, etc. All such messages shall be preceded by the appropriate Urgency Signal (PAN PAN) and/or a DSC call on VHF Channel 70 and/or 2187.5 kHz using the "All Ships Urgency" category. If the Urgency signal has been used and an attack does not, in fact develop, the ship should cancel the message as soon as it knows that action is no longer necessary. This message of cancellation should likewise be addressed to "All Stations".

A3.8. Should an attack occur and, in the opinion of the Master, the ship or crew are in grave and imminent danger requiring immediate assistance, the Master should immediately authorise the broadcast of a Distress message, preceded by the appropriate distress alerts (MAYDAY, SOS, DSC, etc), using the radio communication systems most appropriate for the area taking into account its GMDSS designation; i.e. A1, A2, A3 or A4. The appropriate RCC should acknowledge receipt and attempt to establish communications. To minimise delay, if using a ship earth station, ships should ensure the coast earth station associated with the RCC is used.

A3.9. Masters should bear in mind that the distress signal is provided for use only in cases where the ship and/or its crew are in grave or immediate danger and its use for less urgent purposes might result in insufficient attention being paid to calls from ships really in need of immediate assistance. Care and discretion must be employed in its use, to prevent its devaluation in the future. Where the transmission of the Distress signal is not fully justified, use should be made of the Urgency signal. The Urgency signal has priority over all communications other than Distress signals.

Standard Message Formats

A3.10. The following standard formats were agreed by the IMO Sub-Committee on Radio Communications in January 1993 and updated by MSC Circular 622/Rev 1 published in June 1999, are set out below:

- initial messages - piracy attack alert, and
- piracy attack/sighting/suspicious act reports

A3.11 In addition, guidance for the use of radio signals by ships under attack or threat of attack from pirates or armed robbers is available in Maritime Safety Committee (MSC) Circular 805 published in June 1997. This circular recommends that a “Piracy/ Armed Robbery Attack Message” should be sent through INMARSAT-C or on an available DSC or other distress and safety frequency. Given that some pirates or armed robbers may carry equipment capable of detecting all radio signals, including satellite communications, this circular also recommends that communication should not be attempted if a ship has been boarded and its crew specifically ordered to maintain radio silence.

Secreted VHF Transceiver

A3.12. As a result of communications equipment being damaged in the past by attackers to prevent an early alarm being raised, particularly when attacks have taken place off port, companies and Masters are recommended to secrete a VHF transceiver on the ship to allow contact to be established with the shore authorities if the main communications equipment is put out of action. Consideration could also be given to the installation of handheld iridium telephones. These sets have a longer range than the traditional VHF transceiver, and would allow the ships’ Master to inform, and converse with, more distant authorities as well as the authorities in the region of the attack.

INITIAL MESSAGE-PIRACY/ ARMED ROBBERY ATTACK ALERT

Ship's name and call sign/INMARSAT ID (plus ocean region code) IMO number and MMSI.

MAYDAY/DISTRESS ALERT (see Note below).
URGENCY SIGNAL
PIRACY/ARMED ROBBERY ATTACK.

Ship's position (and time of position UTC) – including Course Speed

Nature of Event.

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

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

If the Master and Crew do not have time to follow the above procedure in the event of an attack, then the covert Ship Security Alert should be activated to inform the Company Security Officer and the relevant Flag State's competent authority.

PIRACY/ARMED ROBBERY ATTACK/SIGHTING/SUSPICIOUS ACT REPORT

Ship's name call sign and IMO number.

Reference initial PIRACY/ARMED ROBBERY ALERT.

Position of incident.

Date/time of incident (UTC).

Details of incident, e.g.
Method of attack.
Description of suspect craft.
Number and brief description of attackers, including weapons carried and/or language spoken.
Injuries to crew.
Damage to ship.
Brief details of stolen property/cargo.

Last observed movements of suspect ships, e.g.

Date/time/course/position/speed.

Assistance required.

Preferred communications with reporting ship, e.g.

Appropriate Coast Radio Station. HF/MF/VHF. INMARSAT ID (plus ocean region code), MMSI.

Date/time of report (UTC)

APPENDIX 4

ACTS OF PIRACY AND ARMED ROBBERY ALLEGEDLY COMMITTED AGAINST SHIPS REPORTED BY MEMBER STATES OR INTERNATIONAL ORGANISATIONS IN CONSULTATIVE STATUS

IMO No.

Name/Type of ship/Flag/Gross Tonnage

Date/Time

Position of the incident*

Details of the incident

Consequences for crew, ship, cargo

Action taken by the Master and the crew

Was the incident reported to the Coastal Authority? If so, to whom?

Reporting State or international organisation

Action taken by the Coastal State

*The position given should be as accurate as possible including latitude and longitude co-ordinates or as bearing and distance from a conspicuous landmark.

APPENDIX 5

SUMMARY OF GENERAL PRECAUTIONS

Be vigilant - the majority of attacks will be deterred if the robbers are aware that they have been observed and that the crew has been alerted and is prepared to resist attempts to board. Ensure that crewmembers are seen to be constantly moving around the ship, making random rather than predictable patrols.

Maintain a 24 visual and security watch - including short range radar surveillance of the waters around the ship. The use of a small marine radar, fitted in such a way to ensure complete coverage of the stern, un-obscured by the radar shadow of the ship itself, should be considered. Keep a special look-out for small boats and fishing boats that attackers often use because they are difficult to observe on radar. In piracy "hotspots", discourage the crew from trading with locals using small craft which may approach the ship.

Strengthen night watches - especially around the rear of the ship and anchor chains/mooring ropes particularly between the hours of 0100 and 0600 when most attacks occur, with continuous patrols linked by "walkie-talkie" to the bridge. A drill should be established for regular two-way communication between the watch and the bridge. If possible, an additional officer should assist the normal bridge watch keepers at night, in order to provide a dedicated radar and visual watch for small craft that might attempt to manoeuvre alongside, and allow the watch keepers to concentrate on normal navigational duties. Night patrols of the ship should be staggered to avoid patterns forming which pirates could observe.

Seal off means of access to the ship - fit the hawse pipe plates, lock doors and hatches etc. While taking due account of the need for escape in the event of fire or other emergency, so far as possible all means of access to the accommodation should be sealed off and windows and doors of crewmembers' quarters should be kept locked at all times. Blocking access between the aft deck and the crewmembers' quarters is particularly important.

Establish radio contact - and agree emergency signals specifically for attacks with crew, shore authorities etc.

Provide adequate lighting - deck and over-side lights, particularly at the bow and stern, should be provided to illuminate the deck and the waters beyond and to dazzle potential boarders. Searchlights should be available on the bridge wings, and torches should be carried by the security patrols to identify suspicious craft. Such additional lighting should not however be so bright as to obscure navigation lights or interfere with the safe navigation of other ships.

Water hose and other equipment - which may be used to repel potential boarders, should be readily available. Keep a constant supply of water provided to the hoses. In danger areas keep the deck wash pump in operation at all times - spray water over the rear deck where it is easiest for the attackers to board. Consider fitting or equipping the ship with passive security/detection equipment e.g. Perimeter Intruder Detection Systems, CCTV, Night Vision equipment and ensure that where possible, they are linked to an alarm system.

Reduce opportunities for theft - remove all portable equipment from the deck, so far as is possible stow containers containing valuables door-to-door and in tiers and seal off access to the accommodation.

Establish a secure area(s) - if large numbers of armed robbers succeed in boarding the ship, it may be essential for crewmembers to retreat to a secure area(s). Depending upon the construction of the accommodation and the extent to which areas can be effectively sealed off, the secure area may be established in the accommodation as a whole or in the Restricted Areas, for example, around the bridge and inside the engine room. Provision should be made, however, for escape during a fire or other emergency.

A secure area in this sense is intended purely for the safety of the crew and should not be confused with a Restricted Area, which is a mandatory SOLAS ISPS Code requirement for the security of the ship.

Inform crewmembers of the Counter-piracy Plan - hold training exercises and ensure that they are fully briefed on the actions that they need to take in the event of an attack.

TABLE OF CONTENTS