Guidance to UK Flagged Shipping on Measures to Counter Piracy, Armed Robbery and Other Acts of Violence Against Merchant Shipping

November 2011

Contents

Key Messages

This guidance aims to assist all UK registered ship owners, companies, ship operators, masters and crews 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 should they occur.

- **Plan the voyage. Carry out a risk assessment and make an assessment of the measures required when transiting high risk areas;**

- **Many attempted piracy and armed robbery "attacks" are unsuccessful, countered by ships' crew who have planned and trained in advance;**

- **Be vigilant;**

- **Maintain high speed where possible in high risk areas;**

- **Good communications with relevant authorities is vital. Report to the relevant authorities before, during or after an attack.**

IMPORTANT – SOMALIA

Shipping transiting the Gulf of Aden or the seas off the coast of Somalia should adhere to the advice and guidance contained in the latest version of the Industry Best Management Practices at http://www.dft.gov.uk/topics/security/maritime/ and on the EU NAVFOR Maritime Security Centre Horn of Africa web site (www.mschoa.org).

The government recognises that the engagement of armed guards is an option to protect human life onboard UK registered ships from the threat of piracy, but only in exceptional circumstances and where it is lawful to do so.

Shipping companies that decide to use armed guards in the exceptional circumstances must refer and adhere to the Government's Interim Guidance to UK flagged shipping on the use of armed guards to defend against the threat of piracy in exceptional circumstances. This is available online at <<insert URL>>

IMPORTANT – FOR ALL AREAS

This guidance should be read in conjunction with International Maritime Organisation (IMO) MSC.1/Circ. 1334 – Piracy and Armed Robbery Against Ships - Guidance to ship owners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships.

Key Definitions

Definition of Piracy

Piracy consists of any of the following acts:

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

(The 1982 United Nations Convention on the Law of the Sea (UNCLOS): article 101)

Definition of Armed Robbery

> *"Armed robbery against ships" means any unlawful act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State's internal waters, archipelagic waters and territorial sea.*

(IMO MSC.1/Circ.1333 - PIRACY AND ARMED ROBBERY AGAINST SHIPS - Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships)

1. Introduction

1.2   This guidance brings to the attention of ship owners and ship operators, Masters and crews, the risk of acts of piracy on the high seas or armed robbery against ships within the territorial sea of a coastal State.

1.3   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 International Maritime Bureau (IMB) reporting centre and to the ship's own maritime administration.

1.4   This guidance also recognises the current problem of piracy off the coast of Somalia.   It draws the attention of seafarers to the particular best practices in place on how to communicate with the various sources of assistance in this area and how to carry out passive counter measures on board the ship to deal with this particular threat.

1.5   It also recognises the difference in nature between piracy and armed robbery and is therefore structured to reflect the particular characteristics common to both as well as characteristics which are specific to each.

Background

1.6   The information included in this guidance document, for the most part, replicates the information formally included in Marine Guidance Note 420(M), which has now been replaced by MGN 440 <<insert URL>>.

1.7   MGN 420(M) set out the Government's policy on the use of armed guards to protect a ship, its cargo and its crew from acts of piracy. This policy has now been reviewed, and the new policy is set out in section 4 of this guidance document.

1.8   This guidance is principally aimed at UK flagged ships and refers in the first instance to UK maritime security/counter-piracy policy and procedures. However, DfT acknowledges that many of its readers may 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. SOMALIA, the Indian Ocean and the Gulf of Aden

Key message

Best Management Practices (BMP)

Prior to transiting through the Gulf of Aden or off the Coast of Somalia, shipping companies and ship operators are advised to consult the latest version of the BMP (available on the EUNAVFOR web site at http://www.eunavfor.eu/press-2/downloads/). This document contains the most up to date advice and guidance on deterring and avoiding attacks in this region, based upon analysis of attacks.

Background

2.1   There has been a marked rise in piracy attacks since 2007, the majority of which have taken place off the coast of Somalia, in the Gulf of Aden or in the wider Indian Ocean.

2.2   The Gulf of Aden is a key strategic route for the trade of goods and oil between the Far East, and Europe and America. The increase in pirate activity has prompted an unprecedented level of cooperation between the world's navies, who – via a number of mechanisms including the United Nations Contact Group on Piracy off the Coast of Somalia – have recognised an Internationally Recognised Transit Corridor for ships transiting the Gulf of Aden, patrolled by warships and supported by information and intelligence gathering centres at the United Kingdom Maritime Trade Organisation (UKMTO) in Dubai, and the European Union's Maritime Security Centre (Horn of Africa). The shipping industry has taken the initiative in promoting Best Management Practices – a document well circulated throughout the shipping world and supported by the industry, IMO Member States and the naval coalitions currently policing the area.

2.3 Although Somalia clearly dominates at the time of writing, the focus may change in the future and the purpose of this document is to remain as comprehensive as possible, whilst at the same time acknowledging the huge amount of effort and assistance made available by various navies, Governments and shipping industry bodies to aid seafarers transiting close to Somalia.

2.4 This guidance, whilst recognising the large numbers of piracy and armed robbery attacks elsewhere in the world, must be mindful of the good advice and work already taking place to combat piracy off Somalia. This document is not intended to duplicate advice provided by the EU Naval Force's Maritime Security Centre web site or the Best Management Practices; both of which can be updated with a greater frequency than this guidance. However, the methods used by Somali pirates could conceivably be replicated by pirates and armed robbers elsewhere – despite the current upsurge in Somalia, piracy is not just a problem off Somalia, it remains a global problem and seafarers need to be aware of it as much as ever.

The use of armed guards

2.5 The government recognises that the engagement of armed guards is an option to protect human life onboard UK registered ships from the threat of piracy, but only in exceptional circumstances and where it is lawful to do so.

2.6 At this time, the exceptional circumstances under which armed guards may be employed for use onboard UK flagged ships are:

- when the ship is transiting the high seas throughout the High Risk Area (HRA) (an area bounded by Suez and the Straights of Hormuz to the North, 10°S and 78°E); AND

- the latest BMP is being followed fully but, on its own, is not deemed by the shipping company and the ship's master as sufficient to protect against acts of piracy; AND

- the use of armed guards is assessed to reduce the risk to the lives and well being of those onboard the ship.

2.7 The use of armed guards in any other circumstances is strongly discouraged, and also unlawful where prohibited firearms are possessed without valid authorisation from the Home Office.

2.8 The Government will continuously review these exceptional circumstances and inform the shipping industry if they change.

2.9 Shipping companies that decide to use armed guards onboard UK flagged ships must refer and adhere to the Government's Interim Guidance to UK flagged shipping on the use of armed guards to defend against the threat of piracy in exceptional circumstances. This is available online at <<insert URL>>

3. Piracy – General Advice

> **Key message**
>
> Areas other than Somalia also remain a concern. Attacks, mainly against the oil industry, have taken place regularly off the coast of Nigeria (20 attacks in 2009 reported to IMB by October, whilst external sources suggest that 50% in this area go unreported). IMB also report an increase in the reported attacks at Chittagong in Bangladesh in 2009 and the number of reported attacks in the South China Sea has also shown a marked increase for the first time since 2004.
>
> The IMB website should be consulted for the latest information on piracy prone areas and warnings (http://www.icc-ccs.org/piracy-reporting-centre/prone-areas-and-warnings).

Attacks When Underway

3.1   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.

3.2   The majority of these attacks have taken place against ships in South East Asian waters and more recently off the coast of Somalia. Evidence indicates that it should be assumed that the attackers are not only carrying but are prepared to use firearms and in a number of cases more powerful weapons such as rocket-propelled grenades have been brandished and used. Such incidents often involve the use of the tactics described in the following paragraphs.

3.3   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.

3.4   It should be noted that ships travelling at slow speeds, especially if this is combined with a low freeboard, are more vulnerable to attack.

3.5   Access to the ship will often be by climbing up ladders or by utilising grappling irons hooked on to the ship's rail. Attackers 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.

3.6   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.

3.7   Attackers have also been known to try to blend in with local fishing boats or to disguise themselves as Coastguard or naval personnel, or Pilots in order to board the ship. 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.

3.8   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.

3.9   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 controlling 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 could additionally result in major pollution.

3.10   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. Recommended Practices to Deter Acts of Piracy

Key message

The following measures (explained below) should be considered:

- Risk Assessment
- The Counter-Piracy Plan
- Routing and Delaying Anchoring
- Prior to Entering Areas where Attacks Occur
- Watch-keeping and Vigilance
- Ship Communications
- Lighting
- CCTV
- Secure Areas
- Alarms
- Evasive Manoeuvring and Use of Hoses
- Use of Distress Flares

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 Security Officers, 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.

Risk Assessment

4.1 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.

The Counter-Piracy Plan

4.2 All UK flagged ships operating in waters where piracy incidents occur should have 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 and should also cover the surveillance and detection equipment that has been provided. The plan should cover:

- the need for enhanced watch keeping;
- the use of lighting and surveillance, detection or perimeter protection equipment;
- the need for high speed and evasive manoeuvres
- crew and passenger response 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.
- specific procedures to register the ship with naval authorities if transiting through the Gulf of Aden / off the coast of Somalia, if appropriate

4.3 The Counter-Piracy Plan can exist as a standalone document to sit alongside (but not be incorporated within) the Ship Security Plan 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 document.

4.4 Where a shipping company decides to use armed guards in the exceptional circumstances set out in section 4, a counter-piracy plan must be completed and sent to DfT inline with the advice included in the

Government's Interim Guidance to UK flagged shipping on the use of armed guards to defend against the threat of piracy in exceptional circumstances. This guidance is available online at <<insert URL>>

Routing and Delaying Anchoring

4.5 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.

Prior to Entering Areas where Attacks Occur

4.6 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 rehearsed. If instructions are to be given over the ship's address system 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.

4.7 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. Early detection of a possible attack is the most effective deterrent. 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.

Watch-keeping and Vigilance

4.8 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.

4.9 When ships are in, or approaching, areas where attacks are known to have taken place, bridge watches and look outs should be increased, manpower resources allowing. Additional watches on the stern or covering radar "blind spots" should also be considered if personnel allows. Companies should consider investing in low light binoculars or night vision equipment for bridge staff and lookouts. Radar stations should be frequently staffed, even though it may be difficult to detect low profile fast moving craft on a ship's radar. 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 or CCTV when the ship is at anchor may also provide warning of the close approach of small craft.

4.10 It is particularly important to maintain a radar and visual watch for craft which may be trailing the ship when underway, but which could close in on 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.

4.11 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.

Ship Communications

4.12 Radio Procedures and Watch-keeping. Detailed guidance on radio procedures, radio watch keeping advice and standard message formats is contained in Appendix 1.

4.13 Ship Security Alert System (SSAS). 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.

4.14 Automatic Identification System (AIS). 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.

Lighting

4.15 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 (other than cruise ships) should where possible switch off deck lights when underway as if kept on they 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.

4.16 It is suggested that ships underway should be blacked out except for mandatory navigation lights (cruise ships should reduce lighting where possible without compromising the safety of the passengers and the crew). 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 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.

CCTV

4.17   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 closed circuit television (CCTV) coverage.

4.18   Companies should seek to provide CCTV coverage, and recording of, the main access points to the ship's secure areas, the corridors approaching the entrances to key areas and the bridge. 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.

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

Secure Areas

4.20   The Master may wish to consider designating a secure area(s) on the ship where the crew and passengers 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. 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.

4.21   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. 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.

4.22 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 allow entries and exits to be secured or controlled whilst incorporating appropriate safety provisions to ensure ease of egress and to permit access by rescue /emergency parties.

4.23 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.

Alarms

4.24 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.

Evasive Manoeuvring and Use of Hoses

4.25 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 ladders, poles or grappling irons to the ship.

4.26 Manoeuvres of this kind should not be used in congested waters, close inshore or by ships constrained by their draught in confined routes.

4.27 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.

4.28 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 has 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.

Use of Distress Flares

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

5. Armed Robbery

Theft or Robbery from a Ship

5.1 The most common form of armed attack consists of boarding a ship, stealing cargo or ship's equipment and withdrawing. 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 small crew and the attacker has both more and easier escape routes than when the ship is at sea

5.2 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.

Attacks at Anchor (Within Port Limits or at Anchorage)

5.3 A ship at anchor is usually boarded from a small boat under the cover of darkness and generally board the ship from the stern using grappling hooks attached to the ship's rail or by climbing the anchor chain. Often the attackers 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

Attacks When Moored Alongside

5.4   A ship moored 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.

Lighting (At Anchor)

5.5   The lighting recommendations 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. Recommended Practices to Deter Acts of Armed Robbery

At Anchor or in Port

6.1 The International Ship and Port Facility Security Code (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. For ships of other nationalities, 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. 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 to 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.

6.2 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, with the patrols 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.

6.3 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.

6.4   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.

<div style="border:1px solid #000; background:#e6f0e6; padding:10px;">

Key message

Factors Encouraging or Favouring Attackers

The following factors should be borne in mind when considering ALL types of attack, whether piracy on the high seas or armed robbery whilst the ship is tied-up:

- Cash in the Ship's Safe
- Smaller Crews

</div>

Cash in the Ship's Safe

6.5   The belief that large sums of cash are carried in the Master's safe attracts attackers. 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.

6.6   By virtue of their size (high freeboard) and the size of their crews, cruise 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 high risk ports, and in particular when they are moored alongside.

Smaller Crews

6.7   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 may 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.

6.8   The provision of 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 that any security personnel they may engage locally are genuine.

7. If Attackers Board

<div style="border:1px solid #000; background:#e6f0e6; padding:10px;">

Key message

- Early detection of potential attacks is key
- Secure greatest level of safety for those on board the ship
- Seek to ensure crew remain in control of navigation

</div>

7.1 Early detection of potential attacks should 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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 5 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.

7.6   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.

7.7   If any attackers are apprehended they 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.

8. If Attackers Gain Control

8.1 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.

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

8.3 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.

8.4 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 fitted with a Ship Security Alert System 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.

9. Action to Take After an Attack and Reporting Incidents

9.1   Ships attacked in the Gulf of Aden or off the coast of Somalia should follow the procedures as set out in the Best Management Practices, i.e. they should provide a detailed report to the Maritime Security Centre (Horn of Africa) (MSCHOA), United Kingdom Maritime Trade Operations Dubai (UKMTO Dubai) and the International Maritime Bureau (IMB).

9.2   Outside of this region, an immediate post attack report should be made to the relevant Rescue and Coordination 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.

9.3   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 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.

9.4   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.

9.5   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.

9.6   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. 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.

9.7   The format required for reports to the IMO is attached at Appendix 2. Reports may also contribute to future refining and updating of the advice in this guidance.

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

9.9   If a UK flagged 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.

10.   Jurisdiction and Intervention

Criminal Jurisdiction

10.1 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 1333 for definitions and additional information/guidance).

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

Naval Intervention

10.3 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.

10.4 Ships operating as part of the naval coalition in the Gulf of Aden or off the Coast of Somalia, under UN Security Council Resolution 1816, may

(a)   Enter the territorial waters of Somalia for the purpose of repressing acts of piracy and armed robbery at sea, in a manner consistent with such action permitted on the high seas with respect to piracy under relevant international law; and

(b)   Use, within the territorial waters of Somalia, in a manner consistent with action permitted on the high seas with respect to piracy under relevant international law, all necessary means to repress acts of piracy and armed robbery;

(United Nations Security Council Resolution 1816 (2008))

10.5 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.

10.6 A naval warship of any State can take robust action to come to the aid of a vessel under attack by pirates in international waters by deterring and disrupting the attack and using reasonable force to defend the victims. Vessels can be boarded and any piracy equipment can be seized as evidence.

10.7 Royal Navy and coalition ships will take all appropriate measures to respond to incidents of piracy on the high seas, whenever they are on hand to do so, and will provide every assistance to a Coastal State if ships are attacked in territorial waters. However since the likelihood of a Royal Navy ship being nearby when an incident occurs, particularly in distant waters, will not be great, British ships should nevertheless seek to rely on their own vigilance and resources to prevent attacks.

Role of the Port and Coastal State

10.8 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.

11.   Conclusion

11.1   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 guidance, 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.

11.2   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.

11.3   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.

Contacts and information

Piracy Reporting Centre

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

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

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.

Travel Advice Notices

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.

The full range of travel advice notices is available on the FCO's web site (http://www.fco.gov.uk). The Travel Advice Unit can also be contacted direct at TravelAdvicePublicEnquiries@fco.gov.uk; or on 0845 850 2829.

Department for Transport

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

- Maritime & Land Transport Security Division
- Department for Transport
- Zone 2/33 Great Minster House
- 33 Horseferry Road
- London
- SW1P 4DR

- 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.gsi.gov.uk

MSCHOA

- Tel: +44 (0)1923 958545

- Fax: +44 (0)1923 958520

- Email: postmaster@mschoa.org

- Web: www.mschoa.org

UKMTO

- Tel: +971 50 552 3215

- Email: ukmto@eim.ae

In the event of a piracy attack off the coast of Somalia or in the western Indian Ocean, contact UKMTO Dubai Hotline: +971 505 523 215.

APPENDIX 1

SHIP COMMUNICATIONS

Radio Procedures

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.

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 Appendix 1) 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.

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

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 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).

The International Maritime Organisation (IMO) recommends in MSC/Circ.597/Rev.1, 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/Circ.597/Rev.1 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, revised and updated by MSC.1/Circ. 1333 in June 2009. 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, revised and updated by MSC.1/Circ. 1334 in June 2009, as an equivalent guide to companies. Reports of attacks against UK flagged ships should also be made to the CSO and DfT via MRCC Falmouth. Other Flag States will have their own reporting requirements which seafarers should make themselves aware of.

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).

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".

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.

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

The following standard formats were agreed by the IMO Sub-Committee on Radio Communications in January 1993 and updated by MSC Circular 1333 published in June 2009, are set out below:

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

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 MSC/Circ.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

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.

SHIPS' MESSAGE FORMATS

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

- Ship's name and, callsign, IMO number, INMARSAT IDs (plus ocean region code) and MMSI
- MAYDAY/DISTRESS ALERT (see note)
- URGENCY SIGNAL
- PIRACY/ARMED ROBBERY ATTACK
- Ship's position (and time of position UTC)
- Latitude Longitude
- Course Speed KTS
- Nature of event

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

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

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

- Ship's name and, callsign, IMO number
- Reference initial PIRACY/ARMED ROBBERY ALERT
- Position of incident
- Latitude Longitude
- Name of the area
- Details of incident, e.g.:
- While sailing, at anchor or at berth?
- Method of attack
- Description/number of suspect craft
- Number and brief description of pirates/robbers
- What kind of weapons did the pirates/robbers carry?
- Any other information (e.g., language spoken)
- Injuries to crew and passengers
- Damage to ship (Which part of the ship was attacked?)
- Brief details of stolen property/cargo
- Action taken by the master and crew

- Was incident reported to the coastal authority and to whom?
- Action taken by the Coastal State
- Last observed movements of pirate/suspect craft, e.g.:
- Date/time/course/position/speed
- Assistance required
- Preferred communications with reporting ship, e.g.:
- Appropriate Coast Radio Station HF/MF/VHF INMARSAT IDs (plus ocean region code)
- MMSI
- Date and Time of the Report (UTC)

APPENDIX 2

FORMAT FOR REPORTING TO IMO THROUGH MARITIME
ADMINISTRATIONS OR INTERNATIONAL ORGANIZATIONS

- Ship's name and IMO number
- Type of ship
- Flag
- Gross tonnage
- Date and time
- Latitude Longitude
- Name of the area**
- While sailing, at anchor or at berth?
- Method of attack
- Description/number of suspect craft
- Number and brief description of pirates/robbers
- What kind of weapons did the pirates/robbers carry ?
- Any other information (e.g., language spoken)
- Injuries to crew and passengers
- Damage to ship (Which part of the ship was attacked?)
- Brief details of stolen property/cargo
- Action taken by the master and crew
- Was incident reported to the coastal authority and to whom?
- Reporting State or international organization
- Action taken by the Coastal State