ABS
FOUNDED 1862

Best Management Practices Against Somali Based Piracy

A quick reference guide to help implement "Best Management Practices for the Protection of Seafarers from Somali Based Piracy"

August 2011

Best Management Practices Against Piracy: A Quick Reference Guide

The best management practices (BMPs) for the protection of seafarers from Somali based piracy, developed by the maritime industry and adopted by the IMO (MSC Res. 324 (89)), can make a significant contribution in preventing a ship from becoming a victim of piracy in the Gulf of Aden, the Somali Basin and the Arabian Sea.

This booklet is based on the BMPs[1] and has been developed primarily for use on board a ship. It provides a quick reference guide for the Master and the Ship Security Officer (SSO) to prepare the vessel for transit through the high-risk area[2]. The guide also identifies actions that should be taken in the event the vessel and the people on board become victims of an attack.

The extent to which the guidance is followed remains at the discretion of the company, Master and the SSO. The measures contained in this guide may not be applicable to all ship types. It is important to note that the guidance is intended to supplement and support, but not replace, the security measures contained in the approved Ship Security Plan (SSP) and any guidance or instructions issued by the flag Administration.

[1] While many of the BMPs against piracy contained in this guide may remain valid, it is recommended that the company check and obtain the latest updates to the BMPs and any guidance issued by the flag Administration.

[2] The high-risk area for piracy attacks is based on where attacks have occurred in the past. For the purpose of following the BMPs in this guide, the high-risk area is bounded by Suez and the Straits of Hormuz to the North at 10°S and 78°E. The Master and SSO are encouraged to obtain the latest information before making the transit. It must be noted that attacks have taken place at the extremities of the high-risk area.

[3] Nothing in this booklet detracts from the Master's overriding authority to protect the crew, ship and cargo.

Assess the Risk

Prior to transiting to the high-risk piracy area, the Master should carry out a thorough risk assessment of the likelihood and consequences of piracy attacks, including measures for prevention, mitigation and recovery based on the latest available information. It is important that the risk assessment be ship and voyage-specific.

As a minimum, this risk assessment should consider:

❑ **Crew Safety:** Recognize potential conflicts with planned security measures, bearing in mind that safety should ALWAYS take precedence. Determine the location of the safe muster point and/or citadel. Ballistic protection should be considered for the crew on essential bridge duties given that pirates tend to fire at the bridge to try to force the vessel to stop.

❏ **Freeboard:** Identify the available protection from the physical characteristics of the vessel. Vessels with a large freeboard have a much greater chance of successfully escaping an attack, though that factor alone may not be enough to deter a piracy attempt. Pirates typically attempt to gain access from the lowest point above sea level which is generally the vessel's stern.

❏ **Speed:** Vessels proceeding at higher speeds (more than 18 knots) are better able to outrun an attempted attack. If able, increase the vessel's speed after identifying a suspicious vessel. If using Group Transit within the International Recommended Transit Corridor (IRTC), the speed may need to be adjusted.

❏ **Sea State:** Generally pirates mount their attacks from very small crafts. It is difficult to operate such craft in sea state 3 and above.

A review of the Ship Security Assessment (SSA) on which the approved ship security plan is based should also be undertaken at this time to determine any additional preventive measures that may be needed to counter the piracy threat.

Reporting Requirements

All vessels must report to the UK Maritime Trade Operations (UKMTO) and the Maritime Security Centre Horn of Africa (MSCHOA) so that naval forces are aware of the vessel's planned sea passage and vulnerability to a pirate attack.

□ Company to register for access on the MSCMOA website in order to access the latest threat information.

□ Prior to entering the high-risk area, obtain the latest information from the MSCHOA and NATO Shipping Centre websites.

□ Submit the "Vessel Movement Registration Form" to MSCHOA prior to entering the voluntary reporting area.

□ Submit the "Vessel Position Reporting Form: Initial Report" to UKMTO when entering the voluntary reporting area.

□ Thereafter, send "Vessel Position Report Form: Daily Position Report" at 08:00 hours GMT each day to UKMTO.

□ Send final report upon departure from the high-risk area or on arrival at port of call.

Pre-transit Planning

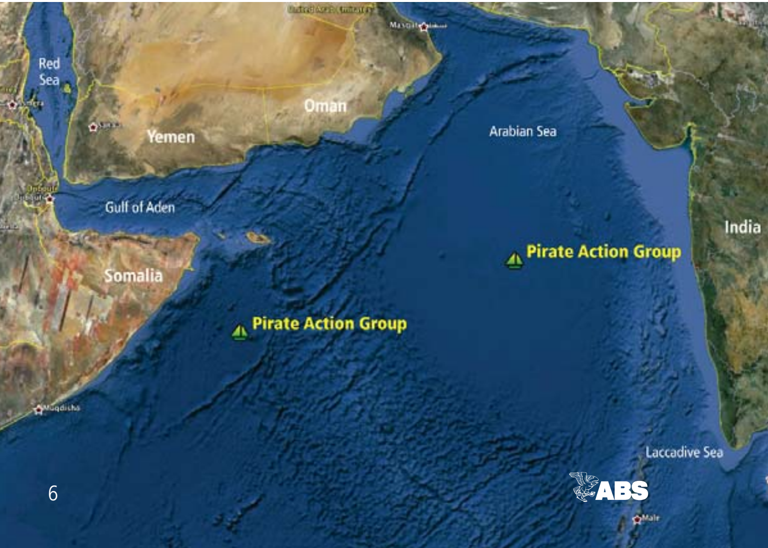
Pre-transit planning is crucial. The majority of attempted hijacks have been successfully repelled by a ship's crew that have planned for possible attacks in advance and have applied the BMPs. This includes:

❑ Review the Ship Security Assessment (SSA) and effectively implement the Ship Security Plan (SSP).

❑ Test the ship's security alert system.

❑ Establish the ship's Automatic Identification System (AIS) policy. It is recommended that AIS transmission is left on, but is restricted to the ship's identity, position, course, speed, navigational status and safety-related information.

❑ Ensure that a contingency plan against piracy and hijacking is in place and has been exercised.



❑ Obtain the latest threat information for the high-risk area from the MSCHOA and NATO Shipping Centre websites, as well as navigational warnings from Navtex and Sat-C.

❑ Carefully review the passage plan in light of the latest information and warnings received.

❑ Brief the crew on preparations and conduct a drill.

❑ Familiarize the crew with alarm signals that signify an attack and an all clear situation.

❑ Implement and test all ship protection measures.

❑ Establish an emergency communications plan and ensure that relevant contact numbers and prepared messages are at hand or permanently displayed near the communications panel.

❑ Restrict maintenance work outside of accommodations to a minimum.

❑ Do not perform maintenance work on any essential equipment.

❑ Verify all engine room machinery and systems are readily available for immediate use.

❑ Establish detailed watchkeeping arrangements.

❑ Ensure vessel's passage planning is carried out through the Internationally Recommended Transit Corridor (IRTC) only.

❑ Avoid entering Yemeni territorial waters (12 miles) during the transit as international naval forces may be unable to assist vessels under attack inside these waters.

❑ Ensure vessel is able to proceed at the full sea speed that is consistent with safety. Transit speed in excess of 18 knots is noted to be an effective deterrent.

Pre-transit Planning (continued)

❑ Master should practice maneuvering the ship. The goal is to establish which series of helm orders produce the most difficult sea conditions for pirate skiffs trying to attack, without causing a significant reduction in the ship's speed.

❑ Obtain the latest information and timings of the Group Transit Scheme[1] from MSCHOA and utilize the group transit.

❑ Be prepared to adjust passage plan for timely arrival at group transit "forming up points" without a prolonged approach at slow speed to reduce the vulnerability to attack.

[1] Information on independent convoy escorts through IRTC offered by some countries may be obtained from MSCHOA website.

Ship Protection Measures

Prior to commencing transit into the high-risk area, the Master is to establish ship protection measures for increased vigilance.

❑ **Watchkeeping and Lookout Arrangements**

1. Establish watchkeeping and lookout roster
2. Consider short watch rotations to enhance alertness
3. Post additional lookouts to monitor activity in vicinity of vessel
4. Brief lookouts and equip them with handheld radios, binoculars and flashlights
5. Use night vision optics, if available
6. Maintain an efficient radar watch
7. Deploy dummies at strategic locations to give the impression of greater crew numbers on watch

❑ **Closed Circuit Television (CCTV)**

1. If available, use CCTV cameras for coverage of vulnerable areas, particularly the poop deck
2. Position CCTV monitors at the rear of the bridge and at the safe muster point and/or citadel
3. Record all CCTV footage

❑ Alarms

1. Establish a distinct piracy alarm
2. Ensure crew members are familiar with the various alarms on board
3. Conduct drills prior to entering the high-risk area to test crew response to piracy alarm
4. Keep ship's whistle and fog horn ready for immediate use

❑ Lighting

1. Inspect and test all lighting equipment
2. Keep search lights ready for immediate use
3. Navigate with only navigation lights illuminated; deck and search lights should be extinguished
4. Once pirates have been identified or an attack commences, illuminate the deck and use search lights to indicate to the pirates that they have been observed

❑ Access Control

1. Develop and test an accommodation lock down procedure so likely access points can be rapidly secured
2. Firmly secure all doors and hatches providing access to the accommodation and machinery spaces
3. Designate a limited number of doors and hatches to use for routine access
4. Secure or lift external ladders on the accommodation block to prevent their use and to restrict external access to the bridge
5. Ensure that all emergency escape routes from a manned compartment that have been secured can be opened from within
6. Verify that all watertight doors and hatches are secured with all clips fully dogged down in addition to any locks; where possible, secure access points with wire straps
7. Protect portholes and windows with deadlights or cross steel bars

❑ Ship's Stores, Tools and Equipment

1. Lock all tools and equipment that may be of use to pirates in a secure location
2. Provide added protection (sand bags, Kevlar blankets, etc.) to areas where gas bottles (i.e. oxyacetylene) or containers of flammable liquids are held to avoid exposure to firearms
3. Consider landing excess items prior to transit

❑ Protection of the Bridge

1. Consider providing Kevlar jackets and helmets for the bridge team to provide a level of protection during an attack (if possible, jackets and helmets should be in a nonmilitary color)
2. Apply security glass film to bridge windows for protection against flying glass
3. Provide fabricated metal plates for covering the bridge side, rear and bridge wing door windows that can be rapidly secured in place in the event of an attack
4. Protect the after part of bridge wings with a wall of sandbags or with a double layer of chain link fence

❑ Physical Barriers

1. Establish physical barriers to make the use of ladders and grappling hooks difficult for pirates to gain access
2. Deploy razor wire or barbed wire fencing on the external perimeter of the vessel
3. Coat external structures with anti-climb[1] paint where feasible
4. Rig hoses with running water to create a shield that impedes easy access
5. Depending on ship type, install electrified barriers on vessel's perimeter (this is not advisable on oil tankers)
6. Display warning signs of electrified barriers facing both inward and outward of vessel.

[1] Anti-climb paint (also known as anti-vandal paint) is a class of paint consisting of a thick oily coating. In appearance it is similar to smooth gloss paint but it remains slippery thereby preventing any intruder from gaining a foothold.

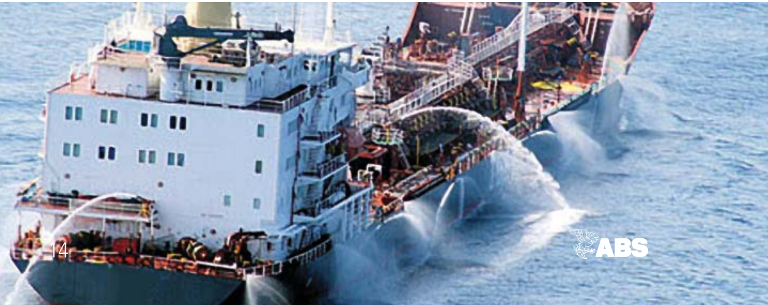
❑ Spray and Foam Monitors, Water Cannons and Ballast Water

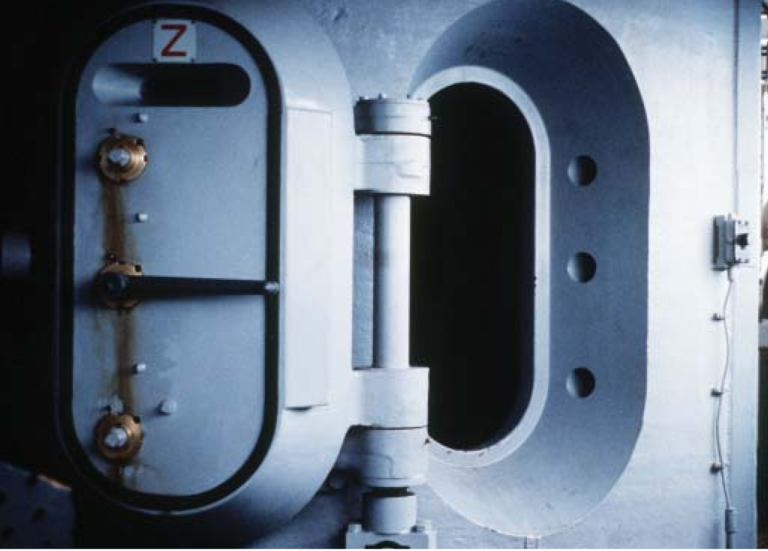
1. Deploy water hoses, foam monitors and water cannons over likely access points to deter and delay pirates from gaining access on board
2. Rig the water spray hoses and foam monitors in a fixed position[1,2]
3. Use hoses in jet mode with a fixed baffle plate a short distance in front of the nozzle to increase coverage area
4. Deploy water cannons that deliver water in a sweeping arc to protect a greater part of the hull; many have been developed from tank cleaning machines
5. Steam and heated water, if available, is an effective deterrent
6. Flood the main deck with water by overflowing ballast tanks[3] through air vents or install spray rails to create a water curtain over the ship's side
7. Avoid maintenance of sea water systems in the high-risk area

[1] Manual handheld operation of hoses and foam monitors is not recommended as it exposes the operator.

[2] Foam, if used, must be in addition to the vessel's standard firefighting equipment stock.

[3] Care must be taken to ensure that ballast tanks are not over-pressurized which can cause damage to the hull and tanks or compromise the vessel's stability.





❑ Safe Muster Points and Citadels

1. Establish a safe muster point where all crew members, except those on essential bridge and engine room duties, can muster in the event of an attack – preferably low down in the vessel. Safe muster points should provide a short-term safe haven and ballistic protection from small arms and RPG rounds.

2. Consider establishing a citadel, i.e. a designated pre-planned and purpose-built area where all crew can seek protection in the event of an attack. Such a space would probably have, but not be limited to, its own self-contained air-conditioning, emergency rations, water supply, external communications' capabilities, emergency shut-down capability for the main and auxiliary engines and remotely-operated CCTV cameras.

❑ Armed and Unarmed Private Maritime Security Contractors[1,2]

1. Notify UKMTO and MSCHOA if armed security contractors are present on board
2. Follow IMO Guidance[3] on the use of armed private maritime security contractors

[1] Whether to use private maritime security contractors within the high-risk area is a decision for the individual shipowner in consultation with the flag Administration, after a thorough risk assessment and after ensuring all other practical means of self protection have been employed.

[2] Private security contractors, if used, should be in addition to and not an alternative to measures contained in the BMPs.

[3] Refer MSC.1/Circ. 1405 "Interim Guidance to shipowners, ship operators and shipmasters on the use of privately contracted armed security personnel (PCASP) on board ships in the high-risk area" and MSC.1/Circ. 1406 "Interim Recommendations for flag States regarding the use of privately contracted armed security personnel on board ships in the high-risk area."

Recommended Actions in the Event of a Pirate Attack

❑ Follow the pre-prepared contingency plan.

❑ Sound the emergency alarm.

❑ Activate the Ship Security Alert System (SSAS).

❑ Ensure that the AIS is switched on.

❑ Activate the Emergency Communication Plan and report the attack to UKMTO.

❑ Make a distress call (Mayday) on VHF Channels 08 and 16.

❑ Send a distress message via Inmarsat and Digital Selective Calling (DSC). Establish telephone contact with UKMTO, if possible.

❑ Increase speed of the vessel.

❑ Maneuver the vessel away from the pirate craft to deter boarding and to increase the pirates' exposure to sea, swell and stern wash. If pirates close in on the vessel, the Master should make small alterations in the course to avoid pirate craft from lying alongside the vessel.

❑ Activate water hoses and spray and other ship protection measures.

❑ Sound the ship's whistle and fog horn continuously.

❑ Ensure all external and internal doors are secure.

❑ Muster crew to the safe muster point and/or citadel, as applicable.

Recommended Actions if Pirates take Control of the Vessel

❑ Remain calm.

❑ If possible, inform UKMTO and the company before pirates gain access to the bridge.

❑ Activate the SSAS and ensure AIS is switched on.

❑ To reduce risk of harm, offer no resistance once the pirates have reached the bridge.

❑ Stop main engine and steer the vessel clear of all other ships if bridge and/or engine room is to be evacuated.

❑ Muster all remaining crew to the safe muster point with their hands visible on their heads.

❑ If vessel is constructed with a citadel[1], stop main engine, ensure vessel has adequate sea room to drift safely, evacuate all crew and secure the citadel from within in accordance with the ship security plan.

❑ Leave any CCTV running.

[1] It is important to note that the benefit of the citadel is lost if any crew member is left outside before it is secured. The use of a citadel does not guarantee a naval and/or military response. The company and Master should obtain the latest guidance on the use of citadels from MSCHOA before transit.

Recommended Actions if Military Action is Taken

❑ Keep low on the deck with hands visible covering the head.

❑ Do not use flash photography.

❑ Cooperate fully with military personnel.

❑ No sudden or aggressive movements.

❑ Provide identification if challenged.

❑ Be aware that all military personnel may not speak English.

Recommended Actions After a Pirate Attack

❑ Maintain a complete record of the incident.

❑ Report the description and distinguishing features of suspicious vessels.

❑ Submit a detailed report to the company, UKMTO, MSCHOA and the IMB.

❑ Submit the standardized piracy report form contained in the Appendix of the BMPs.

❑ Cooperate with law enforcement agencies during debriefing.

❑ Preserve all electronic and physical evidence in a secure location.

Useful Contact Information

UK Maritime Trade Operations (UKMTO)

Email: UKMTO@eim.ae
Tel: +971-50-552-3215

Maritime Security Centre Horn of Africa (MSCHOA)

Web: www.mschoa.org
Email: postmaster@mschoa.org
Tel: +44 (0)-1923-958545
Fax: +44 (0)-1923-958520

NATO Shipping Centre (NSC)

Web: www.shipping.nato.int
Email: info@shipping.nato.int
Tel: +44(0)1923-956574
Fax: +44(0)1923-956575

Maritime Liaison Office (MARLO)

Web: www.cusnc.navy.mil/marlo/
Email: marlo.bahrain@me.navy.mi
Tel: +973-1785-3925
Duty (24 hours): +973-3940-1395
Fax: +973-1785-3920

INTERPOL

Web: www.interpol.int
Email: os-ccc@interpol.int
Tel (24 hours): +33 (0) 472-447676

International Maritime Bureau (IMB)

Email: piracy@icc-ccs.org
Tel: +60-3-2031-0014
Fax: +60-3-2078-5769
Telex: MA34199 IMBPC1