C C S 通 函

Circular

China Classification Society
（2011）Circ.No. 14 Total No. 78
March 2 5, 2011 （Total 6 Pages ）

TO: Related departments of Headquarters; Branches and Offices; and Ship Companies

Notice of Implementation of MI MN No. 2-011-31, Rev. 12/10

----- Piracy, Armed Attacks, Hijacking or Terrorism: Reporting Incidents, Ship Security Plans and Best Management Practices (BMPs)

The Maritime Administration of Marshall Islands issued Marine Notice NO.2-011-31, Rev. 12/10 to Ship-owners, Operators, Masters and Officers of merchant ships and Recognized Organizations. This Notice supersedes Rev. 11/10 and reflects additional clarification on the incorporation of Best Management Practices 3rd edition (BMP3) and the Administrator's additions, based on further lessons learned, into the MI requirements for addressing piracy, particularly regarding Initial Notification and Reporting and Citadels. Both BMP3 and the guidance on post-piracy care for seafarers are dynamic working documents meant to be updated with experience.

It is important to note that the Administrator considers the ISPS Code to be an extension of the International Safety Management (ISM) Code under ―Emergency Preparedness. The ISM Code was recently amended to require companies to assess all identified risks to their vessels, personnel and the environment and to establish appropriate safeguards. These risks include the threat of piracy, armed attacks, hijacking and terrorism, particularly for vessels operating in High Risk Areas as defined in Annex A.

Applicability:

1.0 SSP and BMPs Requirements

In addition to adhering to the reporting requirements, the following MI flagged vessels that are subject to the ISPS Code and operate in High Risk Areas must comply with the SSP and BMPs provisions of this Notice:

- Passenger ships, including high-speed passenger craft;

- Cargo ships, including high-speed craft, of 500 gross tonnage (ITC 69) and upwards;
- Special Purpose Ships of 500 gross tonnage; and
- Self-propelled mobile offshore drilling units capable of making international voyages unassisted and unescorted when underway and not on location.

2.0 Reporting Requirements

All ships under the MI flag must comply with all reporting requirements.

REQUIREMENTS:

1.0 SSP - Risk Assessment

1.1 MI shipowners and operators with vessels identified in the above section on must, along with the Master, carry out a risk assessment of their vessel(s) to determine the likelihood and consequences of a piracy attack, an armed attack, hijacking or terrorism and identify and incorporate prevention, mitigation and recovery measures in their SSPs, taking into consideration the guidance contained in MSC.1/Circ.1337, along with the BMPs Guidelines (see Annex A) and additional Administrator-specific measures, including those pertaining to radio and distress messages, contained in Annex A of this Notice, each as may be updated or amended.

1.2 Incorporation of relevant provisions on piracy, armed robbery, terrorism and armed attack into SSPs is required immediately, but need not be verified and approved until the next scheduled ISM/ ISPS Code Audit. As outlined in §10.3.3 of MI Marine Notice 2-011-16, the provisions can be included as an Annex to the SSP to facilitate the anticipated updates to the BMPs and guidance on post-piracy care for seafarers.

2.0 Reporting

2.1 General

The Administrator recognizes that an essential part of preventing, deterring and suppressing attacks is prompt reporting to the proper authorities and organizations both during and post-incident. As a result, not only must reporting be addressed by Companies and ships as part of their BMPs in accordance with IMO Resolution A.683(17), Prevention and Suppression of Piracy and Armed Robbery Against Ships, the Administrator is required to report in detail all incidents of piracy and armed robbery of its vessels to the International Maritime Organization (IMO).

2.2 Initial Notification and Reporting

.1 Suez, Gulf of Aden (GoA), the Somali Basin and Indian Ocean

.a Pre-Transit Notification

Ships must participate in the pre-transit notification requirements outlined in section 6.0 of the BMPs (see Annex A of this Notice) for each transit made. Refer also to Appendix I of this Notice for all contact details of the military. All ships transiting the Red Sea, GoA, the Somali Basin and Indian Ocean are being tracked through Long-Range Identification and Tracking (LRIT) by EUNAVFOR. The shipowners of those ships reported to the Administrator by EUNAVFOR found not to be participating in LRIT will be contacted by the Administrator and reminded to bring their ship into compliance.

.b SSAS

.i The following ships are required to comply with SOLAS Regulation XI-2/6 for a SSAS:

- passenger ships, including high-speed passenger craft;
- cargo ships, including high-speed craft, of 500 gross tons and above; and
- mechanically propelled mobile offshore drilling units as defined in SOLAS regulation IX/1, not on location. See MI Marine Notice 2-011-18.

.ii If attacked by pirates, or there is a clear and imminent threat of danger, a ship should immediately activate its SSAS. This will alert the Company Security Officer (CSO) and the Administrator. Additionally, if the ship is subscribed to SSRS (see .c, below), it will also directly alert naval forces. If a ship has not subscribed to SSRS, UK Maritime Trade Operations (UKMTO) should be notified after SSAS activation.

.iii The transmission of a Ship Security Alert (SSA) should not be included with any other routine reporting that the ship may conduct. The message transmission should be generated automatically with no input from the operator other than the activation of the system. Remember that two (2) activation points are required: one (1) located on the navigation bridge and one (1) other that would normally be accessible. The second activation point should be kept confidential, known only to the Master, Ship Security Officer (SSO) and other senior ship‘s personnel as may be decided by the CSO.

.iv The SSA message must be capable of reaching the Administrator and CSO from any point along the vessel‘s intended route and must include:

(a) the vessel name;
(b) the IMO Ship Identification Number;
(c) the Call Sign;
(d) the Maritime Mobile Service Identity;
(e) date and time;
(f) position;

(g) course and speed;
(h) name of CSO and 24/7 phone number;
(i) name of alternate CSO and 24/7 phone number; and
(j) a message stating that the SSAS has been activated and indicating the ship is under threat or it has been compromised.

.c SSRS

.i Shipowners are authorized and strongly recommended to subscribe to the SSRS because it provides a real-time link between ship operations and naval operations by enhancing the counter-piracy effectiveness of the existing SSAS.

.ii The SSRS is provided through a commercial service that continuously monitors SSAS alerts and position reports, filters out alerts emanating from outside the High Risk Area and dependent upon the location of the report, routes the information in real time to participating Naval Operations Centres. Shipowners receive a notification email confirming that security alert/position report information is being routed to a Naval Operations Centre.

.iii The SSRS enables a rapid, coordinated response to a security alert by automating alert transmissions and connecting ships directly to Task Forces (via the relevant Naval Operations Centres). It minimizes communication delays between the stakeholders. Naval forces are provided with immediate knowledge of the location of a piracy attack, pre/post attack ship positional information, and relevant ship-specific information such as freeboard, speed and communication terminal details.

.iv Should crew members be under immediate duress, the SSRS offers a covert method of automatically alerting naval forces and is particularly effective in triggering a speedy response when used in conjunction with a telephone call to UKMTO. Note that once activated, it will automatically continue to report to the military authorities.

.v Be prepared to immediately verify SSRS activation with the UKMTO.

.vi The SSRS service can be accessed from the commercial website: www.ssrs.org.

.2 Strait of Hormuz and Arabian Gulf

When transiting the Strait of Hormuz and Arabian Gulf, as soon as the Master feels that a threat is developing, he/she should immediately activate the SSAS and call to report hostile or potentially hostile action (including suspicious activity) to the COMUSNAVCENT Battlewatch Captain and UKMTO (see Appendix I for contact details).

.3 Other High Risk Areas (see Annex A, 1.4(e))

When transiting these areas, as soon as the Master feels that a threat is developing, he/she should immediately activate the

SSAS and call to report hostile or potentially hostile action (including suspicious activity) to the local authorities, Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) and International Maritime Bureau (IMB) (see Appendix I for contact details).

2.3 Follow-up Reporting

.1 Masters, owners or operators must immediately (within 24 hours) report by fax or email the occurrence of all incidents of piracy and armed robbery, armed attacks, attempted or actual hijacking, terrorism or other hostile or suspicious activity, including apparent surveillance being conducted by small vessels, on or near their merchant vessels to:

Republic of the Marshall Islands Maritime Administrator
c/o Investigations
11495 Commerce Park Drive
Reston, Virginia 20191-1506 USA
Fax: +1-703-476-8522
Email: investigations@register-iri.com
dutyofficer@register-iri.com

.2 The report should be submitted to the Administrator on form MI-109-2, Report of Piracy and Armed Robbery Against Ships, contained in Appendix III of this Notice. This form also may be used for submissions to the international organizations (e.g., Maritime Security Centre - Horn of Africa (MSCHOA), UKMTO, Maritime Liaison Office (MARLO), IMB and IMO).

.3 Reports received by the Administrator will be transmitted to:

- National Geospatial-Intelligence Agency (NGA), Bethesda, MD, USA;
- IMO, Maritime Safety Department, London;
- IMB, Essex, UK; and
- The International Shipping Federation, London.

.4 Refer to Appendix I of this Notice for all contact details of the military and IMB.

Summary:

RMI office of the Marine Administrator issued the marine notice 2-011-31 requires SSPs pursuant to the ISPS Code to include security measures to preventing, deterring and delay the incidents of piracy, armed attacks, hijacking or terrorism. And also provides guidance on BMPs to shipowners, operators, and masters. Major updates are shown in Italic.

Action required:

All the CCS Branches and Offices are required to organize the study and training of this Marine notice. Auditors should remind the compliance with this requirement

during the ISM audit to the RMI-flagged Company and vessel, and remind shipowners to carry out a risk assessment of their vessel(s), and establish the corresponding security measures. Meanwhile, the masters are required to promptly report to the proper authorities of all incidents in accordance with the guidance on BMPs (see Annex A) and requirements of the attached forms.

Attachment: 1. Marine Notice NO.2-011-31, Rev. 12/10， 44 pages.

For any problem please contact the Certification Management Dept. of CCS Headquarters without hesitation

REPUBLIC OF THE MARSHALL ISLANDS

OFFICE OF THE MARITIME ADMINISTRATOR

Marine Notice

No. 2-011-31

Rev. 12/10

TO: **ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS OF MERCHANT SHIPS, AND RECOGNIZED ORGANIZATIONS**

SUBJECT: **Piracy, Armed Attacks, Hijacking or Terrorism: Reporting Incidents, Ship Security Plans and Best Management Practices.**

References:

- **(a) International Ship and Port Facility Security (ISPS) Code (MI Marine Notice 2-011-16)**
- **(b) International Safety Management (ISM) Code (MI Marine Notice 2-011-13)**
- **(c) Best Management Practices 3, Piracy off the Coast of Somalia and Arabian Sea Area, Witherby Seamanship International, Ltd, June 2010**
- **(d) International Maritime Organization (IMO) MSC.1/Circ.1337, dated 4 August 2010**
- **(e) IMO Resolution A.683(17), dated 6 November 1991**
- **(f) IMO Resolution MSC. 305(87), dated 17 May 2010**
- **(g) Revised Gulf of Aden Transit Corridor – 1 February 2009 (MI Marine Safety Advisory #2-09)**
- **(h) MSC/Circ. 805, dated 6 June 1997**
- **(i) EU NAVFOR/NATO, CMF WARNING, dated 13 November 2009**
- **(j) Post-Piracy Care for Seafarers Guidelines, Seaman's Church Institute, 16 September 2010**

PURPOSE:

This Notice requires Ship Security Plans (SSPs) pursuant to the International Ship and Port Facility Security (ISPS) Code to include security measures to protect against incidents of piracy, armed attacks (including armed robbery), hijacking or terrorism that at a minimum meet internationally accepted Best Management Practices (BMPs) and Republic of the Marshall Islands (MI) requirements. It also requires the reporting of all such incidents to the Maritime Administrator (the "Administrator") and authorities.

It is important to note that the Administrator considers the ISPS Code to be an extension of the International Safety Management (ISM) Code under "Emergency Preparedness." The ISM Code was recently amended to require companies to assess all identified risks to their vessels, personnel and the environment and to establish appropriate safeguards. These risks include the threat of piracy, armed attacks, hijacking and terrorism, particularly for vessels operating in High Risk Areas as defined in Annex A.

Inquiries concerning the subject of this Notice should be directed to the Office of the Maritime Administrator, Republic of the Marshall Islands, c/o Marshall Islands Maritime and Corporate Administrators, Inc., 11495 Commerce Park Drive, Reston, VA 20191-1506 USA.

The Administrator strongly endorses and recommends that ships subscribe to Ship Security Reporting System (SSRS). This system provides a real-time link between ship operations and naval operations by enhancing the counter-piracy effectiveness of the existing Ship Security Alert System (SSAS) (see section 2.2.2 of this Notice below).

This Notice supersedes Rev 11/10 and reflects additional clarification on the incorporation of Best Management Practices 3rd edition (BMP3) and the Administrator's additions, based on further lessons learned, into the MI requirements for addressing piracy, particularly regarding Initial Notification and Reporting (see section 2.2 below) and Citadels (see section 7.14 below). Both BMP3 and the guidance on post-piracy care for seafarers (Appendix V) are dynamic working documents meant to be updated with experience.

APPLICABILITY:

1.0 SSP and BMPs Requirements

In addition to adhering to the reporting requirements**,** the following MI flagged vessels that are subject to the ISPS Code and operate in High Risk Areas must comply with the SSP and BMPs provisions of this Notice:

- Passenger ships, including high-speed passenger craft;
- Cargo ships, including high-speed craft, of 500 gross tonnage (ITC 69) and upwards;
- Special Purpose Ships of 500 gross tonnage; and
- Self-propelled mobile offshore drilling units capable of making international voyages unassisted and unescorted when underway and not on location.

2.0 Reporting Requirements

All ships under the MI flag must comply with all reporting requirements.

REQUIREMENTS:

1.0 SSP – Risk Assessment

1.1 MI shipowners and operators with vessels identified in the above section on Applicability must, along with the Master, carry out a risk assessment of their vessel(s) to determine the likelihood and consequences of a piracy attack, an armed attack, hijacking or terrorism and identify and incorporate prevention, mitigation and recovery measures in their SSPs, taking into consideration the guidance contained in MSC.1/Circ.1337, along with the BMPs Guidelines (see Annex A) and additional Administrator-specific measures, including those pertaining to radio and distress messages, contained in Annex A of this Notice, each as may be updated or amended.

1.2 Incorporation of relevant provisions on piracy, armed robbery, terrorism and armed attack into SSPs is required immediately, but need not be verified and approved until the next scheduled ISM/ ISPS Code Audit. As outlined in §10.3.3 of MI Marine Notice 2-011-16, the provisions can be included as an Annex to the SSP to facilitate the anticipated updates to the BMPs and guidance on post-piracy care for seafarers.

2.0 Reporting

2.1 General

The Administrator recognizes that an essential part of preventing, deterring and suppressing attacks is prompt reporting to the proper authorities and organizations both during and post-incident. As a result, not only must reporting be addressed by Companies and ships as part of their BMPs in accordance with IMO Resolution A.683(17), Prevention and Suppression of Piracy and Armed Robbery Against Ships, the Administrator is required to report in detail all incidents of piracy and armed robbery of its vessels to the International Maritime Organization (IMO).

2.2 Initial Notification and Reporting

.1 Suez, Gulf of Aden (GoA), the Somali Basin and Indian Ocean

.a Pre-Transit Notification

Ships must participate in the pre-transit notification requirements outlined in section 6.0 of the BMPs (see Annex A of this Notice) for each transit made. Refer also to Appendix I of this Notice for all contact details of the military. All ships transiting the Red Sea, GoA, the Somali Basin and Indian Ocean are being tracked through Long-Range Identification and Tracking (LRIT) by EUNAVFOR. The shipowners of those ships reported to the Administrator by EUNAVFOR found not to be participating in LRIT will be contacted by the Administrator and reminded to bring their ship into compliance.

.b SSAS

.i The following ships are required to comply with SOLAS Regulation XI-2/6 for a SSAS:

- passenger ships, including high-speed passenger craft;
- cargo ships, including high-speed craft, of 500 gross tons and above; and
- mechanically propelled mobile offshore drilling units as defined in SOLAS regulation IX/1, not on location. See MI Marine Notice 2-011-18.

.ii If attacked by pirates, or there is a clear and imminent threat of danger, a ship should immediately activate its SSAS. This will alert the Company Security Officer (CSO) and the Administrator. Additionally, if the ship is subscribed to SSRS (see .c, below), it will also directly alert naval forces. If a ship has not subscribed to SSRS, UK Maritime Trade Operations (UKMTO) should be notified after SSAS activation.

.iii The transmission of a Ship Security Alert (SSA) should not be included with any other routine reporting that the ship may conduct. The message transmission should be generated automatically with no input from the operator other than the activation of the system. Remember that two (2) activation points are required: one (1) located on the navigation bridge and one (1) other that would normally be accessible. The second activation point should be kept confidential, known only to the Master, Ship Security Officer (SSO) and other senior ship's personnel as may be decided by the CSO.

.iv The SSA message must be capable of reaching the Administrator and CSO from any point along the vessel's intended route and must include:

(a) the vessel name;
(b) the IMO Ship Identification Number;
(c) the Call Sign;
(d) the Maritime Mobile Service Identity;
(e) date and time;
(f) position;
(g) course and speed;
(h) name of CSO and 24/7 phone number;
(i) name of alternate CSO and 24/7 phone number; and
(j) a message stating that the SSAS has been activated and indicating the ship is under threat or it has been compromised.

.c SSRS

.i Shipowners are authorized and strongly recommended to subscribe to the SSRS because it provides a real-time link between ship operations and naval operations by enhancing the counter-piracy effectiveness of the existing SSAS.

.ii The SSRS is provided through a commercial service that continuously monitors SSAS alerts and position reports, filters out alerts emanating from outside the High Risk Area and dependent upon the location of the report, routes the information in real time to participating Naval Operations Centres. Shipowners receive a notification email confirming that security alert/position report information is being routed to a Naval Operations Centre.

.iii The SSRS enables a rapid, coordinated response to a security alert by automating alert transmissions and connecting ships directly to Task Forces (via the relevant Naval Operations Centres). It minimizes communication delays between the stakeholders. Naval forces are provided with immediate knowledge of the location of a piracy attack, pre/post attack ship positional information, and relevant ship-specific information such as freeboard, speed and communication terminal details.

.iv Should crew members be under immediate duress, the SSRS offers a covert method of automatically alerting naval forces and is particularly effective in triggering a speedy response when used in conjunction with a telephone call to UKMTO. Note that once activated, it will automatically continue to report to the military authorities.

.v Be prepared to immediately verify SSRS activation with the UKMTO.

.vi The SSRS service can be accessed from the commercial website: www.ssrs.org.

.2 Strait of Hormuz and Arabian Gulf

When transiting the Strait of Hormuz and Arabian Gulf, as soon as the Master feels that a threat is developing, he/she should immediately activate the SSAS and call to report hostile or potentially hostile action (including suspicious activity) to the COMUSNAVCENT Battlewatch Captain and UKMTO (see Appendix I for contact details).

.3 Other High Risk Areas (see Annex A, 1.4(e))

When transiting these areas, as soon as the Master feels that a threat is developing, he/she should immediately activate the SSAS and call to report hostile or potentially hostile action (including suspicious activity) to the local authorities, Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) and International Maritime Bureau (IMB) (see Appendix I for contact details).

2.3 Follow-up Reporting

.1 Masters, owners or operators must immediately (within 24 hours) report by fax or email the occurrence of all incidents of piracy and armed robbery, armed attacks, attempted or actual hijacking, terrorism or other hostile or suspicious activity, including apparent surveillance being conducted by small vessels, on or near their merchant vessels to:

Republic of the Marshall Islands Maritime Administrator
c/o Investigations
11495 Commerce Park Drive
Reston, Virginia 20191-1506 USA
Fax: +1-703-476-8522
Email: investigations@register-iri.com
dutyofficer@register-iri.com

.2 The report should be submitted to the Administrator on form MI-109-2, Report of Piracy and Armed Robbery Against Ships, contained in Appendix III of this Notice. This form also may be used for submissions to the international organizations (e.g., Maritime Security Centre – Horn of Africa (MSCHOA), UKMTO, Maritime Liaison Office (MARLO), IMB and IMO).

.3 Reports received by the Administrator will be transmitted to:

- National Geospatial-Intelligence Agency (NGA), Bethesda, MD, USA;
- IMO, Maritime Safety Department, London;
- IMB, Essex, UK; and
- The International Shipping Federation, London.

.4 Refer to Appendix I of this Notice for all contact details of the military and IMB.

BEST MANAGEMENT PRACTICES GUIDELINES - ANNEX A

In an effort to counter piracy in the GoA, the Somali Basin and Indian Ocean, industry has developed and prepared Best Management Practices (BMPs) Guidelines which are supported and endorsed by the Administrator through the New York Declaration. The BMPs Guidelines aim to assist Companies and ships in avoiding piracy attacks by providing suggested planning and recommended operational practices. The BMPs Guidelines complement guidance provided in IMO's MSC.1/Circ.1337 (reference (d), of this Notice). This Annex is a consolidation of the BMPs and additional guidance provided by the Administrator through lessons learned. See Appendix VI for signatories to and updating of BMPs.

1.0 Definitions

1.1 Armed Robbery

.1 Armed robbery against ships means any of the following acts:

(a) any illegal 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;

(b) any illegal 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; or

(c) any act of inciting or of intentionally facilitating an act described above.

1.2 Piracy

.1 United Nations Convention on Law of the Sea (UNCLOS)

As contained in Article 101 of UNCLOS and as amended consistent with ReCAAP, 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; or

(c) any act inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

.2 BMPs Guidance on Definition of Piracy

To provide a clear, practical, working definition, the BMPs provide the following as guidance for determining whether an attack is piracy:

(a) the use of violence against the ship or its personnel or any attempt to use violence;

(b) attempt(s) to board the vessel where the Master suspects persons are pirates;

(c) an actual boarding whether successful in gaining control of the vessel or not; or

(d) attempts to overcome the ship's self protection measures by the use of:
- ladders
- grappling hooks
- weapons deliberately used against or at the vessel.

1.3 Suspicious Activity

.1 Action taken by another craft may be deemed suspicious if any of the following occur (the list is not exhaustive and should be treated as guidance):

(a) a definite course alternation towards the craft associated with a rapid increase in speed, by the suspected craft, which cannot be accounted for a normal activity in the circumstances prevailing in the area;

(b) small craft sailing on the same course and speed for an uncommon period and distance, not in keeping with normal fishing or other circumstances prevailing in the area;

(c) sudden changes in course toward the vessel and aggressive behavior.

.2 In helping to evaluate suspicious activity, the following may be of assistance to determine the nature of a suspect vessel:

(a) the number of crew on board relative to its size;

(b) the Closest Point of Approach (CPA);

(c) the existence of unusual and non-fishing equipment (e.g., ladders, climbing hooks or large amounts of fuel onboard;

(d) if the craft is armed in excess of the level commonly experienced in the area;

(e) if weapons are fired in the air.

1.4 High Risk Areas

.1 "High Risk Areas" are "areas of the ocean where attacks of terrorism, piracy or armed robbery have taken place." An area defined as High Risk may change over time due to changes in tactics and areas of operations of the perpetrators. Therefore, it is imperative that owners, operators and Masters assess areas of risk based on the latest available information.

(a) **Somalia, the North West Indian Ocean and GoA:** The High Risk Area contained in the BMPs Guidelines is defined as an area bounded by Suez to the North, 10°S and 78°E. While to date, attacks have not been reported to the extreme East of this area, they have taken place at almost 70°E. There remains the possibility that piracy attacks will take place even further to the East of the High Risk Area. Attacks have occurred to the extreme South of the High Risk Area. A high state of readiness and vigilance should be maintained even to the South of the Southerly limit of the High Risk Area and the latest advice from the Maritime Security Centre Horn of Africa (MSCHOA) on the extent of pirate activity always sought.

(b) **Strait of Hormuz:** The Strait of Hormuz is considered a High Risk Area by the Administrator. It is highly recommended that all ships transiting the Strait of Hormuz exercise the highest level of vigilance and caution, particularly during night transits with increased monitoring of small vessel and boat activity. Ship Masters that observe suspicious activity in the area and around their vessel are advised to make as early an assessment of a threat as possible. See section 5.8, below.

(c) **Waters Near Yemen:** A piracy operating area has been established in the southern end of the Red Sea. In addition, information suggests that al-Qaida remains interested in maritime attacks in the Bab-al-Mandeb Strait, Red Sea and the GoA along the coast of Yemen. It should be noted that for reasons of customary international law, it is not possible for international military forces (non-Yemeni) to be able to protect ships that are attacked inside Yemeni Territorial Waters (12 miles).

(d) **Indian Ocean:** Recent attacks indicate that pirates are moving towards the eastern part of the Indian Ocean approaching closer to Indian west and south coast, Lakshadweep/Minicoy Islands, northern Maldives. There are indications that pirates will attempt to operate as far south as the Mozambique Channel and 15°S latitude. Vessels sailing in the western, central, eastern and northern parts of the Indian Ocean should maintain strict antipiracy measures.

(e) **Other Areas:** Areas other than those mentioned above remain a concern. The International Maritime Bureau has reported an increase in attacks at Chittagong in Bangladesh and in the South China Sea. In addition, "serious security incidents" continue to threaten shipping off Nigeria, including near the border with Cameroon. Increases in maritime criminal

incidents (armed theft) have been noted off the Pacific Coast of Latin America, particularly at the Peruvian port of Callao.

1.5 Internationally Recommended Transit Corridor (IRTC)

.1 IMO SN.1/Circ.281 provides the details of the IRTC in the GoA. This corridor includes the creation of separate eastbound and westbound transit lanes. Each lane is 5 nm wide and is separated by a 2 nm buffer zone. The IRTC eastbound lane begins at 045° E between 11° 48'.00 N and 11°53'.00 N. The lane is oriented along a straight line course of 072° and terminates at 053° E between 14°18'.00 N and 14°23'.00 N. The IRTC westbound lane begins at 053° between 14°25'.00 N and 14°30'.00 N. The lane is oriented along a straight line course of 252° and terminates at 045° E between 11°55'.00 N and 12°00'.00 N.

.2 This IRTC is subject to change by military authorities according to prevailing circumstances. Shipowners, ship operators and Masters are urged to obtain up-to-date information from the MSCHOA website or NAV-warnings promulgated for that area.

2.0 Typical Pirate Attacks

2.1 Commonly, two (2) or more small, high-speed (up to 25 knots) open boats/skiffs are used in attacks, often approaching from the starboard or port quarter and/or stern but will also attack from ahead. Pirates appear to favor trying to board ships from the port quarter.

2.2 Attackers also have been known to try to blend in with local fishing boats, lie in wait in the IRTC or to disguise themselves as Coastguard, naval personnel, or pilots in order to board the ship. When a target ship nears, the attackers' boats will break cover and approach the ship to allow the attackers to board the ship.

2.3 The use of a pirate "mother ship" (which is a larger ship carrying personnel, equipment, supplies and smaller assault craft) has enabled the attacks to be successfully undertaken at a greater range from the shore. Pirates are also using larger long range attack craft to attack at much greater distances from the Somali Coast.

2.4 Pirates are opportunistic. Ships travelling at slow speeds, especially if combined with a low freeboard, are more vulnerable to attack.

2.5 Pirates often utilize small craft and attempt to match the speed of the ship on a parallel or following course. Once alongside, one or more armed pirates climb onboard. Pirates frequently use long lightweight ladders or grappling irons hooked to the ship's rail to climb up the sides of the vessel being attacked. Once onboard the pirate (or pirates) will generally make their way to the bridge to take control of the vessel. Once on the bridge the pirate/pirates will demand that the ship slows/stops to enable further pirates to board.

2.6 Attacks have taken place at most times of the day. However, many pirate attacks have taken place early in the morning, at first light. Attacks have occurred at night, but this is less common. Vigilance should be taken at all times, but particularly at first and last light.

2.7 It is not uncommon for pirates to use small arms fire and Rocket Propelled Grenades (RPGs) in an effort to intimidate Masters of ships to reduce speed and stop to allow the pirates to board. In what are difficult circumstances, it is very important to maintain Full Sea Speed, increasing speed where possible, and using careful maneuvering to resist the attack.

2.8 The majority of attempted hijacks have been repelled by ship's crew who have planned and trained in advance of the passage and employed passive countermeasures to good effect.

3.0 Implementing BMPs

3.1 Master's Discretion

While recognizing the absolute discretion of the Master at all times to adopt appropriate measures to avoid, deter or delay piracy attacks in this region, the recommended BMPs provide suggested planning and operational measures for shipowners, ship operators, Masters and their crews**.**

3.2 Liaison with Naval Forces – Passage Plan

.1 The essential part of the BMPs that applies to all ships transiting the GoA and off the Coast of Somalia is liaison with naval forces. This is to ensure that naval forces are aware of the sea passage that a ship is about to embark upon and how vulnerable that ship is to pirate attack. This information is essential to enable the naval forces to best use the assets available to them. The three (3) key naval organizations to contact (see Appendix I for contact details) are:

- MSCHOA;
- UKMTO; and
- MARLO.

.2 Ships navigating within the Red Sea (Suez) and area bound by 22° N, 78° E and 10° S are required to submit an advanced notice of passage plan to the naval authorities so that they can identify vulnerabilities and plan suitable protection. This can be done by either the Master or ship operator and is achieved primarily by making an:

- Initial report to UKMTO (email or fax);
- Initial report to MARLO (email or fax); and
- Four (4) to five (5) days prior to entering the IRTC, registering the vessel movement with MSCHOA (See section 4.1, below).

.3 Once ships have commenced passage of this High Risk Area, it is important that they continue to update the naval forces on progress.

.4 Relying on naval forces alone cannot adequately protect against piracy. Shipowners and ship operators also must employ self-protective measures and train their crews.

3.3 Risk Assessment and Factors to Consider

.1 Any decision to navigate in areas where the vessel's security may be threatened requires careful consideration and detailed planning to best ensure the safety of the vessel and crew. Prior to transiting a High Risk Area, the owner and Master should carry out their own risk assessment to assess the likelihood and consequences of piracy attacks, armed attacks, hijackings or terrorism on the ship, based on the latest available information. Owners are highly recommended to utilize the Automated Voyage Risk Assessment (AVRA) services being offered by BIMCO which will generate an ISPS Code compliant specific threat assessment for the individual ship concerned. The outcome of this risk assessment should identify measures for prevention, mitigation and recovery and will mean combining statutory requirements with supplementary measures to combat piracy. Not all BMPs may be applicable for each ship. Therefore, as part of the risk analysis, an assessment is recommended to determine which BMPs will be most suitable for the ship.

.2 Factors to be considered in the risk assessment should include, but are not limited to:

(a) Crew and Passenger Safety: The primary consideration should be to ensure the safety of the crew and passengers. Care should be taken, when formulating measures to prevent illegal boarding and external access to the accommodation, that crew members will not be trapped inside and should be able to escape in the event of another type of emergency, such as for example, fire.

(b) Freeboard: It is likely that pirates will try to board the ship being attacked at the lowest point above the waterline, making it easier for them to climb onboard. These points are often on either quarter. Experience suggests that vessels with a minimum freeboard that is greater than eight (8) meters have a much greater chance of successfully escaping a piracy attempt than those with less. A large freeboard will provide little or no protection, if the construction of the ship provides assistance to pirates seeking to climb onboard.

(c) Speed: One (1) of the most effective ways to defeat a pirate attack is by using speed to try to outrun the attackers and/or make it difficult to board. To date, there have been no reported attacks where pirates have boarded a ship that has been proceeding at over 18 knots. It is possible however that pirate tactics and techniques may develop to enable them to board faster moving ships. Ships are recommended to proceed at Full Sea Speed in the High Risk Area. If a vessel is part of a Group Transit (GT) within the IRTC, speed may be required to be adjusted. It is important to note that even vessels of low speed have successfully evaded attack by not stopping under threat.

- In the GoA, ships capable of proceeding in excess of 18 knots are strongly recommended to do so. Within the remainder of the High Risk Area ships are reminded that speed is extremely important in

avoiding or deterring a pirate attack. It is recommended that reference should be made to the MSCHOA website for the latest threat guidance regarding attack speed capability.

(d) Sea State: Weather continues to be a primary factor determining when pirates will operate. Pirates mount their attacks from very small craft, even where they are supported by larger vessels or "mother ships," which tends to limit their operations to moderate sea states. While no statistics exist, it is likely to be more difficult to operate these small craft effectively in Sea State 3 and above.

(e) Pirate Activity: The risk of a piracy attack appears to increase immediately following the release of a hijacked vessel and/or following a period of poor weather when pirates have been unable to operate.

4.0 Company Planning and Crisis Management Procedures

4.1 Company Planning

.1 Four (4) to five (5) days before the vessel enters the IRTC it is essential that the ship, managers and/or the operations department ensure that a "Vessel Movement Registration" submission has been logged with MSCHOA (online, email or fax) (http://www.mschoa.org) for each transit between the following coordinates:

GoA:
Point A: 11°50' N 045°00' E; and
Point B: 14°28' N 053°00' E; or

The Indian Ocean bounded by the African Coast: 12° N, 60° E, 10° S.

Vessels due to transit both areas must submit a registration for the GoA leg and a separate registration for the Indian Ocean leg.

User ID and Password are required which may be applied for through the website.

.2 On entering the UKMTO Voluntary Reporting Area (VRA), an area bounded by Suez to the North, 10° S and 78° E, ensure that a UKMTO "Vessel Position Reporting Form" is sent (this can be done by either the ship or ship operator).

.3 Review the Ship Security Assessment and implementation of the SSP as required by the ISPS Code to counter the piracy threat. Companies should have procedures in place to act upon receipt of a ship-to-shore security alert, including notification of the Administrator.

4.2 Crisis Management

.1 Company crisis management procedures should consider appropriate measures to meet the threat of piracy by adopting IMO and other industry recommended practices as appropriate to the particular circumstances and ship type.

.2 The Company Security Officer (CSO) is encouraged to see that a contingency plan for the high risk passage is in place for passage through the High Risk Area(s), exercised, briefed and discussed with the Master and the Ship Security Officer (SSO)

.3 Be aware of any specific threats within the High Risk Area(s) that have been promulgated (by for example Navigation Warning on SAT C, alerts on the MSCHOA website (www.mschoa.org), IMB, ReCAAP or MI Marine Safety Advisories.

.4 Offer the ship's Master guidance with regard to the recommended routing through the High Risk Area(s) and available methods of transiting the IRTC (e.g., GT or national convoy where these exist). Reference should be made to the MSCHOA website for the latest routing guidance and naval escorted convoys.

.5 Conduct crew training sessions and drills prior to transits and debriefing sessions post transits.

.6 The provision of carefully planned and installed Self Protection Measures (SPM) to harden the ship prior to transiting the High Risk Area is very strongly recommended. The use of SPM significantly increases the prospects of a ship resisting a pirate attack (see section 7.0 below).

.7 Consider additional resources to enhance watch keeping numbers.

4.3 Use of Armed Guards

The use of additional private security guards is at the discretion of the Company. Although MI legislation or regulations do not prohibit this activity, the use of armed guards is not recommended due to legal implications. UNCGPCS Working Group 1 has noted the clear statement from the military operations that they do not condone use of armed private military/security companies operating without appropriate co-ordination, control and legal authority. Should a company seek to use armed guards, this decision should not be made without first conducting a thorough risk analysis in cooperation with the vessel's insurance underwriters, charterers and legal counsel.

5.0 Master's Planning

5.1 On entering the UKMTO VRA—an area bounded by Suez to the North, 10°S and 78°E- ensure that a UKMTO Vessel Position Reporting Form is sent (this can be done by either ship or ship operator). Thereafter, vessels should report their position, course and speed daily. Throughout the UKMTO VRA vessels should implement self-protective measures as contained in this Notice.

5.2 Upon receiving the vessel's initial report, UKMTO will reply giving specific threat guidance relevant at the time. Experience has shown that to transit West of 60° E or within 600 nm of the Somali Coast significantly increases the risk of pirate attacks, although attacks have and will occur East of this area.

5.3 Ensure that a "Vessel Movement Registration" submission has been logged with MSCHOA four (4) to five (5) days before entering the following coordinates:

- Point A: 11°50' N 045°00' E; and
- Point B: 14°28' N 053°00' E; or
- The Indian Ocean bounded by the African Coast: 12° N, 60° E, 10° S.

NOTE again: This can be done by either the ship or the Company via online, email or fax. If it is completed by the Company, Masters should satisfy themselves with their companies that their details are correctly registered with MSCHOA.

5.4 Prior to entry into the High Risk Area it is recommended that the crew should be briefed on the preparations and a drill conducted prior to arrival in the area. The plan should be reviewed and all personnel briefed on their duties, including familiarity with the alarm signal signifying a piracy attack, and all clear and the appropriate response to each.

5.5 Masters are advised to also prepare an emergency communication plan, to include all essential emergency contact numbers and pre-prepared messages, which should be ready at hand or permanently displayed near the communications panel (e.g., telephone numbers of UKMTO, MSCHOA, MARLO, IMB Piracy Reporting Centre (PRC), CSO, etc.).

5.6 Define the ship's AIS policy: SOLAS permits the Master the discretion to switch off AIS if he believes that its use increases the ship's vulnerability. However, in order to provide naval forces with tracking information within the GoA it is recommended that AIS transmission is left on, but is restricted to ship's identity, position, course, speed, navigational status and safety related information. Outside the GoA, in other parts of the High Risk Area, the decision on AIS policy is again left to the Master's discretion, but current naval advice is to turn it off completely. This should be verified with MSCHOA.

5.7 If the AIS is switched off it should be activated at the time of an attack. It will be very difficult for responding naval forces to find and identify the ship without it.

5.8 When transiting the Straits of Hormuz, as soon as the Master feels that the threat is developing, he/she should immediately call to report hostile or potentially hostile action to: COMUSNAVCENT Battlewatch Captain and UKMTO. Such reports may also be relayed to MARLO. See Appendix 1 for contact information.

6.0 Prior to Transit – Voyage Planning

6.1 Position Reporting

.1 Masters having registered their ship with MSCHOA should report (noon position, course, speed, and estimated and actual arrival times) to UKMTO and MARLO three (3) to four (4) days before entering the GoA or passing the Coast of Somalia. The reporting scheme covers the Suez area, Red Sea, Indian Ocean North of 10° S and West of 78° E as well as the Arabian Gulf. The UKMTO Vessel Position Reporting Form should be used to make the report.

.2 Vessels are encouraged to increase the frequency of such reports to hourly intervals when within six (6) hours of entering or navigating within the IRTC.

.3 Ships may initially report to the UKMTO team on passing the following reference points:

- Suez for ships entering or leaving the region via the Red Sea;
- 10° S for ships entering or leaving the region via the Indian Ocean (South); and
- 78º E for ships entering or leaving the region via the Indian Ocean (East).

See Anti-Piracy Planning Chart Q6099 (Appendix IV of this Notice).

.4 The initial report should contain the following:

- Ship Name
- Call Sign
- Flag
- IMO Number
- Maritime Mobile Service Identity
- Inmarsat telephone number including satellite prefix
- Email address, Telex and Fax number
- Ship Management Company
- Type of Ship
- Current position and speed
- Itinerary in the region with route way points and destination port(s)

.5 Ships should continue to report their noon positions and speed, actual departure times and estimated arrival times at ports and destination when outbound from the defined area using UTC. The preferred method of communication is email to ukmto@eim.ae. When sending such emails, please copy investigations@register-iri.com, and IMBKL@icc-ccs.org, as well. The UKMTO may also be reached by Phone: +971-50-552-3215 or +971-50-552-6007; Fax: +971-4-306-5710; and Telex: (51) 210473.

.6 As an additional precautionary measure, Masters of vessels are advised to provide passage information to MARLO 48 hours prior to transiting through the GoA via email to marlo.bahrain@me.navy.mil, or telephone +973-1785-1395.

.7 It is very important to understand that naval forces cannot be prepared to assist if they are unaware of the ship's presence and location in the High Risk Areas.

6.2 Inside the GoA

.1 It is strongly recommended that ships conduct their passage within the IRTC, where naval forces are concentrated.

.2 Westbound ships should navigate to the Northern portion of the corridor, and Eastbound ships should navigate in the Southern part of the IRTC.

.3 Naval forces, coordinated by MSCHOA, operate the GT scheme within the IRTC. This scheme groups vessels together by speed for maximum protection for their transit through the IRTC. Further guidance on the GT scheme, including the departure timings for the different groups, are included on the MSCHOA website or can be obtained by fax from MSCHOA. Use of the GT scheme is recommended. Masters should note that warships might not be within visual range of the ships in the GT, but this does not lessen the protection afforded by the scheme.

.4 Ships may be asked to make adjustments to passage plans to confirm to MSCHOA routing advice. Ships joining a GT should:

- carefully time their arrival to avoid a slow speed approach to the forming up point (Point A or B);
- avoid waiting at the forming up point (Point A or B); and
- note that ships are particularly vulnerable to a pirate attack if they slowly approach or wait at the forming up points (Points A and B).

.5 Ships should avoid entering Yemeni Territorial Waters (YTW) (12 miles) while on transit. This is for reasons of customary international law, as it is not possible for international military forces (non-Yemeni) to be able to protect ships that are attacked inside YTW.

.6 During GTs, ships should not expect to be permanently in the company of a warship. But all warships in the GoA, whether part of EU NAVFOR or coordinating with them, will be aware of the GoA GTs and will have access to the full details of vulnerable shipping.

.7 MSCHOA strongly recommends Masters make every effort to plan transit periods of highest risk areas of the GoA for night passage (MSCHOA will advise ships). Very few successful attacks have occurred at night.

6.3 Outside the GoA

.1 Great care should be taken in voyage planning in the High Risk Area outside the GoA given that pirate attacks are taking place at extreme range from the Somali Coast. It is recommended that all vessels not making scheduled calls to ports in Somalia, Kenya or Tanzania keep as far from the Somali Coast as possible. Ships transiting South and East of the Coast of Somalia to ports outside of East Africa should consider navigating to the East of Madagascar or (for guidance) maintain a distance of more than 600 nm from the coastline and when routing North/South consider keeping East of 60° E Longitude until East of the Seychelles. It is important to obtain the latest information from MSCHOA before planning and executing a voyage. Details can be obtained from the MSCHOA website or by fax.

.2 Masters should still update UKMTO in the usual manner with their ship course and details using the UKMTO Vessel Position Reporting Form.

7.0 Prior to Transit – Self Protection Measures

7.1 General

The guidance within this section primarily focuses on preparations that might be within the capability of the ship's crew, using equipment that will normally be readily available. The guidance is based on experience of piracy attacks to date and may require amendment over time if the pirates change their methods. Owners of vessels that make frequent transits through High Risk Areas may consider making further alterations to the vessel and/or provide additional equipment, and/or manpower as a means of further reducing the risk of piracy attack.

.1 Check that self protection measures put in place in advance remain securely fitted and function as intended, being mindful that temporary devices may work loose and consequently may only provide a reduced level of protection.

.2 See Appendix II, Bridge Checklist, as an example of self-protection measures that can be taken to avoid danger.

7.2 Watchkeeping and Enhanced Vigilance

.1 95% of all ships attacked and hijacked have been those where the ship's staff was not alert in their lookout regime. Therefore, prior to commencing transit of a High Risk Area, it is recommended that preparations are made to support the requirement for increased vigilance. Consideration should be given to:

- increasing lookouts/bridge manning, taking into account the vessel's minimum safe manning certificate and rest hour requirements, to ensure additional lookouts for each Watch; additional lookouts should be fully briefed;
- manning the engine room;
- ensuring that there are sufficient binoculars for the enhanced bridge team;
- use of night vision optics, if available;
- mounting a yacht or I-band radar on the stern to detect small craft approaching, particularly for anchored vessel; and/or
- the use of dummies at the rails to simulate additional lookouts, however, if ship design creates lookout black spots and the security assessment identifies this risk then it may have to be covered by manpower.

7.3 Closed Circuit Television (CCTV)

.1 Once an attack is underway and pirates are firing weaponry at the vessel, it is difficult and dangerous to observe whether the pirates have managed to gain access. The use of CCTV coverage allows a degree of monitoring of the progress of the attack from a less exposed position. Recorded CCTV footage also may provide useful evidence after an attack. Consider:

- the use of CCTV cameras, if fitted, to ensure coverage of vulnerable areas, particularly the poop deck;

- positioning CCTV monitors at the rear of the bridge in a protected position; and
- locating CCTV monitors at the Safe Muster Point/Citadel (see section 7.13 below).

.2 If CCTV systems are utilized, proper procedures must be in place for maintenance, including documentation of repairs.

7.4 Maneuvering

Where navigationally safe to do so, Masters are encouraged to practice maneuvering their ships 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. The Master and Officers of the Watch should be familiar with the impact of these zigzag maneuvers onboard their particular ship in all sea conditions.

7.5 Alarms

.1 Sounding the ship's alarm/whistle serves to inform the vessel's crew that a piracy attack has commenced and, importantly, demonstrates to any potential attacker that the ship is aware of the attack and is reacting to it. It is important to ensure that:

- the Piracy Alarm is distinctive to avoid confusion with other alarms, potentially leading to the crew mustering at the wrong location outside the accommodation;
- crew members are familiar with each alarm, including the signal warning of an attack and an all clear, and the appropriate response to it; and
- exercises are carried out prior to entering a High Risk Area.

7.6 Upper Deck Lighting

.1 It is recommended that the following lights are available and tested:

- weather deck lighting around the accommodation block and rear facing lighting on the poop deck, consistent with Rule 20(b) of the International Regulations for the Preventing Collision of Sea; and
- search lights for immediate use when required.

.2 Navigation lights should not be switched off at night. It is recommended that ships proceed with just their navigation lights illuminated and the lighting described above extinguished to avoid leading other ships to assume the ship is at anchor).

.3 .Once pirates have been identified or an attack commences, illuminating the lighting described above demonstrates to the pirates that they have been observed.

.4 The Administrator recommends procurement of high altitude white rocket parachute flares for use in illuminating the local vicinity as well.

7.7 Deny Use of Ship's Tools and Equipment

.1 Pirates generally board vessels with little in the way of equipment other than personal weaponry. It is important to try to deny pirates the use of ship's tools or equipment that may be used to gain entry into the superstructure of the vessel. Tools and equipment that may be of use to the pirates should be stored in a secure location.

.2 Check all ladders and outboard equipment are stowed or up on deck.

7.8 Protection of Equipment Stored on the Upper Deck

.1 Small arms and other weaponry are often directed at the vessel and are particularly concentrated on the bridge, accommodation section and poop deck.

.2 Consider providing protection, in the form of sandbags or Kevlar blankets, to gas bottles (i.e. oxyacetylene) or containers of flammable liquids that must be stored in these locations.

.3 Land excess gas bottles or flammable materials prior to transit.

7.9 Control of Access to Accommodation and Machinery Spaces

.1 It is very important to control access routes to deter or delay pirates who have managed to board a vessel and are trying to enter accommodation or machinery spaces. Secure and control access to bridge, engine room, steering gear room, and crew quarters.

.2 All potential access points (doors, hatches, portholes, vents, etc.) should be risk-assessed and adequately secured, especially where the potential access point is considered large enough for an attacker to gain entry.

.3 All doors and hatches providing access to the accommodation and machinery spaces should be secured to prevent them being opened by pirates gaining access to the upper deck of the vessel. Access to and from the accommodation and internal work spaces should be reduced to a single point of entry when transiting the High Risk Area.

.4 It is recommended that once doors and hatches are secured, a designated and limited number are used for routine access when required, as controlled by the Officer of the Watch (OOW).

.5 Where doors and hatches are required to be closed for watertight integrity, ensure all clips are fully dogged down in addition to any locks.

.6 Check that all outdoor equipment is stowed or up on the deck. This includes blocking or lifting external ladders on the accommodation block to prevent their use and to restrict external access to the bridge.

.7 Any measures employed should not obstruct an emergency EXIT from within the internal space, while remaining secure from access by pirates outside. Where the door or hatch is located on an escape route from a manned compartment, it is

essential that it can be opened by a seafarer trying to effect an exit by that route. Where the door or hatch is locked it is essential that a key is available, in a clear position by the door or hatch.

7.10 Enhanced Bridge Protection

.1 The bridge is usually the focus of the attack. In the initial part of the attack, pirates direct weapons fire at the bridge to try to coerce the ship to stop. Once onboard the vessel they usually try to make for the bridge to enable them to take control. Consider:

- providing Kevlar jackets and helmets to the bridge team for enhanced protection during an attack (if possible, jackets and helmets should be in a non-military color);
- while most bridge windows are laminated, further protection against flying glass can be provided by the application of security glass film;
- fabricated metal (steel/aluminum) plates for the side and rear bridge windows and the bridge wing door windows, which may be rapidly secured in place in the event of an attack; and
- the after part of both bridge wings (often open) can be protected by a wall of sandbags.

7.11 Physical Barriers

Pirates typically use ladders and grappling hooks with rope attached to board vessels underway, so physical barriers should be used to make this difficult. Before constructing any physical barriers, it is recommended that a survey is conducted to identify areas vulnerable to pirates trying to gain access. Such barriers should not materially impede access to life saving equipment.

.1 Razor Wire

- A robust razor wire barrier is particularly effective if constructed outboard of, or overhanging, the ship's structure so as to make it difficult for pirates to hook on their boarding ladder (or grappling hook) to the ship's structure.
- Razor wire (also known as barbed tape) creates an effective barrier when carefully deployed. The barbs on the wire are designed to have piercing and gripping action. Care should be taken when selecting appropriate razor wire as the quality (wire gauge and frequency of barbs) and type will vary considerably. Lower quality razor wire is likely to be less effective.
- Three main types of razor wire are commonly available: unclipped (straight strand), spiral (like a telephone cord) and concertina (linked spirals). Concertina razor wire is recommended as the linked spirals make it the most effective barrier.
- Razor wire should be constructed of high tensile wire, which is difficult to cut with hand tools. Concertina razor wire coil diameters of approximately 730 mm or 980 mm are recommended.
- It is important that the razor wire is properly secured and it is recommended that clips or wire tires are used every 50 cm, alternating between the upper and lower strands. Try not to leave gaps in the razor wire coverage as there

are likely to be exploited by pirates. A double roll of Concertina razor wire provides a very effective barrier.

- When deploying razor wire, personal protective equipment to protect hands, arms and faces must be used. Moving razor wire using wire hooks (like meat hooks) rather than by gloved hand reduces the risk of injury. It is recommended that razor wire is provided in shorter sections (e.g. 10 meter section) as it is significantly easier and safer to use than larger sections which can be very heavy and unwieldy.

.2 "Anti-Climb" Paint

Coating gunwales and other potentially vulnerable structures with 'anti-climb' paint may also be considered.

.3 Electrified Barriers

Electrified barriers are not recommended for hydrocarbon carrying vessels, but following a safety assessment can be appropriate and effective for some other types of vessels.

.4 Warning Signs

It is recommended that warning signs of the electrified fence or barrier are displayed-inward facing in English/language of the crew, outward facing in Somali.

The use of such outward facing warning signs might also be considered even if no part of the barrier is actually electrified.

See below for an example of a warning sign.

Example of a warning sign in Somali, which states –
DANGER HIGH VOLTAGE ELECTRIC BARRIER

7.12 Water Spray and Foam Monitors

.1 The use of water spray and/or foam monitors has been found to be effective in deterring or delaying pirates attempting to board a vessel. The use of water can make it difficult for a pirate skiff to remain alongside and makes it significantly more difficult for a pirate to try to climb onboard.

.2 Manual operation of hoses and foam monitors is not recommended as this is likely to place the operator in a particularly exposed position.

.3 It is recommended that:

- Hoses and foam monitors (delivering water) should be fixed in position to cover likely pirate access routes. Some ships have used spray rails using a GRP (Glass Reinforced Plastic) water main, with spray nozzles to produce a water curtain to cover larger areas.
- Heated water is used to deter pirates as it has been found to be very effective in deterring attacks.
- Once rigged and fixed in position that hoses and foam monitors are in a ready state (pressurized and ready for discharge), requiring just the remote activation of fire pumps to commence delivery of water.
- Actual foam supply not be used (unless an additional quantity for the specific purpose is carried) as this will be depleted relatively quickly and will leave the vessel exposed in the event that the foam supply is required for firefighting purposes.
- The water and foam monitor spray achieved by the equipment be observed, once fixed in position, to ensure effective coverage of vulnerable areas.
- Baffle plates fixed a short distance in front of the nozzle be used to improve water coverage.
- A water curtain be created around the vessel to further deter boarding.

7.13 Safe Muster Point

.1 A safe muster point is a designated area chosen to provide maximum physical protection to the crew. In the event of a pirate attack, those members of the crew not required on the bridge or machinery control room (MCR) will muster here. A Safe Muster Point is a short-term safe haven.

.2 The Administrator recommends that a safe mustering location be designated and mustering procedures rehearsed in order to delay access to control of the ship and to buy time. Ideally this should be away from external bulkheads and portholes. Strategy for placement of a safe muster point also should include due consideration of fire protection systems aboard the vessel.

7.14 Citadel Guidelines

.1 A Citadel is a designated pre-planned area purpose-built into the ship where, in the event of imminent boarding by pirates, all crew will seek protection. A Citadel is to provide longer term protection of the crew as compared to a safe muster point.

.2 Due to the ongoing debate on the use of Citadels and their method of employment, CSOs and Masters are advised to check regularly with UKMTO for proper guidance in its establishment and use. Notwithstanding, recent incidents have shown Citadels to be a useful delaying tactic and means of mitigating the risk of being hijacked.

.3 A Citadel must be designed and constructed to resist a determined pirate trying to gain entry. Such a space would probably have, but not be limited to, its own ventilation and self-contained air-conditioning, toilet facilities, emergency rations, water supply, medical supplies, essential firefighting equipment, protective gear, good external communications (VHF is not considered sufficient), remotely operated CCTV cameras, emergency shut-down capability for the main and auxiliary engines and control of steering.

.4 New ships should be designed with security and safety in mind, particularly if contemplating transits through High Risk Areas. During the design and construction process, consideration should be given as how best to ensure that the accommodation block and decks can be locked down while still meeting all relevant SOLAS requirements, including those for fire protection and means of escape. Owners/operators should contact the Administrator for more specific guidance.

.5 If a Citadel is utilized, clear and comprehensive procedures on its use should be written into the SSP. These procedures should address rules for exiting the Citadel in cases where the pirates are employing weapons, particularly in anger.

.6 Irrespective of the latest guidance, it should be remembered that the whole concept of a Citadel approach is lost if any crew member is left outside before it is secured.

7.15 Crew Training and Drills

.1 Proper awareness and security training for crew members is essential and one (1) of the best self-protective measures available. Owners and operators are encouraged to provide training and drills to their crews – from the most junior levels up to Masters-on how to respond to an attack.

7.16 Other Measures

.1 Consider minimizing external communications (radios, handsets and AIS information) to essential safety and security related communication and SOLAS information only, during transit of the GoA and passing the Coast of Somalia.

.2 Increase readiness and redundancy by running additional auxiliary machinery, including generators and steering motors.

.3 If the ship has a comparatively low freeboard, consider the possibility of extending the width of the gunwales to prevent grappling hooks from gaining hold. Check the MSCHOA website for examples of such measures.

8.0 In Transit – Operations

8.1 Ship's crew should not be exposed to undue risk when employing Self Protective Measures (SPMs).

8.2 All ships inside the GoA are strongly urged to use the IRTC and follow MSCHOA GT advice and timings as promulgated on the MSCHOA website.

8.3 If you intend to follow a GT through the IRTC: Transit at the GT speed but remain aware of the ship's limitations. (Current advice, for example, is that if your maximum speed is 16 knots, consider joining a 14 knot GT and keep those 2 knots in reserve.)

8.4 If you do not intend to follow a GT through the IRTC: Maintain full sea speed through the High Risk Area. (Current advice is that if the maximum speed of the ship is more than 18 knots, then do not slow down for a GT, maintain speed and aim to transit as much of the High Risk Area in darkness as possible).

8.5 Maintain maximum CPA with any ship acting suspiciously.

8.6 Ships should continue to report their noon positions and speed, actual departure times and estimated arrival times during transit using UTC.

8.7 Ships should comply with the International Rules for Prevention of Collision at Sea at all times; navigation lights should not be turned off at night. Masters should endeavor not to impede the safe navigation of other vessels when joining and leaving the IRTC.

8.8 Provide deck lighting only as required for safety. Lighting in the shadow zones around the ship's hull may extend the area of visibility for lookouts, but only where consistent with safe navigation. Where fitted, and deemed suitable, consider the immediate use of "remotely operated" ship search lights. If suspicious activity around the vessel is observed, the use of search lights may startle and deter a potential attack. Current naval advice is to transit with navigation lights only.

8.9 Keep photographs of pirate "mother ships" on the bridge. Immediately report all sightings of suspect mother ships to UKMTO and the IMB PRC at:

UKMTO: +971 505 523 215 / ukmto@eim.ae

IMB PRC: +60 3 2031 0014 / imbkl@icc-ccs.org or piracy@icc-ccs.org

Such reports may also be relayed to MSCHOA or MARLO using the following contact details:

MSCHOA: postmaster@mschoa.org

MARLO: +973 39401395 / marlo.bahrain@me.navy.mil

Such reporting will aid in building a clearer picture of pirate activity which will assist in better protecting shipping and eradicate the threat to freedom of navigation in the area. (See Appendix III of this Notice for an MI Report of Piracy and Armed Robbery Against Ships (MI-109-2) form for forwarding such information or any other information concerning an attack or sighting.)

8.10 The Master should try to make as early an assessment of a threat as possible. As soon as the Master feels that a threat is developing he should immediately activate the SSAS and call the UKMTO.

8.11 Keep a good lookout for suspicious craft, especially from astern. Note that most attacks to date have occurred from the port quarter.

8.12 Protect the crew from exposure to undue risk. Only essential work on deck should occur in transit of the high risk area. Masters should, in so far as possible, keep crew members clear from external deck spaces during hours of darkness, while being mindful of their obligation to maintain a full and proper lookout in all directions at all times.

8.13 Use light, alarm bells and crew activity to alert suspected pirates that they have been detected.

8.14 A variety of other additional commercially available non-lethal defensive measures are available that could be considered; however, these should be assessed by companies on their merits and on the particular characteristics of the ship concerned.

9.0 If a Pirate Attack is Imminent

9.1 Follow the ship's pre-prepared contingency plan.

9.2 Activate the SSAS, which will alert your CSO and the Flag Administrator.

9.3 Activate the Emergency Communication Plan/Call in order of priority:

.1 UKMTO (+971 50 552 3215)

.2 MSCHOA (+44(0) 1923 958545)

.3 MARLO (+973 3940 1395)

.4 IMB (+60 3 2098 5763)

9.4 If the Master has exercised the right to turn off the AIS during transit of the piracy area, this should be turned on once the ship comes under pirate attack.

9.5 Sound emergency alarm and make a "Pirate Attack" (PA) announcement in accordance with the ship's emergency plan.

9.6 Make "Mayday" call on VHF Ch. 16 (and backup Ch. 08, which is monitored by naval ships). Send a distress message via the Digital Selective Calling (DSC) system and Inmarsat-C, as applicable. Establish telephone communication with UKMTO.

9.7 Prevent skiffs from closing in on the ship by altering course and increasing speed where possible. Pirates have great difficulty boarding a ship that is:

.1 Making way at over 18 knots.

.2 Maneuvering - it is recommended that, as early as possible, Masters undertake continuous small zigzag maneuvers to further deter boarding whilst maintaining speed. Consider increasing the pirates' exposure to wind/waves and using bow

wave and stern wash to restrict pirate craft coming alongside. (Masters and the OOW should be fully familiar with the handling and maneuvering characteristics of the vessel and should not wait until attacked to practice their evasive maneuvering techniques.) Particular attention should be given to the effects of varying helm orders and the impact these can have on the ship's speed.

.3 Activate water and spray (e.g., fire pump) and other appropriate defensive measures.

9.8 All crew who are not involved in counter-piracy operations should be mustered, either at their designated Safe Muster Point, or the Citadel if the ship is appropriately constructed.

9. 9 Consider turning on forward facing deck lights to draw attention to your vessel and aid positive identification by arriving military forces as a vessel under attack.

9.10 Maximize ship speed. Evidence to date from failed attacks is that the pirates will give up if unable to board within 30 to 45 minutes. If you can buy time until the military forces can arrive, this often leads the pirates to abort their attack.

10.0 If Boarded by Pirates

10.1 Before pirates gain access to the bridge, inform UKMTO and, if time permits, the Company.

10.2 Provided the ship has not been ordered by the perpetrators to maintain radio silence, contact should immediately be made with the Port State Marine Police on Channel 7 or Channel 12, or other appropriate means to port State authorities and/or with ships in the vicinity and shore authorities by sending a piracy/armed robbery attack message through INMARSAT or on an available DSC distress and safety frequency. Consider utilizing methods contained in MSC/Circ. 805, Guidance for the Use of Radio Signals by Ships Under Attack or Threat of Attack from Pirates or Armed Robbers (reference (h) of this Notice) to make the perpetrators aware that they have been detected.

10.3 Offer no resistance to the pirates once they reach the bridge. Once on the bridge the pirates are likely to be highly agitated; so remaining clam and cooperating fully will greatly reduce the risk of harm.

10.4 If the bridge/engine room is to be evacuated, then the main engine should be stopped, all way taken off the vessel, if possible, and the ship navigated clear of other ships. All remaining crew members should proceed to the designated Safe Muster Point with their hands visible and on their heads.

10.5 Ensure all crew, other than bridge team, stay together in one (1) safe mustering location.

10.6 If the ship is constructed with a Citadel and the Ship's Security Plan (SSP) involves the evacuation of all persons to the Citadel, ensure that the main engine is stopped, the vessel has adequate sea room to drift and the Citadel space is properly secured.

10.7 Leave any CCTV running.

10.8 Use emergency communication methods to communicate with authorities.

10.9 When a ship is ordered by the perpetrators not to make any form of transmission informing shore authorities of the attack, and complying with recommendations 10.7 and 10.8, above, may result in physical violence or death to the crew, it is recommended that any such order should be complied with as they may carry equipment capable of detecting all radio signals, including satellite communications.

10.10 If in a locked down mode in the safe mustering location or Citadel, ensure internal protection/cover is available in case the pirates attempt to force entry. Keep clear of entry point/doors and portholes/windows. Do not resist entry.

10.11 DO NOT use firearms, even if available.

10.12 DO NOT make any sudden movements around pirates.

10.13 DO NOT use flash photography.

10.14 DO NOT use flares of other pyrotechnics as weapons.

11.0 In the Event of Military Action

11.1 In the event that military personnel take action onboard the ship, all personnel should keep low to the deck, cover their head with both hands (always ensuring that hands are visible and not holding anything) and make no sudden movements unless directed to by friendly forces.

11.2 Military Forces may initially secure all persons encountered and question their identity. This is standard practice. Brief and prepare ship's personnel to expect this and to cooperate fully during the initial stages of military action onboard.

11.3 Do not use flash photography.

11.4 Be aware that English is not the working language of all naval units in the region. This is why early registration with MSCHOA, use of GT timings, and updating your position with UKMTO are essential. They all provide a better probability that naval support will be nearby and ready to respond immediately if the pirates attack.

12.0 Post-Incident Reporting

12.1 Following any piracy attack or suspicious activity, it is vital that a detailed report of the event is reported to MSCHOA, UKMTO, IMB and the Administrator.

12.2 This will ensure full analysis and trends in piracy activity are established as well as enabling assessment of piracy techniques or changes in tactics, in addition to ensuring appropriate warnings can be issued to the merchant shipping in the vicinity.

12.3 Masters are therefore requested to complete the piracy report form contained in Appendix III of this Notice. The report form can be used for submissions to the international organizations (e.g., MSCHOA, UKMTO, MARLO, IMB, IMO) as well as to the Administrator.

13.0 Post-Piracy Care for Seafarers

Adherence to BMPs and the presence of naval escorts in High Risk Areas have been shown to reduce the risks of pirate attacks. In spite of these precautions, pirates remain unpredictably capable of attacking and hijacking vessels, placing crew members in harm's way. The Seaman's Church Institute has published guidelines for addressing the needs of the crew and their families should a ship be attacked. These guidelines (reference (j) of this Notice) are provided for informational purposes in Appendix V of this Notice.

APPENDIX I

CONTACT LIST OF MILITARY AND OTHER AUTHORITIES

The following authorities have roles in combating piracy and other attacks against merchant shipping.

1.0 MSCHOA

1.1 MSCHOA is the planning and coordination authority for EU Forces in the GoA and the area off the Coast of Somalia. A Ship and its passage plan should be registered with MSCHOA at http://www.mschoa.org prior to each transit of the Internationally Recommended Transit Corridor (IRTC), the Somali Basin or the Western Indian Ocean.

1.2 MSCHOA may be reached directly at:

+44 (0) 1923 958545 (telephone)
+44 (0) 1923 958520 (fax)
postmaster@mschoa.org (email)

2.0 UKMTO

2.1 UKMTO is the first point of contact for ships in the region. UKMTO administers a Voluntary Reporting Scheme, under which merchant ships are encouraged to send regular updates on their position and intended movements. As such, UKMTO provides the day-to-day interface between Masters and the military by talking to the ships and liaising directly with MSCHOA and the naval commanders at sea. UKMTO uses the emerging and relevant information from the commercial sector to help the naval units maintain an accurate picture of shipping, thereby improving responsiveness to any incident. It is also a material source of information on the establishment and use of citadels.

2.2 The preferred method of communication with UKMTO for routine reporting is email to ukmto@eim.ae; Fax: +971-4-306-5710; or Telex: (51) 210473.

2.3 In case of emergency, the UKMTO may be reached by the 24-hour Duty Phone:

+971-50-552-3215

3.0 MARLO Information Exchange

3.1 MARLO operates as a conduit for information exchange between the Combined Maritime Forces (CMF) and the commercial shipping community within the region.

3.2 Passage information should be provided to MARLO 48 hours prior to transiting through the GoA via email to marlo.bahrain@me.navy.mil, telephone +973-1785-3925, or cell +973-1785-1395.

3.3 In case of emergency, the MARLO may be reached by the 24-hour Duty Phone:

+973-3940-1395

4. NATO Shipping Centre (NSC)

NSC provides the commercial link with NATO's Maritime Forces. The NSC is NATO's primary point of contact with the maritime community and is used by NATO as the tool for communicating and coordinating initiatives and efforts with other military entities (e.g., UKMTO, MSCHOA and MARLO) as well as directly with the maritime community.

Telephone: +44(0) 1923 956574
Fax: +44(0) 1923 956575
Email: info@shipping.nato.int
Website: www.shipping.nato.int

5.0 IMB

5.1 IMB is a specialized division of the International Chamber of Commerce (ICC) whose principal area of expertise is in the suppression of piracy through its PRC in Kuala Lumpur, Malaysia. It maintains a 24/7 watch system reporting pirate attacks in this area to the CMF and issuing warnings about hotspots. It also offers valuable advice as to what to do when pirates actually succeed in getting aboard.

5.2 It is recommended that Masters of vessels transiting the GoA include the IMB PRC as part of the reporting procedures by email to imbkl@icc-ccs.org.

5.3 In case of emergency, the IMB may be reached by the 24/7 Helpline Number: +60-3-2031-0014 or by the 24/7 Help Email: piracy@icc-ccs.org.

5.4 Other useful IMB contact points are:

IMB PRC website: www.icc-ccs.org
Fax: +60 3 2078 5769
Telex: MA34199 IMBPCI.

6.0 COMUSNAVCENT Battlewatch Captain

When transiting the Strait of Hormuz, as soon as the Master feels that the threat is developing, he/she should immediately call to report hostile or potentially hostile action to:

COMUSNAVCENT Battlewatch Captain at +973-1785-3879.

7.0 ReCAAP Information Sharing Centre

Tel: +65 6376 3091
Fax: +65 6376 3066
Website: www.recaap.org
Email: secretariat@recaap.org

8.0 Marshall Islands Duty Officer

Tel: +1-703-476-3762
Email: dutyofficer@register-iri.com

APPENDIX II

BRIDGE CHECKLIST

Vessel owners and operators, Master and crew should limit and avoid danger by taking these additional measures:

- ☐ Transit the GoA by way of the Internationally Recommended Transit Corridor (IRTC).
- ☐ Maintain a minimum distance of 60° E Longitude from the East Coast of Somalia.
- ☐ Avoid sailing between Socotra and Somalia and through the Mozambique Channel.
- ☐ Maintain high alert and be on the lookout for small craft in the Strait of Hormuz.
- ☐ Maintain at least 50 nm radius around Socotra.
- ☐ Establish special operating procedures for vigilance and for the event of an attack.
- ☐ Practice piracy drills, provide refresher training for the crew concerning anti-piracy measures.
- ☐ Ensure crew radios and in-vessel communications are in good working order.
- ☐ Secure a pre-designated safe mustering point for crewmembers to gather.
- ☐ Secure alternative steering location, if possible.
- ☐ Maintain a single point of entry into the house.
- ☐ Secure deck lighting (except for mandatory navigation lights).
- ☐ Maintain contact numbers for MARLO and UKMTO in the wheelhouse.
- ☐ Increase monitoring of VHF communications on Channel 16 (back-up Channel 08).
- ☐ Keep unnecessary communications to a minimum except to make contact with naval units and other vessels as soon as the vessel enters the High Risk Area.
- ☐ Continue the use of AIS but limit information to Vessel Name and Maritime Mobile Service Identity (MMSI) so that it may still be identified by coalition forces. Coalition Maritime Forces have AIS monitoring capability.
- ☐ All available radars should be used and constantly monitored.
- ☐ Post additional 24-hour lookouts forward, amidships and aft.
- ☐ Maintain a 24-hour watch by crew for suspicious activity, including a sharp lookout for suspicious small boats operating in the vicinity.
- ☐ Increase and maintain speed to at least 15 kts. The faster the better.
- ☐ Maneuver to avoid small craft and take aggressive evasive measures, if necessary.
- ☐ Take defensive precautions prior to entering the area including rigging fire hoses, spotlights, concertina wire, etc. Experience has demonstrated the use of high pressure fire hoses to be very effective at repelling boarders.
- ☐ Consider other non-lethal measures such as focused sonic devices, guard dog security teams, etc.

APPENDIX III

MI-109-2, REPORT OF PIRACY AND ARMED ROBBERY AGAINST SHIPS

Phone: +1-703-620-4880 Fax: +1-703-476-8522 Email: investigations@register-iri.com dutyofficer@register-iri.com	**OFFICE OF THE MARITIME ADMINISTRATOR** **REPUBLIC OF THE MARSHALL ISLANDS** **11495 Commerce Park Drive** **Reston, Virginia 20191-1506 USA**	THIS SPACE FOR OFFICIAL USE ONLY

REPORT OF PIRACY AND ARMED ROBBERY AGAINST SHIPS

INSTRUCTIONS

1. This form is to be completed to report incidents of piracy, armed attacks, hijacking or terrorism.
2. An original of this form shall be submitted to the Maritime Administrator as soon after the occurrence of the incident (attempted or actual).
3. This form must be completed in full. Entries which do not relate to a particular case should be indicated as not applicable by inserting the initials "N/A."
4. This form should be completed by the Master or person in charge, or, if neither is available, by the owner or his duly authorized agent.
5. Attach separate form MI-109-1 to this report for each person injured, killed, or incapacitated in excess of 72 hours as a result of this incident.
6. Attach separate form MI-109 to this report for any damage or loss to/of vessel.

I. PARTICULARS OF VESSEL / OWNER / SHIPMANAGER

1. Name of Vessel	
2. Official Number	3. IMO Number
4. Gross Tonnage	5. Type of Vessel
6. Propulsion	7. Ship's Freeboard _____ ☐ meters / ☐ feet
8. Name of Owner	
9. Name, Address and Telephone of Managing Agent	
10. Cargo Details (Type/Quantity)	
11. Numbers of Crew and Nationality	

II. TIME OF DAY / VESSEL POSITION AND STATUS

12. Date of Incident	13. Time (UTC)	14. Period of Day ☐ Day ☐ Night ☐ Twilight

15. Visibility ☐ < 2 miles ☐ 2- 5 miles ☐ > 5 miles	16. Sea State/ Weather

17. Geographic Location of Vessel at Time of Incident

(a) Latitude (b) Longitude

(c) Geographical Name of Body of Water / Name of Port

(d) Last Port of Departure (e) Date of Departure

(f) Port to Which Bound (g) Date of Expected Arrival

18. Anchored (name of anchorage)

MARSEC Level

19. Berthed (name of facility)

MARSEC Level

20. Underway

(a) Ship Heading: deg. True

(b) Speed: knots

III. SHORE / PORT AUTHORITY CONTACT DETAILS

21. Reported to shore authorities

☐ No

☐ Yes If Yes, to whom:

22. Reported to Port Facility Security Officer ☐ No ☐ Yes If Yes, name and contact details

23. Action taken by shore or port authorities

24. Preferred communications with reporting ship

IV. INCIDENT DETAILS

25. Method used by perpetrators to stop or board vessel

26. Type of weapons used by perpetrators

27. Number of perpetrators involved and duration of attack, type of attack (attempted/boarded) and whether attack was aggressive/violent

28. Suspected or known identity and description of perpetrators (dress, physical appearance, language spoken, if known)

29. Injury or loss of life

☐ No ☐ Yes If yes, complete and attach form MI-109-1, Report of Personal Injury or Loss of Life.

30. Damage to, or loss of, vessel

☐ No ☐ Yes If yes, complete and attach form MI-109, Report of Vessel Casualty or Accident

31. Items stolen

Estimated replacement cost US $ _____

32. Details of incident, including consequences to the crew, even if there were no physical injuries (e.g., from which direction approached, craft and communication equipment used, last observed movements of perpetrators/suspect craft, area of ship being attacked, etc.) Attach separate sheet if necessary.

33. Action taken by crew

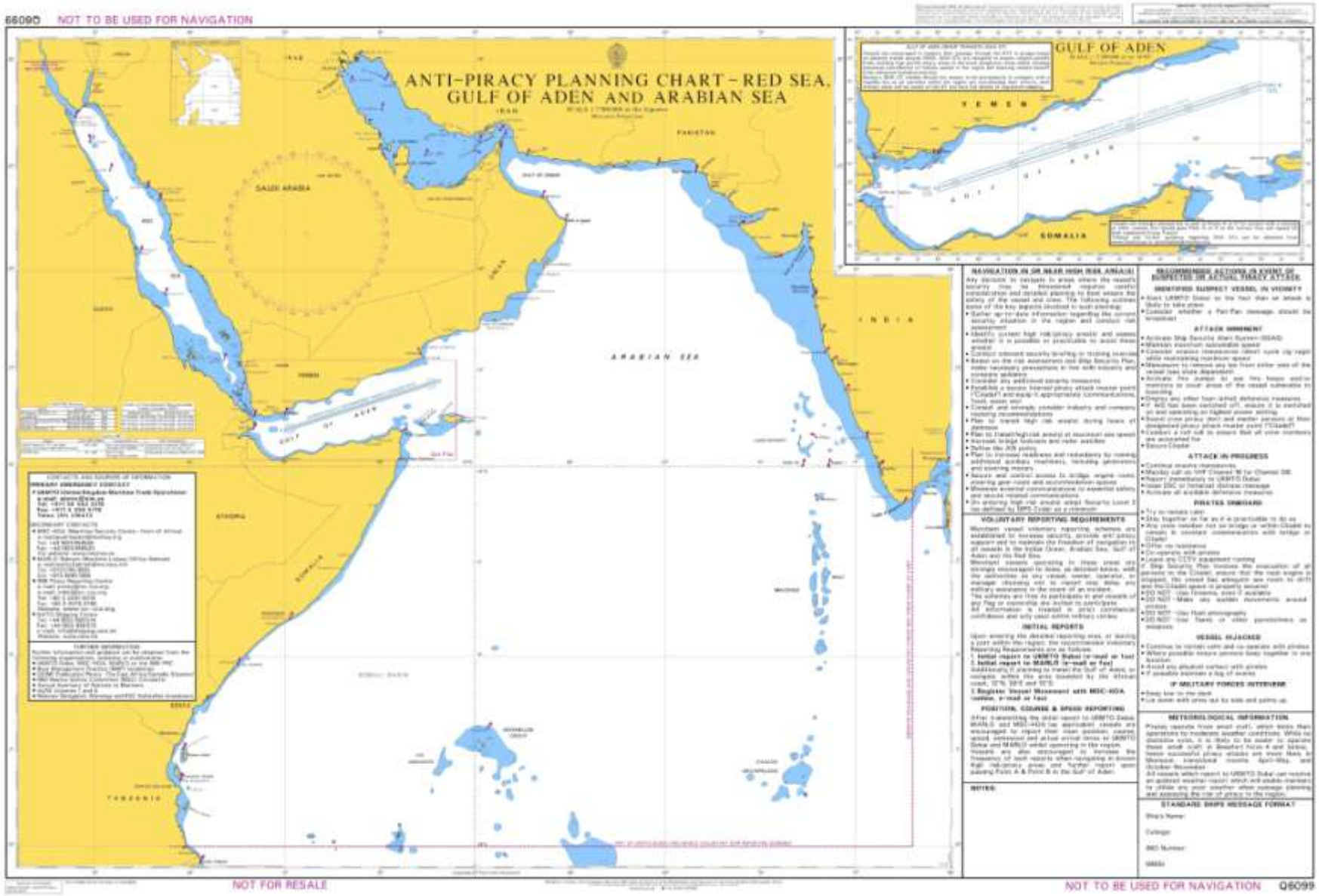
34. Recommended additions to SSP/new measures needed to prevent recurrence, i.e., set higher MARSEC level, additional lighting, etc.

V. REPORT

35. Date of Report	36. Submitted by (Print Name)
37. Signature	38. Title

APPENDIX IV

ANTI-PIRACY PLANNING CHART – RED SEA, GULF OF ADEN AND ARABIAN SEA



POST-PIRACY CARE FOR SEAFARERS

GUIDELINES

CENTER FOR SEAFARERS' RIGHTS
THE SEAMEN'S CHURCH INSTITUTE

SEP 16.2010
VERSION 2.0

PREAMBLE The following guidelines are intended to provide a general structure for caring for seafarers following a piracy incident. These guidelines are based on a study currently underway at the Seamen's Church Institute (SCI) and is a dynamic working document that is designed to develop more specific recommendations for assessment and intervention. SCI welcomes comments from interested parties in its ongoing efforts to develop specific guidelines to address the mental health impact of piracy on seafarer's. This document is not only relevant to cases where seafarers are captured by pirates, but also for all seafarers who traverse waterways where piracy presents even a remote threat.

1. ANTICIPATING THE POSSIBILITY OF PIRACY

Piracy is a threat facing 21st century seafarers. While most piracy incidents are thought to take place around the Horn of Africa, piracy remains problematic on the West Coast of Africa, the Indian Ocean and throughout the South East Asian archipelago. Although adherence to best management procedures and the presence of naval escorts in high risk areas have been shown to reduce the risks of pirate attacks, pirates remain unpredictably capable of attacking and hijacking vessels. Because of this, it is incumbent upon all maritime industry stakeholders to take preparatory steps to protect the wellbeing of their crews at sea.

1.1 THE MAINTENANCE OF ACCURATE MEDICAL INFORMATION It is important that shipowners maintain accurate health records for their crew. Complete medical records include the results of the most recent physical examination. A complete medical record should contain information that would help a stakeholder determine whether the seafarer has any medical condition that could worsen at sea. This includes any medication-dependent condition, as well as any physical ailment that could prove dangerous to the seafarer in a setting where stress increases. A detailed history should provide information about prior surgeries, immunizations, allergies, a complete family medical history, and a complete personal history, including information about prior illnesses, as well as major life events (marriages, divorces. deaths of loved ones). This information will prove helpful in helping a seafarer who is later found to be affected by an encounter with piracy, or in medical planning in anticipation of the release of a captive seafarer.

1.2 ANTICIPATORY TRAINING It is Important that seafarers develop appropriate Instincts and possess the skill-set necessary to contend with captivity. Some of this is accomplished through drills aboard the vessel that practice deterrence techniques. Seafarers should also be trained in basic survival skills, as well as being trained in how best to react to pirates. Cultural sensitivity training to avoid offending and angering the pirates should be included. Most importantly, seafarers should be aware of known intimidation tactics used by pirates, including providing frightening misinformation about family members, making suggestions that the ship owners will neglect them, and other psychological tactics aimed at breaking crew morale, increasing their desperation, and thus pressuring negotiations.

2. AT THE FIRST NEWS OF A PIRACY INCIDENT

The news of a piracy incident can be panic inducing for **all** involved. What is most important and most difficult is maintaining clear and reliable lines of communication between the vessel and its stakeholders and between stakeholders and the families of the crew. It is therefore most important to provide regular briefings from the first sign of a problem.

2.1 WORKING WITH CREWMEMBERS' FAMILIES Families should be notified of an incident within 24 hours to avoid their finding out first from news outlets. After the first contact, families should be updated by telephone, if possible, or by email at intervals no greater than 24 hours even if nothing has progressed. Shipowners should also prepare relatives for the possibility that pirates, as part of their intimidation tactics, will contact them. Families should be instructed to refrain from making statements to the press about the situation, as it should be explained to them that any publicity impedes effective negotiation and may prolong the captivity of their loved ones. Further; the seafarers' dependents should be reassured that they will receive payments from the shipowners according to contract provisions.

3. WHEN A CREW IS BEING HELD

When a vessel is in captivity by pirates, there is often little that can be done directly to address the needs of the crew. However: during this critical time when negotiations are underway, several procedures can begin.

3.1 PREPARING FOR THE CREW'S RELEASE It is important that each crewmember's needs be identified before release. This information should be solicited from the crewmembers medical records, as well as from family members. It is most important to discern whether the crewmember has a pre-existing condition that may be worsened under captivity. These may include:

- Conditions that require medication, which may run out during captivity
- Conditions that worsen under stress (While most medical and psychiatric conditions worsen under stress, here is a partial list of diagnoses of greater concern: cardiac problems, including histories of arrhythmias, heart attacks [myocardial infarctions]; stroke: asthma, emphysema, or chronic bronchitis; an anxiety disorder; post-traumatic stress disorder)

Anticipating possible reactions among crewmembers based on knowledge of their medical history will facilitate preparations for their release.

3.2 PROVIDING TIMELY INFORMATION TO THE CREW'S FAMILIES As stated above in 2.1, families should be updated on a daily basis. Families should be provided a single point-of-contact who is available to them by email and telephone. Much like the owners of hijacked vessels and others with vested interests, the families of crewmembers will most likely feel powerless and afraid. However; unlike those who may be involved in negotiating, families have no means to access current information. Allying with families is important, as they will play an integral role in assisting with any recovery that might be needed by providing supportive home environments, helping to identify psychological symptoms of captivity, and by helping link crewmembers with appropriate caregivers (medical centers. behavioral health clinics).

Families should be asked to maintain the confidentiality of all information shared with them (i.e. they should not disclose this information to the media). Families should also be encouraged to report any attempts by pirates to communicate with them, and they should be encouraged not to respond to these attempts.

3.3 ANTICIPATING THE SEAFARER'S POTENTIAL NEEDS While most seafarers will be protected by their resilience from any debilitating post-captivity side effects, ship operators should prepare for the possibility that a crewmember will need follow-up care. In the midst of a hostage situation, ship operators and insurance companies can identity qualified professionals in the seafarer's home community who can provide care, if needed. Contact information of available and properly trained and licensed medical doctors and mental health professionals (psychologists, psychiatrists. social workers, licensed counselors) should be maintained. These professionals could be placed in a state of readiness in anticipation of possible service. These services, when required, should be covered as part of the standard medical care offered to the seafarer.

4. WHEN RELEASE IS IMMINENT

4.1 PREPARATIONS SHOULD BE MADE TO INFORM FAMILIES immediately after their family members are released. Families should be encouraged to respect the confidentiality of negotiations and should be prepared for the possibility of modifications to any timetable provided. Preparations should be made for crewmembers to be provided with telephones as close to release as possible to talk with their loved ones.

4.2 A DEBRIEFING PROTOCOL should be established by this point that includes the appropriate company, military, and medical interviews. The purpose of a medical evaluation is to determine whether the seafarer is at risk of developing any persistent physical or emotional condition that would impede a crewmember's ability to return to work or that would pose a risk to life. An evaluation that conforms to established standards should be made (the M.I.N.I. is an example of a suitable measure of emotional functioning that could be used for this purpose). Evaluations should be performed by licensed medical doctors or allied health professionals (e.g., nurses), who are qualified to conduct assessments.

5. WHEN THE CREW HAS BEEN RELEASED

5.1 A MEDICAL ASSESSMENT SHOULD BE MADE AS SOON AS POSSIBLE. Ideally, this should precede any debriefing. The information that government/military personnel will receive from a detainee will be less accurate if made in the setting of significant medical or psychological distress. The assessment should be summarized in a written document, translated into the native language of the seafarer by a competent medical translator and then given to the crewmember to bring home to his local medical team.

A follow-up physical and psychological screening should be scheduled before the crew returns to duty. The results of this evaluation should be used to determine whether a seafarer could return to duty or whether treatment is needed. In a case where further treatment is needed, provisions should be made by the ship operator or other responsible party to provide appropriate treatment as part of the post-piracy medical care. The employer should be granted access to follow-up reports only with the seafarer's permission.

5.2 ONCE THE CREW HAS BEEN CLEARED TO TRAVEL, the crew should be repatriated as soon as possible. When crewmembers are unable to leave the point of disembarkation for a period of more than three (3) days, efforts should be made to facilitate family travel to that point to expedite reunification.

- Families should be briefed about the status of their family crewmember in a manner that is culturally appropriate.

- Families and crewmembers should be equipped with a list of symptoms of post-traumatic stress disorder and provided with the contact information of a professional who can provide therapy for any symptoms that occur.

6. WHEN THE CREW IS TO RETURN TO DUTY

6.1 CREW MEMBERS SHOULD BE CLEARED BEFORE RETURNING TO DUTY. Clearance includes a full physical examination, but should also include a psychological assessment.

It would benefit crewmembers and reduce liability to insurers to engage trained, licensed mental health professionals to conduct assessments. In areas of the world where psychologists and psychiatrists are not reasonably available, evaluations can be conducted by telephone or by Internet (several assessments have online forms that have been translated into many languages).

6.2 SYMPTOMS DO NOT ALWAYS OCCUR WITHIN THE PERIOD OF TIME IMMEDIATELY FOLLOWING A TRAUMATIC EVENT. Post-traumatic and other psychiatric symptoms can present themselves when an individual returns to a setting similar to the original incident. Seafarers should be trained to recognize warning signs of symptoms and should be furnished with the contact information of professionals who could be contacted privately if needed. Seafarers who are returning to duty following a piracy incident should be provided with contact information of a suitable person to reach in each expected port of call to reach in case symptoms return at sea

CONCLUDING REMARKS

As our research continues, the Center for Seafarers' Rights at SCI will update guidelines where appropriate. If you have any questions about this preliminary guide or are in need of consultation, refer to the contact information below.

CONTACT INFORMATION

E piracy@seamenschurch.org
T +1 212 349 9090 x240
F +1 212 349 8342
SKYPE drgarfinkle

Center for Seafarers' Rights
The Seamen's Church Institute
241 Water Street
New York, NY 10038-2016 USA

Citation information: Garfinkle, M. S. (2010). Preliminary Guidelines for Post-Piracy Care. Working paper, the Seamen's Church Institute, Center for Seafarers' Rights, New York, Version 2.0.

APPENDIX VI

BMPs SIGNATORIES AND UPDATING BMPs

1.0 BMPs Signatories

1.1 In an effort to counter piracy in the Gulf of Aden (GoA) and off the Coast of Somalia, the following international industry organizations, which represent the vast majority of shipowners and operators transiting the region, are signatories to the BMPs:

- Baltic and International Maritime Council (BIMCO)
- International Chamber of Shipping (ICS)
- International Group of Protection and Indemnity Clubs (IGP&I)
- International Maritime Bureau (IMB)
- International Association of Dry Cargo Ship Owners (INTERCARGO)
- International Association of Independent Tanker Owners (INTERTANKO)
- International Shipping Federation (ISF)
- International Transport Workers Federation (ITF)
- International Parcel Tankers Association (IPTA)
- Joint War Committee (JWC) and Joint Hull Committee (JHC)
- Oil Companies International Marine Forum (OCIMF)
- Society of International Gas Tanker and Terminal Operators (SIGTTO)

1.2 These BMPs are supported by:

- EU NAVFOR (The European Union Naval Force)
- Maritime Liaison Office (MARLO)
- Maritime Security Centre Horn of Africa (MSCHOA)
- Operation Ocean Shield
- NATO Shipping Center (NSC)
- UK Maritime Trade Operations (UKMTO)
- United Nations Contact Group on Piracy off the Coast of Somalia (UNCGPCS)
- Signatories to the New York Declaration

2.0 Updating BMPs

2.1 It is anticipated that these BMPs will be periodically updated based upon operational experience and lessons learned. This Notice incorporates revisions made in the 3rd edition of the BMPs.

2.2 BMPs should be read with reference to the Maritime Security Centre Horn of Africa (MSCHOA) website (www.mschoa.org), "Advice to Masters" section where additional relevant information (e.g., counter-piracy information, including areas of High Risk, coordinates of the Internationally Recommended Transit Corridor and transit speed for GoA GT) will always be posted and available for unrestricted download (PDF format).

2.3 The BMPs Guidelines also can be found on the "Piracy Alert" section of www.icc-ccs.org and on the "Home Page" of www.marisec.org.

2.4 The UK Maritime Operations piracy website (www.noonsite.com/General/Piracy) is another good source of counter-piracy information.

2.5 The National Geospatial Agency (NGA) is a United States Department of Defense combat support agency that maintains a website (http://www.nga.mil/portal/site/maritime) providing global maritime geospatial intelligence. Owners, operators and Masters are encouraged to take advantage of the information on the site which includes Anti-Shipping Activity Messages (locations and descriptive accounts of specific hostile acts), Office of Naval Intelligence (ONI) Worldwide Threat to Shipping Reports (summary of recent piracy acts and hostile actions), and Broadcast Warnings (persons in distress, or objects and events that pose an immediate hazard to navigation).

INDEX