SHIP SECURITY ADVISORY NO. 12-20

To: Owners/Operators, Masters, Company Security Officers, Recognized Security Organizations

Subject: PIRACY IN THE GULF OF GUINEA

Date: 22 December 2020

This Ship Security Advisory (SSA) supersedes SSA No. 10-20 and SSA No. 11-20.

The Republic of the Marshall Islands (RMI) Maritime Administrator (the “Administrator”) hereby draws attention to the recent surge in security incidents and kidnappings reported in the Gulf of Guinea region. Extreme vigilance and caution must be observed while operating in these waters.

According to Dryad Global (Channel 16), there have now been 27 kidnapping incidents and 138 total seafarers kidnapped in the Gulf of Guinea in 2020.

(Source: Risk Intelligence)

This SSA expires one (1) year after its issuance, unless otherwise noted, extended, superseded or revoked.
The Maritime Domain Awareness for Trade – Gulf of Guinea (MDAT-GoG) distributed the following warning on 17 December 2020:

MDAT-GOG has been informed of a HIGH-RISK maritime incident in the coming hours and days in the following AREA’S F/E/D. We highly recommend to the seafarer community and ships transiting in these areas to exercise a sharp look-out and apply BMP WA procedure. All queries regarding Warning Notice ring +33(0) 298 22 88 88 for further information.

Masters and Company Security Officers are advised to maintain Security Level 2 and a heightened state of vigilance within the MDAT-GoG Voluntary Reporting Area (VRA). Please review RMI Marine Guideline 2-11-14 along with Best Management Practices to Deter Piracy and Enhance Maritime Security off the Coast of West Africa including the Gulf of Guinea (BMP WA). This valuable guidance should always be considered whilst performing voyage risk assessments in the Gulf of Guinea.

In addition to following BMP-WA, please note the attached security guidance update and bridge cards recently issued by shipping industry associations for the Gulf of Guinea region.

Please submit any comments or security-related enquiries to shipsecurity@register-iri.com.
Increased Security Threats for vessels operating in the Gulf of Guinea.

21 October 2020

Reference:
A. BMP West Africa.
B. UKHO Security Chart Q6114/SHOM Chart 8801CSD.

As the dry season approaches and sea conditions abate, an increase in attacks has traditionally been seen, so maritime security risks to vessels operating in the Gulf of Guinea require renewed attention. Masters and crews need to be extra vigilant and ensure all security measures are taken.

To ensure the safety of all vessels and afford best protection to global trade it is vital:

- Comply with Flag State Requirements and Guidance.
- CSO’s and Masters apply the recommendations in BMP West Africa.
- The citadel is equipped with a Satellite telephone (BMP WA Page 22).
- Masters familiarise themselves with BMP WA Section 7 (Ships Under Attack).
- Masters register with MDAT-GOG when entering the West African VRA (Ref A & B) and if operating inside the VRA, report daily.
- Any significant changes to ETA’s should be reflected in Line 6 (Other important Info) of the Daily/Transit Position Report to MDAT-GOG (BMP WA Annex D).
- The AIS Policy is clearly defined (BMP WA Page 13). It should be noted the Nigerian Navy arrests any ship found to have switched off their AIS. A decision to switch off AIS should therefore be based on concerns over safety and/or security and recorded in the vessel’s logbook to inform subsequent legal proceedings.
- CSO’s ensure all contact numbers for MDAT-GOG are correct - watchkeepers@mdat-gog.org and Emergency Tel: +33(0) 298 22 88 88.
- Information is protected (BMP WA Page 11).
- In the event of any incident or being concerned, Masters should call MDAT-GOG immediately.
- If Voyage Plans permit, wait at distance offshore and transit at high speed to arrive at any rendezvous point ‘Just in Time’ including STS and/or Offshore Terminals.
- Attacks have previously occurred 200Nm from the coast and the past location of attacks should be considered. Whilst waiting offshore, engines must be ready for immediate manoeuvre.
- Some vessels tender a virtual Notice of Readiness (NOR) whilst staying safely offshore, both tendering a virtual NOR and waiting offshore are accepted practice for many vessels operating in the GoG (BMP WA Page 13).

CSO’s and masters should note, pirate gangs also attack in harbour and on loading installations. In addition to COVID 19 restrictions, crew should only leave the vessel if necessary, during their duties. Gangway staff should be briefed and instructed to keep a good look out for suspicious activity.

MDAT-GOG will share information of vessels being attacked with the navies operating in the region. Questions regarding information sharing can be directed to MDAT-GOG.

Useful BMP Contact details:

MDAT-GoG:
Email: watchkeepers@mdat-gog.org
Telephone (24hrs): +33 298 228888
Website: https://gog-mdat.org/home

Download additional sources of information:
BMP WA: Best Management Practices to Enhance Maritime Security for Vessels & Mariners Operating Off the Coast of West Africa including the Gulf of Guinea
BMP West Africa
Best Management Practices to Deter Piracy and Enhance Maritime Security off the Coast of West Africa including the Gulf of Guinea

BMP West Africa
Quick Reference Card Series

‘Q Card’ BMP West Africa – 1

INDEX
Card 2 REPORTING Card 6 UNDER ATTACK (APPROACH STAGE)
Card 3 THREAT Card 7 UNDER ATTACK (ATTACK STAGE)
Card 4 ASSESSMENT Card 8 SEV OPERATIONS
Card 5 PLANNING Card 9 EVIDENCE COLLECTION

* Note: wording of cards may differ slightly from BMP West Africa text.
Ships and their operators should submit vessel position reporting forms to MDAT-GoG.

MDAT-GoG acts as the primary point of contact for merchant ships and their CSOs, providing liaison with military forces in the region. MDAT-GoG administers the Voluntary Reporting Scheme, under which merchant ships are encouraged to send regular reports.

These include:

- Initial report (upon entering the VRA).
- Daily reports (update on ship’s position, course and speed).
- Final reports (upon departure from VRA or arrival in port).
- Reports of suspicious/irregular activity (when necessary).

MDAT-GoG can offer Masters and CSOs the opportunity to conduct drills and exercises to support their passage planning in the region.

Companies interested in this can make contact on a dedicated exercise line: +33 298 221302.

MDAT-GoG offers regular information to ships on its website https://gog-mdat.org/home and in a weekly report summarising the previous week’s activity.

Ships and their operators should submit vessel position reporting forms to MDAT-GoG.

MDAT-GoG
+33 298 228888

watchkeepers@mdat-gog.org
The likelihood of attack further offshore West Africa is higher during the inter-monsoon season (October-May).

Attacks can take place at any time – day or night. However, the risk of an Undetected Approach is Higher at Night. More seafarers have been kidnapped during the hours of darkness.

Attacks have been reported over 200Nm from the coast.

Attackers may use small arms fire during attacks; the bridge tends to be the main target for these weapons. Attackers may use long lightweight ladders, knotted climbing ropes or long hooked poles to climb up the side of the ship. Once onboard they will make their way to the bridge to try to take control of the ship. When on the bridge they will demand the ship slows/stops to enable others to board. They will also try by all means to gain access to the accommodation to capture crew members before completion of the citadel retreat process.

Experience has shown the crew of a vessel targeted for armed robbery at sea or cargo theft are likely to be treated badly by perpetrators during an attack. Injuries are common and any resistance shown to the attackers may lead to an escalation of violence.

Boarding risk will be higher if vessels are drifting, at anchor, conducting ship-to-ship (STS) operations or at slow speed. A vigilant watch is paramount in order to activate the vessels security procedures as early as possible. If because of the nature of the navigation or of the operations the citadel process is not possible in case of attack, then additional security measures should be considered (secured anchorage, security escort vessels). Attacks against vessels underway occasionally involve some form of deception to force the vessel to stop. Attacks on vessels vary significantly in their form.

Ships and their operators should submit vessel position reporting forms to MDAT-GoG.

MDAT-GoG
+33 298 228888

watchkeepers@mdat-gog.org
A threat is formed of capability, intent and opportunity.

The risk assessment MUST consider but may not be limited to:

- The threat assessment and geographical areas of increased risk.
- Requirements of the Flag State, company, charterers and insurers.
- Secure Anchorage Areas (SAA), Security Escort Vessels (SEV) and or Vessel Protection Detachments (VPDs).
- The ship’s characteristics, vulnerabilities and inherent capabilities, including citadel and/or safe muster points to withstand the threat (freeboard, speed, general arrangement, etc.).
- The ship’s and company’s procedures (drills, watch rosters, chain of command, decision making processes, etc.).
- Background factors shaping the situation, e.g. traffic patterns and local patterns of life, including fishing vessel activity.
- Cooperation with military.
‘Q Card’ BMP West Africa – 5

Ship Master’s Planning

Prior to entering the Voluntary Reporting Area:

- Obtain the latest threat information.
- Check the latest NAVAREA warnings, alerts and the Inmarsat SafetyNet broadcasts.
- Implement VRA vessel registration and reporting requirements as highlighted in section 6 and annex D of BMP West Africa.
- If security services are used, confirm arrangements with the Private Maritime Security Companies (PMSC).
- If used, rendezvous position and communication plan for Security Escort Vessels.
- Contingency plans if security services do not arrive or cannot meet operational requirements.
- Confirm propulsion can operate at full speed.
- Implement security measures in accordance with the Ship Security Plan (SSP).

Location and Time at Anchor

- Keep time at anchor to a minimum.
- Anchor watch to be maintained.
- Avoid setting patterns.
- Consider use of “secure anchorage areas” operated by some countries in the region. More information is contained in local Notice to Mariners or Admiralty Charts.
- Vessels are most at risk when stopped in the water, drifting, at anchor or carrying out STS transfer, Single Buoy Mooring (SBM) operations or slowing down for pilot transfer.

Coordinated Arrival

Many vessels wait offshore and transit at high speed to arrive at any rendezvous point ‘Just in Time’ including STS and/or Offshore Terminals. Some vessels tender a virtual Notice of Readiness (NOR) whilst staying safely offshore, and both are accepted practice for many vessels operating in the GoG.
### Ships Under Attack – Approach Stage

**A proper lookout is critical for the ship’s protection.**
It will ensure the detection of a suspicious approach or attack early on, which allows defences to be deployed.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sound the emergency alarm and make an attack announcement, in accordance with the ship’s emergency communication plan. Initiate emergency procedures.</td>
</tr>
<tr>
<td>Activate water spray.</td>
</tr>
<tr>
<td>Make a mayday call on VHF Ch. 16. Send a distress message via the Digital Selective Calling (DSC) system and Inmarsat-C, as applicable.</td>
</tr>
<tr>
<td>Activate the SSAS.</td>
</tr>
<tr>
<td>If not already at full speed, increase to maximum to open the distance.</td>
</tr>
<tr>
<td>Steer a straight course to achieve maximum speed quickly.</td>
</tr>
<tr>
<td>Activate the emergency communication plan.</td>
</tr>
</tbody>
</table>

**Report the attack immediately to MDAT-GoG by telephone +33 298 228888 and email watchkeepers@mdat-gog.org**

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure the AIS is switched on.</td>
</tr>
<tr>
<td>Ensure that all external doors and, where possible, internal public rooms and cabins are fully secured.</td>
</tr>
<tr>
<td>All crew not required on the bridge or in the engine room should muster at the safe muster point or citadel.</td>
</tr>
<tr>
<td>When sea and navigational conditions allow, consider altering course to increase an approaching skiff’s exposure to wind/waves.</td>
</tr>
<tr>
<td>Sound the ship’s whistle/foghorn continuously and put all deck lights on to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it.</td>
</tr>
<tr>
<td>Check Vessel Data Recorder (VDR) is recording and the data saved.</td>
</tr>
</tbody>
</table>
**ATTACK STAGE**

<table>
<thead>
<tr>
<th>Reconfirm all ship’s crew are in the safe muster point or citadel as instructed by the Master.</th>
</tr>
</thead>
</table>
| **Report the attack immediately to MDAT-GoG**  
**+33 298 228888 by telephone.** |
| As the attackers close in on the ship, Masters should commence small alterations of helm whilst maintaining speed to deter skiffs from lying alongside the ship in preparation for a boarding attempt. These manoeuvres will create additional wash to impede the operation of the skiffs. |
| Large amounts of helm are not recommended, as these are likely to significantly reduce a ship’s speed. |
| Security Escort Vessel if present, will conduct themselves as governed by their rules of engagement. |

**ACTIONS ON ILLEGAL BOARDING**

<table>
<thead>
<tr>
<th>Muster the crew in the citadel. Bridge Team to lock inner doors (leading to the lower decks) when on route to the citadel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use all available means to establish communications from the citadel with MDAT-GoG and company to confirm all crew are accounted for and in the citadel or safe muster point.</td>
</tr>
</tbody>
</table>
| Stay in the citadel until conditions force you to leave or as advised by the military or company.  
(If a military response is not available CCTV from the citadel may be used to assist in assessing the status of the vessel / location of attackers). |
| If any member of the crew is captured it should be considered that the attackers have full control of the ship. |
Companies should check the credentials and licences/permits of the PMSC.

BMP does not recommend or endorse the general use of SEVs to accompany merchant ships; this is a decision taken by individual ship operators.

The escort plan, RV position and communication arrangements should be agreed in advance.

Planning should consider that SEVs may have operating restrictions.

Regular communication should be maintained.

The SEV will be positioned to defend the vessel at all times and be reactive to intercept any approaching suspicious craft.

Authorisation to use force rests with the military detachment onboard the SEV.

The Master / Bridge Crew can aid the SEV with early detection and warning.

SEV should not enter any terminal or facility exclusion zone.

A contract for the provision of SEVs must:

- Not prejudice the ship’s insurance cover arrangements.
- Ensure the PMSC has insurance policies that are current and compliant with the requirements of the contract.
- Ensure the PMSC can legally operate the SEV in accordance with coastal state law.
- Ensure the SEV is fit for purpose.

MDAT-GoG
+33 298 228888
watchkeepers@mdat-gog.org
‘Q Card’ BMP West Africa – 9

Post Incident Protection of Evidence

The collection and protection of evidence is critical.

To give the investigating authorities the best chance of apprehending the perpetrators, it is important that evidence is preserved in the correct manner. Companies, Masters and crew should refer to IMO Guidelines on Preservation and Collection of Evidence A28/Res. 1091 and other industry guidance. The quality of the evidence provided and the availability of the crew to testify will significantly help any investigation or prosecution that follows.

The Master and crew can protect a crime scene until the nominated law enforcement agency arrives by following these basic principles:

- Preserve the crime scene and all evidence if possible.
- Avoid contaminating or interfering with all possible evidence – if in doubt, do not touch and leave items in place.
- Do not clean up the area, including hosing it down. Do not throw anything away, no matter how unimportant it may seem.
- Take initial statements from the crew.
- Take photographs of the crime scene from multiple viewpoints.
- Protect VDR for future evidence.
- Make a list of items taken (e.g. mobile phones with numbers).
- Facilitate access to the crime scene and relevant documentation for law enforcement authorities.
- Make crew available for interview by law enforcement authorities.

INTERPOL can also be consulted to discuss recommended practices for the preservation of evidence that could be useful to law enforcement agents pursuing an investigation.

Contact details are: os-ccc@interpol.int | +33 472 44 7676.