

Republic of the Marshall Islands

MARITIME ADMINISTRATOR

11495 COMMERCE PARK DRIVE, RESTON, VIRGINIA 20191-1506
TELEPHONE: +1-703-620-4880 FAX: +1-703-476-8522
EMAIL: shipsecurity@register-iri.com WEBSITE: www.register-iri.com

SHIP SECURITY ADVISORY No. 01-20

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

Subject: THREATS TO COMMERCIAL SHIPPING IN THE PERSIAN GULF, STRAIT OF HORMUZ, GULF OF OMAN, ARABIAN SEA, AND RED SEA

Date: 20 January 2020

- References:**
- **United States (US) Maritime Advisory #2020-001**, *Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea - Threats to US and International Shipping from Iran*
 - **[Shipping Industry Guidance](#)**, *Safety & Security and the use of Privately Contracted Armed Security Personnel (PCASP) in Arabian Gulf, Strait of Hormuz and Gulf of Oman*
 - **RMI Marine Guideline [2-11-16](#)**, *Maritime Cyber Risk Management*

Operators of Republic of the Marshall Islands (RMI) flagged vessels transiting the Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, and Red Sea are requested to circulate this Ship Security Advisory (SSA) to their ships by the most expeditious means possible. This SSA supersedes SSA No. 08-19.

Issue

Since May 2019, multiple attacks or acts of aggression against merchant ships have occurred in the Persian Gulf, Strait of Hormuz (SoH), Gulf of Oman, and Red Sea:

- 12 May 2019: Explosive charges placed on four commercial ships anchored off Fujairah.
- 13 June 2019: Two oil tankers attacked with explosives near the SoH.
- 05 July 2019: UK seizes Iranian supertanker off Gibraltar suspected of carrying oil to Syria.
- 11 July 2019: Three Iranian gunboats 'attempted to impede' British oil tanker in the SoH.
- 19 July 2019: Iran seizes a UK flagged tanker in retaliation.
- 14 September 2019: Attack on Kingdom of Saudi Arabia oil facilities.
- 07 November 2019: International Maritime Security Construct ([IMSC](#)) opens in Bahrain.
- 02 January 2020: US air strike kills Iran's Quds Force commander at Baghdad Airport.
- 07 January 2020: Iran attacks US military base in Iraq with missiles.

This SSA expires one (1) year after its issuance, unless otherwise noted, extended, superseded, or revoked.

Heightened military activity and increased political tensions in this region continue to pose serious threats to commercial vessels. Associated with these threats is a potential for miscalculation or misidentification that could lead to aggressive actions.

In response, the International Maritime Security Construct (IMSC) has been established to maintain freedom of navigation, international law, and free flow of commerce to support stability and security of the maritime commons in the Persian/Arabian Gulf, Strait of Hormuz, Gulf of Oman, and the Bab el Mandeb. The IMSC is currently supported by Albania, Australia, Bahrain, Kingdom of Saudi Arabia, United Arab Emirates, United Kingdom and United States. For further information and important guidance, please review the [IMSC brochure](#).

Vessels navigating these waters may also encounter GPS interference, bridge-to-bridge communications spoofing, and/or other communications jamming with little to no warning. In at least two incidents, vessels reported GPS interference. One vessel reportedly shut off its Automatic Identification System (AIS) before it was seized, complicating military response efforts. Vessels have also reported spoofed bridge-to-bridge communications from unknown entities falsely claiming to be US or [coalition](#) warships.

The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued Alert [AA20-006A](#) on 06 January 2020, regarding the potential for an Iranian cyber response. In part, the CISA alert notes "Iran's historic use of cyber offensive activities to retaliate against perceived harm", chronicles Iranian cyber activity, and provides recommended actions to mitigate vulnerabilities. Additional maritime cyber risk management information can be found in RMI Marine Guideline [2-11-16](#).

Risk Mitigation Measures

Shipowners and operators are advised to exercise a high level of vigilance at all times in this area. The RMI Maritime Administrator (the "Administrator") highly recommends vessels take precautions as described below when operating in the area:

- Implement security measures equivalent to **Ship Security Level 2** ([flag requirement](#)).
- Review Section 2 of *Best Management Practices 5th Edition* ([BMP5](#)).
- Undertake a new ship and voyage-specific threat assessment before entering any region where there has been an incident or if the threat has changed.
- After performing the risk assessment, review the Ship Security Plan and amend if necessary.
- Ensure ISPS access control measures are strictly in place.
- Ensure Automatic Identification System (AIS) and Long-Range Identification and Tracking (LRIT) systems are switched on and functional.

- Consider transiting at full speed whilst ensuring this is only done where it is commensurate with safe speed, safe navigation and maneuvering permits.
- Privately Contracted Armed Security Personnel (PCASP) should not be used as a risk mitigation measure in the northern Gulf of Oman, Strait of Hormuz or Persian Gulf. Consider the use of extra unarmed lookouts in addition to any contracted security the vessel may have hired for HRA transits, (note the northern part of the Gulf of Oman is not part of the [industry designated HRA](#) for piracy).
- Ensure watch officers save Voyage Data Recorder (VDR / SVDR) data in the event of an attack or suspicious event.
- Consider if a Day/Night transit is appropriate to the threat posed.
- Conduct Security Training/Exercises prior to entering areas of increased risk.
- Tankers in ballast condition should consider purging cargo tanks of hydrocarbons prior to entering the region to reduce the risk of explosion.
- Strictly observe any promulgated exclusion zones or guidance issued by coastal states.
- Consider implementing unmanned machinery spaces (UMS) through confined straits if navigationally safe to do so.
- Maintain a full and vigilant bridge watch. Place additional lookouts to the navigation team and bridge wings with a specific remit to maintain visual watch for small craft approaching.
- Ensure the lookouts are briefed on maintaining a clear watch astern and over the side.
- If a mine-related threat is announced during transit, move all crew to above the waterline.
- Maintain use of night vision binoculars and consider carrying more onboard.
- Maintain a strict communications watch and establish communication with all nearby vessels.
- Rig outboard lighting where possible, provided they do not interfere with keeping a safe lookout, particularly over the stern, and use searchlights if available.
- Monitor relevant VHF and other communication channels.
- Ensure water tight integrity whilst underway or at anchorage.
- Check all fire-fighting equipment is available for immediate use. Make sure the emergency fire pump is available if any maintenance is being undertaken.

- Vessels should follow the advice of coalition military authorities / CMF.
- Review [OCIMF's Ship Security: Hull Vulnerability Study](#).
- Review NATO ATP2: [NCAGS' Guide to Owners, Operators, Masters and Officers Edition A Version 1, Annex D to Chapter 4](#).

Visual check of the hull:

- Undertake a visual search from the deck, all around the vessel to check for anything attached to the hull of the vessel. Particular attention should be paid to the hull at the waterline.
- Crew conducting visual checks should wear appropriate PPE, protective head gear, safety harness and life jackets at all times.
- If a vessel detects anything unusual attached to the hull, it should contact United Kingdom Maritime Trade Operations (UKMTO), the US Fifth Fleet Battle Watch, and the Administrator immediately (see *Contact Info* section below). All crew should be evacuated from the immediate area and mustered in a safe place.

Additional measures for consideration whilst at anchor:

- Rotate the propeller continuously or at short, irregular intervals.
- Operate bow and stern thrusters at zero (0) thrust.
- Turn the rudder frequently.
- Switch the echo sounder to transmit counter/combat swimmer/diver threat.

Guidance

- The Maritime Global Security website at www.maritimeglobalsecurity.org offers industry issued best practices, including BMP5, and guidance to mariners by geographic region and provides contact and subscription information for regional maritime security reporting centers.
- Answer all VHF calls professionally. DO NOT IGNORE.
- All vessels should be aware that US and other coalition naval forces may conduct maritime awareness calls, queries, and approaches to ensure the safety of vessels transiting the Persian Gulf, Strait of Hormuz, Gulf of Oman, and Arabian Sea. If an RMI-flagged vessel suspects it is being hailed from a source falsely claiming to be a US or coalition naval vessel, UKMTO and the US Fifth Fleet Battle Watch should be immediately informed.

- If hailed by non-coalition forces, provide vessel name, flag state, and affirm that the vessel is proceeding in accordance with international law as reflected in the Law of the Sea Convention. The master should immediately inform UKMTO and the US Fifth Fleet Battle Watch. Please also refer to the [IMSC brochure](#) for additional guidance and suggested standard responses.
- If non-coalition forces seek to board an RMI-flagged vessel navigating these waters, the ship's Master should, if the safety of the ship and crew would not be compromised, decline permission to board, noting that the vessel is proceeding in accordance with international law, as reflected in the Law of the Sea Convention, and immediately inform UKMTO and the US Fifth Fleet Battle Watch.
- If non-coalition forces board an RMI-flagged vessel, the vessel should immediately contact UKMTO and the US Fifth Fleet Battle Watch. The crew should not forcibly resist the boarding party. Refraining from forcible resistance does not imply consent or agreement to that boarding.
- Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea ([BMP5](#)), and the [Maritime Global Security](#) website should be consulted prior to operating in the above listed geographic areas.

Reporting

RMI-flagged vessels operating in these areas are advised to report any incidents or suspicious activities to US or Coalition Naval Vessels on VHF Channel 16. In addition:

- For the Red Sea, Arabian Sea, the Gulf of Oman, and the Persian Gulf: Simultaneously register with both the United Kingdom Maritime Trade Office (UKMTO) and the US Naval Forces Central Command Naval Cooperation and Guidance for Shipping (NAVCENT NCAGS) Watch 24 hours prior to entering the Indian Ocean Voluntary Reporting Area by sending **UKMTO and NAVCENT NCAGS**, via a single e-mail, the Initial Report from Annex D of Best Management Practices to Deter Piracy and Enhance Maritime Safety in the Red Sea, Gulf of Aden, Indian Ocean and the Arabian Sea ([BMP5](#)). Utilize other reports included in Annex D of [BMP5](#) as necessary, including both UKMTO and NAVCENT NCAGS on each of these reports.
- Include the estimated times of arrival at the **Suez Canal, Bab el Mandeb Strait (BAM), and Strait of Hormuz (SoH)** in Line 10 of the report, and add a line 14 for comments as needed (e.g., speed restrictions or other constraints, anticipated time of entering/exiting the SoH Traffic Separation Scheme; an outline of the navigation plan for operating in the SoH and Persian Gulf, etc.).
- In the event of an incident or suspicious activity, call UKMTO or the US Fifth Fleet Battle Watch and activate the Ship Security Alert System (SSAS) immediately.

- Vessels operating in this area are advised to establish contact with both UKMTO and the NAVCENT NCAGS Watch, and to include both on all update or incident report emails, as detailed above. By including both as addressees on each email, awareness will be enhanced without creating an additional reporting burden.
- All security incidents and suspicious activities must be reported by RMI-flagged vessels to the Administrator.

Contact Information

- **NAVCENT NCAGS:** cusnc.ncags_bw@me.navy.mil
+973 1785 2983 or +973 1785 0084
- **UKMTO:** watchkeepers@ukmto.org
+44 (0) 2392 222060
UKMTO advisories and warnings www.ukmto.org
- **US Fifth Fleet Battle Watch:** +973 1785 3879
cusnc.bwc@me.navy.mil
- **RMI Maritime Administrator:** dutyofficer@register-iri.com
shipsecurity@register-iri.com
+1 571 441 1885

Supplemental information may also be found on the [RMI Maritime Security web page](#).