U.S. Department of Homeland Security
United States Coast Guard

International Port Security Program
U.S. Coast Guard

Date: May 22, 2009
Contact: LT James Fogle
(202) 372-1038

Port Security Advisory (2-09)

There are several areas in the world where acts of piracy and armed robbery against ships are prevalent. In May 2009, the Coast Guard published Maritime Security (MARSEC) Directive 104-6 (Rev. 2), *Guidelines for U.S. Vessels Operating in High Risk Waters*, providing direction to owners and operators of U.S. vessels to respond to emerging security threats. The MARSEC Directive applies to U.S. flagged vessels operating in certain areas determined to be high risk.

For foreign flag vessels to which MARSEC Directive 104-6 (Rev. 2) **does not apply**, the U. S. Coast Guard recommends that those vessels increase their security level while transiting or operating in areas where acts of piracy and armed robbery at sea are prevalent. The following security measures were directed to **U.S. Flagged Vessels** operating in high risk waters in MARSEC Directive 104-6 (Rev. 2) and **may be considered** by foreign flag vessels:

1. Vessel Security Plans (VSP) for vessels that operate in high risk waters must have security protocols for terrorism, piracy, and armed robbery against ships. The section of the VSP which pertains to terrorism, piracy, and armed robbery against ships should cover the need for enhanced deterrence, surveillance and detection equipment; crew responses if a potential attack is detected or is underway; and communication procedures including the use of the Ships Security Alert System (SSAS), coordination with anti-piracy organizations that could be of assistance, and information control of sensitive security information.

2. Vessels operating, anchored, or berthed in high risk waters shall implement measures equivalent to Maritime Security Level (MARSEC) Level 2. Whenever possible, ships should avoid routes that transit through areas where attacks are known to have taken place.

3. Pirates continue to adapt to piracy counter measures, moving their operations further offshore to find targets of opportunity. They frequently change their tactics to achieve success. Due to the dynamic nature of piracy, counter piracy measures in the MARSEC Directive will be reviewed annually, or more frequently as necessary, by the U.S. Coast Guard to validate security measures.

4. Security Officers are encouraged to review current information provided on websites maintained by the U.S. Office of Naval Intelligence (ONI), ICC Commercial Crime Services, Maritime Security Center-Horn of Africa (MSCHOA), the U.K. Maritime Trade Operations (UKMTO), the U.S. Maritime Liaison Officer (MARLO), the Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia (ReCAAP), and the U.S. Maritime Administration (MARAD) website. These reports will help Security Officers determine where recent incidents involving terrorism, piracy, and armed robbery against ships have occurred. These reports may be accessed at the following web sites:

http://www.nga.mil/portal/site/maritime(ONI)	http://www.icc-ccs.org (ICC) (IMB PRC)
http://www.mschoa.eu (MSC HOA)	http://www.rncom.mod.uk/templates/MaritimeOperations.cfm?id=902 (UKMTO)
http://www.cusnc.navy.mil/marlo/ (MARLO)	http://www.recaap.org/index_home.html (ReCAAP)
http://www.marad.dot.gov/news_room_landing_page/horn_of_africa_piracy/horn_of_africa_piracy.htm (MARAD)	

5. The Directive does not preclude the employment of increased security measures by vessel masters above and beyond those recommended or required herein for designated high risk waters or other waters if, in the master's best judgment, such measures are warranted.

6. To supplement MARSEC Level 2 requirements, the following additional security measures must be implemented to prevent and suppress acts of terrorism, piracy, and armed robbery against ships for vessels operating in high risk waters:

Prior to entering High Risk Waters

a. Conduct a vulnerability assessment on your vessel utilizing the most current intelligence and information available.
b. Vessel masters should contact and provide voyage plans to the appropriate regional liaisons in the region. When operating in regions with no liaisons, operators are encouraged to contact the nearest coastal state as advocated in the MSC/Circ.623/Rev.3.
c. Unless otherwise directed or advised by on-scene military forces, all ships navigating through the Gulf of Aden shall plan voyages using the International Recommended Transit Corridor (IRTC) and follow the Gulf of Aden Group Transits (GOA GT) if vessel speed ranges from 10 to 18 knots. Vessels that make less than 10 knots shall contact UKMTO for routing guidance. Information on IRTC and GOA GT can be found on the MSCHOA website.
d. Establish an anti-piracy plan commensurate to the threat level and vulnerability of the vessel that can be practiced and implemented by the crew. The anti-piracy plan should include:
    a. Hardening the vessel against intrusions.
    b. Non-lethal methods for repulsing intruders.
    c. Ship operations & maneuvers to evade attack.
    d. Communications Procedures: Internal protocol for internal shipboard communications & external communications before, during and after an incident.
    e. Protection of the crew.
    f. Procedures to take if the ship's security is compromised.
    g. Procedures for crew in hostage situations.
    h. Company policy/procedures for confronting intruders.
    i. Training program establishing frequency for drills and exercises.

e. Establish a "safe haven" or area in which crewmembers may take safe refuge prior to or during an attack is recommended. The safe haven should provide crew with survival essentials comparable to what is provided in a lifeboat, including means of external communications suitable for the space utilized.
f. Prepare crew by ensuring crew is well briefed, trained in anti-piracy procedures, and well rested.
g. For vessels with a freeboard less than 15 meters (49.2 feet), rig the vessel with equipment or products that will make scaling the ship difficult (soaps, foams, netting, barbed wire, electric fencing, etc.). Installation of this equipment may not interfere with access to or deployment of the vessel's primary lifesaving equipment (liferafts, lifeboats, etc.) or create an especially hazardous condition.
h. Reinforce or cover all side ports located below the main deck to prevent unauthorized access to the vessel.
i. Equip vessel with non-lethal means to disrupt, disorient, and deter boarders; e.g. loud acoustic devices, high energy light beams or other equipment to repulse attackers is recommended.
j. Outfit vessel with enhanced detection equipment (night vision devices, high beam search lights, cameras, etc.).

k. Modify access to the wheelhouse to prevent unauthorized access. Installation of devices that cannot be tampered with or destroyed by intruders from the outside should be considered.
l. Consider supplementing ship's crew with professional armed or unarmed security. If transiting the Horn of Africa region, all vessels shall supplement ship's crew with armed or unarmed security based on a piracy specific vessel threat assessment conducted by the operator.
m. For vessels intending to operate in the Gulf of Aden or Horn of Africa region, accelerate installation/certification of Long Range Identification & Tracking (LRIT) systems. Equipment shall be installed and operational prior to July 1, 2009.

<u>During transits of a High Risk Area</u>

a. Send position reports regularly (recommended at least every 6 hours) to the appropriate regional operation center.
b. Ensure regular reports are provided to the owner/operator.
c. Use of AIS is recommended at all times; information transmitted should be limited to the vessel name, position, course, speed, navigational status, and safety-related information.
d. Comply with International Rules of the Road for Prevention of Collision at Sea; navigation lights should NOT be turned off at night.
e. Maintain a vigilant anti-piracy watch and ensure all shipboard anti-piracy precautions are in force. Advance warning of a possible attack will give the opportunity to sound alarms, alert other ships and the coastal authorities, illuminate the suspect craft, undertake evasive maneuvering, or initiate other response procedures. Augment bridge watches as necessary to perform lookout duty, including lookouts astern and other locations on the vessel to cover radar blind spots.
f. If capable, maintain vessel speed 16 knots or greater. Faster is better.
g. If practical, join or establish a convoy of vessels.
h. Minimize external communications (radios, handsets) to essential safety and security related communication.
i. If you have supplemental security personnel, activate supplemental security team watches.
j. As soon as the master thinks a threat is developing, contact appropriate regional operation center or on-scene military forces. If no operation center is available, notify the owner/operator.
k. Ensure the engine room is manned with a licensed engineer. While in high risk areas, this includes manning of automated engine rooms.
l. Secure, control access, and regularly inspect restricted areas (bridge, engine room, steering gear room, and crew quarters). Securing doors providing access to, and egress from, secure or key areas may adversely impact safety in the event of an accident. In
1. any instance where there is a conflict between safety and security, the safety requirement should be paramount.
m. Ensure ladders and outboard equipment are stowed or on deck.
n. Fire pumps and fire hoses, or equivalent, shall be ready for discharge overboard. Water pressures of 80 psi and higher have been used to deter or repulse attackers. A number of spare hoses can be rigged, tied down, and/or pressurized to enable short notice use if a potential attack is detected.
o. Alarms/distress signals, including the ship's whistle, should be sounded in the approach of attackers to discourage them. Use of loud acoustic devices or other equipment to repulse attackers is recommended.
p. Avoid anchoring or drifting in high risk waters.
q. If a vessel is at anchor or in port of a high risk area, the provisions all deck lighting should be illuminated at night. Prior to leaving port, the ship should be thoroughly searched and all doors or access points secured or controlled.

r. Follow any guidance from on-scene military forces that have anti-piracy intelligence that may aid the master in avoiding or thwarting piratical attacks.

If attacked or boarded

a. Activate the Ship Security Alert System (SSAS).
b. Inform regional liaison or anti-piracy organization for the region and if time permits, vessel company.
c. Implement procedures established in the anti-piracy plan.
d. In the event that the AIS equipment has been turned off, re-activate AIS so that friendly forces can identify the vessel and position.
e. Unless directed otherwise, all crew, other than the bridge team, should stay together in a pre-planned location or locations.
f. Exercise information control to only essential personnel or agencies with a need to know. Information about vessel movements, capabilities, or the incident itself should be considered Sensitive Security Information and therefore should not be released to family, friends, or media. Email and phone use should be strictly monitored to ensure critical information isn't leaked to the public.
g. If possible, deny use of ship's communications equipment by pirates.
h. Provided that navigation safety allows, masters should consider using heavy wheel movements to "ride off" attacking craft as they approach. The effect of bow wave and wash may deter would-be attackers and make it difficult for them to attach poles or grappling irons to the ship. When performing these maneuvers, the ship should set a course into the prevailing seas and avoid creating a lee on the side of the vessel. Evasive maneuvers will reduce vessel speed giving an attacker an advantage, so use of this tactic is recommended only when the small vessel is in close proximity (less than10 meters). If the small vessel veers off beyond 10 meters, maintain a steady course to regain speed.

Post incident

a. Continue to exercise information control to only essential personnel or agencies with a need to know. No information about vessel movements, capabilities, counter piracy action / tactics employed or the incident itself should be released. Email, internet, and phone use should be strictly monitored to ensure sensitive information is not leaked to family, friends, or media.
b. If a vessel is attacked or boarded by pirates, several agencies will require access to the vessel and crew to conduct a series of investigations. The vessel crew should treat the vessel as a crime scene, preserve any evidence that may be useful to the investigations carried out, and cooperate with investigators.

7. The MARSEC Directive and associated Annex in no way precludes the employment of additional or increased security measures by Security Officer for the safety and security of the vessel.

8. Nothing in the MARSEC Directive shall constrain the master's ability or authority to make operational decisions to protect the lives of the crew, protect the vessel, or its cargo.

9. The MARSEC Directive does not authorize deviation from compliance with U.S. or foreign requirements on the carriage of weapons aboard merchant vessels.

10. The MARSEC Directive does not authorize deviation from compliance with U.S. or International safety requirements, but temporary deviations from existing certificates will be considered given that the owner/operator proposes a suitable equivalent level of safety.

11. Sections 24, 25, and 32 of the Annex to the Maritime Safety Committee (MSC) Circular 623/Revision 3 entitled "Piracy and Armed Robbery Against Ships" provides procedures for vessels encountering suspicious or threatening movements which may result in an imminent attack. The Circular steps vessels through the processes of contacting relevant Rescue Coordination Centers (RCC), radio stations, and vessels in the vicinity of the events.

For questions or concerns pertaining to MARSEC Directive 104-6 (Rev 2) or this Port Security Advisory, contact the U.S. Vessel Security Program Manager for (CG-543) at 202-372-1038 or email to HQS-PF-fldr-CG-543@uscg.mil. For acknowledgements, plan submissions or other matters directly pertaining to the MARSEC Directive for U.S. flagged vessels, please contact the U.S. Coast Guard Marine Safety Center at (202) 475-3444 or email to securityplaninfo@uscg.mil..

The conditions of entry applicable to vessels outlined in Port Security Advisory 01-09 remain in effect.

JAMES A. WATSON
Rear Admiral, U.S. Coast Guard
Director of Prevention Policy