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

International Port Security Program
U.S. Coast Guard

Date: November 23, 2010
Contact: LCDR James T. Fogle
(202) 372-1038

Port Security Advisory (2-09)(Rev 2)

There are several areas in the world where acts of piracy and armed robbery against ships are prevalent. On November 23, 2010, the Coast Guard published Maritime Security (MARSEC) Directive 104-6 (Rev. 4), *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 vessels to which MARSEC Directive 104-6 (Rev. 4) **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. 4) 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. If not, the VSP must be amended. VSP protocols which pertain 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 counter-piracy organizations that could be of assistance, and information control of sensitive security information (SSI).

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, to validate security measures. When necessary, region-specific guidance or requirements will be developed.

4. Company Security Officers (CSO) are encouraged to review the Worldwide Threat to Shipping and Piracy Activity Weekly Warning reports published by the Office of Naval Intelligence (ONI), weekly, and the ICC Commercial Crimes Services, monthly. Other current information is provided on websites maintained by the 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 CSOs 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 (NG-IA)	http://www.icc-ccs.org (ICC) (IMB PRC)
http://homeport.uscg.mil/piracy (U.S. Coast Guard)	http://www.oni.navy.mil/Intelligence_Community/piracy.htm (ONI)
http://www.mschoa.org (MSC HOA)	http://www.rncom.mod.uk/uploadedFiles/Pages/Maritime_Operations/0001-UKMTO.pdf (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. This Directive does not preclude the employment of increased security measures by vessel masters above and beyond those recommended or required herein for designated HRW or other waters if, in the master's best judgment, such measures are warranted.

   To supplement MARSEC Level 2 requirements, the following additional security measures must be implemented by vessel operators and owners to prevent and suppress acts of terrorism, piracy, and armed robbery against ships for vessels operating in HRW:

   Prior to entering High Risk Waters

   (a) Conduct a risk assessment (or review your existing risk assessment) on your vessel and route utilizing the most current intelligence and information available.
   (b) 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.
   (c) Unless otherwise directed or advised by on-scene military forces, 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. For vessels making less than 10 knots, contact UKMTO for routing guidance. Information on IRTC and GOA GT can be found on the MSCHOA website.
   (d) Establish counter-piracy protocols (in the VSP or piracy annex) commensurate to the threat and vulnerability (risk) of the vessel that can be practiced and implemented by the crew in accordance with 33 CFR 104.230. When developing VSP protocols or piracy annexes, owners and operators are encouraged to consider incorporating Industry best management practices (BMPs). For the HOA/GOA region, BMPs are posted on the Maritime Security Centre-Horn of Africa website: http://www.mschoa.org and U.S. Coast Guard's Homeport site: homeport.uscg.mil/piracy.

      Protocols shall include:

      (1) Hardening the vessel against intrusions
      (2) Non-lethal methods for repulsing intruders.
      (3) Ship operations & maneuvers to evade attack.
      (4) Communications Procedures: Internal protocols for internal shipboard communications & external communications before, during and after an incident.

(5) Protection of the crew.
(6) Procedures to take if the ship's security is compromised.
(7) Procedures for crew in hostage situations.
(8) Company policy/procedures for confronting intruders.
(9) Training program establishing frequency for drills and exercises.

(e) Establish refuge area(s) where crewmembers may go in the event of an attack. The refuge area 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 by ensuring crew is well briefed, trained in counter-piracy procedures, and well rested.
(g) For vessels with a freeboard less than 15 meters (49.2 feet), make the vessel difficult to scale. Installation of 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 with locking mechanisms which cannot be disengaged by automatic fire to prevent unauthorized access to the vessel.
(i) Equip vessel with non-lethal means to disrupt, disorient, and deter boarders.
(j) Outfit the vessel with enhanced detection equipment that will allow crewmembers and/or security personnel to become aware of potential pirate activity, in time to implement counter-piracy protocols.
(k) Modify access to the wheelhouse with locking mechanisms which cannot be disengaged by automatic fire to prevent unauthorized access.
(l) Consider supplementing ship's crew with armed or unarmed security personnel. Security personnel shall meet the training requirements in 33 CFR 104.220 and the guidelines set forth in Port Security Advisory (PSA) 5-09 (series); Minimum Guidelines for Contracted Security Services in HRW. If transiting the Horn of Africa region, all vessels shall supplement ship's crew with armed or unarmed security based on a vessel-specific piracy threat assessment conducted by the operator and approved by the Coast Guard.

During transits of a High Risk Area

(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; limit information to the vessel name, position, course, speed, navigational status, and safety-related information. Current intelligence does not support the contention that pirates are using AIS to identify vessels.
(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 counter-piracy watch and ensure all shipboard counter-piracy precautions are in force. Augment watches as necessary to perform lookout duty, including lookouts astern and other locations on the vessel to cover radar blind spots.
(f) Maintain highest practical speed in HRW. If capable, maintain speed 16 knots or greater.
(g) Minimize external communications (radios, handsets) to essential safety and security related communication.
(h) Activate supplemental security team watches, if so equipped.
(i) If the master thinks a threat is developing, contact appropriate regional operation center. If no operation center is available, notify the owner/operator.

(j) Man the engine room with a licensed engineer. While in high risk waters, this includes manning of automated engine rooms. If, due to the degree of automation used on board, manning the engine room is not practicable during transits of HRW, equivalent measures may be proposed.
(k) Secure, control access, and regularly inspect restricted areas (bridge, engine room, steering gear room, and crew quarters) keeping in mind any adverse impact these may have to safety in the event of an accident. In any instance where there is a conflict between safety and security, the safety requirement should be paramount.
(l) Ensure ladders and outboard equipment are stowed or on deck.
(m) Ready non lethal means to discourage attack and or defend the vessel. For example, fire pumps and fire hoses, or equivalent, may be pressurized and ready for discharge overboard.
(n) Follow any guidance from on-scene military forces that have counter-piracy intelligence that may aid the master in avoiding or thwarting piratical attacks.

If anchored in High Risk Waters

(a) Avoid anchoring or drifting in high risk waters, whenever possible.
(b) If the vessel is at anchor in high risk waters, vessels shall implement the security measures in paragraph 5 in addition to security measures equivalent to MARSEC Level 2. Vessel shall also implement the relevant measures from "During transits of High Risk Waters" section. Employ enhanced security measures as if the vessel was transiting through high risk waters.
(c) Illuminate all deck lighting at night.

If berthed in High Risk Waters

(a) If the vessel is berthed in high risk waters, vessels shall implement the security measures in paragraph 5 in addition to security measures equivalent to MARSEC Level 2.
(b) Prior to leaving port, search the ship thoroughly; secure or control all doors and access points.

If attacked or boarded

For Vessel:

(a) Activate the Ship Security Alert System (SSAS). The SSAS shall be used in all instances when attacks occur aboard U.S. vessels, regardless of the location or duration of the attack.[1]
(b) Make a "Mayday" call on VHF Ch 16.
(c) Inform regional liaison or counter-piracy organization for the region.
(d) When/if time permits, inform your company.
(e) Implement procedures established in the counter-piracy plan.
(f) Ensure that the Automatic Identification System (AIS) is operating. If the AIS was previously turned off for the transit, turn it back on.
(g) Send a distress message via Digital Selective (DSC) system and Inmarsat-C, as applicable.
(h) Unless directed otherwise, all crew with exception of bridge team and security personnel should go to pre-planned piracy refuge areas.

[1] When an SSAS is activated, the alert is received by the Coast Guard Regional Command Center in Norfolk, VA and authenticated with the Company Security Officer. The Coast Guard coordinates a response and provides interagency notifications and coordination.

(i) 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.
(j) If possible, deny use of ship's communications equipment by pirates.
(k) Heavy wheel movements are suggested for consideration to "ride off" attacking craft as they approach, with caution given to the effect on speed. Information from analysis of more recent attacks has shown that **maintaining highest practical speed** (which we still assess, along with sea state and weather) is a major determinant in defeating attacks. Masters are therefore advised to undertake maneuvers to increase pirate exposure to wind and waves but, understanding the vessel's maneuvering characteristics, to be very mindful of helm movement effect on speed.
(l) The vessel recordkeeping requirements as per 33 CFR 104.235 shall be adhered to.

For Company:

(a) Upon notification of a pirate attack, notify and coordinate with U.S. Government authorities through the USCG ATLANTIC AREA Command Center at 1-757-398-6700.
(b) All suspicious activities and events, including attacks by pirates, are to be reported to the National Response Center in accordance with 33 CFR Part 101.305. Activation of SSAS alerts in response to pirate attacks will need to be followed up by separate notification to the National Response Center by the owner or operator.

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 Security 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, including but not limited to the FBI and USCG. U.S. Government agencies will attempt to coordinate these interviews and investigations to avoid duplicative efforts that may negatively affect the crew or impact the vessel's ability to return to service. The vessel crew is expected to treat the vessel as a crime scene, preserve any evidence that may be useful to the investigations, and cooperate with investigators. The Coast Guard's authority to investigate the incident includes but is not limited to 14 U.S.C. § 89, 14 U.S.C. § 95, 14 U.S.C. § 141, as well as 46 U.S.C. Chapter 701.
(c) If the vessel is damaged or the crew capacity is diminished as a result of a piratical attack, the USCG may require an inspection to ensure the adequacy of the vessel and crew for the ships intended continued operation. The Coast Guard's authority to inspect the vessel includes but is not limited to 46 U.S.C. Chapters 33 and 63and 14 U.S.C. 89.

6. This MARSEC Directive and associated Annex in no way precludes the employment of additional or increased security measures by Company Security Officers (CSO) or Vessel Security Officers (VSO) for the safety and security of the vessel.

7. 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.

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

9. 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.

For submission of pirate specific vessel security assessments, and counter-piracy plans, contact the Marine Safety Center at (202) 475-3445 or email to securityplaninfo@uscg.mil. For questions or concerns pertaining to this MARSEC Directive and acknowledgement of receipt of the directive, contact the Vessel Security Program Manager for (CG-543) at 202-372-1038 or email to CG543@uscg.mil.

THE CONDITIONS OF ENTRY APPLICABLE TO VESSELS OUTLINED IN PORT SECURITY ADVISORY 3-10 REMAIN IN EFFECT.