BRITANNIA LOSS PREVENTION

B GUIDANCE

NOVEMBER 2020

ONBOARD SECURITY

KEEPING THE CREW SAFE IS THE HIGHEST PRIORITY

This guidance provides valuable advice as to how security measures can be implemented to increase the onboard safety and takes into account industry best practices.

SECURING THE SHIP – KEEP THE CREW SAFE

SECURITY THREATS ARISING FROM GEOPOLITICAL INSTABILITY, LOCAL CONFLICTS AND SOCIAL STRUGGLES ARE SOME OF THE MODERN DAY CHALLENGES OF THE MARITIME INDUSTRY, WHICH MAY IMPOSE AN INCREASED RISK TO A SHIP AND ITS SEAFARERS IN CERTAIN AREAS OF THE WORLD.

Enhanced security measures may have to be implemented on board when operating in these "high-risk" areas to make sure that the seafarers stay safe and feel safe.

The physical security threats include terrorism, piracy, robbery and the illegal trafficking of goods and people. Security on board is not only the job of the ship's security officer, but the job of the entire crew, therefore it is essential to provide the crew with training and appropriate security plans together with the necessary resources to implement them. Various industry guidance has been introduced to assist owners and crew improve security on board. Much of this information deals with specific threats but can be helpful in improving on board safety in general.

SECURITY MEASURES TO PUT IN PLACE

When looking at physical security on board a ship, the following documents are particularly important:

SHIP SECURITY PLAN (SSP)

This is a requirement of the International Ship and Port Facility Security code (ISPS) and was made mandatory by the International Maritime Organisation (IMO) in July 2004 by the newly introduced Chapter XI-2 of the Safety of Life at Sea (SOLAS) convention.

The SSP, based on a Ship Security Assessment and approved by the ship's Flag State, should indicate the operational and physical security measures that the ship should take to ensure that it always operates at a 'normal' level of security, termed as Security Level 1. It should also set out the additional security measures needed for the further heightened levels of Security Levels 2 and 3 and should include details of the:

- Organisational structure of security for the ship, including the duties and responsibilities of all shipboard personnel with a security role
- Established security measures covering all means of access to the ship and its restricted areas
- Security measures relating to cargo handling to prevent tampering; and
- Process of evacuating/safeguarding the crew in the event of a security threat.

The SSP should also identify the on board Ship Security Officer (SSO) and onshore Company Security Officer (CSO) as well as training and security drill requirements. Furthermore, the SSP must also be protected from unauthorised access or disclosure.

IT IS THE RESPONSIBILITY OF THE FLAG STATE AUTHORITIES TO DETERMINE WHICH LEVEL OF SECURITY IS APPLICABLE TO THE SHIP, ALTHOUGH A PARTICULAR PORT STATE AUTHORITY MAY IMPOSE A HIGHER SECURITY LEVEL WHERE APPROPRIATE. HOWEVER, A SHIP MAY ALSO CHOOSE TO ENHANCE STRICTER SECURITY MEASURES, DEPENDING ON THE PARTICULAR CIRCUMSTANCES.

BEST MANAGEMENT PRACTICE (BMP)

This was developed as industry guidance to help prevent piracy attacks and is supported by a number of major maritime industry bodies. It is also now supported by the IMO and recognised as the industry standard when assessing and implementing security measures. The following BMPs are now available, covering various areas and security threats:

- BMP 5 – To deter piracy and enhance maritime security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea
- BMP West Africa – To deter piracy and enhance maritime security off the coast of West Africa, including the Gulf of Guinea
- Global counter-piracy guidance for shipping companies, Masters and seafarers.

Even if a ship is not trading to an area covered by a BMP, it is recommended that these publications are available on board and their prescribed precautions are always taken into account when assessing on board security.

SECURITY THREAT ASSESSMENT

TO DETERMINE THE NECESSITY OF INCREASING SECURITY ON BOARD AND TO IMPLEMENT THE CORRECT COUNTERMEASURES, IT IS IMPORTANT THAT POTENTIAL THREATS ARE QUICKLY IDENTIFIED AND UNDERSTOOD.

As stated above, the Flag or Port State will advise on the applicable security level, as per the ISPS code, which the ship has to comply with in accordance with its SSP.

Other areas may be identified as high risk areas as per the BMP publications. This will provide the ship with some prior knowledge of the potential security threats to enable them to respond accordingly. However, even though an area does not have a raised ISPS security level nor is classified as a high risk area, serious security threats may still exist.

Members should therefore maintain a portfolio of security risk assessments covering their usual trading areas. These should be routinely reviewed as part of the ship's voyage and passage planning preparation and updated accordingly based on the latest intelligence received.

Members should perform due diligence to ensure that intelligence is only gathered from trusted sources, which may include the:

- Port Facility Security Officer (PFSO) in the arrival port;
- Local agent or representative; and
- Local P&I correspondents.

Furthermore, recognised reporting centres can advise on specific risks. These include the: SHIPS

- International Maritime Bureau (IMB) Piracy Reporting Centre, which provides reports on recent attacks or attempted attacks as well as a Live Piracy Map showing attacks reported to the IMB around the world.
- Office of Naval Intelligence, part of the U.S. Navy's Information Warfare Community and which issues weekly piracy reports and a monthly Worldwide Threats to Shipping report.
- Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), which is a regional government agreement that promotes and enhances cooperation to combat piracy and armed robbery against ships in Asia. ReCAAP also publishes reports on attacks in Asia.

Ships should also comply with the requirements of voluntary reporting areas (VRA). where established. They will also be able to provide information on the current situation for the area.

The United Kingdom Marine Trade Operations (UKMTO) together with the French navy operates the Maritime Domain Awareness for Trade-Gulf of Guinea (MDAT-GoG) VRA, which covers large parts of West Africa as per Maritime Security chart Q6114. Furthermore, UKMTO also operates the VRA for the Indian Ocean, specifically Red Sea, Gulf Of Aden, and Arabian Sea as per Maritime Security chart Q6099.

It is also recommended that the security measures identified by the security threat assessment are gathered together in a shipboard plan. This plan may be a part of the ship's SSP or Owners' Safety Management System, and steps must be taken not to disclose any of the confidential details of the SSP.

SECURITY MEASURES

ANY RISKS TO THE SHIP'S SECURITY MUST BE IDENTIFIED AND STEPS TAKEN TO MITIGATE THESE.

Detailed guidance on possible measures to improve security is provided in BMP 5. These measures can be divided into 3 categories or layers of defence, as summarised below:

1. PREVENT BOARDING

The first layer of defence is to prevent intruders from coming on board. The earlier a crew recognises a potential security threat, the better chance they have of dealing with the threat. Therefore, all available means should be used to monitor the surroundings of the ship and secure it. This may include the use of:

a. PROPER LOOKOUT

Enhanced vigilance by maintaining a good lookout using all available navigational means may detect a suspicious craft in sufficient time for the ship to be able to take evasive action or allow for sufficient time for assistance to arrive. In the hours of darkness, searchlights should be fitted and ready for immediate use. Thermal imagery optics and night vision aids may also be considered to better assess the surroundings during hours of darkness.

b. CLOSED CIRCUIT TELEVISION CAMERAS (CCTV)/MOTION SENSORS

If installed, these can be used as a further means of monitoring and recording activity around access points, especially during a port stay. Ideally, these should be monitored from several different locations on the ship e.g. Bridge, Deck Office, Engine Control Room and Citadel.

c. ILLUMINATION

Deck areas and access points should be illuminated during the hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage. The illumination should also include lighting up the ship's side where possible. While underway, external lighting should be limited to just the lights needed for navigation. If intruders are identified, over side lighting, if fitted, should be switched on. This may dazzle the attackers and also make them more visible to the ship's crew.

d. PATROLLING

Patrolling the deck by the crew is generally not recommended during the transit of areas with increased security threats. In ports with increased security threat, deck patrols shall only be done after a thorough assessment of any anticipated risks. The persons on deck should always carry a radio and report to the Officer on Watch with fixed intervals. Special precautions such as patrolling in pairs may be implemented.

e. RESTRICTING ACCESS

This should mostly be covered by the ship's SSP, where access points should be limited and monitored at all times and only authorised personnel shall be allowed access. Furthermore, the use of physical barriers may act as an effective preventive measure, such as:

i. Razor wire

This is relatively cheap and easy to store and, if fitted correctly, provides an efficient security barrier. The disadvantage is that it is time consuming to rig and may cause personal injuries. The quality of razor wire may also vary and a lower quality type may not be as effective.

ii. Water spray and foam monitors

These can make it difficult for an intruding craft to remain alongside and also make it significantly more difficult to climb aboard. The hoses should cover access points of the ship but should not be manually operated as they may expose the operator to increased danger.

iii. Plastic barriers

These are specially designed to fit onto the ships railings and can prevent intruders from climbing on board. These may be effective but can also require a considerable amount of storage space when not in use.

Those on board and on shore should collectively assess which system is most effective for their type of ship, taking into account the trading pattern and available resources on board for rigging and unrigging.

1. SECURE THE ACCOMMODATION

The second layer of defence is to secure the accommodation and identified restricted areas to not only prevent petty theft but also to ensure the safety of the crew inside. This will also help to prevent the intruders gaining access to vital shipboard systems e.g. propulsion. Some of the considerations to be made are:

a. GRATE

A grate may be fitted in front and astern of the accommodation to block unauthorised access to it. The grate may be fitted with spikes or razor wire to make it difficult to climb.

b. ENTRANCE POINTS

Doors and hatches providing access to the bridge, accommodation and machinery spaces and any other restricted areas should be properly secured to prevent them being opened from the outside. Windows should also be made secure where appropriate. All doors, hatches or windows which are part of an escape route must be secured in a way that still allows for escape.

c. EXTERNAL STAIRS AND LADDERS

To restrict external access to the bridge, all external stairs should be blocked and all ladders on the accommodation block removed.

2. SAFE MUSTER PLACE – CITADEL

The third layer of defence is the identification of a designated safe muster point and/or citadel on the ship as part of the risk assessment and planning process. A safe muster point is a designated area, such as a central stairway, that provides the crew with the best possible physical protection during an attack. A designated citadel as an area for the crew to retreat to in case of an imminent boarding which threatens the safety of the crew. The citadel shall be designed to withstand forced entry and be equipped with two-way communication measures, preferably using VHF and satellite phone with their own power supply. Contact details for the CSO and applicable authorities should be available within the citadel. There should also be sufficient food, water, sanitation and other necessities for the crew to survive for a reasonable time Inside the citadel.The Master should take the final decision as to when the crew should withdraw to the citadel.

TRAINING

FOR ALL SECURITY MEASURES TO WORK EFFICIENTLY THE CREW NEED TO BE PROPERLY TRAINED IN THEIR APPLICATION AND LIMITATIONS.

The Standards of Training, Certification and Watchkeeping for Seafarers Convention (STCW) sets out the basic requirements for training as per the ISPS code. There should be frequent on board practice, while ship-to-shore drills are also essential to ensure that the crew responds accordingly in case of an imminent security threat. The drills should include:

- Evacuation to and use of the citadel, including establishing external communication
- Rigging and unrigging of security measures
- Correct use of security equipment
- Identifying illicit behaviour

It is recommended that an on board drill and test of all security equipment are conducted before entering an area with an increased security risk. All security equipment shall be maintained as part of the ship's planned maintenance programme.

PRIVATE SECURITY COMPANIES

THE CLUB DOES NOT RECOMMEND OR ENDORSE THE USE OF PRIVATE MARITIME SECURITY COMPANIES (PMSC) OR PRIVATELY CONTRACTED ARMED SECURITY PERSONNEL (PCASP) BUT DOES NOT OBJECT TO THEM EITHER IF CERTAIN REQUIREMENTS ARE MET (AS DETAILED IN THE INTERNATIONAL GROUP'S FAQs DATED AUGUST 2013).

The engagement of armed or unarmed guards is a decision that should be taken by the individual owner, always subject to the permission of the ship's Flag State and any littoral states. If it is decided to engage such guards, the Club should be notified accordingly to arrange additional "third party" cover and to review the Contract for Employment of Security guards to check the terms are within the scope of Club cover.

The decision to use a PMSC or PCASP should be made on the basis of a thorough risk assessment of the specific transit, in particular the current threat and risk environment, as well as the security weaknesses of the ship. It is recommended that due diligence of such service providers is performed and that only ISO 28007 accredited companies are employed.

Where PMSC or PCASP are engaged, this should not compromise the overriding authority of the Master. Furthermore, the Rules for the Use of Force (RUF) under which the PCASP operates should be acceptable to both the company and Flag State.

CONCLUSION

AWARENESS OF THE POTENTIAL RISKS AND BEING READY TO DEAL WITH THEM ARE THE MOST IMPORTANT PRECAUTIONS TO BE TAKEN WHEN ENTERING AN AREA WITH AN INCREASED SECURITY THREAT.

Ensuring that any potential security threats are assessed using reliable intelligence is essential for the crew to be able to correctly interpret the threat and to enable them to implement efficient mitigation measures.

The ship's SSP and industry best practices, such as the BMPs, should be consulted to guide the crew and help them improve the security of the ship, when necessary. These should be accompanied by sufficient on board training and drills so that the crew can understand how to efficiently implement the security precautions and incorporate the necessary routines in case of an actual security incident.

FOR FURTHER INFORMATION

If you have any questions, or would like further advice on how to enhance security on board, then please feel free to contact the Britannia Loss Prevention team at **lossprevention@tindallriley.com**.

For further specific security advice on preventing drug smuggling please see our **guidance**.

For further specific security advice on preventing stowaways please see our **guidance**.

Furthermore, OCIMF has published **Guidelines to Harden Vessels** which provide further detailed advice on how to increase on board security.