PANAMA MARITIME AUTHORITY
(AUTORIDAD MARÍTIMA DE PANAMÁ)
GENERAL DIRECTORATE OF MERCHANT MARINE
(DIRECCIÓN GENERAL DE MARINA MERCANTE)
DEPARTMENT OF CONTROL AND COMPLIANCE
(DEPARTAMENTO DE CONTROL Y CUMPLIMIENTO)

MERCHANT MARINE CIRCULAR MMC-125

To: Master, Ship-owners, Operators, Company Security Officers, Ship Security Officer, Legal Representatives of Panamanian Flagged Vessels, Recognized Security Organizations (RSO) of Panamanian Flagged Vessel.

Subject: SOLAS 74 /78 Chapter XI-2
ISPS Code Part A and B
MMC 123
MMC 124
MMC 126
MMC 128
MMC 131
MMC 206

Reference: SHIP SECURITY PLAN (SSP)

1. According to the ISPS Code, Part A 9, it is required for each ship to carry on board a Ship Security Plan (SSP) approved by its flag state or by an organization recognized by it to carry out such approvals, known as a Recognized Security Organizations (RSO).

2. The Company Security Officer (CSO) has the responsibility of ensuring that the plan is prepared and submitted for approval. The content of each individual Ship Security Plan (SSP) will vary depending on the particular ship it covers. The Ship Security Assessments (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the Ship Security Plan (SSP) will require these features to be addressed in detail.

3. This Administration states all Ship Security Plans (SSP) have to make provision for the three, internationally adopted, Security Levels:

   3.1 **Security Level 1,** normal; the level at which ships and port facilities will normally operate;
   3.2 **Security Level 2**, heightened; the level applying for as long as there is a heightened risk of a security incident;
   3.3 **Security Level 3,** exceptional; the level applying for the period of time when there is a probable or imminent risk of a security incident.

4. This Administration requires the Plan to be written in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages must be included, preferably English. The Plan must address, at least, the following (Part A 9.4 ISPS Code):

Measures designed to prevent weapons, dangerous substances and devices intended for use against people, ships or ports, and the carriage of which is not authorized on board the ship;

4.2 Identification of the restricted areas and measures for the prevention of unauthorized access;
4.3 Measures for the prevention of unauthorized access to the ship;
4.4 Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
4.5 Procedures for responding to any security instructions Contracting Governments may give at Security Level 3;
4.6 Procedures for evacuation in case of security threats or breaches of security;
4.7 Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
4.8 Procedures for auditing the security activities;
4.9 Procedures for training, drills and exercises associated with the Plan;
4.10 Procedures for interfacing with port facility security activities;
4.11 Procedures for the periodic review and updating of the Plan;
4.12 Procedures for reporting security incidents;
4.13 Identification of the Ship Security Officer (SSO);
4.14 Identification of the CSO including 24-hour contact details;
4.15 Procedures to ensure the inspection, testing, calibration, and maintenance of security equipment provided on board, if any;
4.16 Frequency of testing or calibration of security equipment provided on board, if any;
4.17 Identification of the locations where the ship security alert system activation points are provided (this information should be kept elsewhere on board in a document know to the master, the SSO and other shipboard personnel as decided by the Company);
4.18 Procedures, instructions and guidance on the use of the ship security alert system, including testing, activation, deactivation, resetting, and procedures to limit false alerts.

5. According to Part B 9.2 of the ISPS Code, the Ship Security Plan (SSP) must:

5.1 Detail organizational structure of security for the ship;
5.2 Detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;
5.3 Detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;
5.4 Detail basic security measures for Security Level 1, both operational and physical, that will always be in place;
5.5 Detail the additional security measures that will allow the ship to progress without delay to Security Level 2 and, when necessary, to Security Level 3;
5.6 Provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances;
5.7 Detail reporting procedures to the Department of Maritime Security of the Panama Maritime Authority contact points;

6. In addition, the SSP should establish the following, which relate to all Security Levels (Part B 9.7 ISPS Code);

6.1 Duties and responsibilities of all shipboard personnel with a security role;
6.2 Procedures of safeguards necessary to allow continuous communications to be maintained at all times;
6.3 Procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment systems failure or malfunction;
6.4 Procedures and practices to protect security sensitive information held in paper or electronic format;

6.5 The type and maintenance requirements of security and surveillance equipment and systems, if any;
6.6 Procedures to ensure the timely submission, and assessment, 0of reports relating to possible breaches of security or security concerns;
6.7 Procedures to establish maintain and update an inventory of any dangerous goods or hazardous substances carried on board, including their location.

7. According to ISPS Code Part A 9.6, this Administration establishes the Plan can be kept in an electronic format. In such case, it must be protected by measures aimed at preventing unauthorized access, disclosure, deletion, destruction or amendment (Part A 9.6 ISPS Code).

8. The Ship Security Plan should address the security measures to be taken at each Security Level covering:

8.1 Access to the ship by ship's personnel, passengers, visitors, etc;
8.2 Restricted areas of the ship;
8.3 Handling of cargo;
8.4 Delivery ship's stores;
8.5 Handling unaccompanied baggage;
8.6 Monitoring the security of the ship.

9. Fleet Plans and Sister Ships

Each vessel shall have an individual Ship Security Plan tailored to its Security Assessment. However, there will be information in each ship's plan that will be the same for all of the ships in the company's fleet, for vessels on the same trade route and for sister ships operating in the same trade. The Security Assessment for the first ship can be used as a model for each of the other ships engaged in the same trade on the same routes. In such a case, only the ship's specific variations need be addressed during the on-scene Security Assessment.

10. Restricted Area

All restricted areas should be annotated on a General Arrangement Plan or other drawings of the vessel. The SSP should provide that all restricted areas are clearly marked indicating that access to an area is restricted and that unauthorized presence within an area is considered a breach of security. Clearly marked means that the area is marked in a manner that should communicate its restricted status to any visitors or person on board.

11. Training and Security Drills

The Ship Security Officer, the Company Security Officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of the ISPS Code. 3.5.1.1.

Shipboard personnel without designated security duties should receive security-related familiarization training to be able to:

1. Report a security incident;
2. Know the procedures to follow when they recognize a security threat; and
3. Take part in security-related emergency and contingency procedures.

Security drills must test the proficiency of vessel personnel in assigned security duties at all maritime security levels and the effective implementation of the Ship Security Plan (SSP). They must enable the Ship Security Officer (SSO) to identify any related security deficiencies that need to be addressed.

The SSO must ensure that at least one security drill is conducted once every three months to promote the effective implementation of the Ship Security Plan, except:

1. when a vessel is out of service due to repairs or seasonal suspension of operation provided that in such cases a drill must be conducted within one week of the vessel's reactivation, or if more than 25% of the crew is changed at any one time, with personnel that has not previously participated in any drill on that ship within the last three months, a drill should be conducted within one week of the change.

Security drills may be held in conjunction with non-security drills where appropriate. The PMA accepts that a Safety Drill, which has a security component within it, can be credited as a Security Drill.

Security drills must test individual elements of the SSP, including response to security threats and incidents. Drills should take into account the types of operations of the vessel, vessel personnel changes, and other relevant circumstances.

Shipboard drills should cover such scenarios as:

1. Identification and search of unauthorized visitors on board the ship;
2. Recognition of materials that may pose a security threat;
3. Methods to deter attackers from approaching the ship;
4. Recognition of restricted areas; and mustering for evacuation.

12. Security Exercises

The Company Security Officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals.

Exercises should be carried out at least once each calendar year with no more than 18 months between the exercises.

Exercises should test communications, coordination, resource availability, and response. Exercises may be and not limited:

1. Full scale or live;
2. Table top simulation or seminar; or
3. Combined with other exercises held such as search and rescue or emergency response exercises.

13. Records

This Administration recommends all Panamanian flagged vessels to keep onboard records of the above indicated testing, drills and exercises according to the period of time indicated in the SSP or the time in the internal procedures of the Company. If is not duly stated in the mentioned documents, then the records must be kept for a period of time equivalent to the duration of the International Ship Security Certificate (5 years). These records must be protected from unauthorized access and may be kept in any format (paper or electronic) and must be available for any Authority that requests it.

In this regard, a copy of the radio technician’s report, demonstrating compliance with SOLAS 74’, as amended Chapter XI-2 Regulation 6 paragraphs #2 to #4 inclusive and MSC.1/Circ.1190, shall be kept on board for use by the RSO at the next scheduled ISPS audit.

At subsequent ISPS verification, the RSO shall examine the records of activities on the SSAS equipment, as specified in the ISPS Code A/10.1.10, witness a complete security alert test and verifying the operational requirements and in the case of a SSAS.

This Administration recommends all Panamanian flagged vessels to keep the records of the drills conducted in the vessel for a period of time indicated in their Ship Security Plan. Otherwise, the records must be kept as per stated in the procedures of the company. If this is not indicated in neither of the previous documents, this Administration recommends the records of the drills conducted to the vessel must remain onboard for a period of time equivalent to the duration of the International Ship Security Certificate.

For Inquiries concerning the subject of this Circular or any request should be directed to:

Maritime Ships Security Department
Directorate General of Merchant Marine
Panama Maritime Authority
Phone: (507) 501-5086 / 5037
Email: *isps@amp.gob.pa*

January – Inclusion paragraphs 11 to 13
November - New Paragraph 9, 10
June, 2013 - Changes all throughout the text
September, 2003