PANAMA MARITIME AUTHORITY

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: **SHIP SECURITY PLAN (SSP)**

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

---

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):

    4.1 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. 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*

November - *New Paragraph 9, 10*
June, 2013 - *Changes all throughout the text*
September, 2003