Merchant Marine Circular

Panama Maritime Authority
General Directorate of Merchant Marine
Control and Compliance Department

MERCHANT MARINE CIRCULAR MMC-123

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

Subject: International Ship and Port Facility Security Code (ISPS Code).

Reference: Law No. 38 June 4, 1995, UNCLOS 1982.
Resolution ADM No. 140-2003 of May 15, 2003.
Law No. 78 November 15th, 2010, SUA 2005 and SUA PROTOCOL.
MMC-354 - Guidelines on Maritime Cyber Risk Management.
MMC-359 - Guidance for the implementation and certification of the FAL Convention.
ISPS Code.

---

1. This Merchant Marine Circular supersedes and compiles: **MMC-124**, **MMC-125**, **MMC-126**, **MMC-128**, **MMC-206**, **MMC-223, MMC-252 and MMC-368.**

2. PURPOSE:

2.1 The purpose of this Merchant Marine Circular was issued to provide information and guidance to Ship-owner, Operators, and Master concerning the Administration's requirements for compliance with the International Ship & Port Facility Security Code (ISPS Code). The Code is divided into two sections, Part A and Part B. Mandatory Part A outlines detailed maritime and port security-related requirements which SOLAS contracting governments, port authorities and shipping companies must adhere to, in order to be in compliance with the Code. Part B of the Code provides guidance and information concerning how to implement Part A.

2.2 In 2010, the Republic of Panama ratified the Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA 2005) and the Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (SUA PROT 2005). The aforementioned

was approved by Law No. 78 of November 15, 2010, promulgated in Official Gazette No. 26663-B of November 18, 2010.

3. SCOPE:

3.1 This Merchant Marine Circular applies all Panamanian flagged ships engaged on international voyage of 500 gross tonnages and upwards.

3.2 Background:

3.2.1 The ISPS Code came into force in 2004, when it was passed as an amendment to the SOLAS (Security of Life at Sea) Convention under Chapter IX-2.

4. INDEX:

4.1 ISPS CODE APPLICABILITY:

4.1.1 Applies to all Panamanian flagged ships engaged on international voyages:

- Passenger ships, including high-speed passenger craft.
- Cargo ships, including high-speed craft, of 500 gross tonnages and upwards.
- Self-propelled mobile offshore drilling units capable of making international voyages unassisted and unescorted when underway and not on location.
- Port facilities serving such ships engaged on international voyages.

4.1.2 The ISPS Code does not apply to:

- Warships, naval auxiliaries or others ships Government non-commercial service.
- Cargo ships, including commercial yachts of less than 500 gross tonnages.
- Ships not propelled by mechanical means.
- Private pleasure yachts not engaged in trade.

- Fishing Vessels.
- Non-Self-propelled mobile offshore drilling units.

4.1.3 For those Panamanian flagged vessels operating in national waters of the Republic of Panama and if they want to apply voluntarily for the ISPS Code they must comply with the requirements of SOLAS Chapter XI-2 and part A of this Code and will be subject to the ISPS verifications specified in section Part A/19.1.1. If for some reason do not wish to continue with the implementation of the ISPS Code, they must notify directly to the Administration at the following email: isps@amp.gob.pa and this Administration will proceed to cancel the International Ship Security Certificate (ISSC).

4.2. SHIP SECURITY ASSESSMENT (SSA):

4.2.1 According to the ISPS Code, Part A/8, it is required to all Company Security Officers of Panamanian Flagged vessels to make sure Ship Security Assessments (SSA), are carried out to all the vessels under their responsibility by persons with appropriate skills to evaluate the security of ships in accordance with the ISPS Code.

4.2.2 The Ship Security Assessment (SSA) is an essential and integral part of the process of developing and updating the Ship Security Plan on board Panamanian flagged vessels.

4.2.3 The Ship Security Assessment (SSA) shall include an on-scene security survey but is not limited to the following elements:

- Identification of existing security measures, procedures and operations;
- Identification and evaluation of key shipboard operations that it is important to protect;
- Identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
- Identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

4.2.4 The Ships Security Assessment (SSA) shall be documented, reviewed, accepted and retained by the company.

4.2.5 A Ship Security Assessment (SSA) should address the following elements on board Panamanian Flagged vessels:

- Physical security;
- Structural integrity;
- Personnel protection systems;
- Procedural policies;

- Radio and telecommunication systems, including computer systems and networks, following the **Guidelines on Maritime Cyber Risk Management** described in the MMC-354;
- Other areas that may, if damaged or used for illicit observation, pose a risk to people, property or operations on board the ship or within a port facility.

4.2.6 The Ship Security Assessment (SSA) should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance relevant to:

- Restricted areas;
- Response procedures to fire or other emergency conditions;
- The level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers etc;
- The frequency and effectiveness of security patrols;
- Access control systems, including identification systems;
- Security communications systems and procedures;
- Security doors, barriers and lighting; and
- Security and surveillance equipment and systems.

4.2.7 The Ship Security Assessment (SSA) should consider all possible threats, which may include the following types of security incidents:

- Damage to, or destruction of, the ship or port facility, e.g., by explosive devices, arson, sabotage or vandalism;
- Hijacking or seizure of the ship or of persons on board;
- Tampering with cargo, essential ship equipment or systems or ship's stores;
- Unauthorized access or used, including presence of stowaways;
- Smuggling weapons or equipment, including weapons of mass destruction;
- Use of the ship to carry those intending to cause a security incident and/or their equipment;
- Use of the ship itself as a weapon or as a means to cause damage or destruction;
- Attacks from seaward whilst at berth or at anchor; and
- Attacks whilst at sea.

4.2.8 The SSA shall be sent, together with the SSP, to the RSO by a predetermined method to prevent unauthorized disclosure. The RSO shall review the SSA to ensure that each element required by the code is satisfactorily addressed and is used as a reference for the SSP.

4.2.9 This Administration urges all Panamanian flagged vessels transiting high-risk areas or operating in ports where piracy attacks occur to carry out a security assessment as a preparation for development of measures to prevent attacks of pirates or armed robbers and

on how to react should an attack occurs MSC.1/1334 (For reference visit Maritime Security Link, IMO Documents).

4.3. <u>SHIP SECURITY PLAN (SSP):</u>

4.3.1 All the Panamanian flagged vessel Companies shall develop, implement and maintain a functional SSP aboard its ships in compliance with SOLAS Chapter XI-2, the ISPS Code.

4.3.2 The SSP is developed from the information compiled in the SSA. It ensures application of measures onboard the ship designed to protect persons on board, the cargo, cargo transport units, ship's stores or the ship from all manner of risk security violations. The SSP shall be protected from unauthorized disclosure.

4.3.3 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;
- Identification of the restricted areas and measures for the prevention of unauthorized access;
- Measures for the prevention of unauthorized access to the ship;
- Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
- Procedures for responding to any security instructions Contracting Governments may give at Security Level 3;
- Procedures for evacuation in case of security threats or breaches of security;
- Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
- Procedures for auditing the security activities;
- Procedures for training, drills and exercises associated with the Plan;
- Procedures for interfacing with port facility security activities;
- Procedures for the periodic review and updating of the Plan;
- Procedures for reporting security incidents;
- Identification of the Ship Security Officer (SSO);
- Identification of the CSO including 24-hour contact details;
- Procedures to ensure the inspection, testing, calibration, and maintenance of security equipment provided on board, if any;
- Frequency of testing or calibration of security equipment provided on board, if any;

- 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);
- Procedures, instructions and guidance on the use of the ship security alert system, including testing, activation, deactivation, resetting, and procedures to limit false alerts.

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

- Detail organizational structure of security for the ship;
- Detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;
- Detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;
- Detail basic security measures for Security Level 1, both operational and physical, that will always be in place;
- 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;
- Provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances;
- Detail reporting procedures to the Department of Maritime Security of the Panama Maritime Authority contact points;

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

- Duties and responsibilities of all shipboard personnel with a security role;
- Procedures of safeguards necessary to allow continuous communications to be maintained at all times;
- 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;
- Procedures and practices to protect security sensitive information held in paper or electronic format;
- The type and maintenance requirements of security and surveillance equipment and systems, if any;
- Procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns;
- Procedures to establish maintain and update an inventory of any dangerous goods or hazardous substances carried on board, including their location.

4.3.6 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).

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

- Access to the ship by ship's personnel, passengers, visitors, etc.;
- Restricted areas of the ship;
- Handling of cargo;
- Delivery ship's stores;
- Handling unaccompanied baggage;
- Monitoring the security of the ship

4.3.8 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.

4.3.9 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.

4.4. <u>SECURITY LEVELS AND DECLARATION OF SECURITY (DOS):</u>

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

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

4.4.2 The SSP should include procedures and security measures for interfacing with ports, vessels, platforms and facilities. The Company Security Officer (CSO) and the Ship Security Officers (SSO) are encouraged to contact the Port Facility Security Officer (PFSO) and develop a close working relationship.

4.4.3 When a Panamanian flagged vessel has a Security Level which is lower to the level established in the next port of call, then the Ship Security Officer will inform of the situation to the CSO and the Security Level of the vessel will proceed to increase to the one established by the Port facility.

4.4.4 When a Panama flagged vessel has a Security Level which is higher to the level established in the next port of call, then the SSO and CSO will contact the PFSO andinform him about the situation in order to complete the Declaration of Security (DoS).

4.4.5 According to the ISPS Code provisions the Declaration of Security (Dos) has the purpose to ensure an agreement between the ship and the port facility or with othership with which it interfaces as to the respective security measures each of them will undertake in accordance with the provisions of their respective approved securityplans.

4.4.6 This Administration encourages all the Companies of Panamanian flagged vessels to complete a Declaration of Security (DoS) when:

- The ship is operating at a higher security level than the port facility or anothership it is interfacing with.
- There has been a security threat or security incident involving the ship orinvolving the port facility, as applicable.
- The ship is at a port which is not required to have and implement an approvedport facility security plan.
- The ship is conducting ship-to-ship activities with another ship not requiredto have and implemented an approved security plan.
- When the Ship Security Plan (SSP) provides any other measures.

4.4.7 The Declarations of Security (DoS) shall address the security requirements that could be shared between a port facility and ship (or between ships) and shall state the responsibility for each and shall be acknowledge by the applicable port facility orship.

4.4.8 This Administration recommends all Panama flagged vessels to keep onboard the record of Declarations of Security (DoS) for the period of time indicated in the Ship Security Plan (SSP), or in the procedures of the Company. If this is not duly stated in neither of the mentioned documents, then the Declarations of Security (DoS) mustbe kept for a period covering at least the previous 10 calls at Port Facilities, which they apply, complete and sign a Security of Declaration and will use the model givenin the Appendix of Part B, according to the ISPS Code and Ship Security Plan (SSP)in order to avoid any PSC deficiencies.

4.4.9 All the Panamanian flagged vessels transiting through High Risk Areas (HRA) have to raise the Security Level according to their Ship Security Plan (SSP) and follow the instruction posted in the Merchant Marine Circular (MMC-230).

4.4.10 Any change of security level, or implementation of security measures is to be advised by e-mail to securitylevel@amp.gob.pa

4.4.11 In case you need more information about the current security level in any port, we strongly recommend you please contact directly your local agent in such port, this Administration only provides information about the security levels in the Panamanianports, which is available at www.panamashipregistry.com in the Security Level link.

4.5. SHIP SECURITY OFFICER (SSO):

4.5.1 The Ship Security officer (SSO) is a person designated by the Company Security Officer (CSO) responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the Company Security Officer (CSO), Port Facility Security Officer and this Administration.

4.5.2 According to Part A, Section 12 and Part B, Section 13 the SSO shall have the knowledge of, and receive formal training in the elements of Part B, Section 13.1, and specific Company training in the elements of Part B, Section 13.2, of the Code.

4.5.3 All Panamanian flagged vessels engaged in international voyages in which the ISPS Code applies, must have on board a Ship Security Officer (SSO) shall be a management level officer. It is highly recommended to give this duty to the Master, Chief Officer, Chief Engineer or Second Engineer, who shall have completed an approved training course regarding the requirements and recommendations of the ISPS Code. If the person designated is not the Master, it must be understood that the Master still holds overall responsibility for the security of the ship which cannot be relinquished.

4.5.4 All the Ship Security Officer (SSO) of Panamanian flagged vessels are hereby requested to maintain wide communication with the Company Security Officer (CSO) in order to comply with the measures established in the Ship Security Plan.

4.6. RECOGNITION OF COMPANY SECURITY OFFICERS (CSO):

4.6.1 The Company Security Officer (CSO) is designated by the Company to ensure that a Ships Security Assessment (SSA) is carried out; that a Ship Security Plan (SSP) is developed and submitted for approval, thereafter implemented and maintained, and liaison with Port Facility Security Officer (PFSO) and the Ship Security Officer (SSO).

4.6.2 All the Company Security Officers (CSO) recognized by this Administration has to perform the duties and responsibilities as detailed in Part A, Section 11 and therelevant provisions of Part B, Sections 8, 9 and 13 of the ISPS Code.

4.6.3 The CSO shall ensure that each vessel he or she is responsible for has appointed a trained and qualified SSO.

4.6.4 All the Company Security Officers (CSO's) of the Panamanian vessels transiting high-risk areas are hereby requested to maintain a wide communication with the Panama Maritime Authority and to liase with the International Contact Centers according to the current and most updated BMP version (MMC-230), and raise their Security Level according to the Ship Security Plan.

4.6.5 The Company Security Officers (CSO's) of the Panamanian vessels transiting high-risk areas must develop procedures to prepare crews for thecontingency of their vessels being hijacked when transiting in high risk areas (MSC.1/Circ.1390) (visit Maritime Security link, IMO Documents).

4.6.6 Starting from the September 1st, 2017 the CSO Endorsement online application will be available on the Following website link: http://certificates.amp.gob.pa/certificates . The information submitted by the online application, should be completely accurate in order to avoid mistake(s) of the information transferred to the CSO. Also have to attach the following documents:

- Model of Nomination Letter. (Annex - Letter Head).
- DOC (Document of Compliance), with copy of annual endorsement if it hastaken place.

4.6.7 This Administration urges all company operators, Company Security officer or the interested party that previous to request the CSO Endorsement it makes sure yourCSR is updated and otherwise you must request the issuance of CSR and / or record the amendments in order to proceed with the endorsement.

4.6.8 In case of the company operating changes the technical officer should evaluate the application and must request copy of the SMC to verify the change of company operator prior to proceed with the CSO Endorsement.

4.6.9 The Company Security Officer Declaration (CSO) must be printed out in a single page (letter size (8.5"X 11") or A4 size if letter size is not available) and remain onboard. They should be printed in black and white or colors.

4.6.10 The CSO Endorsements issued before August 1, 2018 without electronic signature and QR Code is fully valid.

4.7. TRAINING, SECURITY DRILLS, SECURITY EXERCISES AND RECORDS:

4.7.1 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.

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

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

4.7.3 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.

4.7.4 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:

- 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.

4.7.5 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.

4.7.6 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.

4.7.7 Shipboard drills should cover such scenarios as:

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

4.7.8 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:
    - Full scale or live;
    - Table top simulation or seminar; or
    - Combined with other exercises held such as search and rescue or emergency response exercises.

4.7.9 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.

4.8. SSAS EXEMPTION:

4.8.1 Starting from the November 1st, 2019, the SSAS exemption must be requested through the following website link http://certificates.amp.gob.pa/certificates, and the following documents will be submitted:

- RSO statement with the alternative security measures on board.
- A formal statement by the Coastal State about vessel operational area.
- Interim ISCC
- Payment Receipt.

4.8.2 The SSAS exemption will only be issue by the head office. According Resolution J.D. No. 038-2014 of November 12, 2014, the cost for SSAS Exemption is US$300.00 **(no handling fee is applicable)** and we recommend using Google Chrome, Opera, Mozilla Firefox, Safari and Microsoft Edge.

4.8.3 The interim SSAS exemption certificate will be valid for the period of validity of the interim ISSC issued by the Recognized Security Organization (RSO). However, once the ISPS verification audit has been carried out according to the ISPS Code/Reg.19.1.1 and this Administration has been already issued the International Ship Security Certificate (FULL TERM ISSC); the operating company should request the permanent SSAS exemption certificate that will be valid for the period of validity of the Full Term ISSC without any cost.

4.9. STOWAWAYS-RISK ASSESSMENT:

4.9.1 This Administration urges Ship-owners, operators, masters, companies of Panamanian flagged vessels to implement the necessary security measures to prevent stowaway's access either at sea or on arrival. The Master should always be aware of regional hot spots for stowaways and put in place measures to prevent stowaways gaining access to the ship when operating in high risk areas.

4.9.2 One of the functional requirements of the International Ship and Port Facility Security (ISPS) Code is preventing unauthorized access to ships. The ISPS Code requires a ship security assessment to be conducted which should consider all possible threats of unauthorized access, including presence of stowaways.

4.9.3 Prevention: The core strategy is to ensure that no unauthorized personnel are able to gain access to the ship, and that all those who have been authorized to board disembark before sailing and follow the procedures to ensure that there is a watchman on duty at every access point, which have to remain unlocked whilst the vessel is in port and that this watchman is familiar with the procedures when visitors, repairmen, stevedores etc. wish to come on board.

4.9.4 All Panamanian flagged vessels when calling ports and during their stay in ports, where there is risk of a stowaway embarkation, must implement preventive measures, as follows but not limited to:

- All doors, hatches and means of access to holds or stores, which are not used during the ship's stay in port should be locked;
- Access points to the ship should be kept to a minimum and be adequately secured;
- Areas seaward of the ship should be adequately secured;
- Adequate deck watch should be kept;
- Boarding's and disembarkations should, where possible, be tallied by the ship's crew or, after agreement with the master, by others;
- Adequate means of communication should be maintained; and
- At night, adequate lighting should be maintained both inside and along the hull.

4.9.5 The personnel on duty should ensure that all locks are locked and that places which cannot be locked are sealed with tamper-proof or wire seals. Different harbors and ports have different access points that are commonly used. In general, some access point entries can be:

- Climbing the mooring ropes,
- Climbing from the sea using hooks,
- Climbing the anchor chain, 21
- Boarding the vessel as stevedores with fake dock identification papers,

- Hiding inside empty containers,
- Hiding in loaded containers, cars, break-bulk,
- Hiding in container lashing bins or container spreader

4.9.6 Prior to departure the crew should conduct a thorough search of all compartments and the result should be recorded in the logbook. When possible, the ship's rudder trunk should be checked for stowaways. The rudder trunk is a typical access point for stowaways and is very often used as hideout. Once the vessel has sailed and the outbound pilot is still on board, again; a search of all compartments should be considered. If stowaways are found at this stage they can be repatriated using the pilot boat.

4.9.7 The discovery of a stowaway indicates a breach of the Ship Security Plan (SSP). As such they should be investigated for their RSO to analyze the cause of the security breach in order to identify the actions necessary to prevent future stowaway occurrences. The operating company shall coordinate an additional audit with their RSO in a period not to exceed 90 days to verify the SSP breach and the report should be provided to the Security Department at isps@amp.gob.pa. However the stowaway should be reported by the master to the appropriate authorities.

4.9.8 Any stowaways found should be placed in secure quarters, guarded if possible, and be provided with adequate food and water. They, as well as the place they were found, should be searched for any identification papers. The stowaway should be questioned as to whether he is alone in this venture or if there are others. Where there is more than one stowaway, they should preferably be detained separately.

4.9.9 When a stowaway is found on board a ship, the Master should prepare a statement containing all available information relevant to the stowaway for presentation to the appropriate authorities at the port of embarkation, the next port of call, flag State and any subsequent ports. In this respect should be used and completed the following Stowaways Incident Report (See Annex).

4.9.10 If a stowaway should die during the voyage, the authorities at the next port of call, in co-operation with the relevant embassy, will decide how to proceed. However, this practice may vary from country to country Masters and Ship-owners are advised to seek the assistance of the vessel's local agent and to follow the instructions provided by the local authorities and the embassy in question.

4.9.11 For reference and use take into account the *Revised Guidelines on the Prevention of access by Stowaways and the allocation of Responsibilities to seek the successful resolution of the Stowaway cases. (Resolution Fal.11(37) adopted on 9 September 2011)* *(For reference visit Maritime Security Link, IMO Documents).*

4.10. EMERGENCY CONTACT POINTS:

4.10.1 For Maritime Security contact points please refer to the following addresses:

Notification Security Level	securitylevel@amp.gob.pa	+ (507) 501-5368
Emergency contact	authorizations@segumar.com asp@amp.gob.pa or worldwide Segumar Offices	+ (507) 501-5350/48 + (507) 501-5032 + (507) 501-5085
Security Incident Report	isps@amp.gob.pa	+ (507) 501-5085

March, 2024 *– The paragraph order number was updated.*
September, 2023 *- Inclusion of purpose and scope. Supersedes and compiles MMC-368. The paragraph order number was updated.*
June, 2023 *– Inclusion of paragraphs 6.9 and 6.10.*
May, 2023 *– Changes through the MMC and supersedes MMC-124, MMC-125, MMC-126, MMC-128, MMC-206, MMC-223 and MMC-252.*
October, 2022 *– Modification of paragraph 13.*
June, 2022 *– Modification in the subject.*
May, 2022 *– Modification of paragraph 11 and 12.*
December, 2020 *– New paragraph 12 and Change of PMA telephone numbers.*
October, 2019 *– Modification of paragraph 10.*
October, 2019*– Inclusion of a paragraph in point 10 and inclusion of paragraph 16.*
September, 2019 *– Modification on paragraph 10.*
June, 2019 *– Modification paragraph 8 to 12*
November, 2017 *– New Point 3.16, 5 and 6.1*
September 2016 *– Change of paragraph 8*
January, 2016 *– Change of paragraph 8*
July, 2013 *– New Point 6 and 7*
June, 2013 *- Changes all throughout the text*
September, 2003.

Merchant Marine Circular

Inquiries concerning the subject of this Merchant Marine Circular or any other request should be forward to:

Maritime Ships Security Department
Directorate General of Merchant Marine
Panama Maritime Authority

Phone: (507) 501-5085 / 5086
E-mail: isps@amp.gob.pa / securitylevel@amp.gob.pa
Website: https://panamashipregistry.com/circulars/