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-123

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

Subject: **INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE (ISPS CODE)**

Reference: SOLAS 74 /78 Chapter XI-2
ISPS Code Part A and B
MMC 124 MMC 133
MMC 125 MMC 183
MMC 126 MMC 128
MMC 206 MMC 359

1. The International Ship and Port Security Code (ISPS Code) was adopted on December 12, 2002 at a Diplomatic Conference held at the International Maritime Organization (IMO). During this Conference, amendments to SOLAS 74 were also adopted. The ISPS Code and SOLAS amendments are a compilation of international maritime security measures that have a significant impact on the operation of a ship owning companies, ships, their operators, and the port facilities they call on.

2. The Regulation 4 of Chapter XI-2 made the ISPS Code mandatory for ships affected as of 1 July 2004. The Code is made up of two (2) parts. Part A is the mandatory portion of the Code, and Part B is the portion that is recommendatory in nature. Part B was created to provide guidance and information concerning how to implement Part A.

3. DEFINITIONS:

3.1. **ISPS Code:** International Ship and Port Facility Security Code (ISPS) it is consisting of Part A and Part B as adopted by IMO.

3.2. **Contracting Government:** A Government signatory to SOLAS but used more specifically to mean Port State (country) receiving a ship at a port facility.

3.3. **Company:** The owner of the ship or any other organization or person such as the manager, or the bareboat Charterer, who has assumed the responsibility for the operation of the ship from the ship owner and who assuming such responsibility, has agreed to do so in writing.

3.4 **Company Security Officer (CSO):** The person ashore designated by the Company to develop and revise the Ship Security Plan (SSP) and for liaison with the Ship Security Officer (SSO), Port Facility Security Officer

(PFSO) and the Flag Administration.

3.5 **Port Facility Security Officer (PFSO)**: The person at the Port Facility designated by the facility to be responsible for implementation of measures required by the ISPS Code.

3.6 **Port Facility Security Plan (PFSP)**: A plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

3.7 **Security Incident:** Any suspicious act or circumstance threatening the security of a ship, including pirates attack or armed robbery against ships.

3.8 **Security Level:** The qualification of the degree of risk that a security incident will be attempted or will occur.

3.9 **Security Level 1:** The level for which minimum appropriate protective and preventive security measures shall be maintained at all times.

3.10 **Security Level 2:** The level for which appropriate additional protective and preventive measures shall be maintained for a period of time as a result of heightened risk of a security incident.

3.11 **Security Level 3**: The level in which further specific protective and preventive measures shall be maintained for a period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

3.12 **Ship Security Assessment (SSA):** The identification of the possible threats to key shipboard operations, existing security measures and weaknesses in the infrastructure, policies and procedures.

3.13 **Ship Security Plan (SSP):** A plan developed to ensure the application of measures onboard the ship designed to protect persons onboard, the cargo, cargo transport units, ship's store or the ship from the risks of a security incident.

3.14 **Ship Security Officer (SSO):** The person on board the ship accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the SSP and for liaison with the Company Security Officer (CSO) and the Port Facility Security Officer (PFSO).

3.15 **Verification:** The audit of the SSP and its implementation on a ship and associated procedures, checking the operational status of the SSAS and a representative sample of associated security and surveillance equipment and systems mentioned in the SSP.

3.16. **Recognized Security Organization (RSO):** An organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or verification, or an approval or a certification activity, required by SOLAS chapter XI-2 or by part A of the ISPS Code.

4. OBJECTIVES:

4.1 To establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security threats or incidents affecting ships or port facilities used in international trade;

4.2. To establish the respective roles and responsibilities of the Contracting Governments, agencies, local administrations and the shipping and port industries at the national and international level for ensuring maritime security;

4.3 To ensure the early and efficient collection and exchange of security related information;

4.4 To provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels and situations;

4.5. To ensure confidence that adequate and proportionate maritime security measures are in place.

5. In order to achieve its objectives, the ISPS Code embodies a number of functional requirements. These include, but are

not limited to:

5.1. Gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments or authorities;

5.2. Requiring the maintenance of communications protocols for ships and port facilities;

5.3. Preventing unauthorized access to ships, port facilities and their restricted areas;

5.4. Preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;

5.5. Providing means for raising the alarm in reaction to security threats or security incidents

5.6. Requiring ship and port facility security plans based upon security assessments;

5.7 Requiring training, drill and exercise to ensure familiarity with security plans and procedures.

5. MANDATORY COMPLIANCE:

This regulation made the ISPS Code mandatory for ships affected as of 1 July 2004. The Code is made up of two (2) parts. Part A is the mandatory portion of the Code, and Part B is the portion that is recommendatory in nature.

Part B was crafted to provide guidance and information concerning how to implement Part A. It was designed this way to take into account the need to continue to expand and develop guidance on a periodic basis without the need to go through time consuming convention amendment procedures.

6. APPLICATION OF THE ISPS CODE:

6.1 The ISPS Code applies to: All Panamanian flagged ships **engaged on international** voyages:

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

7. The ISPS Code does not apply to:

7.1 Warships, naval auxiliaries or others ships Government non-commercial service
7.2 Cargo ships, including commercial yachts of less than 500 gross tonnage
7.3 Ships not propelled by mechanical means
7.4 Private pleasure yachts not engaged in trade
7.5 Fishing Vessels
7.6 Non-Self propelled mobile offshore drilling units

8. 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 chapter XI-2 or part A of this Code and will be subject to the ISPS verifications specified in section Part A/19.1.1.

9. For those vessels which are currently operating in the Republic of Panama and have applied voluntarily for the ISPS Code and that 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 issue a Statement Letter where we will indicated that the vessel stopped applying voluntarily for the ISPS Code and it will be valid for the period of the validity of the special navigation permit and must be kept on board while the vessel is **operating exclusively in jurisdictional waters of the Republic of Panama**.

10. Starting from the November 1st, 2019, the SSAS exemption must be requested through the online platform E-SEGUMAR at the following website link http://certificates.amp.gob.pa/certificates, for vessels which are currently operating in national waters of the Republic of Panama and have applied voluntarily for the ISPS Code. This authorization will only be issue by the Panama office.

We recommend using Google Chrome, Opera, Mozilla Firefox, Safari and Microsoft Edge.

In the meantime, the following documents shall be submitted to the e-mail address: isps@amp.gob.pa or through any of the SEGUMAR Offices:

a) A formal statement by the Coastal State about vessel's operational area.
b) Statement issued by the RSO indicating the alternative security measures recommended.
c) A copy of the Interim ISSC.
d) Payment Receipt of 300.00 USD (three hundred dollars with 00/100) as per instructed in Resolution J.D. 038-2014.

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.

11. All the Panamanian flagged vessels engaged in international voyages in which the ISPS Code applies or have **applied voluntarily** must have on board a Continuous Synopsis Record (CSR) and International Ship Security Certificate (ISSC) according to the Merchant Marine Circulars 183 and 359.

12. For those Panamanian flag vessels operating in international jurisdictional waters or international coastal voyage they must follow the national regulations of the country where it is operating, in order to comply with the ISPS Code.

13. The ISPS Code related a new type of organization for the purpose of providing verification and certification with respect to the Code. These new organization are called Recognized Security Organizations (RO's), and specific experience and qualification requirements must be met prior to approval by this Administration.

14. According to the Section 8 of Part A of the ISPS Code, it requires the Company Security Officer (CSO) to ensure that, for each ship for which he has security responsibilities, a Security Assessment is carried out by persons with appropriate skill to evaluate the security of a ship, in accordance with ISPS Code and the Merchant Marine Circular 124.

15. 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 and the Merchant Marine Circular 125.

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.

16. The Single Voyage Authorization must be requested through the online platform E-Segumar at the following website http://certificates.amp.gob.pa/certificates and it will be evaluated and processed by the Maritime Ships Security Department in Panama or by any international Segumar offices that the client decides.

The following documents will be submitted through the online platform E-Segumar:

1. RSO statement indicating the departure and arrival port.

This Administration encourage all the companies operators, Company Security Officers and Recognized Security Organization which for further assistance and/or inquiries regarding of this ISPS instructions, must to contact the Maritime

Ships Security Department, at the following email: isps@amp.gob.pa, or through any Segumar Offices.

The instructions regarding the Company Security Officer (CSO) and Ship Security Alert System (SSAS) must be fulfilled as of the publication of this Merchant Marine Circular.

The failure to comply with this Merchant Marine Circular will be communicated to the RSO section in order to be considered a mal practice by the RSO.

Inquiries concerning the subject of this Circular or any other request should be directed to:
Maritime Ships Security Department
Directorate General of Merchant Marine
Panama Maritime Authority

Phone (507)501-5037/5085
Fax (507)501-4202
Email: isps@amp.gob.pa

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

PanCanal Building
Albrook, Panama City
Republic of Panama
Tel: (507) 501-5355 mmc@amp.gob.pa