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-359

To: **Recognized Security Organizations (RSO's), Operators and Company Security Officer (CSO)**

Subject: **GUIDANCE FOR THE IMPLEMENTATION AND CERTIFICATION OF THE ISPS CODE.**

Reference: Implementation of SOLAS Chapter XI-2
International Ship and Port Facility Security (ISPS Code)
Resolution MSC 198(80)
MMC-123 - MMC-124
MMC-125 - MMC-126
MMC-133 - MMC-183
MMC-206 - MMC-252
MMC-346 - MMC-368

This merchant marine circular provides information and guidance, referent to the requirements for compliance with the International Ship and Port Facility Security (ISPS) Code. It also contains the Administration's policies and interpretations regarding application and implementation of the ISPS Code.

Starting January 1st, 2020 all Recognized Security Organizations (RSOs) acting on behalf of the Panama Maritime Administration, described in the **(MMC-131)**, should follow this guidance for the implementation and certification of the ISPS Code on board of Panamanian flag vessels engaged on international voyages.

This circular has been restructured and some ISPS scenarios have been elaborate, for more details you can refer to Annex 1.

1. APPLICABILITY OF THE ISPS CODE

- The International Ship and Port Facility Security Code (ISPS Code), is implemented through chapter XI-2 of the SOLAS. The ISPS Code has two parts, one mandatory (part A) and one recommended (part B).

- The ISPS Code applies to all Panamanian flag vessels engaged on international voyages, as described in the MMC-123.

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

2. RESPONSIBILITY OF THE COMPANIES OPERATOR

- The Companies Operator shall designate a Company Security Officer **(CSO)** and must ensure which company security officer has the Declaration of the CSO duly endorsed by the Panama Maritime Authority, prior to carry out the interim, initial, intermediate or renewal verification.

- For vessel entering the Panamanian registry as of **January 1st, 2018**, must schedule the first SSAS TEST through the use of the new platform, which must be verified by their RSO during the initial verification and from that date onwards, every 12 months the CSO should program the next SSAS test.

- All Companies Operators should maintain a proper communication with the Recognized Security Organization **(RSOs)** to carry out all the ISPS verification during the established window of the ISPS Code Part/A 19.1.

- For the change of Recognized Security Organization (RSO), it will be necessary notify this Administration isps@amp.gob.pa and the gaining society must complete the Notification form for Transfer of ISPS Certification, prior to carry out the verification.

- The gaining society should endorse the existing ISSC in the corresponding window and it certificate will remain fully valid.

- If for a special circumstance the ISPS verification cannot be completed within the established window in the ISPS Code Part A/19.1.1, the company operator should request a Flag Authorization to postpone the ISPS verification prior to the expiration of the interim ISSC or prior to the expiration of due date of intermediate or renewal verifications window in the following website: http://certificates.amp.gob.pa/certificates.

- Every Company shall develop, implement, and maintain a functional SSP aboard its vessels that are in compliance with SOLAS Chapter XI-2 and the ISPS Code.

- The company operator must apply for the Full Term ISSC, after completed the initial or renewal verification, prior to expiration of the ISSC interim or short term ISSC (if applies).

- When the operating company changes their RSO, should request the **Continuous Synopsis Record (CSR),** to update the new Recognized Security Organization responsible of the ISPS certification and must pay the cost of the CSR by amendment, according to the MMC-183.

3. RESPONSABILITIES OF THE COMPANY SECURITY OFFICER (CSO) WITH THE FLAG ADMINISTRATION.

The Company Security Officer **(CSO)** is the direct contact point between the company and this Administration in matters related to the ISPS Code. In case of changes the CSO and/or the alternative CSO, the Ship Security Plans (SSP) must be amended accordingly the details on the new CSO and/or alternate CSO and must have the Declaration of the CSO duly endorsed by the Panama Maritime Authority (PMA) on board the vessel.

The CSO has to comply with the following responsibilities:

- Apply for the Declaration of Company Security Officer **(CSO)** duly endorsed by the Panama Maritime Authority, prior to which the Recognized Security Organization **(RSO)** carried out the interim, initial, intermediate or renewal verification. (MMC-206).

- Coordinate all the ISPS verification with the Recognized Security Organization **(RSOs)** within the established window of the ISPS Code.

- Perform the Annual SSAS Test (according MMC-133)

- Ensure that the name of the CSO and contact details shall be identified in the Ship Security Plan (SSP).

4. RESPONSABILITIES OF THE RECOGNIZED SECURITY ORGANIZATIONS (RSOs)

All Recognized Security Organizations **(RSOs)** acting on behalf of the Panama Maritime Administration (listed in the MMC-131) should maintain a proper communication with the company operator and ensure to make all the necessary arrangements to complete all the ISPS verification during the established window in the ISPS Code Part/A 19.1 and should follow the instructions of this Merchant Marine Circular.

All Recognized Security Organizations **(RSOs)** must verify:

- Verify that the **CSO** designated by the Company Operator, already has the Declaration of Company Security Officer duly endorsed by the Panama Maritime Authority.

- Verify that the vessel has a Continuous Synopsis Record **(CSR)** updated, prior to complete the ISPS verification and the auditor must indicate the number and date of issuance of the Continuous Synopsis Record (CSR) in the Audit Report. In case there is no CSR on board, the auditor must raise an observation in order for the company operator to request the CSR, according to the (MMC-183).

- Check that the SSAS equipment is already configured to the following email account threat@amp.gob.pa, according to the MMC-133.

- Verify the confirmation of the Annual SSAS Test by the Flag and from that date onwards, every 12 months the CSO should program the next SSAS test.

- The Ship Security Plan must be approved before carrying out the initial verification. This Administration does not specify minimum implementation period, however, the company shall ensure that the security measures included in the (SSP) have been in place on the vessel on a sufficient period of time for the Ship Security Officer to develop sufficient evidence documenting implementation before the verification audit taken place.

- For the change of Recognized Security Organization (RSO), it will be necessary notify this Administration isps@amp.gob.pa and the gaining society must complete the Notification form for Transfer of ISPS Certification, prior to carry out the verification.

- The gaining society should endorse the existing ISSC in the corresponding window and it certificate will remain fully valid.

- The RSO which carried out the intermediate verification must submit as soon as possible and no later than 30 days from the date of the audit report, a copy of the ISSC duly endorsed and audit report should be send to us at the following email: isps@amp.gob.pa.

  Note: Failure to comply with this requirement will be considered a bad practice.

- When an interim ISSC is suspended or withdrawn by the Recognized Security Organization (RSO) it must be inform to the following email address: isps@amp.gob.pa.

- For the invalidation of the Full Term ISSC, the Recognized Security Organization **(RSO)** must send us the notification of invalidation to the following email address: isps@amp.gob.pa, in order to this Administration to proceed on cancelling the Full Term ISSC in our system.

5. RESTRICTIONS OF THE RECOGNIZED SECURITY ORGANIZATION (RSOs)

All Recognized Security Organization (RSO) acting on behalf of the Panama Maritime Administration should not by any circumstance:

- Issue a consecutive interim ISSC (without authorization)
- Issue a short term certificate after carried out the initial verification
- Issue the Full Term ISSC
- Issue the Interim ISSC if a Mayor-Nonconformity was found during the ISPS verification and compromises the vessels ability to operate at security levels 1, 2 or 3.
- Set the applicable security level

6. THE ISPS AUDIT REPORT SHOULD AT LEAST CONTAIN THE FOLLOWING INFORMATION:

Each vessel in which Part A of ISPS Code applies shall be subject to verification specified in section 19.1 Part A of the ISPS Code.

The report should include at least the following information:

- Place and date of verification
- Identification of the audit team
- Type of verification (interim/initial/intermediate/renewal/ additional)
- Audit plan
- Company security officer (CSO) name
- Identification of SSO
- Number and date of issuance of the CSR
- SSAS Test Date (verify the Flag confirmation)
- Any observations and possible required action
- Recommendations
- Conclusion

If the Recognizes Security Organization (RSO) found mayor non-conformity on board during the ISPS verification and compromises the security of the vessel, cargo or the crew it should be documented and reported to the CSO and to the Maritime Ship Security Department at isps@amp.gob.pa.

Any failure of security equipment or systems, or suspension of a security measure that does not compromise the ship's ability to operate at security levels 1 to 3 shall be reported without delay to the Maritime Ship Security Department with details of the equivalent alternative security measures the vessel is applying, until the failure or suspension is rectified together with an action plan specifying the timing of any repair or replacement.

7. TYPES OF ISPS VERIFICATION AUDIT

- Interim Verification: short period allowed for implementation on board newly operated vessels, where the Recognized Security Organization must verify vessel´s compliance with provisions of the ISPS Code A/19.4.2

- Initial Verification: when the vessel is in compliance with all the ISPS requirements the section 19.1, or before the required certificate under section 19.2 is issued for the first time.

- Intermediate Verification: is carried out between the dates of second and third anniversary of the issuance of the Full Term ISSC, according to the ISPS Code Part A, Rules 19.1.1.3

- Renewal verification: renewal verification audits shall take place at intervals not exceeding five (5) years and should be carried out within three (3) month before or after the expiring date of the certificate.

- Additional Verification: shall be conducted at request of this Administration, Port State Control Authorities and at any case described in the item 9.

8. TYPES OF ISSC CERTIFICATES

8.1 **Interim ISSC:** A certificate that may be issued after 1st July 2004, to a vessel which has newly joined under management of a Company, or which has changed Flag. This certificate must identify with the nomenclature "Interim" and the validity should **not to exceed more than six (6) months.** The Interim ISSC shall be issued in a form corresponding to the template given in the Appendix 2, of the ISPS Code.

8.2 **Full Term ISSC** : Full term ISSC **shall be issued only by the Panama Maritime Authority (PMA)** after the vessel has successfully completed an initial or renewal verification in compliance with the applicable requirements of Chapter XI-2, ISPS Code Parts A, relevant provisions of Part B and additional flag requirements, for a period of up to five **(5)** years from the date of successful completion of the initial or renewal verification Audit. During this time the original certificate must remain on board the vessel.

8.3 **Short Term ISSC** : A certificate issued after renewal verification audit. This certificate must be identified with the nomenclature **"Short Term"** when applies and the validity should not exceed more than five (5) months.

9. ISPS CERTIFICATION

9.1 The interim ISSC only will be issued if the RSO previously verified that the vessel is in compliance with provisions of the **ISPS Code A/19.4.2** and for the following purposes:

- A vessel without a certificate, on delivery or pior to its entry or re-entry into service
- For a Change of Flag
- when a Company newly commences management of the vessel

The initial verification must be carried out within the period of validity of the interim certificate, in compliance with provisions of the **ISPS Code A/19.1.1.**

This Administration does not authorize the issuance of a **SHORT TERM CERTIFICATE** or a consecutive **INTERIM ISSC** after having the initial verification taken place.

9.2 Once the **INITIAL VERIFICATION** has been carried out, the operator company must apply for the issuance of the Full Term ISSC, through the website: http://certificates.amp.gob.pa/certificates, only issued by the Panama Maritime Authority (PMA).

Starting January 1st, 2020, the Panama Maritime Authority (AMP) will issue the International Ship Security Certificate (Full Term ISSC) with the same type of vessel **as indicated in the Safety Management Certificate (SMC)** issued by the RO.

(*) Insert the type of ship from among the following: passenger ship, passenger high-speed craft; cargo high-speed craft; bulk carrier; oil tanker; chemical tanker; gas carrier; mobile offshore drilling unit; other cargo ship.

9.3 INTERMEDIATE VERIFICATION:

9.3.1 During the validity of the Full Term ISSC at least one intermediate verification will be performed**,** between the dates of the second and third anniversary of the issuance of the Full Term ISSC, according to the ISPS Code Part A, Rules 19.1.1.3

9.3.2 The Company Security Officer, or Company Operator shall contact the Recognized Security Organization (RSO) who carried out the initial verification on which the full term ISSC is based, to carry out the intermediate verification on board within the established window and the surveyor or auditor must endorse the verification in the existing ISSC.

9.3.3 In case a Ship-owner or Company Operator decides not to use the RSO that performed its initial verification (for the purpose of getting an intermediate verification), it will be necessary notify this Administration isps@amp.gob.pa and the gaining society must complete the following document for the change of RSO, prior to carry out the verification and follow the instructions indicated in the **(ANNEX 1).**

9.3.4 The Recognized Security Organization which performing the intermediate verification must submit as soon as possible but no later than 30 days from date of verification the following documents at: isps@amp.gob.pa

- Copy of the Full Term ISSC duly endorsed in the corresponding space.
- Audit Report

9.4 RENEWAL VERIFICATION

9.4.1 The renewal verification audits shall take place at intervals not exceeding five (5) years, if the renewal verification is completed within three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiration of the existing certificate.

9.4.2 When the renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

9.4.3 When the renewal verification is completed more than three months before the expiry date of the existing certificate, the new certificate shall be valid from the of completion of the renewal verification to date not exceeding five years from the date of completion of the renewal verification.

9.4.4 The Recognized Security Organization may issue a **SHORT TERM ISSC,** after performing the renewal verification or endorse the existing certificate and such certificate shall be accepted as valid for a futher period which shall not exceed five (5) months from the expiry date, in order for the company operator must apply for the Full Term ISSC, before the expiration of the Short Term ISSC or endorsement of the Full Term ISSC.

10. PROCEDURES TO REQUEST AUTHORIZATION TO POSTPONE ISPS VERIFICATION AUDIT.

If for a special circumstance the ISPS verification (Initial, Intermediate or Renewal Verification) cannot be completed within the established window as indicated in the ISPS Code Part A/19.1.1, the operator company, owners, recognized security organization or legal representatives should request an authorization to postpone the verification audit prior to the expiration of the interim ISSC or prior to the expiration of due date of the intermediate or renewal verifications window through the online platform E-Segumar at the following website http://certificates.amp.gob.pa/certificates and shall submit the following documents:

- Email or letter issued by the RSO indicating the reason for not performing the verification and stating the exact date and place where the ISPS Verification will take place.
- Interim ISSC only if the extension requested is due to the initial verification.
- ISSC Full term dully endorsed or intermediate verification report if the extension requested is to carry out the renewal verification.

Once the verification is done, the Recognized Security Organization should send us a copy of the report to the following email: isps@amp.gob.pa

- ISPS Audit Report
- Copy of the ISSC with endorsement when is applicable.

10.1 This authorization will be granted for a period no longer than 3 months and this Administration does not authorize to issuance of a second interim ISSC after granting an ISPS authorization.

These authorization are free and will be sent to the applicant and (RSO) in electronic form, with Digital Signature, Stamp and QR Code and must be kept on board at all time together with the ISSC (interim or Full Term), for reference of the maritime authorities with the specification posted in the MMC 368.

AFTER CARRIED OUT THE ISPS VERIFICATION, PLEASE PROCEED ACCORDING TO THE FOLLOWING SCENARIOS:

a) If the extension was granted to postpone the Initial Verification, the Company Operator must apply immediately for the Full term ISSC, prior to the expiration of the ISPS authorization granted through the online platform E-Segumar.

b) If the extension was granted to postpone the Intermediate Verification, the RSO must endorse the existing ISSC and shall indicate the authorization number granted, which authorizes them to carry out the intermediate verification out of time frame.

c) If the ISPS extension was granted to postpone the Renewal Verification, the RSO may issue a short term certificate, valid for 5 months, after performed the renewal verification.

d) If for any circumstance the verification cannot be completed during the period granted, the user must to request another authorization prior to the expiration date, in order to be granted by the same office that issued the previous one (reference item 10.1).

11. ADDITIONAL AUDIT AUTHORIZATION

Starting January 1st, 2020, this Administration inform all Recognized Security Organizations (RSOs) that will not be necessary request an authorization to carry out the additional audit for the following cases.

- Change of vessel name
- Change of tonnage
- Change of type of vessel
- (*) PSC detention (it will be necessary send us the PSC report and Audit report immediately) at isps@amp.gob.pa

For those cases it will be necessary request an additional authorization through the following website http://certificates.amp.gob.pa/certificates.

- Flag State detention
- Security Incident (Stowaways)
- To verify effective corrective actions were taken regarding any major nonconformity.
- When substantial modifications have been made to the SSP.
  When the Administration considers it necessary to request an additional audit in view of the nature of any Non-conformity regarding of the SSP.

The Full Term ISSC shall be endorsed upon successful completion of the additional audit by the Recognized Security Organization (RSO).

12. TRANSFER OF SECURITY MANAGEMENT SYSTEM CERTIFICATION (CHANGE OF RSO)

a) **Starting January 1st, 2020** all Recognized Security Organizations (RSOs) should notify the change of RSO to this Administration isps@amp.gob.pa and complete the Notification form for Transfer of ISPS Certification.

b) After the vessel has successfully completed the verification, the surveyor or auditor must endorse the existing ISSC on board and it will not be necessary to reissue the certificate by the Panama Maritime Authority.

c) It will be necessary that the Recognized Security Organization send us copy of the audit report and the ISSC duly endorsed to the following email isps@amp.gob.pa, in order to update the new Recognized Security Organization (RSO) responsible of the ISPS certification on board.

If the transfer of Security Certification occurs during the annual, intermediate or renewal window, the RSO should proceed according to the provisions described in the **(ANNEX 1).**

13. SHIP OUT OF SERVICE MORE THAN SIX (6) MONTHS (RE-ENTRY INTO SERVICES)

If the ship is out of service for more than six months, an interim verification as required by the ISPS Code A/19.4.2 and follow the instruction described in the **(ANNEX 1).**

14. OVERDUE INTERMEDIATE VERIFICATION

In case of the intermediate verification was not carried out within the established window this Administration may consider the revalidation of the ISSC to carry out the intermediate verification out of window but it should not have been more than 6 months from the closing of the intermediate window.

The Recognized Security Organization must request a Flag authorization through our website http://certificates.amp.gob.pa/certificates, to carry out the intermediate verification out of window.

It will be necessary that the surveyor or auditor on board writes down "This certificate was revalidated" in accordance with PMA authorization granted.

15. HARMONIZATION OF ISM/ISPS CERTIFICATION

The harmonized ISM/ISPS audit reduces the number of auditor/inspector visits onboard which saves valuable time and personnel resources while still ensuring regulatory compliance. This Administration recognizes the harmonization system.

Upon successful completion of the harmonized audit, the SMC and ISSC will be issued with the same issuance and expiry dates and the company operator must apply for the Full Term ISSC, according to the provisions described in the **(ANNEX 1).**

16. CHANGES DURING THE VALIDITY OF THE INTERIM ISSC

The RSO shall issue an interim ISSC with the same validity as the existing certificate if the vessel changes any of the following information:

a) When the name of vessel changes
b) When the tonnage changes
c) When the physical address of the operator company changes
d) When the name of the operator company changes
e) When the type of vessel changes

17. CHANGES DURING THE VALIDITY OF THE FULL TERM ISSC

If the vessel changes any of the following information below described during the validity of the Full Term ISSC the RSO shall issue a **short term ISSC** valid for (5) months and afterwards this Administration will issue the Full Term ISSC with the same validity as the existing certificate. When the following conditions are given:

a) When the name of vessel changes
b) When the tonnage changes
c) When the physical address of the operator company changes
d) When the name of the operator company changes
e) When the type of vessel changes

18. EXPIRED CERTIFICATE PRIOR TO REQUEST THE FULL TERM ISSC

In those cases where the RSO has completed the ISPS verification within the established period of the ISPS Code and the company operator applies for the full term ISSC, after the expiration of the interim ISSC or short term; this Administration will issue the Full Term ISSC with a validity of less than 5 years, taking as reference the expiry date of the ISSC with the request date.

19. NOTIFICATION OF INVALIDATION OF ISSC CERTIFICATE

The Interim ISSC may only be invalidated at the determination of the **RSO** and the Full Term ISSC will only be canceled by the **Panama Maritime Authority** (PMA), through the notification of invalidation sent to this Administration isps@amp.gob.pa

An existing certificate shall become invalid when, but is not limited to, the following deficiencies:

- When a vessel has not undergone the periodical Audit (initial, intermediate or renewal verification).
- When a Company cease managing the ship
- When a ship changes her Flag
- When an ISSC is issued to replace an interim ISSC
- When a Company requests withdrawal of the ship from the ISPS Register.
- A part of the SSP which requires approval upon amendment has been amended without approval
- Corrective actions for non-compliance set out at the Audit have not been completed within the agreed period of time
- When a vessel is not operated in compliance with the Rule requirements
- The vessel failure to maintain its Ships Security Plan in compliance with the requirements of the ISPS Code.
- Any other notification of invalidation described by the RSO

20. ISPS CERTIFICATION GUIDANCE (SCENARIOS) AND REQUIEREMENTS FOR THE ISSUANCE OF THE FULL TERM ISSC. (ANNEX 1)

From January 1st, 2020 the following Merchant Marine Circular (MMC) 205 it will cancel, to more reference, please see the **ANNEX 1**.

For further assistance and/or inquiries please note the following contact points:

A. Maritime Ships Security Department
Phone: +507-501-5037/5086
E-mail address: isps@amp.gob.pa

B. SEGUMAR Panama (Evenings, Weekends and Holidays)
Phone: +507-501-5350/48 or +507-501-5032
E-mail address: authorizations@segumar.com

December 2019 – Modification of the item 9.2 and item 5, 9, 12 and 17 of the Annex 1.
October 2019 – Change of the MMC subject and Restructuring of the numerical sequence and modification paragraph 8,9, 10, 11,12,13,14
June 2019 - Including Annex of Application for SSAS Exemption Certificate.
March, 2019 - Modification of paragraph 7 and 9 and new paragraph 9.1, 14, 20.1 and 21
January, 201 - Inclusion of paragraphs 19 and 20
December, 2018 - modification of paragraph 18 point 4.
December, 2018 - Modification and new paragraphs of item 11, 17 and 19
February, 2018 - inclusion of new paragraphs 2.10, modification of item 8 to 9 and 12
November - 2017