ISPS Technical Notice No.06/2017

DATED: 05.12.2017

SUBJECT:

PANAMA CIRCULAR MMC-359
INSTRUCTIONS AND PROCEDURE FOR THE IMPLEMENTATION AND CERTIFICATION OF THE ISPS CODE.

TO: INSB AUDITORS/MANAGING COMPANIES

Starting from April 1st, 2018 all the Companies Operators and Recognized Security Organizations shall follow present PMA circular.

For your easy reference we have included below the main points of the circular, however in any case reference should be made to the original circular itself.

RESPONSIBILITY OF THE COMPANY OPERATOR

Company Security Officer **(CSO)** has already the **Declaration of the CSO duly endorsed** by the Panama Maritime Authority

For ships to enter the Panamanian registry as of **January 1st, 2018**, they 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.

If for a special circumstance the ISPS verification cannot be completed within the window established in the ISPS Code Part A/19.1.1, the company operator **must request an ISPS authorization issued by this Administration** 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.

Every Company shall develop, implement, and maintain a functional SSP aboard its ships that is compliant 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, and submit all the requirements of the MMC-205, prior to expiration of the ISSC interim or short term ISSC.

RESPONSIBILITIES OF THE COMPANY SECURITY OFFICER (CSO)

The Company Security Officer **(CSO)** is the direct contact point between the company and this Administration in cases of matters related to the ISPS Code.

The name of the Company Security Officer **(CSO)** and contact details shall be identified in the Ship Security Plan **(SSP).**

Apply for the Declaration of Company Security Officer **(CSO)** duly endorsed by the Panama Maritime Authority, prior any **RSO** verification.

Coordinate timely initial, Intermediate and Renewal verifications.

RESPONSIBILITIES OF THE RECOGNIZED SECURITY ORGANIZATIONS (RSOs)

The recidivism of overdue certificates or overdue verification audit windows will be considered mal practice by the RSO, if not notified in a timely manner.

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

1. Verify that the **CSO** has the **Declaration of Company Security Officer duly endorsed by PMA**, and the auditor shall indicate the full name of the CSO in the Audit Report, prior to issue or endorsement of any certificate.

2. Verify that the ship 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).

3. The RSO who carried out the interim verification must **verify during the initial verification that the SSAS system is working properly**, and **shall performing a real TEST** and sending it to threat@amp.gob.pa, and the Maritime Ships Security Department will confirm the reception of the same in the date scheduled in the Electronic Platform, according to the instruction of the (MMC-133) and from that date onwards, **every 12 months the CSO should program the next SSAS test.**

4. 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 insure that the security measures included in the (SSP) have been in place on the ship a **sufficient period of time for the Ship Security Officer to develop sufficient evidence** documenting implementation before the verification audit is carried out.

5. When the companies' operator decides to **change their Recognized Security Organization (RSO), the new RSO must inform immediately the Administration** at the

following email address: isps@amp.gob.pa, prior to re-initiate the ISPS process and issue the interim ISSC or endorse the Full Term ISSC.

6. The RSO which carried out the inter**mediate 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** at the following email: isps@amp.gob.pa

7. When an interim **ISSC is suspended or withdrawn** by the Recognized Security Organization (RSO) it must **inform the Administration** at the following email address: isps@amp.gob.pa, and the **RSO** must indicate the reasons why the certificate was invalidated, in order for this Administration to update the information in our system.

8. For **invalidation of the Full Term ISSC**, the Recognized Security Organization **(RSO)** must send us a **notification** of invalidation at the following email address: isps@amp.gob.pa, in order for the Panama Maritime Authority to proceed to cancel the Full Term ISSC in our system.

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:

1. Set the applicable security level
2. Issue a consecutive interim ISSC
3. **Issue a short term certificate after carried out the initial verification**
4. Issue the Full Term ISSC
5. **Issue the Interim ISSC if any ISPS deficiency** was found during the ISPS verification and **compromises** the ship´s ability to operate at security levels 1, 2 or 3.

THE ISPS AUDIT REPORT AT LEAST SHOULD TO CONTAIN THE FOLLOWING INFORMATION

The report should include at least the following information:

1. Place and date the verification
2. Identification of the audit team
3. Type of verification (interim/initial/intermediate/renewal/ additional)
4. Audit plan
5. Company security officer (CSO) name

6. Identification of SSO
7. Number and date of issuance of the CSR
8. Any observations and possible required action
9. Recommendations
10. Conclusion

The INSB Form 1215225 SEC5 "Shipboard Security Audit Log" Rev.03 covers all the above requested inputs.

Interim verification

The RSO must verify during the interim verification the following items:

1. The Company Security Officer **(CSO)** has already the Declaration of company security officer **duly endorsement by the PMA**, according to the (MMC-206).
2. The **name** of the Company Security Officer **(CSO)** must be **identified** in the ISPS Audit **Report.**
3. Verify if the vessel has a Continuous Synopsis Record **(CSR)** updated on board.

In case the company operator decides to ch**ange RSO during the validity of the ISSC interim**, the **ISPS process must re-initiate again with the interim verification** and the new RSO which will carry out the interim verification, should **have previous authorization of the Administration** and must carry out the Initial verification during the validity of the interim ISSC.

Initial Verification

The Administration **does not authorize the issuance of a SHORT TERM CERTIFICATE** or a consecutive interim ISSC after having carried out the Initial Verification.

A Full term ISSC will NOT be issued when:

1. When the SSP has not been approved before to carry out the Initial Verification
2. When the technical equipment specified in the SSP is not 100% operative
3. When there is sufficient objective evidence found through the verification audit that the ship is not operating in accordance with the provisions of the approved SSP

4. If the Company Security Officer (CSO) designated by the company, does not have already the Declaration of company security officer duly endorsed by the Panama Maritime Authority.

5. If the name of the Company Security Officer was not identified in the ISPS audit Report 6. If the interim ISSC or Short Term has not been identified with the correct nomenclature

6. When the ship does not comply with all the Requirements of the MMC-205

Intermediate verification

In case a Ship-owner or Company Operator decides not to use the RSO that carried out its initial verification (for the purpose of getting in intermediate verification), it will be necessary that the new Recognized Security Organization **(RSO)** contacts the Administration and request an authorization to **carry out the intermediate verification with scope of an initial verification.**

The RSO carrying out the intermediate verification must submit as soon as possible but no later than 30 days from date of verification to the Maritime Security Department the following documents at: isps@amp.gob.pa

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

Renewal verification

1. **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.

2. 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 expiry of the existing certificate.

3. When the renewal verification is completed after the expiry date of the existing certificate three months audit is carried out later than the three (3) months prior to the expiry date, the new certificate shall be issued from the completion date of the renewal verification audit.

4. 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.

5. This Administration authorizes only the issuance of a **Short Term ISSC** after carried out the Renewal Verification and the company operator must apply for the Full Term ISSC, before the expiration of the Short Term ISSC.

NON-CONFORMITIES AND ADDITIONAL VERIFICATIONS

An **ISSC will not be issued if there are any ISPS Code deficiencies**. Deficiencies identified during the verification audit shall 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 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 ship is applying until the failure or suspension is rectified together with an **action plan** specifying the timing of any repair or replacement.

The **Additional verifications shall be conducted with previous authorization** of the Administration in the following cases, and it must be requested at the following email isps@amp.gob.pa

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

For the following cases, the Recognized Security Organization (RSO) may carry out the following verification:

1. For Change of tonnage (verification on board or documentary verification)

2. For Change of vessel name (verification on board or documentary verification)

PROCEDURES TO POSTPONE ISPS VERIFICATION AUDIT

If for a special circumstance the ISPS verification cannot be completed within the windows as indicated in the ISPS Code Part A/19.1.1, the Company Operator may 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 the intermediate or renewal verifications window.

The following documents shall be submitted at isps@amp.gob.pa, in order to evaluate the ISPS request and proceed with the issuance of ISPS authorization.

1. Email or letter issued by the RSO indicating the reason for not having carried out the verification and stating the exact date and place where the ISPS Verification will take place.
2. Interim ISSC only if the extension requested is due to the initial verification.
3. ISSC Full term if the extension requested is due to the intermediate or renewal verification.

This authorization will be granted for a period **no longer than 3 months**, and during the period requested the Recognized Security Organization **(RSO)** must carry out the ISPS verification.

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 in the website link: http://certificates.amp.gob.pa/certificates.

If the extension was granted to postpone the **intermediate verification**, the RSO must endorsed the Full term ISSC and shall **indicate the ISPS authorization number** granted, which authorizes them to carry out the intermediate verification out of the window.

If the ISPS extension was granted to postpone the **Renewal Verification**, the RSO may issue a short term certificate, valid for 5 months, after having carried out the renewal verification.

The ISPS authorization granted by this Administration must be kept on board at all time together with the ISSC (interim or Full Term), for reference of the maritime authorities.

TRANSFER OF SECURITY MANAGEMENT SYSTEM CERTIFICATION

This Administration recognizes the IACS agreement for the transfer of the ISPS certification (PR-18).

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:

1. When the name of vessel changes
2. When the tonnage changes
3. When the physical address of the operator company changes
4. When the name of the operator company changes
5. When the type of vessel changes

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:

1. When the name of vessel changes
2. When the tonnage changes
3. When the physical address of the operator company changes
4. When the name of the operator company changes
5. When the type of vessel changes

SHIP MORE THAN SIX (6) MONTHS OUT SERVICES

If the ship is out of service for more than six months, the Recognized Security Organization (RSO) must re-initiate the ISPS certification process with the interim verification as required by the ISPS Code A/19.4.2 and issue an interim ISSC, with **previous notification of the Administration.**

OVERDUE ISPS VERIFICATION

If the ISPS verification is not carried within the established window, the certificate will be invalid and the RSO shall inform to the Flag Administration immediately at the following email: isps@amp.gob.pa, in order to cancel the Full Term ISSC in our data base and the ISPS process needs to be **re-initiate with the interim verification**, with previous authorization of this Administration.

EXPIRED CERTIFICATE PRIOR TO REQUEST THE FULL TERM ISSC

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

From April 1st, 2018 the following Merchant Marine Circular (MMC) 145, 207 and 326 will be cancelled.

P. Klavdianos
Marine Management
Systems Certification Division

INSB Class
International Naval Surveys Bureau

Attachment

PMA Circular MMC-359 – *open online* -

Instructions and Procedure for the implementation and certification of the ISPS Code.

PANAMA MARITIME AUTHORITY

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

MERCHANT MARINE CIRCULAR MMC-359

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

Subject: Instructions and Procedure for the implementation and certification of the ISPS Code.

Reference: Amendment to SOLAS Chapter XI-1, Regulation 5
Resolution MSC 198(80)
ISPS Code
MMC-123 - MMC-126 - MMC-206
MMC-124 - MMC-131 - MMC-252
MMC-125 - MMC-133 - MMC-346

Starting from April 1st, 2018 all the Companies Operators and Recognized Security Organizations (RSOs) acting on behalf of the Panama Maritime Administration **(MMC-131)**, shall follow these instructions and procedures to carry out the verification audit process for the correct implementation and certification of the ISPS Code on board of the Panamanian flagged vessels engaged on international voyages.

In order to comply with the following instructions please refer to the Merchant Marine Circulars, 123, 123,124, 125, 126, 131, 133, 206 and 346.

This Administration kindly requests that any ISPS authorization or flag confirmation, is requested directly to our Head office in Panama, in the Maritime Ships Security Department at the following email: isps@amp.gob.pa, however, please take into account that your ISPS requests must be made in advance and taking in consideration our work schedule (weekdays 08:30-16:30 hrs).

1. APPLICABILITY OF THE ISPS CODE

1. 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 recommendatory (part B).

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

3. 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.

2. RESPONSIBILITY OF THE COMPANY OPERATOR

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

2. For ships to enter the Panamanian registry as of **January 1st, 2018**, they 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.

3. 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.

4. If for a special circumstance the ISPS verification cannot be completed within the window established in the ISPS Code Part A/19.1.1, the company operator **must** request an ISPS authorization issued by this Administration 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.

5. Every Company shall develop, implement, and maintain a functional SSP aboard its ships that is compliant with SOLAS Chapter XI-2 and the ISPS Code.

6. The company operator **must apply for the Full Term ISSC**, after completed the initial or renewal verification, and submit all the requirements of the MMC-205, prior to expiration of the ISSC interim or short term ISSC (when applies).

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 cases of matters related to the ISPS Code. In case of changes to the CSO and/or the alternate CSO, the Ship Security Plans (SSP) must be amended accordingly to contain the details of 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 of the vessel.

The name of the Company Security Officer **(CSO)** and contact details shall be identified in the Ship Security Plan **(SSP).**

The CSO has to comply with the following responsibilities:

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

2. Coordinate the initial, Intermediate and Renewal verifications of the ship with the Recognized Security Organization **(RSOs)** within the established window of the ISPS Code, in order to avoid re-initiate again the ISPS certification process with the interim verification.

4. RESPONSABILITIES OF THE RECOGNIZED SECURITY ORGANIZATIONS (RSOs)

All Recognized Security Organizations **(RSOs)** acting on behalf of the Panama Maritime Administration (listed on 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 windows in the ISPS Code Part/A 19.1 and the instructions of this Merchant Marine Circular.

The recidivism of overdue certificates or overdue verification audit windows will be considered mal practice by the RSO, if not notified in a timely manner.

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

1. Verify that the **CSO** designated by the Company Operator, already has the Declaration of Company Security Officer duly endorsed by the Panama Maritime Authority, during the interim, initial, intermediate and renewal verification, and the auditor shall indicate the full name of the CSO in the Audit Report, prior to issue the ISSC interim or endorsement the Intermediate verification or complete the renewal verification.

2. Verify that the ship 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).

3. The RSO who carried out the interim verification must verify during the initial verification that the SSAS system is working properly, and shall performing a real TEST and sending it to threat@amp.gob.pa, and the Maritime Ships Security Department will confirms the reception of the same in the date scheduled in the Electronic Platform, according to the instruction of the (MMC-133) and from that date onwards, every 12 months the CSO should program the next SSAS test.

4. 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 insure that the security measures included in the (SSP) have been in place on the ship a sufficient period of time for the Ship Security Officer to develop sufficient evidence documenting implementation before the verification audit is carried out.

5. When the companies' operator decides to change their Recognized Security Organization **(RSO)**, the new **RSO** must inform immediately this Administration at the following email address: isps@amp.gob.pa, prior to re-initiate the ISPS process and issue the interim ISSC or endorse the Full Term ISSC.

6. 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 at the following email: isps@amp.gob.pa

7. When an interim ISSC is suspended or withdrawn by the Recognized Security Organization (RSO) it must inform this Administration at the following email address: isps@amp.gob.pa, and

the **RSO** must indicate the reasons why the certificate was invalidated, in order for this Administration to update the information in our system.

8. For invalidation of the Full Term ISSC, the Recognized Security Organization **(RSO)** must send us a notification of invalidation at the following email address: isps@amp.gob.pa, in order for the Panama Maritime Authority to proceed to cancel 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:

1. Set the applicable security level
2. Issue a consecutive interim ISSC
3. Issue a short term certificate after carried out the initial verification
4. Issue the Full Term ISSC
5. Issue the Interim ISSC if any ISPS deficiency was found during the ISPS verification and compromises the ship´s ability to operate at security levels 1, 2 or 3.

6. TYPES OF ISPS VERIFICATION AUDIT

1. 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**

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

3. 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

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

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

7. THE ISPS AUDIT REPORT AT LEAST SHOULD TO CONTAIN THE FOLLOWING INFORMATION

Each ship to 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:

1. Place and date the verification
2. Identification of the audit team
3. Type of verification (interim/initial/intermediate/renewal/ additional)
4. Audit plan

5. Company security officer (CSO) name
6. Identification of SSO
7. Number and date of issuance of the CSR
8. Any observations and possible required action
9. Recommendations
10. Conclusion

8. TYPES OF ISSC CERTIFICATES

1. **Interim ISSC:** A certificate that may be issued after 1st July 2004, to a ship which has newly joined under management of a Company, or which has changed her Flag. This certificate must 8410330identify with the nomenclature "Interim" and the validity should **not 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.

The interim ISSC will only 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:

- New ships on delivery
- Transfer from another Flag
- when a Company newly commences management of the ship

The RSO must verify during the interim verification the following items:

1. The Company Security Officer **(CSO)** designated by the company, has already the Declaration of company security officer duly endorsement by the Panama Maritime Authority, according to the (MMC-206).

2. The name of the Company Security Officer **(CSO)** must be identified in the ISPS Audit Report.

3. Verify if the vessel has a Continuous Synopsis Record **(CSR)** updated on board.

The RSO and the Company Operator should ensure to make all the necessary arrangements to complete the **initial verification** prior to the expiration of the interim ISSC.

This Administration **does not authorize the issuance of a SHORT TERM CERTIFICATE** or a consecutive interim ISSC after having carried out the Initial Verification.

In case the company operator decides to change RSO during the validity of the ISSC interim, the ISPS process must re-initiate again with the interim verification and the new RSO which will carry out the interim verification, should have previous authorization of this Administration and must carry out the Initial verification during the validity of the interim ISSC.

This Administration does not authorize to issue a consecutive interim ISSC to a ship if, in the judgment of the Administration, one of this purposes of the ship or company is requesting such certificate to avoid full compliance with chapter XI-2 and this Part of the code beyond the period of the interim certificate as specified.

2. **Full Term ISSC** : Full term ISSC **shall be issued only by the Panama Maritime Authority (PMA)** after the ship 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.

The Maritime Ship Security Department or any Segumar Offices will issue the Full Term ISSC, with the same type of ship as indicated in the interim ISSC or Short Term (when applicable) issued by the RSO and the same type of ship must be identified in the Ship Security Plan.

A Full term ISSC will **NOT** be issued when:

1. When the SSP has not been approved before to carry out the Initial Verification
2. When the technical equipment specified in the SSP is not 100% operative
3. When there is sufficient objective evidence found through the verification audit that the ship is not operating in accordance with the provisions of the approved SSP
4. If the Company Security Officer (CSO) designated by the company, does not have already the Declaration of company security officer duly endorsed by the Panama Maritime Authority.
5. If the name of the Company Security Officer was not identified in the ISPS audit Report
6. If the interim ISSC or Short Term has not been identified with the correct nomenclature
7. When the ship does not comply with all the Requirements of the MMC-205

Intermediate verification:

1. During the validity of the Full Term ISSC at least one intermediate verification will be carried out by approved **RSO,** 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

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 window established.

3. In case a Ship-owner or Company Operator decides not to use the RSO that carried out its initial verification (for the purpose of getting in intermediate verification), it will be necessary that the new Recognized Security Organization **(RSO)** contacts the Administration and request an authorization to **carry out the intermediate verification with scope of an initial verification**, at the following email address: isps@amp.gob.pa, in order to know who is the new Recognized Security Organization **(RSO)** responsible of the ISPS system of the vessel and update our system.

4. If the Recognized Security Organization **(RSO)** was canceled from the MMC-131, the company operator must to contact another RSO, however, the new Recognized Security Organization (RSO) must contact the Administration and **request an authorization to carry out the intermediate verification with scope of an initial verification,** at the following email address: isps@amp.gob.pa, in order to know who is the new Recognized Security Organization (RSO) responsible of the ISPS system of the vessel and update our system.

5. The ISSC shall be endorsed upon successful completion of an intermediate audit by the Recognized Security Organization (RSO) or by the Panama Maritime Authority at the request of the company operator.

6. The RSO carrying out the intermediate verification must submit as soon as possible but no later than 30 days from date of verification to the Maritime Security Department the following documents at: isps@amp.gob.pa

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

Renewal verifications:

1. **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.

2. 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 expiry of the existing certificate.

3. When the renewal verification is completed after the expiry date of the existing certificate three months audit is carried out later than the three (3) months prior to the expiry date, the new certificate shall be issued from the completion date of the renewal verification audit.

4. 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.

5. This Administration authorizes only the issuance of a **Short Term ISSC** after carried out the Renewal Verification and the company operator must apply for the Full Term ISSC, before the expiration of the Short Term ISSC.

9. NON-CONFORMITIES AND ADDITIONAL VERIFICATIONS

An ISSC will not be issued if there are any ISPS Code deficiencies. Deficiencies identified during the verification audit shall 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 ship is applying until the failure or suspension is rectified together with an action plan specifying the timing of any repair or replacement.

The Additional verifications shall be conducted with previous authorization of this Administration in the following cases, and it must be requested at the following email isps@amp.gob.pa

1. PSC detention
2. Flag State detention
3. Security Incident (Stowaways)
4. When substantial modifications have been made to the Shipboard SMS or SSP.
5. To verify effective corrective actions were taken regarding any major nonconformity.
6. 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).

For the following cases, the Recognized Security Organization (RSO) may carry out the following verification:

1. For Change of tonnage (verification on board or documentary verification)
2. For Change of vessel name (verification on board or documentary verification)

10. 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 issue and expiration dates and the company operator must apply for the Full Term ISSC, according to the requirement of the MMC-205.

11. PROCEDURES TO POSTPONE ISPS VERIFICATION AUDIT

This Administration encourages owners, operators and RSOs to complete the initial, intermediate and renewal verification during the period established in section A/19.1 and 19.4.4. 4 and the instructions of this Merchant Marine Circular.

If for a special circumstance the ISPS verification cannot be completed within the windows as indicated in the ISPS Code Part A/19.1.1, the Company Operator may 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 the intermediate or renewal verifications window.

The following documents shall be submitted at isps@amp.gob.pa, in order to evaluate the ISPS request and proceed with the issuance of ISPS authorization.

1. Email or letter issued by the RSO indicating the reason for not having carried out the verification and stating the exact date and place where the ISPS Verification will take place.

2. Interim ISSC only if the extension requested is due to the initial verification.

3. ISSC Full term if the extension requested is due to the intermediate or renewal verification.

This authorization will be granted for a period no longer than 3 months, and during the period requested the Recognized Security Organization **(RSO)** must carry out the ISPS verification.

Once the ISPS verification is carried out, the Recognized Security Organization should send us the following documents:

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

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 in the website link: http://certificates.amp.gob.pa/certificates.

If the extension was granted to postpone the **intermediate verification**, the RSO must endorsed the Full term ISSC and shall indicate the ISPS authorization number granted, which authorizes them to carry out the intermediate verification out of the window.

If the ISPS extension was granted to postpone the **Renewal Verification**, the RSO may issue a short term certificate, valid for 5 months, after having carried out the renewal verification.

The ISPS authorization granted by this Administration must be kept on board at all time together with the ISSC (interim or Full Term), for reference of the maritime authorities.

This Administration does not authorize to issue a second interim ISSC.

This Administration requests all Company Operators and RSO to avoid requesting for ISPS authorization for more than 3 months. These cases will be evaluated case by case.

12. TRANSFER OF SECURITY MANAGEMENT SYSTEM CERTIFICATION

This Administration recognizes the IACS agreement for the transfer of the ISPS certification (PR-18) and their members must comply with the internal procedures and these instructions.

If the transfer of Security System Certification occurs during the annual, intermediate or renewal verification, the gaining society **RSO** must inform this Administration prior to the transfer of the ISPS system certification, in order to know who is the new Recognized Security Organization (RSO) responsible of the ISPS system of the vessel and update our system.

This procedure shall not apply in cases involving a change of Company Operator.

13. 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:

1. When the name of vessel changes
2. When the tonnage changes
3. When the physical address of the operator company changes
4. When the name of the operator company changes
5. When the type of vessel changes

14. 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:

1. When the name of vessel changes
2. When the tonnage changes
3. When the physical address of the operator company changes
4. When the name of the operator company changes
5. When the type of vessel changes

15. SHIP MORE THAN SIX (6) MONTHS OUT SERVICES

If the ship is out of service for more than six months, the Recognized Security Organization (RSO) must re-initiate the ISPS certification process with the interim verification as required by the ISPS Code A/19.4.2 and issue an interim ISSC, with **previous notification of this Administration**.

16. OVERDUE ISPS VERIFICATION

If the ISPS verification is not carried within the established window, the certificate will be invalid and the RSO shall inform to the Flag Administration immediately at the following email: isps@amp.gob.pa, in order to cancel the Full Term ISSC in our data base and the ISPS process needs to be re-initiate with the interim verification, with previous authorization of this Administration.

17. EXPIRED CERTIFICATE PRIOR TO REQUEST THE FULL TERM ISSC

In those cases where the RSO has completed the ISPS verification within the established windows 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 expiration date of the interim ISSC with the date of issuance of the Full Term ISSC.

18. NOTIFICATION OF INVALIDATION OF ISSC CERTIFICATE

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

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

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

19. 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 directly the Maritime Ships Security Department (weekday's 08:30-16:30 hrs), at the following email: isps@amp.gob.pa, when the following conditions are given:

- ISPS Inquiries
- SSAS Exemption
- SSAS Malfunction
- Additional Audits Request
- To Postpone any ISPS verification
- Transfer of Security System Management (IACS)
- Change of RSO (during intermediate and renewal verification)
- Notification of Invalidation of ISSC Certificate

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.

From April 1st, 2018 the following Merchant Marine Circular (MMC) 145, 207 and 326 will be cancelled.

For further assistance and/or inquiries regarding of this ISPS instructions, please contact directly

November 2017

Panama Maritime Authority
Maritime Ships Security Department
Phone: +507-501-5086/5085/5028
E-mail address: isps@amp.gob.pa