No.24 Procedural Requirements for ISPS Code Certification

(Rev.0 July 2009) (Rev.1 Dec 2010)

Note:

1. This Procedural Requirement applies from 1 July 2009.

2. Rev.1 of this Procedural Requirement applies from 1 July 2011.

No.24 (cont)

Introduction

This document provides the Classification Societies with the methods and criteria for carrying out Ship Security Plan (SSP) approvals and for issuing ~~an~~ International Ship Security Certificates (ISSCs) to ~~a ship upon~~ ships following verification by audit ~~of its~~ that their security systems and any associated security equipment ~~covered by the relevant~~ comply with the requirements of the ISPS Code and the provisions of the ~~ISPS Code and the~~ corresponding approved ~~Ship Security Plan (SSP). The objective of the verification is to ensure that the security system and associated security equipment of the ship fully complies with the Code and is in satisfactory condition~~ SSPs.

The Classification Societies may conduct approvals of SSPs or amendments thereto and verification of SSPs necessary for issuing an ISSC on behalf of ~~an~~ Administrations. Certificates will comply with the format required by the flag Administrations.

1. Scope and Application

1.1 This document establishes the procedures for:
(i) review and approval of SSPs
(ii) verification of compliance with the requirements of the ISPS Code
(iii) ~~issuance~~ issue of Interim, Initial, and Renewal ISSCs
(iv) intermediate verification
(v) additional verification
(vi) withdrawal of certification

1.2 This procedure is to be ~~used~~ applied by ~~a~~ Classification ~~Society,~~ Societies when acting as ~~an RSO, issuing an ISSC when requested by a Company, as well as when acting~~ RSOs on behalf of Administrations in the conduct of SSP approvals, audits and the issue of certificates in accordance with the ISPS Code. ~~the Administration during the mandatory implementation of the ISPS Code under SOLAS Chapter XI-2.~~

1.3 The scopes of the verifications carried out ~~under~~ in accordance with this procedure shall be restricted to the Requirements of ~~the~~ SOLAS Chapter IX-2 and the ISPS Code Part A taking into account ISPS Code part B/8.1 to 13.8.

1.4 For minimum requirements ~~for~~ relating to non-routine ISPS Code certification scenarios, please refer to Annex 1.

2. Definitions

2.1 “Auditor” means a ~~member of the RSO personnel duly~~ person trained, qualified and authorized in accordance with PR 10 to carry out SSP ~~plan~~ approval and ~~verification~~ audits.

2.2 “Convention” means the International Convention for the Safety of Life at Sea, 1974 as amended.

2.3 “ISPS Code” means the International Ship and Port Facility Security Code~~” (ISPS) means the ISPS Code~~, (consisting of Part A and Part B), as adopted by the IMO ~~Organisation~~.

2.4 “Ship Security Assessment” (SSA) means ~~the identification of the~~ an exercise carried out to identify possible threats to key ship board operations~~,~~ and the likelihood of their occurrence and an evaluation of existing security measures and weaknesses in the infrastructure, policies and procedures.

No.24 (cont)

2.5 "Ship Security Plan" (SSP) means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, the cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

2.6 "Security System" is the system in place on board the ship which implements the procedures, documentation and required records which are examined to verify compliance with the requirements of the ISPS Code.

2.7 "Security Equipment" is equipment used in the implementation of the security measures specified in the SSP.

2.8 "Company Security Officer" (CSO) means the person designated by the company ~~to develop and revise the~~ for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval and thereafter implemented and maintained, and for liaison with the Port Facility Security Officer (PFSO) and the Ship Security Officer (SSO).

2.9 "Ship Security Officer" (SSO) means 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 ship security plan and for the liaison with the CSO and the Port Facility Security Officer (PFSO).

~~2.10 Any combination of CSO, SSO and master may be the same physical person.~~

2.~~11~~10 "Security Incident" means any ~~suspicious~~ act or circumstance ~~threatening~~ that theatens the security of a ship, ~~including~~ a mobile offshore drilling unit ~~and~~, a high speed craft, ~~or of~~ a port facility ~~or of any~~, a ship/port interface or any ship to ship activity.

2.~~12~~11 "Security Level" means the qualification of the degree of risk that a security incident will be attempted or will occur.

2.~~13~~12 "Security Level 1" means the level for which minimum appropriate protective security measures shall be maintained at all times.

2.~~14~~13 "Security Level 2" means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

2.~~15~~14 "Security Level 3" means the level ~~of~~ for which further specific protective security 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).

2.~~16~~15 "Regulation" means a regulation of the Convention.

2.~~17~~16 "Chapter" means a chapter of the Convention.

2.~~18~~17 "Section" means a section of the ISPS Code Part A.

2.~~19~~18 "Paragraph" means a paragraph of the ISPS Code Part B.

2.~~20~~19 "Ship" when used in this Code, includes self propelled mobile offshore drilling units and high speed craft as defined in chapters XI-2/1.

2.~~21~~20 "Failure" means the non-fulfilment of a specified requirement ~~or~~ that does not compromise the ~~subject matter is inappropriate for the ship which is identified~~ ship's ability to

No.24 (cont)

operate at security levels 1, 2 and 3. It may also be referred to as a Non-conformity. ~~times other than at an initial or renewal verification for the issue of an ISSC or a verification for the issue of an Interim ISSC.~~

2.~~22~~21 "Major Failure" means the non-fulfilment of a specified requirement that compromises the ship's ability to operate at security levels 1, 2 or 3. It may also be referred to as a Major Non-conformity.
~~"Verification" means an audit through a representative sample that the security system is being implemented effectively, verification that all security equipment specified in the SSP complies with applicable requirements.~~

2.~~23~~22 "Observation" means a statement of fact made during an audit and substantiated by objective evidence. It may also be a statement made by the auditor referring to the SSP which, if not corrected, may lead to a Failure in the future.
~~"Recognised Security Organisation" (RSO) means an organisation authorised by a Contracting Government in accordance with SOLAS Chapter X1-2/1.16.~~

2.23 "Verification" is confirmation through the evaluation of objective evidence that specified requirements have been fulfiled. (See also 2.26)

2.24 "Recognised Security Organisation" (RSO) means an organisation authorised by a Contracting Government in accordance with SOLAS Chapter X1-2/1.16. When "Classification Society" is used in this Procedural Requirement, it is always intended as "Classification Society acting as RSO".

2.2~~4~~5 "Ship Security Alert System" (SSAS) means a system installed on board, either interfaced with another ~~onboard~~ radio installation~~,~~ or self-contained (abbreviated to SSAS-SC in this PR), ~~fully complying~~ that complies with the functional requirements of SOLAS XI-2/6.2-6.4 and the performance criterion of IMO MSC.147(77).

2.26 "Audit" means a process of systematic and independent verification by obtaining objective evidence to determine whether the ship security related activities comply with the ISPS-Code and the planned arrangements of the SSP and whether these arrangements are implemented effectively to achieve the objectives of the ISPS-Code.

2.27 Any capitalized terms used in this Procedure which are not defined above have the meanings given them in the Convention.

3. Criteria for Verification

3.1 Criteria for verification of compliance with the requirements of the ISPS Code shall be in accordance with the applicable sections of the SOLAS XI-2 and the ISPS Code Part A.

3.2 A Classification Society performing verification of compliance with the requirements of the ISPS Code shall meet the requirements of MSC/Circ. 1074 Appendix 1, paragraphs 3 to 5.

3.3 If a Classification Society~~, as an RSO,~~ has been involved in either the conduct of the SSA or the development of the SSP or any amendments for a specific ship, ~~or of any amendments, such a~~ that Classification Society shall not, due to potential conflict of interest, ~~accept authorisation to~~ approve the SSP or conduct verifications for the certification ~~for that specific~~ of the ship.

3.4 A Classification Society that approves ~~approving~~ a SSP or ~~issuing~~ issues an ISSC shall have implemented a documented system for the qualification and continuous updating

No.24 (cont)

of the knowledge and competence of auditors who ~~are to~~ perform such approvals or verifications in compliance with PR 10.

3.5 Only auditors who are qualified as required by PR 10 shall carry out approvals and verifications.

3.6 A Classification Society that approves ~~approving~~ a SSP or issues ~~issuing~~ an ISSC shall have implemented a documented system ~~ensuring that~~ for the performance of the ~~certification process is~~ processes involved ~~performed~~ in ~~compliance~~ accordance with this Procedural Requirement. This system shall, inter alia, include procedures and instructions for the following:

(i) the establishment of contract agreements with Companies in respect of their ships
(ii) the scheduling and performance of ~~performing~~ SSP approvals and verifications
(iii) the reporting of the results of ~~from~~ SSP approvals and verifications
(iv) the ~~issuance~~ issue of ~~i~~Interim and full term ISSC certificates

3.7 The entire SSP approval and ~~verification to the ISPS Code as adopted~~ implementation audit process shall verify:

(i) ~~determine~~ that the SSP and~~/or~~ any amendments ~~have met provisions for~~ are appropriate to the three security levels ~~as~~ defined by the ISPS Code ~~on behalf of the Administration~~
(ii) ~~determine compliance~~ that the SSP is complaint with the ISPS Code ~~on board ships~~
(iii) that the SSP is being effectively implemented on board ~~determine the effectiveness of the implementation of the SSP on board ships~~

4. Obligations of the Company

4.1 Where the verification of an SSP is to be carried out by ~~an RSO which~~ a Classification Society that did not carry out the SSP approval, the Company shall provide, if requested by the ~~RSO~~ Classification Society, a copy of the SSA report and the SSP prior to the ~~verification~~ audit on board.

4.2 The Company shall carry out ~~both~~ internal audits and reviews of security activities at least once every ~~twelve (~~12~~)~~ months ~~onboard~~ on board each ship.

4.3 The Company and the ship are to maintain records of external security verifications for a minimum period of five (5) years.

4.4 ~~The Company shall ensure that~~ A~~a~~ny amendments made to the security system, the security equipment or the SSP ~~during the certification period,~~ and that are related to the requirements of ISPS Code A/9.4.1 to A/9.4.18, ~~are~~ must be submitted to the ~~RSO~~ Classification Society for review and approval.

4.5 At the initial installation of the SSAS, the Company shall arrange for an approved Radio Technician to test and issue a report on the equipment's compliance with the requirements of ~~the technical functionality and performance criteria for the SSAS (except a~~ SOLAS XI-2/6, paragraphs 2 to 4. A SSAS-SC ~~which~~ may be tested and reported on by the SSO~~) with SOLAS XI-2/6, paragraphs 2-4 inclusive~~.

4.6 Following the initial installation of the SSAS, the Company ~~has the responsibility~~ is responsible for:

- ~~to ensure that~~ testing and maintaining the SSAS ~~is tested and maintained~~ to satisfy operational requirements according to the approved SSP; and
- ~~to keep~~ maintaining on board the SSAS records specified in ISPS Code A/10.1.10.

No.24
(cont)

5. Ship Security Plan Approval ~~Assessment~~

5.1 The Company is to prepare and submit to the Classification Society a SSP for each ship. This SSP is to be reviewed and approved on behalf of the Administration. ~~The SSA is to be carried out by persons with appropriate skills to evaluate security risks and issues of each ship.~~

5.2 Unless otherwise specified by the Administration, all changes to an approved SSP related to the requirements of ISPS-Code A/9.4.1 to A/9.4.18 should be reviewed and approved before implementation by the RSO that approved the SSP. The SSP and the amendments are to be accompanied by the SSA from which they were developed.
~~The SSA must include an on-scene survey and include the following elements:~~
~~(i) identification of existing security measures, procedures and operations~~
~~(ii) identification and evaluation of key ship board operations~~
~~(iii) identification and risk analysis of threats to these key ship board operations~~
~~(iv) identification of weaknesses in the system, including the human element, policies and procedures~~

5.3 The SSP shall be developed in accordance with the requirements of ISPS Code Part A taking into account ISPS Code B/8.1 to 13.8, and shall be written in the working language, or working languages, of the ship. If the language, or languages, used is not English, French or Spanish, a translation into one of these languages shall be included. The Classification Society undertaking the approval shall only consider the version of the SSP written in English, French or Spanish.
~~The security assessment must be documented, reviewed, accepted and retained by the Company for submission during the approval process of the SSP.~~

5.4 When reviewing and approving a SSP, the auditor shall verify that the Company has taken into account relevant security-related guidance and best management practices, including the latest IMO Circulars concerning piracy, hijacking and armed robbery.
~~Security assessments should be performed based on the examination of specific threat scenarios, including regular trading patterns, with consideration of the vulnerability of the ship and the consequence of those scenarios.~~

5.5 When the Classification Society approves the SSP and any amendments it should retain, as a minimum, a copy of the:
(i) Letter of Approval
(ii) SSP title page
(iii) SSP index
(iv) Revision history of the SSP

The title page shall be stamped as approved. All other pages of the SSP should be marked to indicate review. The approved SSP shall be held on the ship.
~~Elements to be taken into account in the SSA are listed in ISPS Code B/8.1 to 13.8.~~

5.6 The Classification Society that approves an amendment to an SSP shall determine whether any additional verification is required relating to its implementation.

5.7 Where a Company has its SSP in electronic format, the Classification Society may issue a Letter of Approval and retain a printed copy of the pages noted in 5.5 (ii) to (iv) which shall be marked to indicate approval.

5.8 During the certification period, no Classification Society shall approve amendments to a SSP approved by another RSO or an Administration.

No.24
(cont)

5.9 Evidence should be sought that the Company Security Officer (CSO) has received training in accordance with ISPS Code A/13.1. If evidence is not provided by the Company or if there is objective evidence that the CSO has not received such training, the auditor should inform the Company and the relevant Classification Society. When applicable, the information should then be passed to the Classification Society (or Societies) that issues the ISSCs to the Company's ships for consideration at the shipboard audit.

~~**6. Ship Security Plan Approval**~~

~~6.1 The Company is to prepare and submit to the RSO a SSP for each ship. This SSP is to be reviewed and approved on behalf of the Administration.~~

~~6.2 The SSP and amendments are to be accompanied by the SSA from which the SSP has been developed.~~

~~6.3 The SSP shall be developed in accordance with the requirements of ISPS Code Part A taking into account ISPS Code B/8.1 to 13.8, and shall be written in the working language, or working languages, of the ship. If the language, or languages, used is not English, French or Spanish, a translation into one of these languages shall be included. The RSO undertaking the approval shall only consider the version of the SSP written in English, French or Spanish.~~

~~6.4 When the RSO approves the SSP and any amendments, as a minimum requirement the RSO is to retain a copy of the:~~

~~(i) Letter of Approval~~
~~(ii) SSP title page~~
~~(iii) SSP index~~
~~(iv) revision history of the SSP~~

~~All such retained pages shall be stamped as Approved. All other pages of the SSP are not required to be retained by the RSO but should be marked to indicate approval. The Company should be the only party to hold complete copies of the approved SSP. The approved SSP shall be held on the ship.~~

~~6.5 An RSO approving amendments to an SSP shall determine whether any additional verification is required to verify implementation.~~

~~6.6 Where a Company has its SSP in electronic format, the RSO shall issue a Letter of Approval and retain a printed copy of the pages noted in 6.4 (ii) to (iv) which shall be marked to indicate approval.~~

~~6.7 During the certification period, one Classification Society may only approve amendments to an SSP initially approved by another Classification Society or Administration, if this Classification Society takes over the responsibility as RSO and issues a new PAL. The Classification Society that initially approved the SSP and flag needs to be notified accordingly.~~

~~6.8 Evidence should be sought that the Company Security Officer (CSO) has received training in compliance with ISPS Code A/13.1. If evidence is not provided by the company or there is objective evidence that the CSO has not received such training, the auditor should inform the company and his Classification Society. The information should then be passed, if applicable, to the RSO that issues ISSCs to the company ships for consideration at the on-board verification audit.~~

No.24
(cont)

~~7~~6.~~0~~ ~~Verification~~ Audit of Ships

~~7~~6.1 ~~The verification~~ Audits for ~~issuing or renewing the ISSC consists~~ the issue or renewal of ISSCs shall consist of the following steps:

(i) verification that an approved SSP is on-board
(ii) verification through a representative sample that the security system is being implemented effectively
(iii) verification that all security equipment specified in the SSP complies with applicable requirements
(iv) verification that all security equipment specified in the SSP, including the ship security alert system (SSAS), is operational.

~~7~~6.2 Initial, Intermediate and Renewal ~~verification~~ audits shall be performed only under normal operating conditions and when ~~with~~ the ship is fully manned in accordance with the Safe Manning Certificate.

~~7~~6.3 The auditor shall verify the effective implementation of the approved SSP and its documented procedures based on objective evidence ~~demonstrating the effectiveness of the documented procedures. This verification is achieved via~~ obtained by interviews, inspections, review of documents and examination of records ~~of drills and training~~.

~~7~~6.4 Following the initial installation of the SSAS, the ~~RSO~~ Classification Society ~~shall~~ may approve the related provisions in the SSP and verify, ~~through a shipboard security verification including~~ by audit and the witnessing of a complete security alert test, the effective implementation of ~~the operational requirements of the~~ those provisions. Confirmation that the SSAS complies ~~in accordance~~ with the requirements of paragraphs 2 to 4 of SOLAS XI-2 will be found in ~~ISPS Code A/9.4.17 to A/9.4.18 and~~ the Radio Technician's report (or the SSO's report, in the case of a SSAS-SC) ~~on the compliance with SOLAS XI-2/6, paragraphs 2-4 inclusive. At each subsequent regular verification the auditor shall examine the records of activities on the SSAS specified in ISPS Code A/10.1.10, witness a complete security alert test and verify the operational requirements of the SSAS in accordance with the requirements in ISPS Code A/9.4.17 to A/9.4.18~~.

6.5 At each subsequent scheduled audit the auditor shall examine the records of the testing of the SSAS, identify the SSAS activation points and verify the effective implementation of the procedures, instructions and guidance relating to the SSAS as specified in A/9.4.18.

~~7.5~~6.6 Intermediate and renewal ~~verifications are to~~ audits shall include a review of F~~f~~ailures reported ~~in relation to previously conducted verifications.~~ following previous audits. The auditor shall select a sample of the reported F~~f~~ailures and ~~shall~~ verify that the company ~~investigation, analysis,~~ is investigating, analyzing and resolving them effectively and ~~resolution of failures in accordance with the requirements of ISPS Code A/9.4.8 and 9.4.11.~~ in a timely manner.

~~7.6~~6.7 The auditor has the authority to ask for information from any other RSO or, if relevant the Administration, in order to check the accuracy of the information provided by the Company.
~~Evidence should be sought that the Ship Security Officer (SSO) has received training in compliance with ISPS Code A/13.2. If evidence is not provided by the company or there is objective evidence that the SSO has not received such training, and after taking into consideration any advice supplied under 6.8 above concerning the CSO, the auditor shall consider this to be a failure in the security system.~~

No.24
(cont)

~~7.7~~6.8 Where the audit of a ship is to be carried out by a Classification Society that did not carry out the SSP approval, the Classification Society may review the SSP either at, or prior to, the audit on board.
~~The auditor has the authority to ask for information from any other RSO or, if relevant the Administration, in order to check the accuracy of the information presented by the Company.~~

~~7.8 If the verification under 7.1 is not satisfactorily completed, then an ISSC is not to be issued.~~

~~7.9 If at an intermediate or additional verification, the auditor identifies through objective evidence a failure in the security system or associated equipment that **does** compromise the ship's ability to operate at security levels 1 to 3, it shall be reported immediately to the flag Administration together with the remedial action proposed by the Company. If authorised by the Flag to do so, the auditor shall verify the implementation of the alternative security measures and approve the remedial action plan before the ship sails. The RSO shall request the Administration to authorise an additional verification before the expiry date of the approved remedial action plan to verify that the action plan has been completed.~~

~~7.10 If at an intermediate or additional verification, the auditor identifies through objective evidence a failure of the security system or associated equipment, or the suspension of a security measure which **does not** compromise the ship's ability to operate at security levels 1 to 3, it shall be reported without delay to the Administration. If authorised to do so, the auditor shall approve the remedial action plan. The completion of the action plan shall be verified by the RSO no later than the next scheduled verification.~~

~~7.11 Intermediate verification shall take place between the second and third anniversary date of the certificate.~~

~~7.12 Renewal verification should take place at intervals not to exceed five (5) years and should be carried out within the three (3) months prior to the expiry date of the existing certificate.~~

~~7.13 Initial, Intermediate or Renewal verification may be carried out in conjunction with an ISM audit of the ship.~~

~~7.14 Additional verification shall be carried out as may be authorised by the Administration or a duly authorised officer of a Contracting Government.~~

~~7.15 Where the verification of a ship is to be carried out by an RSO which did not carry out the SSP approval, the RSO may review the SSP either at, or prior to, the verification audit on board.~~

7 Failures and Corrective Action Follow-up

7.1 Audit findings shall be reviewed by the auditor(s) in order to determine whether they should be reported as Major Failures, Failures or Observations.

7.2 At the end of the Audit, the auditor(s) shall hold a meeting with the senior management of the ship and those responsible for the functions concerned. The purpose is to present Major Failures, Failures and Observations to the ship's management in such a manner that they are clearly understood.

7.3 Failures shall be raised against the corresponding requirement of the ISPS Code, the relevant sections or paragraphs of the SSP and any specific Flag State requirements.

No.24
(cont)

7.4 An ISSC is not to be issued or renewed if a Major Failure exists. Immediate action is required to restore compliance. The auditor shall verify the implementation of these measures before the ship sails and a schedule for the implementation of preventative action shall be agreed between the Company and the auditor to prevent recurrence. At least one additional audit shall be carried out within the period agreed for the implementation of the corrective action.

7.5 An ISSC shall not be issued or renewed until all identified Failures have been resolved and compliance has been restored. In addition, depending on the nature and seriousness of the Failure identified, a schedule for the implementation of preventative action may need to be agreed between the Company and the auditor to prevent recurrence. Additional audits may be carried out as necessary.

7.6 An ISSC shall not to be endorsed if a Major Failure exists. Immediate action is required to restore compliance, thereby permitting the Major Failure to be down-graded. The auditor shall verify the implementation of these measures before the ship sails and a schedule for the implementation of preventative action shall be agreed between the Company and the auditor to prevent recurrence. At least one additional audit shall be carried out within the period agreed for the corrective action.

7.7 An ISSC may be endorsed following identification of a Failure, provided that a schedule has been agreed between the Company and the auditor for the completion of corrective action to restore compliance and to prevent recurrence. Additional audits may be carried out as necessary.

8.~~0~~ Issuance and Endorsement of the International Ship Security Certificate (ISSC)

8.1 The ISSC shall be issued after an Initial or Renewal audit ~~verification~~ in accordance with ~~7~~6.1.

8.2 The “type of ship” to be entered on the ISSC shall be selected from those ~~as~~ defined in SOLAS chapter IX Regulation 2.

8.3 The ISSC ~~is to~~ shall be endorsed at the Intermediate ~~verification~~ audit and at any additional ~~verification~~ audit required by the Administration.

8.4 On completion of the audit, to facilitate the review of the auditor’s report prior to the issue of the full-term certificate, an ISSC with validity not exceeding five (5) months may be issued by the auditor. ~~The ISSC certificate shall be valid for a period not to exceed five (5) years.~~

8.5 If, at the time when its ISSC expires, a ship is not in a port in which it is possible to carry out a renewal audit, the Administration may extend the period of validity of the certificate, but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to a port in which the audit may take place. No certificate shall be extended more than three months. Documentary evidence of the granting of the extension by the Administration must be reviewed by the Classification Society before the extension is endorsed.
~~On completion of the verification, to facilitate the review of the auditor’s report prior to the issue of the full-term certificate, an ISSC with validity not exceeding five (5) months may be issued by the auditor.~~

~~8.6 Not withstanding 8.3, when the Renewal verification is completed within three months before the expiry date of the existing certificate, the new certificate shall be valid from the~~

No.24
(cont)

~~date of the completion of the renewal verification to a date not exceeding five years from the date of the existing certificate.~~

~~8.7 When the Renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be valid from the date of the completion of the Renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.~~

~~8.8 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 date of the completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.~~

~~8.9 If a Renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the RSO on behalf of the Administration, may endorse the existing certificate and such a certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.~~

~~8.10 If a ship at the time when the certificate expires is not in a port which it is to be verified, the Administration may extend the period of validity of the certificate, but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is verified. No certificate shall be extended more than three months. Documented evidence from the Administration granting this request is to be reviewed by the RSO prior to endorsement of extension.~~

~~8.11 If an Intermediate verification is completed before the period specified in section 7.11, then:~~

~~(i) the expiry date shown on the certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the Intermediate verification was completed;~~
~~(ii) the expiry date may remain unchanged provided one or more additional verifications are carried out.~~

~~8.12 A copy of the ISSC and copy of the verification report shall be transmitted to the Administration in a timely manner, if required.~~

8.~~13~~6 At the request of the Company, the expiry date of ISSC may be aligned with ~~to~~ the expiry date on the Safety Management Certificate (SMC) provided that this does not exceed the five (5) year period specified in ISPS Code A/19.3.

~~8.14 An ISSC shall cease to be valid in any of the following cases:~~
~~(i) relevant verifications not carried out within the specified period~~
~~(ii) if the certificate is not endorsed at intermediate or additional verifications~~
~~(iii) the Company operating a ship ceases to operate that ship~~
~~(iv) upon transfer of the ship to the flag of another Administration~~

9.0 ~~Interim Certification~~ Opening and Closing Meetings

9.1 ~~An Interim Certificate can be issued for the following reasons:~~
~~(i) a ship without a certificate, on delivery or prior to entry or re-entry into service,~~
~~(ii) transfer of a ship from one Administration to the flag of another Administration,~~
~~(iii) transfer of a ship to a signatory Administration from one that is not a signatory Administration,~~
~~(iv) a Company assumes the responsibility for the operation of a ship.~~

No.24
(cont)

~~9.2 The scope of~~ Shipboard verification ~~for the issue of an Interim ISSC shall be as defined in ISPS Code A/19.4.2 and detailed in Appendix 1.~~

~~9.3 An Interim ISSC shall be valid for six (6) months. No extensions can be granted.~~

~~10.0 Plan Approval, Verifications and Reports~~

~~10.1 Plan approval, if carried out at the Company premises or on board the ship, and verification~~ audits shall start with an opening meeting, the purpose of which is to:

(i) introduce the auditor to the ~~Company and /or~~ ships management
(ii) explain the scope and ~~objective~~ purpose of the ~~approval or verification as applicable~~ audit
(iii) provide a short summary of the methods and procedures to be used
(iv) establish the official communication line between the auditor and the ~~Company and/or the~~ shipboard management
(v) confirm that the necessary resources, documentation and facilities ~~needed~~ are available
(vi) confirm the time and date of the closing meeting and any ~~possible~~ interim meetings

~~10.2 Findings are to be documented in a clear, concise manner and supported by objective evidence.~~

9.2 On completion of each audit, the auditor shall hold a closing meeting with the shipboard management, as appropriate, to present the findings so that they are fully understood.

10. Reporting Plan Approvals and Shipboard Audits

10.~~3~~1 A report is to be ~~prepared by the auditor following both the~~ produced after every ~~plan~~ SSP approval and ~~verification, as applicable, based on the information gathered~~ audit.

10.~~4~~2 In the case of a ~~plan~~ SSP approval, the Letter of Approval ~~of the SSP~~ shall include the following wording: “In the development of the Ship Security Plan, in accordance with ISPS Code A/9.4, the provisions of ISPS Code B/8.1 to 13.8 have been duly taken into account and applied as appropriate for the ship”.

10.~~5~~3 ~~In the case of a verification the report shall include the following items:~~
~~(i) the date of completion of the verification.~~
~~(ii) status of the implementation of the SSP~~
~~(iii) report on the operational status on all security equipment and systems on board.~~
~~(iv) reports of any failures found during the verification in accordance with 7.9 and 7.10.~~
The Letter of Approval shall be given to the company and retained on board the ship, together with a copy of the audit report.

10.4 In the case of an audit, the report must include the following:
(i) the date and time of completion of the audit.
(ii) the status of the implementation of the SSP.
(iii) confirmation of the operational status of all security equipment and systems on board.
(iv) reports of any Failures found during the audit.

~~10.6 On completion of the SSP approval, if carried out at the company premises or on board the ship, and also after the verification audit, the auditor is to hold a meeting with the~~

No.24
(cont)

~~senior management and/or master. The purpose is to ensure that the findings of the approval or verification audit are clearly understood.~~

~~10.7 The Letter of Approval shall be given to the company and retained on board the ship, together with a copy of the verification audit report.~~

11.~~0~~ Responsibilities Pertaining to ~~Verifications~~ Audits

11.1 Responsibilities of the ~~Company~~ Classification Society.

11.1.1 The ~~Company~~ Classification Society is responsible for~~:~~ performing the audit and certification process in accordance with this Procedure and relevant Administration requirements.

~~(i) informing the vessel crew about the objectives of the verification~~
~~(ii) appointing responsible members of staff to accompany the auditor~~
~~(iii) provide the resources needed by the auditor to ensure an effective and efficient verification process~~
~~(iv) providing access and objective evidence as requested~~
~~(v) co-operating with the auditor to permit the verification objectives being achieved~~

~~11.1.2 The verification of compliance with the requirements of the ISPS Code does not relieve the Company, management, officers or seafarers of their obligation to comply with national and international legislation or security levels in the area they are employed or operating.~~

11.2 Responsibilities of the ~~RSO~~ Auditor.

11.2.1 ~~The RSO is responsible for ensuring that the verification and certification process is performed in accordance with this Procedure and relevant Administration requirements.~~ The auditor is responsible for:

(i) carrying out the audit effectively and efficiently
(ii) complying with the applicable procedural and regulatory requirements
(iii) noting in the report any obstacles to the effective conduct of the audit
(iv) organizing any special technical assistance required to verify compliance
(v) reporting the audit results clearly, concisely and without undue delay

11.2.2 ~~The RSO is responsible for submitting the verification report to the Administration, if required, in a timely manner.~~ Auditors shall treat all the information to which they have access during the course of SSP approvals and shipboard verification audits in the strictest confidence.

~~11.3 Responsibilities of the Auditor~~

~~11.3.1 The auditor is responsible for:~~
~~(i) carrying out the assigned verification effectively and efficiently~~
~~(ii) complying with applicable requirements and other appropriate directives~~
~~(iii) noting in the report any major obstacles encountered in performing the verification~~
~~(iv) organizing special technical assistance required to fulfill the compliance requirements~~
~~(v) reporting the verification results clearly, conclusively and without any undue delay~~

~~11.3.2 Personnel participating shall ensure confidentiality of documents pertaining to the certification and treating privileged information with discretion.~~

No.24
(cont)

~~**12.0 Withdrawal of certification**~~

~~12.1 If the RSO has reasons for invalidating an ISSC, these reasons are to be communicated to the ship and to the Administration the RSO is acting on behalf of.~~

~~12.2 The communication is to be limited to the identity of the ship, the Company, the reason for invalidation and the date of the verification.~~

~~12.3 The RSO shall recommend to the Administration that an ISSC should be withdrawn in the following circumstances:~~

~~(i) the alternative security measures agreed are not in place~~
~~(ii) an approved action plan has not been complied with~~

~~12.4 A RSO can only re-issue an ISSC following a SSP approval and an additional verification with the scope of an initial verification of the ship. The expiry date of the new certificate shall be that of the withdrawn certificate.~~

~~**13.0 Action by a Duly Authorised Officer (DAO) of a Contracting Government**~~

~~13.1 When attending a ship required by, or as a result of action by, a DAO due to the failure of the ship to meet the requirements of SOLAS Chapter XI-2, the auditor from the RSO that issued the ISSC is to carry out an additional verification based upon the failures identified by the DAO in the report.~~

~~13.2 The auditor shall advise the company and the Administration of the findings of the additional verification. Any failures identified shall be handled in accordance with the requirements of 7.9 and 7.10 above.~~

~~13.3 If the auditor disagrees with the reasons for the failure(s) identified by the DAO, the auditor shall document the disagreement to the DAO and inform the company and Administration.~~

12. Withdrawal of Certification

12.1 An interim ISSC shall not be issued to a ship from which a full-term ISSC has been withdrawn.

12.2 When an ISSC has been withdrawn, a new certificate may be issued only after the successful completion of an initial audit.

12.3 The new certificate shall have the same expiry date as the certificate that was withdrawn.

13. Actions Following Port State Control Detentions

13.1 When a ship is detained and deficiencies relating to the ISPS Code are given as reasons for the detention, the RSO that issued the ISSC shall carry out an additional audit.

13.2 Any Failures shall be dealt with in accordance with the relevant requirements of paragraph 7 above.

13.3 If the auditor disagrees with the conclusions of the Duly Authorised Officer, the reasons for the disagreement shall be documented in the audit report. The Duly Authorised Officer, the Company and the Administration must be made aware of the auditor's comments in this respect.

PR 24 Annex 1: *Minimum Requirements for ISPS Code Certification Scenarios*

Scenarios	*Possible Cases*	*Ship Security Plan (SSP)*	*Certification*
Change of ship's name	If conducted by a surveyor	Check change of name in title page, index page and revision page of SSP. Change name on Plan Approval Letter (PAL). Send copy of amended PAL to issuing office. *Note: A new PAL cannot be issued because the SSP may contain other changes made since the last review. A surveyor is not authorized to issue a PAL*	Amend ISSC with new name. Send copy of amended certificate to issuing office. Issuing office issues replacement ISSC with same expiry date as the original certificate. *Note: One society cannot amend or endorse the ISSC of another.*
	If conducted by an auditor	Review and approve ALL changes to the SSP as required by PR24 6.4. Issue replacement PAL.	Issue replacement ISSC with same expiry date as previous one
Change of flag	With additional requirements and when authorized to approve SSPs	Carry out a SSP approval and issue a PAL on behalf of the new flag Administration.	If it is possible to verify compliance with the additional requirements immediately, a replacement ISSC with the same expiry date as the original certificate may be issued. If it is not possible to verify compliance with the additional requirements immediately, carry out an interim verification as required by ISPS Code A/19.4.2 and detailed in PR 24 Appendix 1. Issue Interim ISSC
	Without additional requirements and when authorized to approve SSPs		Issue a replacement certificate with the same expiry date as the original certificate.
	With or without additional requirements and when **not** authorized to approve SSPs	Check that the SSP is on board, that ISPS Code A/9.4.1 to 9.4.18 has been addressed and that a copy has been submitted to the flag Administration or its RSO for approval.	Carry out an Interim verification as required by ISPS Code A/19.4.2 and detailed in PR 24 Appendix 1. Issue Interim ISSC

PR 24 Annex 1: *Minimum Requirements for ISPS Code Certification Scenarios*

Scenarios	*Possible Cases*	*Ship Security Plan (SSP)*	*Certification*
Change of management	---	Carry out a SSP approval and issue a PAL. If not authorized by the flag Administration to carry out SSP approval on its behalf, check that the SSP is on board, that ISPS Code A/9.4.1 to A/9.4.18 has been addressed and that a copy has been submitted to the flag Administration or its RSO for approval.	Carry out an Interim verification as required by ISPS Code A/19.4.2 and detailed in PR 24 Appendix 1. Issue Interim ISSC.
Re-activation following lay-up	ISSC still valid	Contact flag Administration for instructions.	Contact flag Administration for instructions.
	ISSC not valid	Carry out a SSP approval and issue a PAL on behalf of new flag Administration. If not authorized by the flag Administration to carry out SSP approval on its behalf, check that the SSP is on board, that ISPS Code A/9.4.1 to A/9.4.18 has been addressed and that a copy has been submitted to the flag Administration.	Carry out an Interim verification as required by ISPS Code A/19.4.2 and detailed in PR 24 Appendix 1. Issue Interim ISSC.
Change from voluntary to mandatory certification	---	Approve SSP amendments including sections relating to SOLAS XI-1 Reg. 3 and 5, and SOLAS XI-2 Reg. 6	Issue replacement ISSC with same expiry date as voluntary one
Change of Company name and address	---	Company requested to confirm that SSP contains no unapproved amendments. Issue replacement PAL. If SSP does contain unapproved amendments, company to submit SSP for approval. Issue replacement PAL.	Issue replacement ISSC with same expiry date as previous one

Note 1: The above instructions apply in the absence of any flag administration requirements to the contrary.
Note 2: The instructions relating to re-activation following lay-up do not apply to ships for which seasonal lay-ups are a normal part of their operational routine.

Annex 1 ISPS Code Certification Scenarios - Minimum Requirements

No.	Scenario	Condition	Type of Audit	Ship Security Plan	Scope of Audit and Certification
1	***Change of ship's name***	If conducted by a surveyor	Verification on board	1. Verify correct name on all certificates and in the title page, index page and revision page of SSP. 2. Change name on SSP Approval Letter (PAL). 3. Send copy of amended PAL to issuing office if appropriate. *Note: A surveyor is not authorized to issue a PAL.*	1. Amend ISSC with new name. 2. Send copy of amended certificate to issuing office. 3. Issuing office issues replacement ISSC with same expiry date as the original certificate if appropriate. *Note: One RSO cannot amend or endorse the ISSC of another.*
		If conducted by an auditor	Verification on board	1. Review and approve amendments to the SSP as required by PR24 6.4. 2. Issue replacement PAL if appropriate. A PAL should only be issued, if changes to the SSP apply, which go beyond the change of vessel's name.	1. Issue replacement ISSC with same expiry date as previous one if appropriate.

No.	Scenario	Condition	Type of Audit	Ship Security Plan	Scope of Audit and Certification
2	***Change of ship's flag***	When SSP has not yet been approved and when authorized to approve SSPs	Additional Audit	1. Carry out SSP approval. 2. Issue a PAL on behalf of the new Administration.	1. Verify compliance with the requirements of the SSP. 2. Issue a replacement certificate with the same expiry date as the original certificate.
		When SSP has not yet been approved and when **not** authorized to approve SSPs	Interim Audit	1. Check that the SSP is on board. 2. Check that SSP addresses ISPS Code A/9.4.1 to 9.4.18. 3. Check that a copy of the SSP has been submitted to the Administration or its RSO for approval.	1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC.
		When SSP has already been approved	Additional Audit		1. Verify compliance with the requirements of the SSP. 2. Issue a replacement certificate with the same expiry date as the original certificate.

No.	Scenario	Condition	Type of Audit	Ship Security Plan	Scope of Audit and Certification
3	***Ship more than 6 months out of service***	ISSC is not valid	Interim Verification	1. Carry out a SSP approval (if required) and issue a PAL. 2. If not authorized by the flag Administration to carry out SSP approval on its behalf, check that the SSP is on board, that ISPS Code A/9.4.1 to A/9.4.18 has been addressed and that a copy has been submitted to the flag Administration for approval.	1. Interim verification as required by ISPS Code A/19.4.2. 2. Issue Interim ISSC.
4	***Change from non-convention to convention***		Additional Audit	1. Approve SSP and issue PAL on behalf of the flag administration.	1. Issue replacement ISSC with same expiry date as non-convention ISSC.
5	***Change of Company name and address***			1. Request Company to confirm that SSP contains no amendments. Issue replacement PAL. 2. If SSP does contain amendments, company to submit SSP for approval. Issue replacement PAL.	1. Issue replacement ISSC with same expiry date as previous ISSC.

Note 1: The above instructions apply in the absence of any flag administration requirements to the contrary.
Note 2: The instructions relating to re-activation following lay-up do not apply to ships for which seasonal lay-ups are a normal part of their operational routine.

Annex 2

Application of the ISPS Code to FPSOs and FSUs

See MSC-MEPC.2/Circ.9 of 25 May 2010 **"GUIDANCE FOR THE APPLICATION OF SAFETY, SECURITY AND ENVIRONMENTAL PROTECTION PROVISIONS TO FPSOs AND FSUs".**

Annex 3

Notification of Invalidation of ISPS Certification (ISSC)

Ship's Name:	IMO No.
Company Name and Address:	Certificate No.
	Issued by:
The audit was conducted on behalf of the government of:	
Type of audit; Intermediate Additional Renewal (Tick as appropriate)	

REASON FOR INVALIDATION OF CERTIFICATION (specify):
Name: Position: Society: Date:

Distribution:

Copy to Company

Copy to Administration

Copy to Port State Authority (if appropriate)

Copy to Classification Society

~~Appendix 1~~

~~Issue of an Interim ISSC~~

~~The ISPS Code A/19.4.2 defines the requirements for the issue of an Interim ISSC.~~

~~The following criteria shall be taken by auditors as the minimum to demonstrate the effective implementation of a Ship Security Plan (SSP).~~

~~1.0 The auditor shall verify through interview that:~~

~~1.1 Personnel with security duties are familiar with their duties and responsibilities as specified in the SSP.~~

~~1.2 The Ship Security Officer has received appropriate training.~~

~~2.0 The auditor shall sight records to demonstrate that:~~

~~2.1 The SSP is on board, that ISPS Code A/9.4.1 to 9.4.18 has been addressed and the SSP has been submitted for approval to the flag Administration or RSO ***or*** the SSP has been approved by, or on behalf of, the flag Administration.~~

~~2.2 Any additional flag Administration requirements have been addressed.~~

~~2.3 At least one drill specified in the SSP has been either carried out or planned by the SSO/CSO before the ship's departure.~~

~~2.4 Security equipment as specified in the SSP has been included in the maintenance system and maintained in accordance with the requirements of the system.~~

~~3.0 The auditor shall check that:~~

~~3.1 All security and surveillance equipment identified in the SSP is operational and is fit for the service for which it was intended.~~

~~3.2 If the mandatory implementation date for compliance with SOLAS XI-2/6 (SSAS) has passed, the auditor shall examine the records of the maintenance and testing of the SSAS specified in ISPS Code A/10.1.10, witness a complete security alert test and verify the operational requirements of the SSAS in accordance with the requirements in ISPS Code A/9.4.17 to A/9.4.18.~~

~~3.3 The ship complies with, or has plans to comply with, SOLAS V/19 (AIS) and SOLAS XI-1/3 (Ship Identification Number) prior to the mandatory implementation dates. The ship has on board a CSR in compliance with SOLAS XI-1/5. Any deficiency identified shall be reported to the responsible RO or the Administration.~~

~~Appendix 2~~

~~Application of the ISPS Code to FPSOs and FSUs~~

~~At IMO Maritime Safety Committee (MSC) meeting 77, it was decided that neither of the two types of floating production, storage and offloading units (FPSO) and floating storage units (FSU), are ships subject to the provisions of the ISPS Code, but they should have some security procedures in place to prevent "contamination" of ships with which they interface and port facilities subject to the ISPS Code. This decision was disseminated in MSC/Circ.1097 "Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code".~~

~~AS FPSOs and FSUs operate as part of offshore oil production facilities, it can be expected that the State on whose Continental Shelf or within whose Exclusive Economic Zone (EEZ) the activity is being undertaken, will have developed appropriate security measures and procedures under its national law to protect its offshore activities. FPSOs and FSUs may be required to comply with these or flag Administration requirements. As an alternative a Classification Society may issue a voluntary ISSC based upon full implementation of SOLAS chapter XI-2 and the ISPS Code".~~

~~No specific advice is offered by IMO as to the security measures or procedures that should be taken by a ship to which the ISPS Code applies which has an interface with either a FPSO or FSU. However the SSP should contain security measures and procedures as recommended in ISPS B/9 5.1. This could include the agreement of a Declaration of Security with the FPSO or FSU indicating the security measures each ship undertook during the interface.~~

****

End of Document