

MARINA CIRCULAR NO. 193
Series of 2003

TO : ALL SHIPPING COMPANIES OPERATING PHILIPPINE-REGISTERED SHIPS FOR INTERNATIONAL VOYAGES

SUBJECT : RULES ON THE IMPLEMENTATION OF MARITIME SECURITY MEASURES FOR PHILIPPINE - REGISTERED SHIPS ENGAGED IN INTERNATIONAL VOYAGES

Pursuant to the provisions of Presidential Decree No. 474 and Executive Order No. 125, as amended, and in conformity with Chapter XI-2 on the Enhancement of Maritime Security of the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, and the International Code for the Security of Ships and Port Facilities (ISPS Code), the following rules on the implementation of maritime security in the Philippines was approved by the Maritime Industry Board in its meeting on 11 August 2003.

I. OBJECTIVES:

1. To provide specific guidelines in the implementation of Chapter XI-2, SOLAS, 1974, as amended, and the International Code for the Security of Ships and Port Facilities;
2. To establish the roles and responsibilities of companies operating ships registered in the Philippines and the crew on board such ships in maintaining security of ships in accordance with SOLAS, 1974 as amended and the ISPS Code;
3. To ensure that adequate and proportionate maritime security measures are in place on Philippine-registered ships; and
4. To ensure the efficient generation and exchange of updated security-related information.

II. COVERAGE:

1. All companies operating/managing Philippine-registered ships engaged in international voyages.
2. All Philippine-registered ships engaged in international voyages under the following categories:
 - 2.1. Passenger ships including high-speed passenger crafts regardless of size;
 - 2.2. Cargo ships, including high-speed crafts, of 500 gross tonnage or more; and

- 2.3. Mobile offshore drilling units.
3. All Philippine-registered ships primarily engaged in domestic trade but temporarily allowed by the Administration to undertake international voyages.
4. This circular does not apply to warships, naval auxiliaries or other ships owned or operated by the Government of the Philippines and used only on government non-commercial service.

III. DEFINITIONS:

1. **Administration** – refers to the Maritime Industry Authority (MARINA);
2. **Contracting Government** – refers to the duly authorized officers of the port facility or the control officers of a state within whose territory ship covered by this Circular may call/undertake ship/port interface.
3. **Company** - refers to the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the Code.
4. **Ship/port interface** - means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship;
5. **Port facility** - is a location, as determined by the contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.
6. **Security incident** - means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high speed craft, or of a port facility or of any ship/port interface or any ship to ship activity.
7. **Security level** - means the qualification of the degree of risk that a security incident will be attempted or will occur.

8. **Declaration of security** means an agreement reached between a ship and either a port facility or another ship with which it interfaces specifying the security measures each will implement.
9. **Recognized security organization** means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by Chapter XI-2 of SOLAS 1974 as amended or by Part A of the ISPS Code and this Circular.
10. **Ship** means a Philippine registered ship to which this Circular is applicable.
11. **Ship Security Plan (SSP)** – a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ships stress or the ships from the risks of a security incident.
- 12.. **Ship Security Officer (SSO)** – the persons on board the ships, accountable to the master designated by the company and responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.
13. **Company Security Officer (CSO)** – the person designated by the company 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 port facility security officers and the ship security officer.
14. **ISPS Code** – means the International Code for the Security of ships and Port Facilities.

IV. GENERAL PROVISIONS:

1. Companies and ships covered by this Memorandum Circular shall by 01 July 2004 comply with the requirements of Chapter XI-2 on the Enhancement of Maritime Security of SOLAS, 1974, as amended and the ISPS Code as herein further elaborated.
2. By 01 July 2004, all ships covered by this Circular shall carry on board a Ship Security Plan (SSP) duly approved by the Administration or by a recognized security organization (RSO) acting on its behalf.

3. Ships shall by 01 July 2004 have on board an International Ship Security Certificate issued pursuant to paragraph XII.2 of this Circular.
4. Companies shall be primarily responsible for the implementation of this Circular.
5. The company shall ensure that the CSO, the master and the SSO are given the necessary support to fulfill their duties and responsibilities in accordance with Chapter XI-2 of SOLAS, 1974, as amended, Part A of the ISPS Code and this Circular.
6. The master shall be given overriding authority and responsibility to make decisions with respect to the safety and security of the ship. This shall include denial of access to persons (except those identified as duly authorized by a Contracting Government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.
7. The company shall ensure that the master has available onboard, at all times, information through which officers duly authorized by a Contracting Government can establish:
 - 7.1. Who is responsible for appointing the members of the crew or other persons currently employed or engaged onboard the ship in any capacity on the business of that ship;
 - 7.2. Who is responsible for deciding the employment of the ship; and
 - 7.3. Who are the parties to the charter party(ies) if the ship is employed under a charter party(ies).
8. If a conflict arises between any safety and security requirements during the operation of the ship, the master shall give effect to these requirements necessary to maintain the safety of the ship; provided that the master shall implement temporary security measures commensurate with the prevailing security level; provided further that the information of such facts are given to:
 - 8.1. The Administration; and
 - 8.2. The Contracting Government in whose port facility/territory the ship is operating or intends to enter.
9. Every ship to which this Circular applies and intending to enter a port of a Contracting Government shall provide, upon request of the officers duly authorized by that Government, the following information:

- 9.1. That the ship possesses a valid ISSC and the name of the issuing authority;
- 9.2. The security level at which the ship is currently operating;
- 9.3. The security level at which the ship operated in any previous port where it has conducted a ship/port interface, at least for the last 10 port calls;
- 9.4. Any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface, at least for the last 10 port calls;
- 9.5. That the appropriate ship security procedures were maintained during any ship to ship activity, at least for the last 10 port calls; or

Other practical security related information (but not details of the ship security plan) taking into account the guidance given in Part B of the ISPS Code.

V. SHIP SECURITY:

1. Ships shall in compliance with this Circular be able to provide security measures that corresponds to the following security levels:
 - 1.1. Security level 1 – the level for which minimum appropriate protective security measures shall be maintained at all times.
 - 1.2. Security level 2 – 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.
 - 1.3. Security level 3 – the level for which further specific security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.
2. At security level 1, the following activities shall as minimum, be carried out through appropriate measures, taking into account the guidance given in Part B of the ISPS Code, in order to identify and take preventive measures against security incidents:
 - 2.1. Ensuring the performance of all ship security duties;
 - 2.2. Controlling access to the ship;
 - 2.3. Controlling the embarkation of persons and their effects;

- 2.4. Monitoring restricted areas to ensure that only authorized persons have access;
 - 2.5. Monitoring of deck areas and areas surrounding the ship;
 - 2.6. Supervising the handling of cargo and ship's stores; and
 - 2.7. Ensuring that security communication is readily available.
3. At security level 2, the additional protective measures, specified in the SSP shall be implemented for each activity detailed in paragraph V.2, taking into account the guidance given in part B of the Code.
 4. At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in paragraph V.2, taking into account the guidance given in part B of the ISPS Code.
 5. A ship should always operate at security level 1 unless instructed by the Administration or a Contracting Government to whose Port Facility it is to undertake a ship/port interface, to move to and operate at security level 2 or 3. In case there is a change to a higher security level, the ship shall respond without undue delay.
 6. Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.
 7. A ship prior to entering a port, or while in the port within the territory of a Contracting Government that has set security level 2 or 3 shall acknowledge receipt of the instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan. The ship shall likewise report any difficulties in implementation.
 8. If a ship is required by the Administration to set, or is already at a higher security level than that set for the port it intends to enter or in which it is already located, the ship shall advise, without delay, the competent authority of the Contracting government within whose territory the port facility is located and the port facility security officer of the situation.

VI. DECLARATION OF SECURITY:

1. The ship can in the following cases request for a Declaration of Security (DoS):

- 1.1. The ship is operating at a higher security level than the port facility or another ship it is interfacing with;
- 1.2. There is an existing agreement on Declaration of Security between the Government of the Philippines and the Government of the Country to whose port the ship is to enter;
- 1.3. There has been a security threat or a security incident involving the ship or the port facility as applicable;
- 1.4. The ship is at a port which is not required to have and implement an approved port facility security plan; or
- 1.5. The ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan.
- 1.6. The Declaration of Security shall be completed by the master or the ship security officer.
- 1.7. Where a ship is not in compliance with the requirements of either Chapter XI-2 of SOLAS, 1974, as amended, Part A of the ISPS Code, or this Circular, or cannot comply with the security level set by the Administration or by another Contracting Government and applicable to that ship, then the ship shall notify the appropriate competent authority prior to conducting any ship/port interface or prior to entry into port, whichever occurs earlier.

VII. SHIP SECURITY ASSESSMENT:

1. There shall be a Ship security Assessment (SSA) carried out for each ship covered by this Circular. The Company may take guidance under Part B of the ISPS Code when conducting the SSA.
2. The SSA shall be carried out by persons with appropriate skills to evaluate the security of a ship taking into account the Guidance given in Part B of the ISPS Code.
3. The SSP shall be developed based on a ship security assessment (SSA) which shall include an on-scene security survey and at least the following elements:
 - 3.1. Identification of existing security measures, procedures and operations;
 - 3.2. Identification and evaluation of key ship board operations that it is important to protect;
 - 3.3. Identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and

- 3.4. Identification of weaknesses, including human factors in the infrastructure, policies and procedures.
4. The SSA shall be documented, reviewed, accepted and retained by the Company.

VIII. SHIP SECURITY PLAN:

1. Development Of Ship Security Plan

- 1.1. The SSP shall be developed on the basis of a ship security assessment which shall form part of the submission to the Administration when approval of the SSP is being sought.
- 1.2. The SSP shall make provisions for the three security levels as provided under paragraph V.1 and must clearly stipulate the security measures that should be taken at each security level.
- 1.3. The SSP shall contain a clear statement emphasizing the master's authority and responsibility in respect of the safety and security of the ship.
- 1.4. The SSP shall be written in the English language.
- 1.5. The SSP may be kept in an electronic format provided that it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.
- 1.6. The SSP shall be protected from unauthorized access or disclosure.
- 1.7. The SSP shall, address, at the minimum, the following:
 - 1.7.1. Measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;
 - 1.7.2. Identification of the restricted areas and measures for the prevention of unauthorized access to them;
 - 1.7.3. Measures for the prevention of unauthorized access to the ship;
 - 1.7.4. Procedures for responding to security threats or breaches of security including provisions for maintaining critical operations of the ship or ship/port interface;

- 1.7.5. Procedures for responding to any security instructions which the Administration or a Contracting Government may give at security level 3;
 - 1.7.6. Procedures for evacuation in case of security threats or breaches of security;
 - 1.7.7. Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
 - 1.7.8. Procedures for auditing the security activities;
 - 1.7.9. Procedures for training, drills and exercises associated with the plan;
 - 1.7.10. Procedures for interfacing with port facility security activities;
 - 1.7.11. Procedures for the periodic review of the plan and for updating;
 - 1.7.12. Procedures for report security incidents;
 - 1.7.13. Identification of the ship security officer;
 - 1.7.14. Identification of the company security officer including with 24-hour contact details;
 - 1.7.15. Procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board, if any;
 - 1.7.16. Frequency for testing or calibration any security equipment provided on board, if any;
 - 1.7.17. Identification of the locations where the ship security alert system activation points are provided; and
 - 1.7.18. Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.
- 1.8. The information under paragraph VIII.1.7.17/.18 shall be kept in a document known only to the master, the SSO and senior officers of the ship.
 - 1.9. The ship security plan shall not be subject to inspection by officers duly authorized by a contracting Government to carry out control and compliance measures save in circumstances specified in paragraph VIII. 10 hereof.
 - 1.10. Should the control officers of a Contracting Government require a review of the SSP after determining that there are clear grounds to believe that the ship is not in compliance with the requirements of Chapter XI-2 of SOLAS, 1974 as amended or Part A of the ISPS Code or this Circular, such review shall be made only after consent is given by the Administration or the master; provided, that the provisions

in the plan relating to paragraph VIII.1.7 subsections .2, .4, .5, .7, .15, .17 and .18 of this Circular cannot be subject to inspection unless otherwise consent by the Administration had been granted.

1.10.1. The SSP to be developed shall:

1.10.1.1. Detail the organizational structure of security for the ship;

1.10.1.2. Detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;

1.10.1.3. Detail the communication systems to allow effective continuous communication with the ship and between the ship and others, including port facilities;

1.10.1.4. Detail the basic security measures for security level 1, both operational and physical, that will always be in place;

1.10.1.5. detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;

1.10.1.6. Provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and

1.10.1.7. Detail reporting procedures to the Administration and to the appropriate Port Facilities' contact points.

1.10.2. Subject to the provisions of paragraph VIII.3.1 of this Circular, a security organization recognized (RSO) by the Administration may prepare the ship security plan.

1.10.3. Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the company or the ship.

2. Amendments To The Ship Security Plan

- 2.1. Any amendment to the SSP shall likewise be based on a ship security assessment which shall form part of the submission to the Administration or the RSO acting on behalf of the Administration.
- 2.2. Changes to an approved SSP or to any security equipment specified in the approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. For this purpose, the Administration shall issue advisories to which specific area(s) of the SSP this particular provision shall apply.
- 2.3. The changes/amendments shall be at least as effective as those measures prescribed in chapter XI-2 of SOLAS 1974 as amended, Part A of the ISPS Code and this Circular.
- 2.4. The approval granted by the Administration to any amendment/change to the SSP which shall be documented in a manner that clearly indicates such approval, shall be made available on board and shall form part of the International Ship Security Certificate; provided that if the amendment/change be of a temporary nature, the reinstatement of the originally approved measures or equipment, shall render the approval for the amendment ineffective. The approval for the amendment so invalidated need not be retained onboard.

3. Review And Approval Of The Ship Security Plan

- 3.1. The SSP shall be subject to the review and approval by the Administration or any of the Security Organization so recognized by it; provided that if an RSO is to undertake the review and approval of the SSP or its amendments, such RSO should not have been involved in either the preparation of the ship security assessment, or of the ship security plan or of the amendments under review.
- 3.2. The Administration, shall to the extent possible, test the effectiveness of the SSP or of any amendment thereto which it had approved or had been approved on its behalf; provided that in the following cases, the Administration shall undertake such test:
 - 3.2.1. The ship had been denied entry by a Contracting Government upon a finding that the SSP does not

- conform with the requirements of the SOLAS, 1974, as amended and the Code;
- 3.2.2. Control officers of a Contracting Government had so reported to the Administration non conformity by the ship with the SSP.

IX. COMPANY SECURITY OFFICER:

1. The company shall designate a company security officer (CSO) with the following duties and responsibilities:
 - 1.1. Advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
 - 1.2. Ensuring that ship security assessments are carried out by persons with appropriate skills to evaluate the security of the ship;
 - 1.3. Ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
 - 1.4. Ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the ship;
 - 1.5. Arranging for internal audits and reviews of security activities;
 - 1.6. Arranging for the initial and subsequent verifications of the ship by the Administration or the RSO;
 - 1.7. Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;
 - 1.8. Enhancing security awareness and vigilance;
 - 1.9. Ensuring adequate training for personnel responsible for the security of the ship;
 - 1.10. Ensuring effective communication and co-operation between the SSO and the relevant port facility security officers;
 - 1.11. Ensuring consistency between security requirements and safety requirements;
 - 1.12. Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately;
 - 1.13. Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained; and

- 1.14. Ensuring the effective coordination and implementation of the SSP by participating in exercises at appropriate intervals.
2. The CSO shall have knowledge and have received training, as may be appropriate, in the areas specified under paragraph X.2 of this Circular.
3. The Company may designate more than one CSO depending on the number or types of ships it is operating, provided that there is a clear identification of the CSO who is responsible for which ships covered by this Circular.

X. SHIP SECURITY OFFICER:

1. The company shall designate a ship security officer (SSO) on each ship covered by this Circular who shall undertake the following functions:
 - 1.1. Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
 - 1.2. Maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;
 - 1.3. Coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;
 - 1.4. Proposing modifications to the ship security plan;
 - 1.5. Reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;
 - 1.6. Enhancing security awareness and vigilance on board;
 - 1.7. Ensuring that adequate training has been provided to shipboard personnel, as appropriate;
 - 1.8. Reporting all security incidents;
 - 1.9. Coordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and
 - 1.10. Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

2. The ship security officer shall have knowledge and must have received training, in some or all of the following, as appropriate:
 - 2.1. Security administration;
 - 2.2. Relevant international conventions, codes and recommendations;
 - 2.3. Relevant Philippine legislation and regulations;
 - 2.4. Responsibilities and functions of other security organizations;
 - 2.5. Methodology of ship security assessment;
 - 2.6. Methods of ship security surveys and inspections;
 - 2.7. Ship and port operations and conditions;
 - 2.8. Ship and port facility security measures;
 - 2.9. Emergency preparedness and response and contingency planning;
 - 2.10. Instruction techniques for security training and education, including security measures and procedures;
 - 2.11. Handling sensitive security related-information and security-related communications;
 - 2.12. Knowledge of current security threats and patterns;
 - 2.13. Recognition and detection of weapons, dangerous substances and devices;
 - 2.14. Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
 - 2.15. Techniques used to circumvent security measures;
 - 2.16. Security equipment and systems and their operational limitations;
 - 2.17. Methods of conducting audits, inspection, control and monitoring;
 - 2.18. Methods of physical searches and non-intrusive inspections; Security drills and exercises, including drills and exercises with port facilities; and
 - 2.19. Assessment of security drills and exercises.

XI. RECORDS:

1. Records of the following activities addressed in the SSP shall be left on board for at least the last two (2) years:
 - 1.1. Training, drills and exercises;
 - 1.2. Changes in security level;
 - 1.3. Communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been, in;
 - 1.4. Internal audits and reviews of security activities;
 - 1.5. Periodic review of the ship security assessment;

- 1.6. Periodic review of the ship security plan;
 - 1.7. Implementation of any amendments to the plan; and
 - 1.8. Maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.
2. In addition to the information listed in paragraph IV.7, records of the following for the last 10 port calls shall be kept on board.
 - 2.1. Security threats;
 - 2.2. Breaches of security;
 - 2.3. Declaration of security;
 - 2.4. Security level of the ship at each port call; and
 - 2.5. Information enumerated in paragraph IV.7 of this Circular.
 3. The records referred to in the proceeding paragraph shall be in the English language.
 4. The records may be kept in an electronic format, provided that they are protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment.
 5. The records shall be protected from unauthorized access or disclosure.

XII. VERIFICATION AND CERTIFICATION OF SHIPS:

1. Verifications

- 1.1. Ships covered by this Circular shall be subject to the verification as specified hereunder:
 - 1.1.1. An initial verification before the ship is put in service or before the ISSC required under paragraph XII.2.1 is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of Chapter XI-2 of SOLAS, 1974 as amended, the ISPS Code and this Circular and the SSP. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of Chapter XI-2 of SOLAS, 1974, as amended and the ISPS Code and this Circular, is in satisfactory condition and fit for the service for which the ship is intended;

- 1.1.2. A renewal verification which the Administration may specify but in no case exceeding five years, except where paragraph XI.3.1 or paragraph XII.3.6 is applicable. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of Chapter XI-2 of the SOLAS, 1974, as amended and the ISPS Code and the approved ship security plan, is in satisfactory condition and fit for the service for which the ship is intended;
- 1.1.3. At least one intermediate verification which shall take place between the second and third anniversary date of the ISSC as defined in Regulation I/2(n) of SOLAS 1974, as amended. The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate; and
- 1.1.4. Any additional verifications as may be determined/required by the Administration.
 - 1.1.4.1. Verification of ships shall be carried out by officers of the Administration or a recognized security organization acting on behalf of the Administration.
 - 1.1.4.2. The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of Regulations XI-2/4.2 and XI-2/6 of SOLAS 1974, as amended, the ISPS Code, this Circular and the SSP.
 - 1.1.4.3. After a verification has been undertaken, no changes shall be made in the security system and any associated security equipment or the approved ship security plan without the approval of the Administration.

2. Issue Or Endorsement Of Certificate

- 2.1. The Administration shall issue or endorse an International Ship Security Certificate (ISSC) after the initial or renewal

verification in accordance with the provisions of paragraph XII.1 of this Circular.

- 2.2. Where verification was undertaken by a recognized security organization, the Administration shall on the bases of the audit report by the RSO issue the ISSC.

3. Duration And Validity Of Certificate

- 3.1. The ISSC shall have a validity not exceeding five years upon its issuance.
- 3.2. When the renewal verification is completed within three months before the expiry date of the existing ISSC, 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 ISSC.
- 3.3. When the renewal verification is completed after the expiry date of the existing ISSC, 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 the expiry of the existing ISSC.
- 3.4. When the renewal verification is completed more than three months before the expiry date of the existing ISSC, 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 the completion of the renewal verification.
- 3.5. If the ISSC is issued for a period of less than five years, the Administration may extend the validity of the certificate beyond the expiry date to a maximum period of five years, provided that the verifications referred to in paragraph XII.1.1 of this Circular under this Circular and applicable when an ISSC is issued for a period of five years are carried out as appropriate.
- 3.6. 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 ISSC, the Administration or the recognized security organization acting on behalf of the Administration may endorse the existing ISSC and such a certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

- 3.7. If a ship, at the time when the ISSC expires, is not in port in 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 to be verified, and then only in cases where it appears proper and reasonable to do so. No ISSC shall be extended for a period longer than three months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new ISSC. When the renewal verification is completed, the new Certificate shall be valid to a date not exceeding five years from the expiry date of the existing Certificate before the extension was granted.
- 3.8. An ISSC issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the Administration for a period of grace up to one month from the date of expiry stated on it. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the date of expiry of the existing ISSC before the extension was granted.
- 3.9. If an intermediate verification is completed before the period specified in paragraph XII.1.1, then:
 - 3.9.1. The expiry date shown on the ISSC 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;
 - 3.9.2. The expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the verifications prescribed by paragraph XII.1.1 are not exceeded.
- 3.10. An ISSC issued under paragraph XII.2 shall cease to be valid in any of the following cases:
 - 3.10.1. If the relevant verifications are not completed within the periods specified under paragraph XII.1.1;
 - 3.10.2. If the Certificate is not endorsed in accordance with paragraph XII.1.1.3 and paragraph XII.3.9.2 if applicable;
 - 3.10.3. When a Company assumes the responsibility for the operation of a ship not previously operated by that Company; and

3.10.4. Upon transfer of the ship to the flag of another State.

3.11. In case a ship being operated by the company is to be transferred to another company, the company as herein covered by the Circular, shall, as soon as possible, transmit to the receiving company copies of any information related to the International Ship Security Certificate or to facilitate the verification described in paragraph XII.4.2.

4. Interim Certification

4.1. After 01 July 2004, the Administration may cause an Interim International Ship Security Certificate (Interim-ISSC) to be issued in any of the following cases:

4.1.1. A ship without a certificate, on delivery or prior to its entry or re-entry into service;

4.1.2. Transfer of a ship from the flag of a Contracting Government to the Philippine flag;

4.1.3. Transfer of a ship to the Philippine flag from a State which is not a Contracting Government;

4.1.4. When a company assumes the responsibility for the operation of a ship not previously operated by that Company.

4.2. A interim ISSC shall only be issued after the Administration or the RSO, acting on behalf of the Administration, has verified that:

4.2.1. A ship security assessment required by the ISPS Code and this Circular has been completed;

4.2.2. A copy of the SSP meeting the requirements of chapter X1-2 of SOLAS,1974 as amended, this Circular and Part A of the Code is provided on board and has been submitted for review and approval, and is being implemented on the ship;

4.2.3. The ship is provided with a ship security alert system meeting the requirements of Regulation X1-2/6 of SOLAS, 1974 as amended, if required;

4.2.4. The Company Security Officer:

4.2.5. Has ensured:

4.2.5.1. The review of the SSP for compliance with this regulation of the Circular;

4.2.5.2. That the SSP has been submitted for approval;

4.2.5.3. That the plan is being implemented on the ship; and

- 4.2.5.4. Has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the CSO is satisfied that the ship will successfully complete the required verification in accordance with paragraph XII.1.1.1 of this Circular within six (6) months;
- 4.2.5.5. Arrangements have been made for carrying out the required verifications under paragraph XII.1.1.1 of this Circular;
- 4.2.5.6. The master, the SSO and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in the ISPS Code and in this Circular and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the English language; and
- 4.2.5.7. The SSO meets the requirements of this Circular.
- 4.2.6. An interim-ISSC may be issued by the Administration or by a recognized security organization, authorized to act on its behalf.
- 4.2.7. An interim-ISSC shall be valid for 6 months, or until the certificate required by paragraph XII.1.1.2 of this Circular is issued whichever comes first, and may not be extended.

XIII. SANCTIONS AND PENALTIES:

1. A Company found to have violated any of the provisions of this Memorandum Circular shall be imposed the following fines:

First Violation	-	P50,000.00
Second Violation	-	100,000.00
Third and succeeding violations	-	200,000.00
2. The Administration may, after proper determination of the gravity of non-compliance with this Circular, order a ship to cease operations until corrective action is instituted and clearance by the Administration thereto had been granted.

XIV. REPEALING CLAUSE:

All memorandum circulars, rules and regulations and other issuances inconsistent with this Memorandum Circular are hereby amended, repealed or modified accordingly.

XV. EFFECTIVITY CLAUSE:

The provisions of this Memorandum Circular shall take effect fifteen (15) days after publication once in a newspaper of general circulation unless otherwise herein specified.

Manila, Philippines, 11 August 2003.

BY AUTHORITY OF THE BOARD:

(Sgd.) OSCAR M. SEVILLA
Administrator

SECRETARY'S CERTIFICATE

This is to certify that Memorandum Circular No. 193 has been approved by the MARINA Board on its Special Board Meeting held on 11 August 2003.

(Sgd.) ATTY. GLORIA V. BAÑAS
Acting Corporate Board Secretary

Published on 16 August 2003 at Today's Newspaper copy filed with UP Law Center on _____.