



INTERNATIONAL SHIP REGISTRY OF GABON
COMMISSIONAIRE OF MARITIME AFFAIRS

INTERSHIPPING SERVICES LLC.
OFFICE 601, AL SAWAN 1, AL RASHIDIYA 03, AJMAN, U.A.E P.O BOX 4295
T: + 971 6 74 28 120 F: +971 6 744 1270
EMAIL: admin@intershippingsservices.com WEBSITE: www.intershippingsservices.com

MARCIR: 06/2019

DATE: 24th AUG 2019

To : Owners/Operators, Masters, Flag State Surveyors, Recognized Organizations.

Subject : International Ship & Port Facility Security Code (ISPS Code)

PURPOSE:

This Marine Circular is to provide guidance and instructions to the owners, operators, Recognized Organizations and Masters of Gabonese flagged ships concerning the Administration's requirements for compliance with the International Ship & Port Facility Security Code (ISPS Code). This guidance encompasses information how Companies operating Gabonese flagged ships can gain International Ship Security Certification along with policies of Administration and interpretations regarding application and implementation of the ISPS Code Part A, and incorporation of the relevant sections of Part B.

The International Ship Registry of Gabon requirements are not intended to be all-inclusive or to prohibit a Company from incorporating procedures, processes or other items that go beyond the ISPS Code, when developing or implementing the Ship's Security Program on board their vessels. Questions regarding the ISPS Code should be referred to the:

International Ship Registry of Gabon
Office of the Commissionaire of Maritime Affairs
Intershipping Services LLC
Office 601, 6th Floor, Al Sawan Tower 01
Taqeef Showroom Building
P.O 4295 Ajman,
U.A.E.

1. **APPLICATION:** This Notice is applicable to the following Gabon flagged ships engaged on international voyages:
 - Passenger ships, including high-speed passenger craft,
 - Cargo Ships, including high speed craft, of 500 gross tonnage and upwards; and
 - Self-Propelled Mobile Offshore Drilling Units. Where applicable specific equipment requirements for specific classes or types of ships are spelled out elsewhere in these instructions.

1.1 The ISPS Code does not apply to:



- Government-operated ships used for non-commercial purposes;
- Cargo ships, including commercial yachts of less than 500 gross tonnage (ITC 69), voluntary compliance as of 1 July 2006 (see §4.4 below);
- Ships not propelled by mechanical means;
- Wooden craft of primitive origins;
- Private pleasure yachts not engaged in trade;
- Fishing vessels;
- Non-self-propelled mobile offshore drilling units, nor to mobile offshore drilling units of any description while on location, making field moves, or in port;
- Mobile and immobile floating production, storage and offloading units (FPSOs) and floating storage units (FSUs), floating production units (FPUs), moored oil storage tankers (MOSTs) and mobile offshore units (MOUs) but should have some security procedures in place; and
- Single buoy moorings (SBMs) attached to an offshore facility that are covered by the facility's security regime, or if connected to a port facility, covered by the port facility security plan (PFSP).

2. DEFINITIONS:

Definitions have been taken from the ISPS Code Part A, Paragraph 2 and SOLAS Chapter XI-2, Regulation 1.

2.1 Administration:

The Office of Commissioner of Maritime Affairs of the Republic of Gabon.

2.2 Company:

The owner of the ship, or the organization or person such as the Manager or the Bareboat Charterer, assuming the responsibility for operation of the ship from the ship owner, and when assuming such responsibility has agreed in writing in accordance with ISM Declarations filed with the Administration to take over all the duties and responsibilities imposed by the ISM Code.

2.3 Recognized Security Organization (RSO):

Classification Society, with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized by the Administration to carry out security verifications and certification aboard Gabon Flagged Ships.

2.4 Security Consultants:

Organizations, which may perform threat assessments, vulnerability assessments, develop security plans and/or provide training to CSOs and SSOs.

2.5 Port Facility Security Officer (PFSO):

The person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with ship security officer and company security officer.

2.6 Company Security Officer (CSO):

The person designated by the Company for ensuring that a Ship Security Assessment is carried out; that the ship security plan is developed, submitted for approval and thereafter



implemented and maintained and for liaison with the port facility security officer, ship security officer and the Administration.

2.7 Ship Security Officer (SSO):

A Person on board the ship, who if not the Master, is accountable to the Master and designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the Company Security Officer, Port Facility Security Officer and the Administration.

2.8 Security Level 1:

The level for which the minimum appropriate protective security measures shall be maintained at all times.

Security Level 2:

The level for appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of security incident.

Security Level 3:

The level for which further specific protective 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.

2.9 Ship Security Assessment:

A process of defining the threats, and examining the ship's vulnerability to attack in order to design an effective security plan.

2.10 Ship Security Plan (SSP):

A plan developed for each vessel in the fleet by a competent Company Security Officer or a security consultant to ensure the application of measures on board the ship designated to protect persons on board, cargo, cargo transport units, ship's stores or ship from risks of a security incident.

2.11 Verification (Audit):

Evaluation of the ISPS Code and Security Plan implementation on board a Ship by an auditor or by RSO to determine compliance with the ISPS Code.

3. COMPLIANCE GUIDANCE:

3.1 ISPS Code compliance requirements:

Every ship to which the Code applies must have:

- A Company Security Officer,
- A Ship Security Officer,
- Implemented an approved SSP,



- The IMO Number marked on the vessel, (please see section 8.1)
- Installed AIS, (please see section 8.2)
- A Continuous Synopsis Record - CSR (please see section 8.3) and
- Installed Security Alert System (please see section 8.4).

3.2 Training of CSO and SSO:

Company Security Officers and Ship Security Officers receive the appropriate training and thus it is the responsibility of the Company to ensure.

3.3 Other Mandatory Minimum Security-Related Training and Instructions for Seafarers – Please Refer Instructions (STCW Regulation VI/6)

3.4 Use of Consultant for Security:

Companies shall decide to hire or train people to develop the required ship security expertise within their organization. They are to draft their own Ships Security Plans and conduct the Ship Security Assessments.

3.5 Requirement of Manning:

Once the vulnerability assessment is carried and identified, the company should take into account any additional workload which may result from implementation of the SSP and ensure that the ship is sufficiently and effectively manned. The company should consider the need to use contracted personnel for short periods of time to augment the ship's security force in order to provide sufficient protection.

3.6 Verification Audits and Certification:

All Ships Security Plans are to be submitted to the Administration for approval in accordance with Section 4.11 for ISPS Code implementation and will carry out verifications on Gabon flag ships.

Auditors shall conduct verification audits under the ISM Code which may be “harmonized” with security audits. The Administration has also designated RSO for the purpose of conducting ISPS verification audits. A company can choose whether to have the Administration or the RSO conduct the verifications. These Classification Societies are also Gabonese Recognized Security Organizations.

3.7 Incorporation of ISPS into Company's ISM Code (SMS)

Although it is not a requirement, the company should contemplate incorporating the relevant shipboard security requirements into the company's Safety Management System (SMS).

The Safety Management system should:

- Define the security duties and responsibilities for the Company Security Officer, the Ship Security Officers and the crew.



- Shall have incorporated procedures for immediately reporting any noncompliance with the ISPS Code, threats and breach of security to the Administration.
- Shall maintenance requirement for the security equipment.
- Provide for the logging of actions or measures taken to rectify deficiencies and non-conformities noted during Security Assessments and notification of the Administration and the RSO of any corrective actions taken.
- Provide the list of records to retain on board and retention period.
- Discuss who will be responsible for organizing security drills and exercises.
- Define the procedures for the harmonized internal ISM and ISPS Code audits.
- State the company will provide the support necessary to the Company Security Officer, the Master and/or the Ship Security Officer to fulfill their duties and responsibilities in accordance with chapter XI-2 and the ISPS Code.

3.8 Part B as Mandatory

While the Gabonese Maritime Administration has not mandated compliance with sections of ISPS Code Part B, companies are advised that Port State Control Authorities may require mandatory compliance with Part B.

3.9 Master's Authority

The Gabonese Maritime Law defines the Rights and Duties of the Master. The Administration also acknowledges the importance of IMO Resolution A.443 (XI), "Decisions of the Shipmaster with regard to Maritime Safety and Marine Environment Protection". The Ship's Security Plan shall incorporate the elements of both A.443 (XI) and the National Requirements to ensure the Master's authority on board the ship. Therefore, any system of operational control implemented by Company shore based management must allow for the Master's absolute authority and discretion to take whatever action he/she considers to be in the best interest of passengers, crew, and the cargo.

4. Compliance Monitoring

Compliance with the ISPS Code is closely monitored and enforced by the Administration. Ships that fail to comply with the ISPS Code will be considered in violation of SOLAS and may be prevented from trading.

4.1 Designation of Company Security Officer

The owner or operator of each vessel must provide the Office of the Commissioner with the name, address, telephone, fax, email, telex numbers and after office hours contact information



of the individual(s) in their Company who have been designated as the Company Security Officer and Deputies. This information should be in the Ship's Security plan. Changes should be sent by e-mail or fax or mail. A Declaration of Company Security Officer form (QP/CSO/A/REV 1/ 2018) should be completed and forwarded to admin@intershippingsservices.com

4.2 Selecting a Ship Security Officer

One of the senior officers onboard (Master or Chief Officer or Chief Engineer or 2nd Engineer) to perform the Ship Security Officer duties to be nominated by the Company. The individual selected shall be familiarized and trained to fulfill this duty.

4.4 Conducting the Ship Security Assessment

The Company may use their Company Security Officer, other trained personnel/ consultants to conduct the on-scene Ship Security Assessment with appropriate skills to evaluate the security of a ship. Auditor shall be independent of the activities being assessed unless this is impracticable due to the size and the nature of the Company or of the ship. Specifically, the person conducting the Ship Security Assessment should not be any of the officers or crewmembers permanently assigned or serving onboard the ship.

On new ships or ships new to a Company, the Ship Security Assessment can be carried out by the SSO or any other qualified officer who has not been assigned or served onboard this ship before as in case of initial interim verification).

4.5 Ship Security Assessments (ISPS Code Part A/8)

4.5.1 The Ship Security Assessment is an essential and integral part of the process of developing and updating the Ship Security Plan.

4.5.2 The Ship Security Assessment shall include an on-scene security survey, which incorporates but is not limited to the following elements:

- Identification of existing security measures, procedures, operations;
- Identification and evaluation of key ship board operations that need protection;
- 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
- Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

4.5.3 The Ship Security Assessment shall be documented, reviewed, accepted and retained onboard the ship and in the Company's office.

4.6 Drafting the Ship Security Plan

The Company may choose to prepare the Ship Security Plans using their trained Company Security Officer, or they may use a Security Consultant. When using a consultant the company should make sure the plan reflects the company's security policies and practices that are achievable.



4.7 Fleet Plans and Sister Ships

Each vessel shall have an individual Ship Security Plan tailored to its Security Assessment. However, there will be information in each ship's plan that will be the same for all of the ships in the company's fleet, for vessels on the same trade route and for sister ships operating in the same trade. The Security Assessment for the first ship can be used as a model for each of the other ships engaged in the same trade on the same routes. In such a case, only the ship's specific variations need be addressed during the on-scene Security Assessment.

4.8 Restricted Areas

All restricted areas should be annotated on a General Arrangement Plan or other drawings of the vessel. The SSP should provide that all restricted areas are clearly marked indicating that access to an area is restricted and that unauthorized presence within an area is considered a breach of security. Clearly marked means that the area is marked in a manner that should communicate its restricted status to any visitors or person on board.

4.9 Declaration of Security (DOS)

The Ship's Security Plan shall reflect the Administration's requirement that the Ship's Security Officer shall complete a Declaration of Security as described in the ISPS Code Part A/5 and when deemed necessary by the Master or SSO.

The Administration requires that the *last 10 completed "Declaration of Security"* reports be maintained onboard.

4.10 Language and Record keeping

All Ship Security Plans shall be written in English and the working language of the crew if other than English. Also, all records that should be presented to an auditor or port authorities shall be recorded in English. The records should be detailed as much as possible.

To assist some of the crew it is recommended to have parts of the SSP translated as instructions manuals in a working language which is understood by most of the crew.

All Records listed under ISPS Code part A/10.1 shall be kept for at least 3 years. This is to ensure they will be available for review during the following verification audits.

4.11 Ship Security Plan Approval

4.11.1 All SSPs are required to be approved by the Administration. The company shall submit a single hard copy of each Ship Security Plan to the Administration, in English, for approval. All plans shall include the current Security Assessment that forms the basis of the plan, or the amendments.



To facilitate the plan approval process, it is recommended to complete the checklist used by the Administration for plan approval and attach it to the submitted plan. The checklist identifies the applicable sections of ISPS code Part A and Part B for the Ship Security Plan in order to be approved as meeting the Code.

4.11.2 After the Ship Security Plan has been approved by the Administration, the company will receive an approval certificate with the returned plan. The following pages of the plan shall be stamped and scanned for control purposes:

- SSP Title Page.
- SSP Index (Table of Contents).
- SSP Amendments Page (Revisions, History of Changes, etc.)

The following pages of the plan will be retained by the Administration in vessel SSP file:

- SSP Title Page.
- SSP Index (Table of Contents).
- SSP Amendments Page.
- Vessel Particulars (Ship Specific Information).
- Sections describing unique Communications and/or Security Equipment.

4.12 Sending the Ship Security Plan in a secured manner

The plan shall be mailed to the Commissionaire of Maritime Affairs, International Ship Registry of Gabon, Ajman, U.A.E using a courier service which has a tracking facility. It shall be sent in a sealed envelope or box inside the shipping container supplied by the courier service. The company sending the Ship Security Plan shall send an email to shipalert@intershippingsservices.com stating the date the plan was sent, the contact information for the courier service and the tracking number. The Administration will follow a similar process in returning the plan.

4.13 Amendments to an approved Ship Security Plan

Revisions to the ship security plan shall be sent to the Administration by e-mail or mail, for review and approval. A cover letter shall be included with the document forwarded stating the nature of the revisions.

Amendments relating to the following matters must be approved by the Administration:

- Any changes in security procedures and equipment used on board a ship.
- Change of Owners or contact details. Only affected pages should be submitted to the Administration.
- Change of Name. Only affected pages should be submitted to the Administration.
- Change of management. A new Ship Security Assessment and Ship Security Plan shall be submitted to the Administration for approval. A Security Verification will be required.



The nature of any changes to the Ship Security Plan or to the security equipment or procedures that have been specifically approved by the Administration shall be clearly documented in the revised plan. The CSO shall submit the amendments record sheet with each revision.

The Administration's approval letter shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate).

4.14 Electronic Format

The Ship Security Plan may be maintained by the company and aboard their ships in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction, amendment or observation by unauthorized persons. The Company must send one hard copy for approval accompanied with the electronic version.

4.15 Security of the Ship Security Plan

The Plan shall be protected from unauthorized use or exposure. The Company Security Officer and the Ship's Security Officer are responsible for the security of the plan. The Company Security Officer will determine which parts of the plan shall be available to the crew and which items are to be kept confidential, taking in consideration the following:

- Identification of the restricted areas,
- Procedures for responding to security threats,
- Procedures for responding to security instructions from contracting governments or administrations when setting security level 2 and level 3,
- Duties of shipboard personnel assigned security duties,
- Procedures for ensuring the inspection, testing, calibration and maintenance of security equipment on board,
- The location of the Ship Security Alert activation switches,
- Guidance or instructions on the use of the ship security alert system, including testing activation, deactivation and resetting and the methods for limiting false alerts.

4.16 Company Security Exercises

In accordance with the provisions of the ISPS Code companies should plan and conduct periodic security exercises to test the company's procedures for responding to security alerts and incidents. The Exercise required to be carried out at least once each calendar year with no more than 18 months between exercises. The exercise must test communications, company co-ordination, resource availability and response (ISPS Code B/13.7).

Exercise participants may include the Flag Administration, Port Facility Security Officer (PFSO) or coastal state authorities, Ship Security Officer (SSO), and the Company Security Officer (CSO) along with other shore based management of the vessel involved with security and/or emergency response. If possible, it should also include, as applicable, the alternate company security officer(s). The exercises may be held in concert with other exercises such as search and rescue or emergency response.



4.16.1 The Administration' Guidelines for Security Exercises

4.16.1.1 The Exercise should involve at least one vessel of the fleet, which may be Gabonese or a non-Gabonese flag vessel. Operators with large fleets are encouraged to include additional vessels when conducting an exercise in order to provide an opportunity for a greater number of their officers to gain more experience and training.

4.16.1.2 The Administration will accept as meeting the requirements of ISPS Code, a real security incident in which one of the company's vessels, including a non- Gabonese flag vessel, is involved provided all of the exercise elements were implemented and the company provides an incident summary report to all other Gabon Flagged vessels in the fleet and to the Administration.

4.16.1.3 The primary aim should not simply be to comply with ISPS requirement, but also to ensure the continuous improvement of the company's and ship's emergency preparedness and the ability to respond in security situations.

4.16.1.4 The CSO may consider coordinating the security exercise with the onboard security drill with participation of the officers and crew as per the procedure laid down in the SSP. The exercise scenario should replicate as closely as possible as an emergency so that when an emergency occurs, the company and vessel personnel will respond as intended to the incident, rather than taking valuable time to develop a response.

4.16.1.5 The following records are suggested to be collected during the exercise:

- The date held and description of the Exercise scenario.
- Times of key communications, including initial exercise (Ship/Shore) Notification issued by the Master/ SSO or the CSO.
- List of all participants.
- Copy of the Crew List at the time of the security drill, if applicable.
- All correspondence between the vessel and various shore authorities / companies involved in the exercise.
- Any other documentation and/or photographs considered relevant.
- An evaluation of the exercise by the SSO & Master forwarded to the CSO.
- The CSO should review and evaluate the Master's report and make his recommendations including lessons learned and improvements to the SSP.

4.16.1.6 As documentary evidence of the exercise, the CSO will provide a summary of the exercise to the vessels in fleet, as applicable, and to the Administration, that includes:

- Description of the scenario,
- A summary of the exercise, (time/date/location-participants sequence of major events),
- A list of all parties involved, and
- Description of any lessons learned that could improve the SSP.

4.16.1.7 The Administration may want to participate in your Company Security Exercises to evaluate the effectiveness of the Plan and the interaction of the Company Security Officer with the



Security Plan. The Company Security Officer, when requested by the Administration, will provide the following information:

- The date of the exercise,
- The name of the Ship,
- The place where the exercise will take place, and
- The type of exercise.

4.17 Planning the Verification

The Flag administration surveyor or the approved RSO auditor will prepare the verification plan and update the Company Security Officer.

4.17.1 The Verification plan shall be sufficiently flexible to permit changes based on the information gathered during the verification.

4.17.2 The Verification plan shall include the following elements:

- Date and place where the verification will be conducted;
- Objectives and scope;
- The expected time and duration for each activity; and
- Findings after review of the Ship Security Plan;
- Identification of Company and Ship Security Officer;
- Identification of reference documents such as the Code, Ship Security Assessment, on scene survey and Ship Security Plan as applicable;
- Confidentiality requirements.

The verification plan shall be part of the report which will be provided to the Administration for final review.

4.18 Full term and Interim Verification

4.18.1 Requirements: Only the Flag Auditor or an approved RSO auditor is authorized to conduct verifications on behalf of the Administration.

- Flag surveyor or the RSO may not carry out ISPS Code verification on a Gabonese ship in which they or any of their organizations subsidiaries or commonly owned affiliates have performed Ship Security Assessments or prepared the Ship Security Plan for that ship.
- The company must contact the Administration or RSO to arrange for the initial verification. Failure to have a valid International Ship Security Certificate (ISSC) will be considered a violation of SOLAS and the ship may be prevented from trading.
- No full term verification shall be conducted if the review of the Ship Security Plan indicates that the Ship Security Assessment conducted by the Company Security Officer or his contracted Security Consultant does not meet the requirements of the ISPS Code.
- The Ship Security Plan must be implemented on board before the initial verification. The Administration does not specify minimum implementation period, however, the company



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

4.18.2 Interim Verification: The Administration is aware of the short period allowed for implementation onboard newly operated vessels; therefore the following minimum requirements will be verified during Interim Verification:

- The ship has a Draft copy of Security Plan on board.
- The Ship Security Assessment and Ship Security Plan have been submitted to the Administration for approval.
- The Company Security Officer has been designated and trained.
- The Master and senior officers are familiar with their security duties.
- The crew has received security training before the vessel gets underway.
- All Security related forms and documents are onboard.
- The required records have been started.
- Security instructions which the company has identified as essential to be provided to the Master prior to the vessel's first voyage under Gabon flag have, in fact, been given to the Master.
- There is a plan to conduct full term verification within six months

4.18.3 Verification by Flag State surveyor

An Audit carried out will be conducted as described below:

- Preparation of the Audit: The auditor shall coordinate his visit onboard the vessel with the local agent and CSO.
- When executing the audit the auditor shall:

Conduct an opening meeting with at least the Master and SSO using the following agenda:

- Confirmation of the security level of the vessel and the port.
- Confirm the working language.
- Introduction of the members of the audit team.
- Explanation of the scope and requirement of the audit.
- Outline the audit program and ensure there is sufficient time to complete the audit.
- Set communication guidelines for auditors and crew.
- Agree who in the crew will accompany the auditors as they verify the security measures on board the vessel.
- Verify vessel's crew list.
- Confirm that adequate resources and accessibility to restricted areas shall be provided to the auditors.
- Confirmation that the auditor will ensure the confidentiality of the information obtained during the audit.
- Schedule the closing meeting.



Conduct an audit team briefing with all parties who participate in the audit and familiarize himself with the approved SSP. A photocopy of the SSP shall not be accepted and if an approved SSP is not available, the auditor will not continue with the audit

- Conduct the audit with the audit team.
- Conduct an audit team debriefing to gather conclusions and recommendations.
- Conduct a closing meeting with at least the Master and SSO.
- Final report to be submitted to the head office.

4.19 Non-Conformities and Additional Verifications

4.19.1 An International Ship Security Certificate (ISSC) will not be issued if there are any ISPS Code deficiencies. Deficiencies identified during the verification audit shall be documented and reported to the Company Security Officer and the Administration.

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

4.19.3 The Administration retains the right to conduct verification and inspection activities independent of or in concert with those of a RSO in order to verify proper implementation, application, and enforcement of the provisions of the ISPS Code

4.20 Certification

An ISSC shall be issued to each ship following a satisfactory verification either by the Flag Administration or an approved RSO auditor working on behalf of the Administration.

4.20.1 The ISSC will not be issued until all deficiencies in the implementation or the plan itself have been rectified.

4.20.2 The ISSC will be issued for a period of up to five years from the date of successful completion of the initial verification. It may be issued for a shorter period of time if the Company wants to harmonize the ISSC with the SMC.

4.20.3 The validity of the ISSC is subject to at least one intermediate verification (by the Administration or an approved RSO) between the dates of second and third anniversary of the issuance of the ISSC. If the ISSC is issued for a period of less than three years the verification will be conducted upon the renewal and an intermediate verification will not be required.

4.20.4 The company is responsible for conducting an internal security audit each year on each ship to assess the functioning and effectiveness of the Ship Security Plan on board. This can be done in concert with the internal ISM audit.

4.20.5 Re-issuance of the ISSC is contingent upon the satisfactory verification of the effectiveness of the Ship's Security Plan in meeting the objectives specified by the ISPS Code.



4.21 Interim Certification

4.21.1 Interim International Ship Security Certificates may only be issued if the Administration or an approved RSO acting on behalf of the Administration verified compliance with provisions of the ISPS Code A/19.4.2 and for the following purposes:

- New ships on delivery,
- Existing ships on reactivation,
- Transfer from another Flag, or
- A company takes on responsibility for the operation of a ship which is new to the company.

4.21.2 Prior to the expiration of the Interim International Ship Security Certificates, the Administration or the approved RSO should issue full term International Ship Security Certificates upon satisfactory verification that the Ships Security Plan has been implemented on board the ship.

NOTE: The Interim ISSC may not be extended (See 19.4.4 of Part A of the ISPS Code)

4.22 Exemptions and Dispensations

While the Administration may consider issuing manning dispensations in the event that the Ship Security Officer becomes incapacitated, companies are advised that Port State Control Authorities may prohibit entry into a port of a vessel with such a dispensation.

5. NONCOMPLIANCE WITH THE ISPS CODE

5.1 Certificate Withdrawal ISPS Certificates may only be withdrawn at the determination of the Administration.

Cause for certificate withdrawal may include, but is not limited to, the following deficiencies:

- Failure to coordinate and conduct the periodic or intermediate verifications;
- The information on the CSR is not correct;
- The Company Security Officer fails to ensure compliance of a vessel;
- The Ship's failure to maintain its Ships Security Plan in compliance with the requirements of the ISPS Code;
- The Ship's failure to install required hardware such as AIS, or SSAS and/or failure to mark the IMO Number as required.
- Deviations or defects related to the ISPS Code requirements which remain uncorrected beyond their due date.

5.2 Appeals

In the event a Company disagrees with a determination made by the Flag Auditor or the approved RSO auditor, the Company Security Officer may make a direct appeal to the Administration. The final determination will be based upon both the substance of the appeal.



6. Alternative security agreements

At the request of the vessel's operators, the Administration will conclude Alternative Security Agreements with other Contracting Governments for vessels engaged upon limited short International voyages, usually on fixed routes between ports that must also be party to the agreement. As part of the agreement, Gabon or one of the other Contracting Governments signing the agreement shall agree to inform other Contracting Government which may be affected by providing a notice to the appropriate subcommittee at IMO. In no case, shall such agreement compromise the level of security of other ships, and port facilities not covered by this agreement. Ships covered by such an agreement, may not engage in ship-to-ship activities with ships not covered by said agreement. Such agreements shall be reviewed by this Administration annually or earlier if the need arises and shall be reviewed by all parties at least every five years. It is the vessel operator's responsibility for working with the other Contracting Government to develop the first draft of the agreement for signature.

7. Interfacing with port and coastal authorities

7.1 Interaction

The SSP should include procedures and security measures for interfacing with ports, vessels, platforms and facilities. (ISPS Code B/9.5.1). The Company Security Officer and the Ship Security Officers are encouraged to contact the Port Facility Security Officer (PFSO) and develop a close working relationship. Port Facility contacts are available on the International Maritime Organization's ISPS Code database which may be accessed via the IMO website, www.imo.org by following the links to "GISIS" and by selecting "Maritime Security"; or using the URL <http://gisis.imo.org/public/>

7.2 Differences in the Security levels set

If a ship is at a security level, which is different from that of the Port or Coastal State Authorities in which the ship sails, then the ship will set the higher security level of the two. If the Ship's security level is higher than the port, facility, vessel or platform then the Ship Security Officer will notify the Company Security Officer. The CSO should provide this information to the PFSO together with any background information that he has available.

7.3 Report of Port Facility Security concerns

When a Ship Security Officer has concerns about security of a port facility, which is supposed to operate in accordance with an approved Port Facility Security Plan he should report the problem to the Master and contact the PFSO to discuss the matter. If the concerns cannot be resolved, he should:

- Report such concerns to the Company Security Officer.
- Record the actions taken by the CSO and/or SSO to establish contact with the Port Facility Security Officer (PFSO), and/or any other persons responsible for the security of the port, ship or platform being interfaced;
- Record security measures and procedures put in place by the ship, bearing in mind the security level set by the Administration and any other available security related information; and request a Declaration of Security or complete and sign, on behalf of the ship alone, a Declaration of Security, if the PFSO declines or is unavailable;



- Implement and maintain the security measures and procedures set out in the Declaration of Security throughout the duration of the interface; and
- Report the actions taken to the CSO and through the CSO to the Administration.

The CSO shall contact the Administration if assistance in obtaining a resolution is needed.

7.4 Report of Ship Security defects

When a Port State inspector has determined that there is a problem with the Ship's Security Plan or the implementation of the plan on board a ship, the Master is to report the problem to the CSO. The CSO shall notify the Administration. The Administration will consider sending a Surveyor to verify the compliance onboard the vessel. The CSO shall send a corrective action report to the Administration covering all deficiencies found.

8. Technical and Equipment Requirements

8.1 Ship Identification Number (SOLAS Chapter XI-1 Regulation 3):

Ships constructed before 1 July 2004 by the first scheduled dry-dock after 1 July 2004 and for all vessels built on or after 1 July 2004, the ships identification number (IMO number) shall be permanently marked on the vessel in accordance with the regulations. The number includes the letters IMO in front of the number (example: IMO1234567).

8.1.1 The permanent marking will be plainly visible, clear of any other markings on the hull and shall be painted in a contrasting colour.

8.1.2 The markings shall be made by raised lettering or by cutting it in or by centerpunching it or by any other equivalent method that ensures the marking is not easily expunged.

8.1.3 On ships constructed of material other than steel or metal, the Administration shall have to approve the method of permanently marking.

8.2 Automatic Identification Systems (AIS)

All Gabonese Flag Ships engaged in international voyages are required to have an Automatic Identification System approved by the vessel's Classification Society.

8.2.1 If an AIS has not been installed on the ship the ship must have either an exemption certificate issued by the Administration. The Administration may exempt ships from the application of these requirements when such ships will be taken permanently out of service within two years after the implementation date.

8.3 Continuous Synopsis Record (CSR) SOLAS Chapter XI-1 Regulation 5

All vessels that are required to comply with the ISPS Code are required to maintain a Continuous Synopsis Record, which includes a history of registration, ownership, and management of the vessel. The vessel's owners shall ensure the vessel's CSR records include all original CSRs, CSR Amendment request forms, and Index of Amendments. The Administration will maintain a copy of the CSR record for Gabon Flagged ships as long as they remain in the registry. The vessel operator is responsible for keeping the Administration informed of any changes regarding their vessels CSR record. Failure to keep the



Administration informed of any changes is cause for the Administrations withdrawal of a ship's ISSC.

A CSR Attestation letter shall be issued by the Administration for a maximum validity of 3 months for new registration taken as a lead time to enable updated CSR cancelling from previous Flag.

8.4 Ships Security Alert (SOLAS Chapter X1-2 Regulation 6)

All vessels listed below and engaged on international voyages shall have a ship's security alert system installed.

The following vessels of 500 gross tonnage and upwards;

Oil tankers
Chemical tankers
Gas carriers
Bulk carriers
Cargo high-speed craft
Other Cargo Ships and
Self-Propelled Mobile offshore drilling units
High-speed passenger craft

8.4.1 Verification of Installation:

8.4.1.1 Initial SSAS Verification: The on board installation and operation of the SSAS must be verified upon installation by a security auditor from the Administration or the RSO that issued the ISSC for a particular vessel. The issuer of the ISSC is already familiar with the SSP and the vessel.

The SSAS equipment and its operation are confidential. In order to maintain the confidentiality of the SSAS, the verification of the SSAS should be conducted by the same organization that issued the ISSC. The number of individuals involved in review and verification process, and who have knowledge of the location of the activation buttons should be kept to a minimum.

8.4.1.2 Verification Procedure:

- A SSAS message marked "TEST" shall be sent by the ship to the Administration in order to verify that the system works properly, prior to having the installation verified by an auditor. Confirmation of receipt of the SSAS message will be sent by email to the CSO. The CSO should provide a copy of the confirmation message to the ship's Master, so it can be available for viewing by the auditor that verifies the SSAS installation.
- Throughout the SSAS verification, the security auditor will evaluate the procedures outlined in the SSP, interview the Master and SSO on their knowledge of the procedures, and verify the installation and programming of the SSAS.
- In order for ship owners to not incur additional costs, no special attendance is required. The SSAS verification can take place in conjunction with another scheduled inspection, audit or survey provided. the on board verification takes place within one year of the installation.



8.4.1.3 SSAS Verification Endorsement of ISSC: This is one time verification of the SSAS to be conducted on vessels with new SSAS installations. An email confirmation from the Administration indicating satisfactory test of SSAS should be retained on board as proof that the SSAS is operational. A letter will be provided by the auditor on satisfactory completion of the verification.

8.4.1.4 SSAS message sent in error: Should a SSAS message be sent that is not a test or an actual alert, the Company Security Officer should immediately confirm that the SSAS message was sent in error. The CSO will then inform all concerned parties and the Administration that the alert is false and that no emergency response action should be taken.

8.4.2 Ship security alert process and programming:

8.4.2.1. At a minimum the SSAS message should provide:

- Name of ship
- IMO Ship Identification Number;
- Call Sign;
- Maritime Mobile Service Identity;
- Satellite position (Latitude and Longitude) of the ship;
- Course and speed of the Ship and
- Date and time (UTC) of the Satellite position.

Additional information, such as the name and contact phone number for the CSO may be included if the SSAS is capable of such programming, but this additional information is not required.

8.4.2.2 Destination:

The Ship Security Alert shall be sent directly to both the company and the Administration. The SSAS should be programmed to send an alert message to: shipalert@intershippingsservices.com. If the company has authorized a third party service provider to receive the SSAS messages on behalf of the company, please provide this Administration with the name and contact information for the service provider of the ship security alert system and coverage for your ships.

8.4.2.3 Confirmation of SSAS Test Messages:

Starting from the date of this notice the Administration will only provide confirmation of receipt of SSAS test message for audit and compliance verification purposes. Confirmation of other test messages will not be provided. To obtain confirmation of a SSAS test message for audit and compliance verification purposes the vessel or the company should request such a confirmation in advance. The request should be sent by e-mail to shipalert@intershippingsservices.com and include:

- Date time of proposed test.
- Purpose of the test.



- E-mail address of the CSO (or the company) where the CSO requests the Administration to send the acknowledgement of the test message.
- Vessel name and IMO Number.

Please additionally note the following:

- The Administration requires a test message only once a year or before / during SSAS verification.
- Test messages will only be confirmed during the working hours of the Administration.
- The SSAS test message should, as far as possible, be transmitted at the date and time specified in the request message.
- The confirmation e-mail of the SSAS test message by the Administration should be retained on board as evidence until the next audit.

References

- i. International Ship and Port Facility Security Code (ISPS Code),*
- ii. International Safety Management Code IMO Resolution A.741(18),*
- iii. IMO Resolution MSC.104 (73),*
- iv. IMO Resolution MSC.160(78)*
- v. SOLAS 74 Chapter V Regulation 19,*
- vi. SOLAS 74 Chapter XI-1 Regulations 3 & 5,*
- vii. SOLAS 74 Chapter XI-2,*
- viii. SOLAS 74 Chapter IX, Management for the Safe Operation of Ships,*
- ix. IMO Resolution MSC/Circ.1111*
- x. STCW'78 as amended*