

maintenance of the ship security plan and for liaison with the Company Security Officer, Port Facility Security Officer and the *Administration*.

2.9 Security Level 1:

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

2.10 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.

2.11 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.

2.12 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.

2.13 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.

2.14 Verification (Audit):

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

3.0 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;

- Approved and implemented SSP;
- The IMO Number marked on the vessel (see 8.1);
- Installed AIS (see 8.2);
- A Continuous Synopsis Record - CSR (see 8.3); and
- Installed and operational Ship Security Alert System (see 8.4).

3.2 Security Training:

The International Convention on Standards of Training, Certification and Watch-keeping for Seafarers, 1978, as amended (STCW) and the associated Code (STCW Code) require persons onboard ships to which the International Ship and Port Facility Security Code (ISPS Code) apply to have appropriate security training or instructions.

- .1 A list of approved training institutes can be found on LISCR website, www.liscr.com under the “SEAFARERS” tab, then click “Training Center Approval” and then the “List of Current Approved Training Centers (Click [HERE](#)).”
- .2 Any person designated as a SSO shall have a valid Liberian Certificate of Proficiency (CoP) attesting to their competence under the STCW Code A-VI/5 as found in the RLM 118.

3.3 Other Mandatory Minimum Security-Related Training and Instructions for Seafarers – Refer to **RLM-118** Mandatory Minimum Security-Related Training and Instructions (STCW Regulation VI/6).

- .1 Proficiency in designated security duties: Training in designated security duties must be undertaken by seafarers, engaged on ships which are required to comply with the provisions of the ISPS Code, who have designated duties under the ships security plan. This training/instruction must meet the requirements of Section A-VI/6 paragraphs 6-8 of the amended STCW Code. Training leads to the issue of an STCW Certificate of Proficiency.

Standard of competence for seafarers with designated security duties:

Every seafarer who is designated to perform security duties, including anti-piracy and anti-armed-robbery-related activities, shall be required to demonstrate competence to undertake the tasks, duties and responsibilities listed in column 1 of table A-VI/6-2.

The level of knowledge of the subjects in column 2 of table A-VI/6-2 shall be sufficient to enable every candidate to perform on board designated security duties, including anti-piracy and anti-armed-robbery-related activities.

Every candidate for certification shall be required to provide evidence of having achieved the required standard of competence through:

- demonstration of competence to undertake the tasks, duties and responsibilities listed in column 1 of table A-VI/6-2, in accordance with the methods for demonstrating

competence and the criteria for evaluating competence tabulated in columns 3 and 4 of that table; and

- examination or continuous assessment as part of an approved training program covering the material set out in column 2 of table A-VI/6-2.

- .2 Proficiency in security awareness: Certificates of Proficiency in security awareness issued under the STCW requirements, by any Administration on the STCW “White List” will be recognized by Liberia.

Otherwise: Standard of competence for security-awareness training Seafarers employed or engaged in any capacity on board a ship which is required to comply with the provisions of the ISPS Code on the business of that ship as part of the ship's complement without designated security duties shall, before being assigned to any shipboard duties:

- receive appropriate approved training or instruction in security awareness as set out in table A-VI/6-1;
- be required to provide evidence of having achieved the required standard of competence to undertake the tasks, duties and responsibilities listed in column 1 of table A-VI/6-1:
 - by demonstration of competence, in accordance with the methods and the criteria for evaluating competence tabulated in columns 3 and 4 of table A-VI/6-1; and
 - by examination or continuous assessment as part of an approved training program in the subjects listed in column 2 of table A-VI/6

3.4 Using a Security Consultant:

Companies may decide to train or hire people to develop the required ship security expertise within their organization. Such staff will draft their own Ships Security Plans and conduct the Ship Security Assessments. Other companies may use Security Consultants to assist with ISPS implementation.

A company choosing to use Security Consultants should verify the validity of the information provided by the Consultants and their ability to assist the company to comply with the ISPS Code requirements. (ISPS Code Part B/8 and B/9).

3.5 Manning:

As part of the vulnerability assessment, 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:

The Administration is taking an active role in the security of ships flying the Liberian Flag.

All Ships Security Plans shall be submitted to the Administration for approval in accordance with Section 4.11. We are directly involved in the ISPS Code implementation and will carry out verifications on Liberian flagged ships.

The Administration has trained a cadre of Liberian nautical inspectors to serve as Liberian security auditors in order to provide effective and efficient security verification on board the ships. These Auditors are also trained to conduct verification audits under the ISM Code which may be “harmonized” with security audits (See Marine Notice ISM-001 for further details). The Administration has also designated IACS members as RSOs for the purpose of conducting ISPS verification audits. A company may choose whether to have the Administration or the RSO conduct these verifications. The list of RSOs can be found on LISCR website, www.liscr.com under the “Maritime” tab, click on “Regulations and Standards Department” and then “Recognized Organizations.” (Click [HERE](#)). These Classification Societies are also Liberian Recognized Security Organizations.

Companies choosing or interested in using the Liberian Security Auditors should contact the Administration at audit@liscr.com for coordination. The International Ship Security Certificate will be issued by either the Administration or the RSO conducting the verification.

Specific information of the plan approval, verification, and certification can be found in Section 4 of this Notice.

3.7 ISPS and the ISM Code

Although it is not a requirement, the company should contemplate incorporating the relevant shipboard security requirements into the company’s Safety Management System (SMS) developed and implemented following IMO [Resolution A.741\(18\)](#), as amended by IMO [Resolutions MSC.104\(73\)](#), and IMO [Resolution MSC.160\(78\)](#).

The Safety Management System should:

- Define the security duties and responsibilities for the Company Security Officer, the Ship Security Officers and the crew.
- Discuss who will be responsible for organizing security drills and exercises.
- Contain procedures for immediately reporting any noncompliance with the ISPS Code, threats and breach of security to the Administration.
- Defined maintenance requirement for 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.
- 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 Liberian 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. If a vessel meets the requirements of the applicable sections of Part B, the Administration has included a statement in its Ship Security Plan “Letter of Approval” to confirm compliance with both Parts A and B. When the SSP is approved as meeting part B of the ISPS Code, the vessel must follow the applicable guidance found in Part B of the ISPS Code.

3.9 Master’s Authority

The Liberian 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.

4.0 **LIBERIAN NATIONAL REQUIREMENTS:**

These National Requirements are supplemental to the Maritime Regulations (**RLM- 108**) and Marine Notices contained in the Combined Publication Folder (RLM-300).

4.1 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.

4.2 Designation of Company Security Officer

The owner or operator of each vessel must provide the Office of the Deputy 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 (RL 5004) should be completed and forwarded to:

Vesselcertificates@lisr.com.

4.3 Selecting a Ship Security Officer

The Company should designate one of the senior officers onboard (such as Master, Chief Officer, Chief Engineer or 2nd Engineer) to perform the Ship Security Officer duties. The individual selected shall be trained to fulfill this duty.

It is also recommended that more than one officer on each ship be trained to carry out SSO's duties.

4.4 Conducting the Ship Security Assessment

The Company may use their Company Security Officer, other trained personnel or security consultants to conduct the on-scene Ship Security Assessment, provided they have appropriate skills to evaluate the security of a ship. Personnel conducting Ship Security Assessments 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. (This most likely will take place at the initial stage of taking over a ship prior to interim verification).

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

- .1 The Ship Security Assessment is an essential and integral part of the process of developing and updating the Ship Security Plan.
- .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.
- .3 The Ship Security Assessment shall be documented, reviewed, accepted and retained on board the ship and in the Company's office.

4.5 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. Liberian security auditors and RSOs that assist a Company with developing their Ship Security Plans or conducting Ship Security Assessments may not conduct ship verification audits on behalf of the Administration for that company.

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 shall 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 instruction 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 (SSP) Approval

.1 All SSPs are required to be approved by the Administration. The company shall submit a soft-copy (electronic copy) of each Ship Security Plan to the Administration, in English, for approval.

- .2 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. For a copy of the checklist, please [click HERE](#).
- .3 Shipowners and Operators are to upload their vessel plans directly to WayPoint for approval by the Administration. Guidance concerning WayPoint is provided separately in attachment 1. If this does not work for the vessel operator, the vessel operator may forward the plans electronically by email to planapproval@liscr.com. The regional offices conducting plan review will also have access to this email folder.
- .4 The Ship's Security Plan, is to be submitted as two separate PDF documents:
 - (1) The Security Plan, and
 - (2) The Ship Security Assessment.
- .5 The uploaded documents must be less than 10 MB and the attachments sent via Email shall be less than 10MB. If any plan or assessment to be submitted is greater than 10MB, this will require a separate email submission of the plan as WayPoint cannot currently accept plans of greater than 10 MB.
- .6 The Ship's Security Plan and Ship Security Assessments sent as email attachments, shall be submitted as a secured document with the access key sent in a separate email to planapproval@liscr.com, or may be sent to one of our regional offices conducting plan review:
 - LISCR Deutschland
 - LISCR Dubai
 - LISCR Hellas
 - LISCR Singapore
 - LISCR Japan
- .7 In addition, for amendments to previously approved plans, a submission of a PDF copy of the full plan is not required, but will be appreciated, as it will help us to maintain and update our records in WayPoint.
- .8 The Administration is no longer stamping the approved plans. Ship owners and operators shall ensure that all plans submitted for approval shall contain the revision date, that will be referenced in the letter of approval.
- .9 The plan may still be submitted in hard-copy, but the review process will be delayed as we will have to scan and upload the plan to WayPoint and in the near future we may charge for this service.
- .10 If only a hard copy is available, it shall be mailed to LISCR Headquarters with attention to our security department, or to one of the regional offices listed above for review and

approval.

4.12 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 Operators. Only affected pages are to be submitted to the Administration or one of the regional offices to update the records. If listed as part of the ship's profile in the appendix it will not require the reissue of the Approval Certificate and will not result in a fee.
- Change of Name for the vessel. Only affected pages should be submitted to the Administration. (Note if the plan is submitted using only the IMO number with the vessel name listed only on the ship's profile in an appendix, we will update the record but it will not require a new approval certificate and will not result in a fee.)
- 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.

As stated above, it is recommended to place ship details, CSO information, and other information such as owner's name that may change periodically, in an annex or an appendix to the SSP, which will not require approval.

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).

4.13 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 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 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.

4.14 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.

The Administration's Guidelines for Security Exercises

- .1 The Exercise should involve at least one vessel of the fleet, which may be Liberian or a non-Liberian 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.
- .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-Liberian flag vessel, is involved provided all of the exercise elements were implemented and the company provides an incident summary report to all other Liberian vessels in the fleet and to the Administration.
- .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 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 a real 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.
- .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.
- .6 As documentary evidence of the exercise, the CSO will provide a summary of the exercise to Liberian vessels in the 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.

Confirmation of receipt of the information in 4.14.1.6 from the Administration is not required to be retained on board the vessel.

- .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.

4.15 Planning the Verification

The Liberian Security Auditor or the approved RSO auditor will prepare the verification plan and update the Company Security Officer.

- .1 The Verification plan shall be sufficiently flexible to permit changes based on the information gathered during the verification.
- .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; and
 - Confidentiality requirements.

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

4.16 Full term and Interim Verification

- .1 Only the Liberian Security Auditor or an approved RSO auditor is authorized to conduct verifications on behalf of the Administration.
 - The Liberian Security Auditor or the RSO may not carry out ISPS Code verification on a Liberian ship in which they or any of their organization's 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.
- .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 Liberian flag have, in fact, been given to the Master.
 - There is a plan to conduct full term verification within six months.
- .3 Verification by Liberian Security Auditors: When scheduling a security verification using the services of a Liberian security auditor, the Company Security Officer should complete Form 201. "Audit Inspection Application Form", Click [HERE](#)) and submit it to the Audit and Inspection Coordination Division at audit@liscr.com. The approved SSP (or draft SSP for Interim Verifications) must be available on board the ship.

An Audit carried out by a Liberian Security Auditor (LSA) will be conducted as described below:

- Preparation of the Audit: The LSA shall coordinate his visit onboard the vessel with the local agent and CSO.
- When executing the audit, the LSA 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 (audit team) 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.
- Send the report to the Audit and Inspection Coordination Division at audit@lisr.com.

4.17 Non-Conformities and Additional Verifications

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

4.18 Certification: An ISSC shall be issued to each ship following a satisfactory verification either by the Liberian Security Auditor or an approved RSO auditor working on behalf of the Administration.

- .1 The ISSC will not be issued until all deficiencies in the implementation or the plan itself have been rectified.
- .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.
- .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 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.
- .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.
- .6 The date and place of issue stated on the ISSC is where the certificate was printed

regardless the date and place of the verification. e.g. the verification took place on 25 June 2019 in Singapore and the certificate was issued in LISCR head office Dulles, Virginia on 25 July 2019 then the date and place of issue will be 25 July 2019 at Dulles, Virginia. The ISSC will be valid until 24 June 2024.

- .7 Full term ISSC issued by the Liberian Administration cannot be endorsed by RSO, without the authorization of the Administration.

4.19 Interim Certification

- .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.
- .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: An Interim ISSC shall be valid for six (6) months, or until the Certificate required by section 19.2 of the ISPS Code is issued, whichever comes first and may not be extended.

4.20 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.

5.0 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 systems such as Long Range Identification and Tracking (LRIT), Automatic Identification System (AIS), or Ship Security Alert System (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, and
- The recommendation of the approved RSO or Liberian Security Auditor based upon evidence of the vessel's noncompliance with the Code.

5.2 Appeals

In the event a Company disagrees with a determination made by the Liberian Security 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 and the recommendation of the Liberian security auditor or the approved RSO.

6.0 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, Liberia 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. These 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 to work with the other Contracting Governments to develop the first draft of the agreement for signature.

7.0 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 Company Security Officer. The CSO shall notify the Administration. The Administration will consider sending a Liberian Security Auditor to verify the compliance onboard the vessel. The CSO shall send a corrective action report to the Administration addressing all non-conformities and/or deficiencies found.

8.0 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).

- .1 The permanent marking will be plainly visible, clear of any other markings on the hull and shall be painted in a contrasting color.
- .2 The markings shall be made by raised lettering or by cutting it in or by center-punching it or by any other equivalent method that ensures the marking is not easily expunged.
- .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 Liberian Flag ships engaged in international voyages are required to have an AIS approved by the vessel's Classification Society, installed in accordance with SOLAS Chapter V Regulation 19.2.

- .1 If an AIS has not been installed on the ship the ship must have 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. Please contact the Security Department at security@liscr.com if you believe that the vessel may be exempted.

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 Liberian 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.

Marine Notice **ISP-002** contains specific guidance regarding CSRs.

8.4 Ship Security Alert System (SSAS) (SOLAS Chapter X1-2 Regulation 6)

All vessels listed below and engaged on international voyages shall have an operational Ship's Security Alert System (SSAS) installed.

Passenger Ships, including high-speed passenger craft and 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.

.1 Verification of Installation:

- a. 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.
- b. The SSAS equipment and its operation is 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 the review and verification process, and who have knowledge of the location of the activation buttons should be kept to a minimum.

.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.
- The SSAS verification can take place in conjunction with another scheduled inspection, audit or survey provided the inspector or surveyor is also an authorized security auditor and the on board verification takes place within one year of the installation. For example, the on board installation verification may be conducted in conjunction with a Liberian annual safety inspection.
- Although a Verification Letter is not required, the Administration will provide a letter confirming successful installation of the SSAS when requested.

- .3 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.
- .4 Ship security alert process and programming:
- a. At a minimum the SSAS message should provide:
- Name of vessel
 - IMO Vessel Identification Number;
 - Call Sign;
 - Maritime Mobile Service Identity;
 - Course and speed of the vessel
 - GNSS position (Latitude and Longitude) of the ship; and
 - Date and time (UTC) of the GNSS 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.

- b. Competent Authority: The competent authority for Liberia is the Office of the Deputy Commissioner for Maritime Affairs, Attn: Maritime Security Department.
- c. Destination: For Liberian flag vessels 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: alarm@liscr.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 vessels.
- d. Testing: The Administration requires a test message as soon as the SSAS has been initially activated (new buildings, change of flag to Liberia, when the system is replaced and annually thereafter. During testing of the system, it is requested that the test message contains the word: "TEST" in order to identify it as such and avoid the need for additional communication between the CSO and the Administration. If the system is not capable of inserting the word "TEST" into the alert message, then the CSO must send the Administration an email to: security@liscr.com in advance of sending the alert advising the Administration that the system will be tested.
- e. Confirmation of SSAS Test Messages: The Administration will only provide confirmation of receipt of test messages required in 8.4.2.4. Confirmation of other test messages will not be provided unless specifically requested in advance of the test. To obtain confirmation of a SSAS test message for compliance verification purposes, the vessel or the company shall request such a confirmation in advance

and upon completion of the test. The request should be sent by e-mail to security@liscr.com and include:

- Vessel name and IMO Number
- 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.

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 normal office 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 sent by the Administration should be retained on board as evidence of a successful operation until the next audit.

9.0 ADMINISTRATION'S PROGRAM FOR SETTING SECURITY LEVELS

9.1 The Administration will post the current Security Level on its website www.liscr.com (Click [HERE](#)) and notify CSO's of setting of security levels of 2 or 3 through Marine Security Advisories by Email, or direct contact to the vessels, as appropriate. The Marine Security Advisories and special security bulletins are issued to indicate threats to the Liberian fleet regardless of the security level in specific ports. The CSO and SSO should obtain the security level of ports to be visited through the appropriate port authorities.

The vessel will comply with the port security level if the port security level is higher than the security level set onboard.

9.2 The Administration will consider the following when setting the appropriate security Level at a port of another Contracting Government or a High Risk Area:

- The degree that the threat information is credible;
- The degree that the threat information is corroborated;
- The degree that the threat information is specific or imminent;
- The potential consequences of such a security incident, and
- The relevancy of the information to the vessel's operating area.

10. GUIDANCE ON ACCESS TO VESSELS (SHIPS) UNDER THE ISPS CODE

10.1 MSC/Circ.1156 relates to ships and recommends procedures to facilitate the boarding of official authorities in order to carry out their duties and/or services onboard ships. In particular, it addresses how the vessel should treat public authorities, emergency response

services and pilots, including boarding procedures, searches, escorting and carriage of firearms. For example, in such cases where official authorities have to board a vessel for law enforcement or to respond to an emergency situation, it may not be possible or reasonable for ship's security personnel to implement the normal access control provisions required by the Ship Security Plan.

- 10.2 Ship operators and their Company Security Officers should thoroughly review the above mentioned circular and ensure the Guidance therein is incorporated into Ship Security Plans in order to avoid conflicts between the ship's security personnel and official authorities and to allow them to perform their duties without unnecessary delays and without any obstructions. Also, it is recommended that a copy of these circulars be included in SSP as an appendix.

* * * * *

ANNEX I



INTERNATIONAL SHIP SECURITY CERTIFICATE
REPUBLIC OF LIBERIA

Certificate No. _____

Issued under the provisions of the
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND PORT FACILITIES

(ISPS Code)

SAFETY OF LIFE AT SEA, 1974, as amended

Under the authority of the Government of
The Republic of Liberia

by _____

(person or organization authorized)

Name of ship: _____

Distinctive number or letters: _____

Port of registry: **MONROVIA**

Type of ship: _____

Gross Tonnage: _____

IMO Number: _____

Name and address of Company: _____

Company Identification Number: _____

THIS IS TO CERTIFY:

1. That the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS code.
2. That the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of Chapter XI-2 of the Convention and part A of the ISPS Code.
3. That the ship is provided with an approved ship security plan.

Date of initial/renewal verification on which this certificate is based.....

This Certificate is valid until.....subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at

(Place of issue of certificate)

Date of issue

(Signature of the duly authorized Official issuing the Certificate)

(Seal or Stamp of issuing authority, as appropriate)

Certificate No. _____

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of part A of the ISPS Code the ship was found to comply with the relevant provision of Chapter XI-2 of the Convention and part A of the ISPS Code.

INTERMEDIATE VERIFICATION

(to be completed between the second and third anniversary date)

Signed:.....

(Signature of authorized official)

Place:

Date:

ADDITIONAL VERIFICATION

Signed:

(Signature of authorized official)

Place:

Date:

ADDITIONAL VERIFICATION

Signed:

(Signature of authorized official)

Place:

Date:

ADDITIONAL VERIFICATION

Signed:

(Signature of authorized official)

Place:

Date:

ANNEX II



INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

REPUBLIC OF LIBERIA

Certificate Number: _____

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIP AND PORT FACILITIES

(ISPS CODE)

**Under the authority of the Government of
LIBERIA**

by:
(person(s) or organization authorized)

Name of ship: _____

Distinctive number or letters: _____

Port of registry: **MONROVIA** _____

Type of ship: _____

Gross tonnage: _____

IMO Number: _____

Name and address of Company: _____

Company Identification Number: _____

Is this a subsequent, consecutive, Interim Certificate? Yes/No*

If yes, the date of issue of initial Interim Certificate: _____

This is to certify that the requirements of Section A/19.4.2 of the ISPS Code have been complied with.

The Certificate is issued Pursuant to section A/19.4 of the ISPS Code.

The Certificate is valid until: _____

Issued at: _____
(Place of issue of the Certificate)

Date of issue
(Signature of the duly authorized Official issuing the Certificate)
(Seal or Stamp of issuing authority, as appropriate)

* delete as appropriate