საქართველოს
ეკონომიკისა და მდგრადი
განვითარების სამინისტრო

სსიპ საზღვაო ტრანსპორტის
სააგენტო

MINISTRY OF ECONOMY
AND SUSTAINABLE
DEVELOPMENT OF GEORGIA

LEPL MARITIME TRANSPORT
AGENCY

KA020117739530222

სსიპ საზღვაო ტრანსპორტის სააგენტო საქართველო, ქ.ბათუმი, 6000, ბაქოს ქუჩა N50. ტელ.:+995 422 27 49 25/26
50 Baku Str., 6000, Batumi, Georgia. Tel.:+995 422 27 49 25/26

№ 12/CIRC/FSI **2022 / 06 /24**

To: All Shipowners, Managers and Representatives of Ships flying Georgian Flag, Masters and Officers, Recognized Organizations, Flag State Inspectors, Recognized Agents

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

Reference:

- **International Convention for the Safety of Life at Sea (SOLAS), as amended;**
- **International Ships and Port Facilities Security (ISPS) Code, as amended;**
- **IMO Guide to Maritime Security and the ISPS Code, 2021 Edition;**
- **IMO Circular MSC/Circ.1154, guidelines on training and certification for company security officers, adopted on 23 May 2005;**
- **Maritime Code of Georgia;**
- **Decree of the government of Georgia N685 of December 31, 2018 "on approval of the security rules for Ships Flying the Georgian Flag and Georgian ports"**

1. **Purpose:**

1.1 The purpose of this Circular is to provide information and guidance to the shipowners, recognized organizations (RO), ship managers, operators, companies and other and relevant parties regarding the requirements, policies, and interpretations for compliance with the International Ship and Port Facility Security (ISPS) Code.

2. Background:

2.1 The ISPS Code entered into force under SOLAS chapter XI-2 on 1 July 2004. Since then, it has formed the basis for a comprehensive mandatory security regime for international shipping. The Code is divided into two sections, Part A and Part B.

- Mandatory Part A outlines detailed maritime and port security-related requirements to which SOLAS contracting governments, port authorities, and shipping companies must adhere to comply with the Code.
- Part B of the Code provides guidelines on how to meet the requirements and obligations set out in the provisions of Part A.

3. Application:

3.1 This Circular applies to all ships registered in the State Ships Registry of Georgia engaged in the international voyage, as follows;

- Passenger ships, including high-speed passenger craft;
- Cargo ships more than 500 GT, including high-speed craft;
- Mobile offshore drilling units.

3.2 This circular does not apply to warships, naval auxiliaries or other ships owned or operated by a national Government and used only on Government non-commercial service.

4. Definitions:

4.1 Ship security plan - means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ships stores or the ship from the risks of a security incident.
4.2 Ship security officer - means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer

and port facility security officers.
4.3 Company – means the Owner of the ship or any other organization or person such as the Manager, or the Bareboat Charterer, who has assumed the responsibility for operation of the ship from the Shipowner and who on assuming such responsibility has agreed to take over all the duties and responsibility imposed by the ISPS Code and national law.
4.4 Company security officer - means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.

5. Obligations of the Company:

5.1 For all its ships, every company shall develop, implement, and maintain a functional SSP that is compliant with SOLAS Chapter XI-2 and the ISPS Code.
5.2 The company shall ensure that the SSP contains a clear statement emphasizing the Master's authority and that the Master has overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request assistance of the company or of any Contracting Government as may be necessary. The Master of the ship has the ultimate responsibility for both safety and security aboard the ship.
5.3 The company shall ensure that the Master has available on board, at all times, the following information required by SOLAS Chapter XI-2, Regulation 5, to provide to Coastal State authorities:

- contact details for the person or entity responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;
- contact details for the person or entity responsible for deciding the employment of that ship;
- in cases where the ship is employed under the terms of charter party(ies), contact details of such charter party(ies).

5.4 The company shall ensure that the CSO, the Master and the SSO are given the necessary support to fulfil their duties and responsibilities in accordance with Chapter XI-2, Part A and the relevant provisions of Part B of the ISPS Code.
5.5 Every Company has to fulfill ISPS Code compliance requirements:

- Company Security Officer;
- Ship Security Officer;
- Approved and implemented SSP;
- The IMO Number marked on the vessel;
- Installed AIS;
- A Continuous Synopsis Record – CSR;
- Installed and operational Ship Security Alert System.

6. Ship Security Plan:

6.1 A Ship Security Plan (SSP) must be developed, implemented, and maintained onboard each vessel to which the ISPS Code applies.
6.2 SSP shall be developed in accordance with regulation 9.4 of the ISPS CODE and taking into account the guidance given in part B of the mentioned code.
6.3 MTA recognized Security organization authorized only to verify, implement or certify a work product that it has developed (e.g. preparation ship security assessments, preparation ship security plans or of amendments under review).
6.4 The SSP must be reviewed and approved by the MTA.

7. Ship Security Officer (SSO):

7.1 The companies shall appoint a ship security officer on board of ships that are under its operations and security requirements are applies. The Ship Security Officer is responsible for implementation the requirements of ISPS CODE on the Ship.
7.2 The SSO shall be a management level officer, (master or chief mate).
7.3 The Ship Security Officer shall:

- coordinate security measures with interfacing security regulated ports and port facilities;
- ensure the development, submission and implementation of required SSP;
- conduct ships security drills and exercises;
- conduct ship security inspections;
- ensure adequate ship security personnel training;
- maintain records as required by the ISPS Code;
- enhancing security awareness and vigilance on board;
- ensure the execution of any required Declarations of Security;
- notify law enforcement personnel, emergency responders and relevant port security authorities of applicable ship security incidents; and
- ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

7.4 SSO must hold certificate of proficiency in accordance with regulation V/5 of the STCW convention, as amended.
7.5 SSO are entitled exercise physical control over the ship's security.

8. Company Security Officer (CSO):

8.1 The companies shall designate responsible person for the security of ships. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible.
8.2 A Company may, depending on the number or types of ships they operate designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.
8.3 The Company Security Officer shall:

- ensure the completion and timely audit of required security assessments;

- ensure the development, submission, implementation and timely audit of required SSP;
- ensure the conduct of ship security drills and exercises;
- conduct ship security inspections;
- ensure adequate company security personnel training;
- maintain records as required by the ISP Code;
- enhancing security awareness and vigilance;
- notify law enforcement personnel and other emergency responders of applicable ship security incidents;
- ensure effective communication and co-operation between the ship security officer and the relevant port facility security officers;
- ensure consistency between security requirements and safety requirements;
- ensure that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and
- ensure that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

8.4 The companies must ensure that CSOs are trained in accordance with regulation 13.1 of the part A, of the ISPS code and taking into account the guidance given in part B of the mentioned Code.
8.5 Every person designated as a Company security officer (CSO) should be able to demonstrate competence to undertake the tasks, duties and responsibilities listed in the annex of IMO Circular MSC/Circ.1154, (guidelines on training and certification for company security officers).
8.6 MTA recognizes all CSO training courses that are based on IMO model course 3.20.
8.7 The CSO must arrange internal (once every 12 months) security audits onboard each ship in accordance with ISPS Code Part A, regulation 11.2.5 and 19.4.2.4.2 as part of their duties.

9. Ship Security Assessment (SSA):

9.1 The purpose of a SSA is to identify and analyze the security risks for a given type of ship in a trading area. The results of the security assessment provide the basis for measures which are essential to develop, implement, maintain and update the ship security plan. This assessment shall take into account the additional workload such measures will rise up.
9.2 The CSO is responsible for satisfactory development of the SSA whether prepared by the company or RO. The SSA serves as a tool for development of a realistic SSP. It takes into account the unique operating environment of each individual ship, the ship's compliment and duties, structural configuration and security enhancements and also taking into account the guidance given in part B - 8 of ISP Code.
9.3 SSA shall include an on-scene security survey and, at least, the following elements:

- Identification of existing security measures, procedures and operations;
- Identification and evaluation of key ship board operations that it is important to protect;
- 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.

9.4 SSA shall be documented, reviewed, accepted and retained by the Company.

10. Declaration of Security (DoS):

10.1 The Ship Security Plan shall clearly state that the SSO must complete a DoS as described in the ISPS Code, Part A, regulation 5.

11. Security Levels:

11.1 Security Level 1: The level for which the minimum appropriate protective security measures shall be maintained at all times.
11.2 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.
11.3 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.

12. Security Equipment and Systems:

12.1 Security equipment specified in the SSP must always remain operational.
12.2 Any Major Failure must be reported immediately to:

- MTA or RO, or both;
- The Port Facility Security Officer (PFSO); and
- The competent authorities of any relevant coastal State(s).

12.3 An ISSC shall not be issued or endorsed if a Major Failure exists. Immediate action is required to restore compliance and the Major Failure must be downgraded before departure. An additional verification audit must be carried out within an agreed period to verify effective implementation of corrective actions.
12.4 Any Failure must be reported without delay to:

- MTA; or
- RO

12.5 The report must include:

- details of equivalent alternative security measures the ship is applying until the failure or suspension is rectified; and
- an action plan specifying the timing of any repair or replacement

12.6 If a Failure is identified, the ISSC may be endorsed, provided compliance has been restored prior to departure or a schedule has been agreed between the Company and the auditor for the completion of corrective action to restore compliance and to prevent recurrence.

Additional audits may be carried out as necessary.

13. Documentation:

13.1 The SSP must remain strictly confidential. Port State Control Officers are not permitted to access the plan.
13.2 MTA qualified maritime security inspector/auditors or trained RO auditors that certify the ship are granted access to the plan.

14. Verifications:

14.1 Initial, renewal, and intermediate verifications are conducted by the trained auditor of the RO, as required by ISPS Code Part A, regulation 19.
14.2 A ship detained on maritime security grounds must undergo an additional verification before being allowed to navigation.

15. Drills and Exercises:

15.1 The SSP shall address drill and training frequency. Drills shall be conducted at least every three (3) months. In cases where more than 25% of the ship's personnel have changed, at any one time, with personnel previously not participating in any drill on that ship within the last three (3) months, a drill shall be conducted within one (1) week of the change.
15.2 Records indicating type of drill or exercise, SSP element(s) covered, and attendance shall be maintained by the SSO for a period of three (3) years. They may be kept in any format but must be protected from unauthorized access or disclosure. The records shall be in a form to be readily available to Port State Control officials if so requested.
15.3 Various types of exercises, which may include participation of the CSO, PSO, relevant authorities of contracting governments as well as SSO, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resources availability and response. These exercises may be:

- full scale or live;
- table top simulations or seminars;
- combined with other exercises such as search and rescue or emergency response exercises.

16. Records:

16.1 Records of activities detailed in Part A, regulation 10.1 addressed in the SSP shall be kept onboard for a minimum period not less 3 years.
16.2 The records shall be kept in the working language of the ship. If the working language of the ship is not English or French, then a translation into one of these languages shall be included.
16.3 Records may be kept in any format but must be protected from unauthorized access or disclosure and loss. The records shall be in a form to be readily available to Port State control officials if so requested.
16.4 Due to the security sensitive nature of these records, they shall be protected from unauthorized disclosure.

17. International Ship Security Certificate (ISSC):

17.1 MTA is entitled to issue the International Ship Security Certificate (ISSC) and certificate is valid till 5 year.
17.2 When intermediate verification is carried out by RO, they are entitled to endorse intermediate verification of ISSC.
17.3 After the renewal verification new ISSC is issued by MTA. Such certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

18. Interim certification:

18.1 MTA is entitled to issue an Interim International Ship Security Certificate, with validity of 6 months, or until the certificate required by regulation 19.2 of the ISPS CODE is issued, whichever comes first, and may not be extended.
18.2 An Interim International Ship Security Certificate shall only be issued when the MTA, has verified that:
18.2.1 the ship security assessment required by ISPS Code has been completed;
18.2.2 a copy of the ship security plan meeting the requirements of chapter XI-2 and part A of this Code is provided on board, has been submitted for review and approval, and is being implemented on the ship;
18.2.3 the ship is provided with a ship security alert system meeting the requirements of regulation XI-2/6, if required;

18.2.4 the company security officer:
18.2.4.1 has ensured:4.1.1 the review of the ship security plan for compliance with this Part of the ISPS Code,
18.2.4.2 that the plan has been submitted for approval, and
18.2.4.3 that the plan is being implemented on the ship, and
18.2.4.4 has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the company security officer is satisfied that the ship will successfully complete the required verification in accordance with section 19.1.1.1, of the ISPS code, within 6 months;

18.3 arrangements have been made for carrying out the required verifications under section 19.1.1.1, of the ISPS code;
18.4 the master, the ship's security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in this Part of the Code; and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the working language of the ship's personnel or languages understood by them; and
18.5 the ship security officer meets the requirements of this Part of the ISPS Code.

19. Noncompliance with the ISPS Code:

19.1 ISPS Certificates may only be withdrawn at the discretion of the MTA.
19.2 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 RO or MTA flag state inspectors based upon evidence of the vessel's noncompliance with the ISPS Code.

20. Ship Security Alert System (SSAS):

20.1 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.

20.2 Verification of Installation:

- Initial SSAS Verification: The on board installation and operation of the SSAS must be verified after installation by RO representative;
- The SSAS equipment and its operation is confidential. 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.

20.3 The Company designated Security Officer (CSO) must:

- be available at all times (on a 24/7 basis) to receive and act on SSAS alerts;
- be able to accurately identify and react to real, test, or false alerts;
- understand the SSAS requirements (Part A) and recommendations (Part B) of the ISPS Code;
- maintain a current contact list of relevant authorities (Administrator, Maritime Rescue Coordination Centers (MRCCs), Coastal State Authorities, Information Sharing Centers) to be used in the event of an actual alert and
- participate in exercises involving tests of the SSAS

20.5 Verification Procedure:

- SSAS message marked "TEST" shall be sent by the ship to the MTA 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;
- During each subsequent ISPS verification, the RO auditor must examine the activity records of the SASS as specified in ISPS Code Part A and The auditor must also witness a complete SSAS test alert during each ISPS verification;
- 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 MTA that the alert is false and that no emergency response action should be taken.

20.6 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

20.7 For Georgian flag vessels the Ship Security Alert shall be sent directly to both the company and the MTA. The SSAS should be programmed to send an alert message to mrcc@mta.gov.ge and fsi@mta.gov.ge.
20.8 The MTA requires a test message as soon as the SSAS has been initially activated (new buildings, change of flag to Georgia, 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 MTA. If the system is not capable of inserting the word "TEST" into the alert message, then the CSO must send the MTA an email to mrcc@mta.gov.ge and fsi@mta.gov.ge and in advance of sending the alert advising the MTA that the system will be tested.
20.9 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 fsi@mta.gov.ge, and/or mrcc@mta.gov.ge and include:

- Vessel name and IMO Number
- Date time of proposed test.
- Purpose of the test.

- E-mail address of the CSO where the MTA will send the acknowledgement of the test message.

20.10 Additionally note the following:

- The MTA 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 MTA.
- 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 MTA should be retained on board as evidence of a successful operation until the next audit.

21. Continuous Synopsis Record (CSR):

21.1 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 MTA will maintain a copy of the CSR record for Georgian ships as long as they remain in the registry. The vessel operator is responsible for keeping the MTA informed of any changes regarding their vessels CSR record.

22. Contact Details:

22.1 Recognized Organizations, Ship owner, Ship Operator or Management Company of a ship flying the Georgian flag, may contact MTA for additional consultation and assistance.

LEPL- Maritime Transport Agency of Georgia
Ships Registry and Flag Control Department
Tel: +995 (422) 274925
E-mail: fsi@mta.gov.ge
Hotline/AOH: +995 (577) 221622

Director SIGNED/SEALED ELECTRONICALLY Tamar Ioseliani

Georgia International Maritime Forum