საქართველოს
ეკონომიკისა და მდგრადი
განვითარების სამინისტრო

სსიპ საზღვაო ტრანსპორტის
სააგენტო

MINISTRY OF ECONOMY
AND SUSTAINABLE
DEVELOPMENT OF GEORGIA

LEPL MARITIME TRANSPORT
AGENCY

KA020194817742621

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

№ 4/CIRC/FSI **27 / January / 2021**

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

Subject : Maritime Cyber Risk Management

Reference:

- **Maritime Code of Georgia;**
- **IMO Circular MSC-FAL.1/Circ.3 "Guidelines on Maritime Cyber Risk Management", adopted 5 July 2017;**
- **IMO Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems", adopted 16 June 2017;**
- **ISO/IEC 27001 "Information Security Management"** ;

1. Introduction:

1.1 This circular provide high-level recommendations for maritime cyber risk management. Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

1.2 Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

2. Purpose:

2.1 The purpose of this Circular is to provide information regarding the International Maritime Organization in June 2017 at the 98th session of the Maritime Safety Committee (MSC) adopted the MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management and the Resolution MSC.428 (98) on Maritime Cyber Risk Management in Safety Management Systems (SMS) to safeguard shipping from current and emerging cyber threats and vulnerabilities.

3. Background:

3.1 Cyber technologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

1. Bridge systems;
2. Cargo handling and management systems;
3. Propulsion and machinery management and power control systems;
4. Access control systems;
5. Passenger servicing and management systems;
6. Passenger facing public networks;
7. Administrative and crew welfare systems;
8. Communication systems.

4. Maritime Cyber Risk Management in Safety Management Systems (SMS):

4.1 According to the IMO Resolution MSC.428 (98), an approved Safety Management System (SMS) should take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code.

4.2 The objectives of the ISM Code include the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment.

4.3 all Management Companies of ships flying the Georgia flag should address the cyber risks in their safety management system no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

5. Recommendation/Request:

5.1 Maritime Transport Agency of Georgia strongly recommends/request to the all ship-owners and operators to take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping to ensure that cyber risks are appropriately addressed in safety management **systems no later than the first annual verification of the company's Document of Compliance (DOC) after 1 January 2021.**

5.2 ROs are expected to verify compliance with the above mentioned requirement during the **first annual verification of the company's Document of Compliance after 1 January 2021.**

6. PSC and FSC Inspection:

6.1 In case of the cyber risk management has not been incorporated into the ships SMS by the company's **first annual verification of the DOC after January 1, 2021, the PSC inspector shall be issued appropriated deficiencies.**

6.2 Hereby, you are requested to take into account the above-mentioned requirement in order to avoid non-compliance with Flag State requirements, which may result in monetary sanctions, removal of registration or suspension of registration of subject vessel found in violation.

7. Contact Details:

7.1 Recognized Organizations, Shipowner, ship operator or Management Company of a ship flying the Georgian flag, may contact on below information for Additional consultations 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

Attachments:

Annex I – IMO Circular MSC-FAL.1/Circ.3 "Guidelines on Maritime Cyber Risk Management", adopted 5 July 2017
Annex II – IMO Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems", adopted 16 June 2017

Director SIGNED/SEALED ELECTRONICALLY Tamar Ioseliani

Georgia International Maritime Forum