Date: 21st November 2020

Circular no.: 0049C/TG/11/20

To: Ship-Owners / Ship-Managers / Operators / Representatives of Togo flagged vessels /Agents / Masters and Flag State Surveyors / Deputy Registrars / IT Officers of Togo Registered Ships to which the ISM Code applies

Subject: "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS"

Scope: This notice aims to inform Owners and Managers of Togo registered ships of the need to raise awareness of cyber risk threats and vulnerabilities in the shipping industry. As per applicable IMO MSC Resolution, Cyber Risks should be appropriately addressed within the Safety Management System no later than the first annual verification of the Document of Compliance after 1st January 2021.

References:

a. I.M.O. Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems.

b. I.M.O. MSC-FAL.1/Circ.3 – Guidelines on Maritime Cyber Risk Management.

c. The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

Applicability: All vessels registered in the International Ship Registry of Togo to which the ISM Code applies (all commercially operated vessels over 500GT)

General

- Technology has become essential to the operation and management of systems critical to the safety and security of shipping. This technological advancement also means increased exposure of the maritime sector to a greater risk of cybercrime.
- IMO has adopted resolution MSC.428 (98) on "Maritime Cyber Risk Management in Safety Management Systems" to address the issues and raising awareness related to cyber risk threats and vulnerabilities. Emphasis is assigned to the fact that ships are becoming more and more complex and increasingly dependent on the extensive use of digital and communications technologies. The IMO provided also high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines set out in the Annex to MSC-FAL.1/Circ.3, also include functional elements that support effective cyber risk management and can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by the Organization.

Inquiries concerning the subject of this Circular or any requests should be directed to:
INTERNATIONAL REGISTRATIONS BUREAU (LB)
Phone Number: +961-1-883794
E – Mail: administration@togoregistrar.com

IMO REQUIREMENTS

- Resolution MSC.428(98) requires cyber risk management to be undertaken under the objectives and requirements prescribed by the ISM Code. Cyber risks should be appropriately identified, analyzed, and addressed within the Safety Management System no later than the first annual verification of the Document of Compliance after 1st January 2021. In practice, this means that vessel owners/managers need to identify and manage cyber risks the soonest possible in preparation for the first annual verification of the company's document of compliance after 1 January 2021.

IMPLEMENTATION & RECOMMENDATIONS

- Appropriate safeguards should be developed and implemented based on the company's risk assessment taking into account guidance provided within MSCFAL.1/Circ.3. These provide advice on (a) Developing a cybersecurity assessment and plan to manage risk, (b) Handling security breaches and incidents, (c) Highlighting national and international standards used, and (d) The relationship to existing regulation. Besides, the IMO guidelines on cyber risk management (MSCFAL.1/Circ.3) provide functional elements of the risk management framework: identifying risk, detecting risk, protecting assets, responding to risk, and recovering from attacks. Based on these guidelines, shipping companies are recommended to undergo a cyber risk analysis to assesses threats and vulnerabilities, as well as the impact of potential hackers on systems critical for the safe operation of their ships. Based on the risk analysis, shipping companies should implement mitigation strategies to strengthen assets both ashore and onboard their ships. The IMO guidelines identify a list of potentially vulnerable systems on ships, which include, but are not limited to:
    - bridge systems;
    - cargo handling and management systems;
    - propulsion and machinery management and power control systems;
    - access control systems;
    - passenger servicing and management systems;
    - passenger facing public networks;
    - administrative and crew welfare systems; and
    - communication systems.
- Cyber risk management measures are required to be aligned with existing requirements contained in the ISM & ISPS Codes – the procedures relating to cyber risk management should be reflected in the safety management system (SMS) of the company, while the physical security aspects of cybersecurity should be addressed in the Ship Security Plan (SSP). Due to chapter 8 of the ISPS Code, the ship is obliged to conduct a security assessment, which should include all operations that are important to protect.

CONCLUSION

- Togo flagged vessels are required to ensure that cyber risks are appropriately addressed in the safety management system no later than the first annual verification of the company's Document of Compliance after 1st January 2021.
- Flag State auditors will be concentrating on cyber security systems at the company DOC audit in 2021. It is also expected that Port State Control will ask for evidence of compliance with cyber security best practice during inspections after **1st January 2021**.

Inquiries concerning the subject of this Circular or any requests should be directed to:
INTERNATIONAL REGISTRATIONS BUREAU (LB)
Phone Number: +961-1-883794
E – Mail: administration@togoregistrar.com

- In this respect, ship owning and ship managing companies operating vessels under the Togolese flag are recommended to seek ways to efficiently close cybersecurity gaps by supporting the development of improvement plans, updating systems, increasing awareness, and enhancing procedures, as per applicable IMO requirements. In particular they are strongly advised to promote awareness of cybersecurity to their stakeholders, including their shipboard personnel.

For the International Ship Registry of Togo

Vera N. Medawar
Ship Registrar

For the Togolese Maritime Authority

MATCHONNAWE BAKAI
Director

Encl.: a. I.M.O. Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems.
b. I.M.O. MSC-FAL.1/Circ.3 – Guidelines on Maritime Cyber Risk Management.
c. The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

Inquiries concerning the subject of this Circular or any requests should be directed to:
INTERNATIONAL REGISTRATIONS BUREAU (LB)
Phone Number: +961-1-883794
E – Mail: administration@togoregistrar.com