Kiribati Ship Registry

Singapore Operations Office:
10 Anson Road #25-14, International Plaza, Singapore 079903
Tel: +65 6225 0555 Email: info@kiribaship.com Website: https://kiribaship.com

MARINE CIRCULAR
59/2021

28 June 2021

TO : Ship Owners, Ship Managers, Ship Operators, Charterers, Ship Masters, Classification Societies and the Shipping Community

SUBJECT : Guidelines on Maritime Cyber Risk Management

PURPOSE:

This circular serves to provide ship owners/managers/operators with IMO specific guidance relating to maritime cyber risk management in view of the recommended compliance to IMO Resolution MSC.428(98) from 01 January 2021.

REFERENCES:

(a) IMO Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems, 16 June 2017

(b) IMO MSC-FAL.1/Circ.3/Rev.1 – Guidelines on Maritime Cyber Risk Management, 14 June 2021

APPLICATION

This circular is applicable to all Kiribati flagged vessels.

CONTENTS

1. Background

Recognizing that cyber technologies is essential to the operation and management of numerous systems critical to the safety and security of shipping and the protection of the marine environment, the IMO acknowledged the vulnerabilities of these technologies to cyber risks and cyber threats, and on 16 June 2017, adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, and subsequently issued (b) IMO MSC-FAL.1/Circ.3/Rev.1 – Guidelines on Maritime Cyber Risk Management on 14 June 2021.

Noting that the rapidly changing technologies and threats makes it difficult to address these cyber risks through only technical standards, the IMO has recommended that cyber risks are addressed in existing safety management systems required by the International Safety Management (ISM) Code.

2. Recommendations

2.1. Ship owners and operators are encouraged to comply with Resolution MSC.428(98) no later than the first annual verification of the company's DOC after 01 January 2021. This is however not mandatory.

2.2. MSC-FAL.1/Circ.3/Rev.1 provides guidance on how to conduct an assessment of the cyber risks for complying with the Resolution.

2.3. Additional guidance is available from publications by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, InterManager, IUMI, OCIMF, SYBAss, US NIST, WSC, and Consolidated IACS Recommendation on cyber resilience (Rec 166).. For e.g., BIMCO has published its "Cyber Security Workbook for On Board Ship Use, 2nd Edition 2021" which uses detailed, step by step checklist to provide a ship's crew with

day-to-day management of on board cyber security to protect vulnerable on board systems. It also gives guidance on how best to detect, respond and recover in the event of a cyber-attack.

2.4. Vessels intending to call at US ports should take into account the “Vessel Cyber Risk Management Work Instruction / CVC-WI-027”, as amended, issued by the U.S. Coast Guard.

Yours sincerely,

Deputy Registrar
Kiribati Ship Registry