NIUE SHIP REGISTRY

Website: www.niueship.com

MARITIME CYBER RISK MANAGEMENT
(Circular NMC7.2017 (rev3))

PURPOSE: Provide ship owners/managers/operators with IMO (International Maritime Organization) guidance on maritime cyber risk management to safeguard shipping from current and emerging cyber-threats and vulnerabilities in view of the recommended compliance to IMO Resolution MSC.428(98) from 01 January 2021.

RELATED DOCUMENTS:

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

2. IMO MSC-FAL.1/Circ.3/Rev.2 – Guidelines on Maritime Cyber Risk Management, 7 June 2022

CONTENTS

A. INTRODUCTION

The IMO acknowledges how cyber risks and cyber threats threaten the cyber technologies that have now become essential to the operation and management of numerous systems critical to the safety and security of shipping, and the protection of the marine environment. Thus, on 16 June 2017, the IMO adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems.

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

B. REQUIREMENTS

Ship owners and operators are strongly recommended, even though it is not mandatory, to have cyber risks appropriately addressed in the company's Safety Management Systems no later than the first annual verification of the company's DOC after 01 January 2021. (**Note:** The U.S. Coast Guard has issued CVC-WI-027(02) - "Vessel Cyber Risk Management Work Instruction" which should be taken into account if vessels intend to enter U.S. waters).

MSC-FAL.1/Circ.3/Rev.2 provides guidance on how to conduct an assessment of the cyber risks for complying with the Resolution.

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 example, the "Cyber Security Workbook for On Board Ship Use, 2nd Edition 2021" published by BIMCO, provides detailed, step by step checklists to assist the ship's crew with day-to-day management of onboard cyber security to protect vulnerable onboard systems. It also gives guidance on how best to detect, respond and recover in the event of a cyber attack.

Please do not hesitate to contact the Registry at technical@niueship.com or call: +65 6226-2001 for further assistance.