REPUBLIC OF THE MARSHALL ISLANDS

MARITIME ADMINISTRATOR

Marine Guideline

No. 2-11-16

Rev. Mar/2023

TO: ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS OF MERCHANT SHIPS, AND RECOGNIZED ORGANIZATIONS

SUBJECT: Maritime Cyber Risk Management

References:
(a) **IMO Circular** MSC-FAL.1/Circ.3/Rev.2, *Guidelines on Maritime Cyber Risk Management*, issued 7 June 2022
(b) **IMO Circular** MSC/Circ.1154, *Guidelines on Training and Certification for Company Security Officers*, issued 23 May 2005
(c) **RMI Marine Notice** 2-011-13, *International Safety Management (ISM) Code*
(d) **RMI Marine Notice** 2-011-16, *International Ship and Port Facility Security (ISPS) Code*
(e) **Shipping Industry Associations and Organizations**, *The Guidelines on Cyber Security Onboard Ships*

PURPOSE

This document provides guidance and resources to help mitigate maritime cyber risks. It also provides for the voluntary reporting of maritime cyber incidents to the Republic of the Marshall Islands (RMI) Maritime Administrator (the "Administrator"). This version has been streamlined and supersedes that of May/2021.

APPLICABILITY

This Guideline may be used by Companies while integrating safeguards against cyber risks into:

- Safety Management Systems (SMS) as required by RMI Marine Notice 2-011-13; and
- Ship Security Plans (SSPs) under the ISPS Code, as agreed by the International Maritime Organization's (IMO) Maritime Safety Committee (MSC) at its 101st session.[1]

1. At its 101st session, the MSC agreed that aspects of cyber risk management should be addressed in SSP under the ISPS Code, including physical security aspects of cyber security. This does **not** require a Company to establish a separate cyber security management system operating in parallel with the Company's SMS.

DEFINITIONS

Maritime cyber risk is defined as a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping- related operational, safety, or security failures because of information or systems being corrupted, lost, or compromised; and

Cyber risk management is defined as the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.[2]

GUIDANCE

1.0 Maritime Cyber Risk Management Resources

1.1 When used together, the following documents provide a solid foundation for mitigating cyber risks throughout the SMS and SSP:

.1 IMO Circular MSC-FAL.1/Circ.3/Rev.2, which contains high-level recommendations and functional elements for effective maritime cyber risk management; and

.2 The Guidelines on Cyber Security Onboard Ships, which is published by a consortium of shipping industry organizations. These guidelines have been aligned with the IMO Circular MSC-FAL.1/Circ.3/Rev.2. They address:

a. managing ship-to-shore interfaces;

b. network segregation;

c. port risks; and

d. maritime cyber insurance coverage.

.3 Annex 2 of these Guidelines identifies relevant sections of the ISM and ISPS Codes and provides advice on how the cyber-risk element of the Code can be met.

1.2 The Administrator maintains a comprehensive list (SS-200) of maritime cyber risk management resources compiled from shipping industry associations, standard-setting organizations, government agencies, classification societies, and insurers.

2. IMO has defined these terms in IMO Circular MSC-FAL.1/Circ.3/Rev.2.

2.0 Training Resources for Cyber Risk Management

2.1 The Administrator considers cyber risk management and awareness training as a specialized subcategory of overall safety and security training. IMO Circular MSC/Circ.1154, *Guidelines on Training and Certification for Company Security Officers*, provides training for shipboard and shore-based personnel.

2.2 Many third parties have developed maritime cyber risk awareness training courses which may be beneficial to Companies in developing a comprehensive cyber risk management system. Companies that wish to provide this training should ensure that training courses are based on the principles contained in MSC-FAL.1/Circ.3/Rev.2 and *The Guidelines on Cyber Security Onboard Ships*.

3.0 Maritime Cyber Incident Reporting

3.1 All maritime cyber incidents should reported to the Administrator by completing the Report of Maritime Cyber Incident (MI-109-5) form.

.1 Data received by the Administrator will remain strictly confidential and reported incidents will not be attributed to any vessel or Company.

.2 However, anonymized data trends may be used in a Ship Security Advisory as necessary.

3.2 Feedback or concerns should be directed to: marsec@register-iri.com.