



REPUBLIC OF THE MARSHALL ISLANDS

MARITIME ADMINISTRATOR

Marine Guideline

No. 2-11-16

Rev. Aug/2025

**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.3](#)** *Guidelines on Maritime Cyber Risk Management*, issued 4 April 2025
(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 Marine Guideline (MG) provides guidance and resources to help mitigate maritime cyber risks. It also provides the procedure for reporting maritime cyber incidents to the Republic of the Marshall Islands (RMI) Maritime Administrator (the “Administrator”).

This MG supersedes Rev. Mar/2025 and has been updated with references to the latest edition of International Maritime Organization (IMO) Circular [MSC-FAL.1/Circ.3/Rev.3](#), *Guidelines on Maritime Cyber Risk Management*.

APPLICABILITY

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

- Safety Management Systems (SMSs) as required by MN [2-011-13](#); and
- Ship Security Plans (SSPs) under the ISPS Code, as agreed by the IMO’s 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 in §1.1 of IMO Circular [MSC-FAL.1/Circ.3/Rev.3](#) as “a measure of the extent to which Computer Based Systems are 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”.

Additional definitions can be found in §2.1 of the Circular.

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:
 - 1.1.1 IMO Circular [MSC-FAL.1/Circ.3/Rev.3](#), contains high-level recommendations and functional elements for effective maritime cyber risk management; and
 - 1.1.2 [*The Guidelines on Cyber Security Onboard Ships*](#), published by a consortium of shipping industry organizations. These guidelines have been aligned with the IMO Circular and address:
 - .1 identification and assessment of cyber risk (threats, vulnerabilities, likelihood, and impact);
 - .2 protection and detection measures;
 - .3 contingency plans; and
 - .4 response and recovery from cyber security incidents.
 - 1.1.3 Annex 2 of the guidelines identifies relevant ISM Code sections and provides advice on how the cyber-risk element of the Code can be met.
- 1.2 The Administrator maintains a comprehensive list ([MARSEC-200](#)) of maritime cyber risk management resources compiled from shipping industry associations, standard-setting organizations, government agencies, classification societies, and insurers.

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 IMO Circular [MSC-FAL.1/Circ.3/Rev.3](#) and [The Guidelines on Cyber Security Onboard Ships](#).

3.0 Maritime Cyber Incident Reporting

- 3.1 All maritime cyber incidents should be reported to the Administrator by completing a *Report of Maritime Cyber Incident* ([MI-109-5](#)).
 - .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.