



**REPUBLIC OF
THE MARSHALL ISLANDS**
MARITIME ADMINISTRATOR

Marine Guideline

No. 2-11-16

Apr/2018

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

SUBJECT: Maritime Cyber Risk Management

- References:**
- (a) **IMO Resolution [MSC.428\(98\)](#), *Maritime Cyber Risk Management in Safety Management Systems*, adopted 16 June 2017**
 - (b) **IMO Circular [MSC-FAL.1/Circ.3](#), *Guidelines on Maritime Cyber Risk Management*, issued 05 July 2017**
 - (c) **RMI Marine Notice [MN-2-011-13](#), *International Safety Management (ISM) Code***
 - (d) **RMI Marine Notice [MN-2-011-16](#), *International Ship and Port Facility Security (ISPS) Code***

PURPOSE

This document identifies information sources that may aid in establishing policies and procedures for mitigating maritime cyber risks.

APPLICABILITY

This Guideline should be used by Companies to develop safeguards against cyber risks for their Republic of the Marshall Islands (RMI)-flagged vessels.

BACKGROUND

IMO Resolution MSC. 428(98) encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems (SMS) no later than the first annual verification of the Company's Document of Compliance after 1 January 2021.

The RMI Maritime Administrator (the "Administrator") has implemented this Resolution through RMI Marine Notice 2-011-13, *International Safety Management (ISM) Code*. Section 3.3.3 of that Notice provides that in the development of plans for shipboard operations:

The ship's operations plans must ensure that cyber risks are addressed in the SMS no later than the first annual verification of the Company's Document of Compliance after 01 January 2021. See IMO Resolution [MSC.428\(98\)](#), *Maritime Cyber Risk Management in Safety Management Systems*.

The Administrator considers the International Ship and Port Facility Security (ISPS) Code has been and will continue to be an extension of the ISM Code and an integral part of emergency preparedness and compliance with international conventions in a Company's Safety Management System.

GUIDANCE

1.0 International Maritime Organization Guidelines

- 1.1 International Maritime Organization (IMO) Circular [MSC-FAL.1/Circ.3](#), *Guidelines on Maritime Cyber Risk Management*, contains high-level recommendations and functional elements for effective maritime cyber risk management.
- 1.2 It defines:
 - 1.2.1 **maritime cyber risk** 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 as a consequence of information or systems being corrupted, lost, or compromised; and
 - 1.2.2 **cyber risk management** 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.
- 1.3 The IMO guidelines set out the following principles in support of an effective cyber risk management strategy:
 - 1.3.1 **Identify:** Define the roles responsible for cyber risk management and identify the systems, assets, data and capabilities that, if disrupted, pose risks to ship operations.
 - 1.3.2 **Protect:** Implement risk control processes and measures, together with contingency planning to protect against a cyber incident and to ensure continuity of shipping operations.
 - 1.3.3 **Detect:** Develop and implement processes and defenses necessary to detect a cyber incident in a timely manner.
 - 1.3.4 **Respond:** Develop and implement activities and plans to provide resilience and to restore the systems necessary for shipping operations or services which have been halted due to a cyber incident.
 - 1.3.5 **Recover:** Identify how to back-up and restore the cyber systems necessary for shipping operations which have been affected by a cyber incident.

2.0 Shipping Industry Guidelines on Cyber Security

- 2.1 *The Guidelines on Cyber Security Onboard Ships*, published by a consortium of shipping industry associations, are intended to mitigate the risk of major safety and security issues that could result from a cyber incident on board a ship. The guidelines address managing ship-to-shore interfaces, network segregation, port risks, and maritime cyber insurance coverage. They are a working document which is expected to be updated as necessary.
- 2.2 The shipping industry guidelines have been aligned with the IMO *Guidelines on Maritime Cyber Risk Management*. Taken together, these documents provide a solid basis to develop a cyber risk management section in the SMS.

3.0 Maritime Cyber Risk Management Resources

- 3.1 The Administrator maintains and regularly updates a [maritime cyber risk management resources list](#) compiled from industry associations, standards-setting organizations, classification societies, and insurers.

4.0 Maritime Cyber Risk Management Training

- 4.1 The Administrator notes that cyber security training is a specialized subcategory of overall security training. The following training exists for shipboard and shore-based personnel:
 - 4.1.1 Security training for shipboard personnel is required by *RMI Seafarer's Certification Requirements (MI-118)*, §5.23, Mandatory Minimum Security Training; and
 - 4.1.2 Security training for shore-based personnel is covered by IMO Circular [MSC/Circ.1154](#), *Guidelines on Training and Certification for Company Security Officers*, issued 23 May 2005.
- 4.2 The IMO is updating its security model courses to incorporate maritime cyber risk management. Also, third parties are developing maritime cyber security training courses which may be beneficial to the Company in developing their cyber risk management strategy.

5.0 Administrator Contact

- 5.1 Feedback should be directed to the Administrator at: shipsecurity@register-iri.com.