The Bahamas Maritime Authority

Version No. 1.0

Issue Date 03/09/2020

Effective Date 03/09/2020

Cyber Security

Notice to ship owners, managers, Masters, Approved Nautical Inspectors, Recognised Organisations and surveyors

1. Purpose

1.1. This Marine Notice (MN) outlines the position of the Bahamas Maritime Authority (BMA) with respect to establishing policies and procedures for mitigating maritime cyber risk.

2. Application

2.1. This MN is applicable to all Companies to which the ISM Code applies.

2.2. The BMA recommends that this MN is also applied by Companies to which the ISM Code does not apply.

3. Cyber risks to be addressed in Safety Management System

3.1. Cyber risks should be appropriately addressed in safety management systems no later than the first annual verification of the company's ISM Document of Compliance after 01 January 2021, as indicated in IMO Resolution MSC. 428(98).

3.2. Accordingly, Bahamas Recognised Organisations are to ensure that cyber risks are appropriately addressed in the safety management system at the first ISM DOC audit after 01 January 2021.

4. Guidance on maritime cyber risk management

4.1. **International Maritime Organization (IMO) Guidelines**

4.1.1. 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.

4.1.2. MSC-FAL.1/Circ.3 defines:

i. **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 failure as a consequence of information or systems being corrupted, lost, or compromised; and

ii. **cyber risk management** as the purpose of identifying, analysing, 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.

4.1.3. The IMO guidelines set out the following principles in support of an effective cyber risk management strategy:

i. **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.

ii. **Protect:** Implement risk control processes and measures, together with contingency planning to protect against a cyber incident and to ensure continuity of ship operations.

iii. **Detect:** Develop and implement process and defences necessary to detect a cyber incident in a timely manner.

iv. **Respond:** Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services which have been halted due to cyber incident.

v. **Recover:** Identify how to back-up and restore the cyber system necessary for shipping operations which have been affected by a cyber incident.

4.2. **Shipping Industry Guidelines on Cyber Security**

4.2.1. 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-store interfaces, network segregation, port risks, and maritime cyber insurance coverage.

4.2.2. The shipping industry guidelines have been aligned with IMO Guidelines on Maritime Cyber Risk Management. Taken together, these documents provide a solid basis to develop a cyber risk management section in the Safety Management System.

Revision History

Version	Description of Revision
1.0	First Issue