THE REPUBLIC OF LIBERIA
LIBERIA MARITIME AUTHORITY

22980 Indian Creek Drive
Suite 200
Dulles, Virginia 20166, USA
Tel: +1 703 790 3434
Fax: +1 703 790 5655
Email: regsandstandards@liscr.com
Web: www.liscr.com

29 December 2020

Marine Security Advisory: 02/2020

SUBJECT: Maritime Cyber Risk Management in Safety Management Systems

Ref:
a) Marine Notice ISM-001
b) IMO Resolution MSC.428(98)
c) MSC-FAL.1/Circ.3
d) Guidelines on Cyber Security Onboard Ships
e) Marine Security Advisory 02/2019

Dear Shipowner/Operator/Master:

The purpose of this Marine Advisory is to provide guidance to shipowners, operators and Master's on actions to be taken to ensure that safety management systems take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Background

Cyber technologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. The vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, a risk management approach to cyber risks is recommended that is resilient and evolves as a natural extension of existing safety and security management practices.

The safety management objectives of a company under the ISM Code includes, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships.

Liberian Marine Notice ISM-001 in Paragraph 6.10 - Development of Plans for Shipboard Cyber Risk Management, makes addressing cyber risks in the SMS mandatory.

Definitions

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.

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 as a consequence of information or systems being corrupted, lost, or compromised.

Action

Shipowners and operators shall ensure their safety management system takes into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code, including assessment of all identified risks to their ships, personnel and the environment, and the establishment of appropriate safeguards and the continuous improvement of safety management skills of personnel ashore and aboard ships. In addressing cyber risk management, shipowners, operators and Masters should consider the guidance provided in **MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management** and the latest version of **The Guidelines on Cyber Security Onboard Ships** developed by a consortium of shipping industry associations.

MSC-FAL.1/Circ.3 provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management and the industry guidelines provide the minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS. Both refer to several standards to help identify and mitigate cyber risk consistent with the US National Institute of Standards and Technology (NIST) framework, including five functional elements:

a. Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, post risks to ship operations.
b. Protect: Implement risk control processes and measures, and contingency planning to protect against cybersecurity events and ensure continuity of shipping operations.
c. Detect: Develop and implement activities necessary to detect a cybersecurity event in a timely manner.
d. Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
e. Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cybersecurity event.

Crew Cyber Awareness

Also, with regards to addressing the need for crew awareness of cyber risk management and cyber-security, this Administration has developed Cyber and Ship Security Computer Based Training (CBT), which provides a comprehensive overview of cyber-security issues. Details are provided in **Marine Security Advisory 02/2019**.

Reporting of Cyber Incidents

Cyber incidents should be reported to the Administration in accordance with Liberian Marine Notice ISM-001 para 6.12. “Reports and Analysis of Non-Conformities, Accidents and Hazardous Occurrences, as soon as possible after the incidents.

Please note that data received by the Administration will remain confidential and, if reported to IMO or other interested parties, the incidents will not be attributed to any particular ship or Company, unless such identification is agreed to by the Company.

Potential Compliance Assessments by Port States

Port State Authorities have advised their intention to carry out assessments to determine if cyber risk management has been incorporated into the ship's SMS, as required, from 1 January 2021. If objective evidence is found that cyber risk management is not addressed in the ships SMS and/or the ship has failed to implement cyber risk management on board, the ship may be issued a deficiency and required to undergo an internal audit prior to departure or detained pending rectification of the deficiency.

For more information regarding the guidance in this Advisory, please contact Regulations and Standards at RegsandStandards@liscr.com / +1 703 790 3434).

* * * * *