Office of
Deputy Commissioner
of Maritime Affairs

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: security@liscr.com
Web: www.liscr.com

June 18, 2019

MARINE SECURITY ADVISORY – 02/2019

(This Advisory supersedes Marine Security Advisory 07/2017)

Subject: Maritime Cyber Risk Management

References: **MSC-FAL.1/Circ.3** Guidelines on Maritime Cyber Risk Management.
Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems

Dear Owners/Operators/Company Security Officers/Masters:

The purpose of this Advisory is to inform shipowners and operators of available guidance to assess their operations and establish the necessary procedures and actions to address cyber risk.

Company plans and procedures for cyber risk management should be seen as complementary to existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.

MSC-FAL.1/Circ.3, Guidelines On Maritime Cyber Risk Management provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

The approach to cyber risk management described in the Guidelines provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. For detailed guidance on cyber risk management, users of these guidelines should also refer to the latest version of relevant international industry standards and best practices as developed by BIMCO, CLIA, ICS, INTERCARGO and **INTERTANKO (The Guidelines on Cyber Security Onboard Ships)**.

Owners and Operators are encouraged to take into account further guidance in MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Additional guidance and standards may be found in the following:

ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). https://www.iso.org/isoiec-27001-information-security.html.

United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity - https://www.nist.gov/cyberframework.

This Administration has developed Cyber and Ship Security Computer Based Training (CBT), which provides a comprehensive overview of cyber-security issues. The Administration will accept satisfactory completion of the CBT as fulfilling the requirements of STCW security awareness training and special qualification. To order Liberia's Cyber & Ship Security training CD, please complete our Publications Order Form: http://www.liscr.com/order-publications.

For more information, please contact the Security Department at telephone + 1 703 790 3434, email security@liscr.com.

In case of an afterhours emergency please contact the LISCR Duty Officer + 1 703 963 6216, email dutyofficer@liscr.com.

* * * * *