St. Kitts and Nevis International Ship Registry

Flying the Flag of the Federation Worldwide

Stolt-Nielsen House
1-5 Oldchurch Road
Romford
RM7 0BQ
UK

Tel: +44 (0) 1708 380400
Fax: +44 (0) 1708 380401
Email: mail@StKittsNevisRegistry.net

www.StKittsNevisRegistry.net

Circular Letter to Maritime Registrars, Ship Owners and Ship Operators

Maritime Circular No. MC/76/18 **DATE: 1st February 2018**

MARITIME CYBER RISK MANAGEMENT

The purpose of this Maritime Circular is to inform ship owners and ship operators that the International Maritime Organization (IMO) has recently adopted measures for implementation to mitigate cyber security risks on board of vessels and in the shipping industry in general.

Recognizing the need to address the issues related to a raising awareness on cyber risk threats and vulnerabilities to support safe and secure shipping the IMO on 16th June 2017 adopted Resolution MSC.428(98) on *Maritime Cyber Risk Management in Safety Management Systems* taking into consideration MSC-FAL.1/Circ.3 on *Guidelines on Maritime Cyber Risk Management* approved by the Facilitation Committee at its 41st session and by the Maritime Safety Committee at its 98th session.

The Guidelines provide high-level recommendations for maritime cyber risk management to safeguard shipping from current and emerging threats and vulnerabilities. As it is advised, the cyber risk management is a process 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. The Guidelines also present the functional elements that have to be incorporated in a risk management framework to support effective cyber risk management.

The Guidelines refer to a maritime cyber risk as to a measure of the extent to which a technology asset is 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.

The Resolution MSC.428(98) affirms that an approved Safety Management System should take into account cyber risk management in accordance with the objectives and functional requirements in the International Safety Management (ISM) Code. The objectives of the ISM Code include the provisions of safe practices in ship operations and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguard, and the continuous improvement of safety management skills. It is further advised that cyber risks should be addressed in a Safety Management System no later than the first annual verification of the company's Document of Compliance after 1st January 2021.

With regards to the above, this Administration urges ship owners and ship operators to take the necessary actions to safeguard shipping from current and emerging cyber threats and vulnerabilities. Company cyber risk management procedures and plans should be included as complementary to existing security and safety risk management requirements contained in the

International Safety Management (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.

For detailed guidance on cyber management, this Administration also advises to refer to the latest version of *the Guidelines on Cyber Security Onboard Ships* developed by BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO.

If you have any questions on this matter, please do not hesitate to contact us.

Yours truly,

Nigel E. Smith
International Registrar of Shipping and Seamen

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, 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,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to 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;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***