Type of newsletter: ***STATUTORY NEWSLETTER, ISM Code***
Number: ***03.08.2020, revision 0***

APPLICATION:
Type of ships: ***All ships and managing companies to which ISM Code applies***
Flag(s): ***All flags***

MARITIME CYBER SECURITY RISK MANAGEMENT

The purpose of this Newsletter, revoking CRS Technical circular QC-T-313, is to remind ship owners and ship managers on necessity to establish policies and procedures for mitigating maritime cyber risks through the implementation of International Safety Management Code (ISM Code).

Policies and procedures for cyber risk management to be established are to be considered as complementary to already existing risk management requirements contained in the International Safety Management Code (ISM Code) and in the International Ship and Port Facility Security Code (ISPS Code).

Maritime cyber risk should be understood 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.

Maritime cyber risk management should be understood as the 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.

IMO Facilitation Committee, through its Circular MSC-FAL.1/Circ.3, has approved the Guidelines on maritime cyber risk management which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and being complementary to the safety and security management practices established by IMO.
Subject Guidelines are providing 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.

Noting the above, and by taking into account requirements of IMO Res. MSC.428(98) - Maritime Cyber Risk Management in Safety Management, all Companies operating ships on international voyages and to which provisions of ISM Code applies, should address the cyber related risks in their safety management systems not later than the first annual verification of the company's Document of Compliance (DOC) after **1st January 2021**.

CRS, when acting on behalf of Maritime administrations is expected to verify compliance with the above mentioned requirement during the first annual verification of the company's DOC after 1st January 2021.

Apart from above cited IMO documents, for more detailed guidance on cyber risk management reference can be also made to the latest version of relevant international industry standards and best practices developed by BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO, with additional standards also being available in ISO/IEC 27001.

Glavni ured / Head Office:
HRVATSKI REGISTAR BRODOVA
21000 SPLIT
Marasovića 67
P.P. 187
HRVATSKA

Telefon / Phone No:
+ 385 (0)21 408 111 (centrala)
Fax:
+385 (0)21 358 159

URL: www.crs.hr
Email:
tech.coord@crs
csys@crs.hr
fleet.services@crs.hr
constr@crs.hr