Isle of Man Ship Registry
Technical Advisory Notice

Maritime Cyber Risk Management	Ref. 007-20 Issued:14 Dec 2020

This Notice applies to operators of ships subject to the ISM Code.

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 if not addressed, may result in operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

The International Maritime Organization adopted Resolution MSC.428(98) which states 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. This Resolution requires that from **1 January 2021,** it must be verified no later than the first annual verification of a company's Document of Compliance that measures ensuring cyber risks have been addressed in safety management systems.

In order to raise awareness of cyber risk threats and vulnerabilities, the IMO has published MSC-FAL.1/Circ.3 guidelines on maritime cyber risk management. These guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The guidelines are recommendatory, although this Administration encourages managers and operators of IoM registered ships, to undertake the cyber risk management process stated in MSC-FAL.1/Circ.3. This is in order to ensure cyber risks have been appropriately addressed for all the vulnerable systems on their ships.

Vulnerable systems could include, but are not limited to:

- Bridge systems;
- Cargo handling and management systems;
- Propulsion and machinery management and power control systems;
- Access control systems;
- Passenger servicing and management systems;
- Passenger facing public networks;
- Administrative and crew welfare systems; and
- Communication systems.

It is recognised that no two companies are the same and ships with limited cyber-related systems may, after review of their systems and vulnerabilities, find the simple application of the recommendations sufficient, while ships with complex system requirements may require substantially increased mitigation of the identified risks. It is therefore up to the DOC company to implement a system that best suits their ship's requirements.

DOC & SMC audits after 1 January 2021

At each DOC audit and each SMC audit following the first annual verification of the company's DOC after 1 January 2021, the company and the company's ship(s) will need to demonstrate that 'cyber risks are appropriately addressed in safety management systems'.

The attending Isle of Man or Recognised Organisation surveyor, will verify that this has been addressed and relevant cyber risks have been considered and documented. Any mitigating measures defined by the company would be within the scope of the audit and could be reviewed by the attending auditor, with the potential for observations or non-conformities to be raised should non-compliance with the company's requirements be found.

Reference material

- Resolution MSC.428(98) Maritime cyber risk management in safety management systems
- IMO MSC-FAL.1/Circ.3 Guides on maritime cyber risk management