Maritime & Coastguard Agency

MARINE INFORMATION NOTE

MIN 647 (M)

Incorporation of Cyber Security measures within Safety Management Systems

Notice to all Surveyors, recognised organisations, Certifying Authorities, ship operators, ship owners, masters, officers and crew

This MIN expires 31st December 2021

Summary

This Notice advises industry of the need to incorporate Cyber Security within the management procedures on board UK Registered Ships where required and advises other operators to recognise and address the risks associated with breaches in Cyber Security in the operation of their vessels.

1. Introduction

1.1 As technology has advanced ships have become increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life. The pace of change in the industry is such that the level of reliance on digital technology for the safe operation of ships is increasing.

1.2 Cyber security is not just about preventing unauthorised persons gaining access to systems and information. It also addresses the maintenance of integrity and availability of information and systems as well as supporting business continuity. Consideration needs to be given to not only protecting ship systems from physical attack, but also to ensuring that the design of systems is resilient and that appropriate reversionary modes are available in the event of compromise.

1.3 Personnel security aspects are also important. The insider threat from shore-based or shipboard individuals who may behave in a malicious or non-malicious manner cannot be ignored. Ship owners and operators need to understand cyber security and promote awareness of this subject to their stakeholders, including their shipboard personnel.

1.4 In June 2017, the International Maritime Organization (IMO) adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems - which recognised that all maritime industry stakeholders needed to expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities, encouraging administrations to ensure that cyber risks are appropriately

addressed in existing safety management systems (as defined in the International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code)) no later than the first annual verification of the company's Document of Compliance (DOC) after 1 January 2021.

1.5 Whilst the IMO Resolution is specific to those vessels to which the ISM Code applies, it is recommended that all operators assess the risks to their operations from a cyber security perspective and put in place relevant mitigations.

2. Operators of vessels operating under the requirements of the ISM Code.

2.1 IMO Resolution MSC.428(98) encourages administrations to ensure that cyber risks are appropriately addressed, and it is the responsibility of the company to ensure that all risks are appropriately identified and mitigated.

2.2 The IMO provided high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines set out in the Annex to MSC-FAL.1/Circ.3, also include functional elements that support effective cyber risk management.

2.3 The safety management systems implemented by the company for compliance with the ISM Code should, by the first Document of Compliance (DOC) audit after 1st January 2021, incorporate measures to address identified cyberthreats and vulnerabilities, noting that these will be specific to each particular operation.

2.4 From the 1st January 2021, ISM Audits for the DOC and subsequent Safety Management Certificate (SMC) audits conducted by the MCA will verify that that the safety management systems contain elements showing that cyber risks have been addressed.

2.5 Guidance on Cyber Security on board ships may include, but are not limited to the following:

2.5.1 *Code of Practice Cyber Security for Ships* produced by the Institution of Engineering and Technology (IET), supported by the Department for Transport (DfT) and the Defence Science and Technology Laboratory (Dstl)

2.5.2 *The Guidelines on Cyber Security Onboard Ships* produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

2.5.3 *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).

2.5.4 *Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).* United States National Institute of Standards and Technology

2.6 Reference should be made to the most current version of any guidance or standards used.

3. Operators of vessels not operating under the requirements of the ISM Code.

3.1 Though the IMO Resolution refers directly to those vessels and operators where the ISM Code applies, the need to address identified cyberthreats and vulnerabilities is not limited to those vessels and operators of companies and vessels to which the ISM Code does not apply are strongly advised to note the guidance available on the subject of Cyber Security and assess their own systems against the threats apparent in the increasingly technical environment in which they operate.

More Information

UK technical Services (Operations)
Maritime and Coastguard Agency
Bay 2/20
Spring Place
105 Commercial Road
Southampton
SO15 1EG

Tel: +44 (0) 203 8172000
e-mail: hq_maritimesecurity@mcga.gov.uk

Website Address: www.gov.uk/government/organisations/maritime-and-coastguard-agency

General Enquiries: infoline@mcga.gov.uk

Published: November 2020
Please note that all addresses and
telephone numbers are correct at time of publishing

Safer Lives, Safer Ships, Cleaner Seas