INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
109th session
Agenda item 7

MSC 109/7/1
27 September 2024
Original: ENGLISH
Pre-session public release: ☒

REVISION OF THE GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/CIRC.3/REV.2) AND IDENTIFICATION OF NEXT STEPS TO ENHANCE MARITIME CYBERSECURITY

Proposal for next steps to enhance maritime cybersecurity

Submitted by Antigua and Barbuda, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Chile, Croatia, Cyprus, Czechia, Denmark, Ecuador, Estonia, Finland, France, Germany, Greece, Guatemala, Hungary, Ireland, Israel, Italy, Japan, Latvia, Liberia, Lithuania, Luxembourg, Malta, Marshall Islands, Mexico, Netherlands (Kingdom of the), Norway, Panama, Peru, Philippines, Poland, Portugal, Republic of Korea, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, United Arab Emirates, United Kingdom, United States of America, Uruguay, European Commission, IACS, and IAPH

SUMMARY

Executive summary:	This document discusses the importance of further cybersecurity measures for ships and port facilities following the Committee's approval of the draft revised Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.3) and proposes next steps to enhance maritime cybersecurity.
Strategic direction, if applicable:	2
Output:	2.8
Action to be taken:	Paragraph 18
Related documents:	MSC 108/6, MSC 108/6/1, MSC 108/20, paragraphs 6.1-6.11, MSC 108/20/Add.1, Annex 25, MSC 108/WP.10; MSC 107/17/9, MSC 107/17/28, MSC 107/20, paragraphs 17.26-17.28, MSC 107/INF.11, MSC 107/INF.17; MSC 104/7/1; FAL 48/5/5, FAL 48/17; FAL 46/23/2; resolution A.1110(3); resolution MSC.428(98); MSC-FAL.1/Circ.3/Rev.2; MSC.1/Circ.1526 and MSC-MEPC.7/Circ.1

Introduction

1 MSC 107 agreed to include an output on the "Revision of the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.2) and identification of next steps to enhance maritime cybersecurity". A drafting group was established at MSC 108 and the Committee subsequently approved the draft revised *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.3) and agreed to forward them to the Facilitation Committee for its concurrent approval.

2 This document aims to identify next steps to enhance maritime cybersecurity, following the Committee's approval of the draft revised *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.3).

Background

3 As highlighted by document MSC 107/17/9 (Australia et al.), along with documents MSC 107/INF.17 (Brazil) and MSC 104/7/1 (IAPH), the maritime industry has an urgent need for enhanced cybersecurity measures to protect commercial ship and port facility operations from increased cyberthreats and risks.

4 The co-sponsors greatly appreciate all the work that was done at MSC 108 by the Committee to approve the revised *Guidelines on Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.3), with the objective to set and ensure a level playing field and predictability on board ships regarding what to expect during surveys and inspections with respect to cyber risk management.

5 However, the co-sponsors are of the view that unified cybersecurity standards would be the most effective means to ensure consistent application and instil confidence that ships and port facilities meet a minimum cybersecurity level to protect against increasing cyberthreats and risks.

Discussion

6 The rapid advancement in technology, including digitalization, autonomous, and remote-control technologies, associated with the use of a broad communications infrastructure, are driving significant change in the maritime industry. The improvements in connectivity have greatly increased efficiencies in the global economy, and the interconnection between ships and port facilities will only continue to grow.

7 These innovations and technologies, while beneficial, also introduce increased vulnerabilities in the maritime transportation system. This includes the increasing threat of cyber attacks by malicious cyberactors.

8 Converging information technology and operational technology systems, combined with hardware and software on board which is often outdated, increases a ship's susceptibility to malicious cyberactors. Additionally, the absence or weakness of security technologies and software, vulnerable communication infrastructure, a lack of visibility over vast and complex networks, and a lack of crew cybertraining, hygiene, and awareness leave innumerable entry points for cybercriminals.

9 These vulnerabilities are becoming increasingly problematic due to increased incentives to target the maritime sector. Cyberincidents have the potential to cripple the international economy, disrupt critical supply chains, endanger industry personnel, and devastate the marine environment. Blockage of traffic flow through congested waterways,

equipment damage, ship groundings, and the release of hazardous chemicals are all examples of foreseeable effects of a cyberincident. The opportunity for global disruption through an easy, simple access point makes the maritime domain the perfect target.

10 While the main focus at IMO to date has been on ship cyber risk management, port facilities are also at risk of cyberincidents. Port facilities are the access points for international shipping and are critical for the movements of goods and services by simultaneously servicing multiple commercial ships. The potential impact of a cyberincident on a port facility or multiple port facilities may have an exponentially greater crippling effect on the maritime transportation system and supply chain resiliency. Therefore, port cyber risk management is as critical as ship cyber risk management.

11 The interconnected nature of maritime infrastructure with sectors such as energy, transport, and information technology mean that disruptions in one area can have consequences for other critical infrastructure sectors.

12 Given the challenges presented, it is essential to encourage the creation of a collaborative environment for the maritime sector, with the aim of facilitating the sharing of information and best practices. A collaborative approach aimed at addressing cyberthreats in a multidisciplinary manner, improving cyber awareness among all those involved in ship operations and the port sector, as well as collaborating in the updating of cybersecurity training standards and methodologies.

13 Some Member States have recognized this trend and have begun to set national frameworks for cybersecurity requirements for ships and port facilities within their jurisdiction. Classification societies and industry groups have also published cybersecurity guidelines and requirements. The co-sponsors are of the view that, while national requirements and industry standards are important, there is a need to set expectations for ships and seafarers sailing internationally.

14 In its crucial role as the primary international forum for addressing technical matters of all kinds impacting global shipping, IMO should proactively lead efforts to establish unified cybersecurity standards for ships and port facilities following the approval of the revised *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.3). This approach would not only set explicit expectations but also foster confidence by ensuring that both ships and port facilities adhere to a minimum cybersecurity level. Such measures are essential for safeguarding the international economy against evolving cyberthreats and risks.

15 Such an approach should also take into account, to the extent possible, relevant horizontal cybersecurity frameworks and standards, such as legislative frameworks setting out cybersecurity requirements for critical infrastructure and operators, such as port facilities, as well as for hardware or software and their supply chains.

16 Considering the Committee's proposed working groups at MSC 109, the shorter duration of MSC 109, and the working group capacity constraints for each session, the co-sponsors recommend that the next steps to enhance maritime cybersecurity output remain on the agenda to be discussed at MSC 110 in order to give a proper amount of time to discuss this critical issue.

Proposal

17 The co-sponsors invite the Committee to:

.1 agree to further develop cybersecurity standards for ships and port facilities;

.2 encourage interested Member States and non-governmental organizations to submit proposals to the next session of MSC; and

.3 establish a working group at the next session of MSC.

Action requested of the Committee

18 The Committee is invited to consider the information provided in paragraphs 6 to 16 and the proposal in paragraph 17, and take action, as appropriate.