INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
110th session
Agenda item 7

MSC 110/7/2
11 April 2025
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

Development of cybersecurity standards for ships and port facilities

Submitted by the United States

SUMMARY

Executive summary:	This document outlines the approach to identify the next steps for enhancing maritime cybersecurity, including proposed terms of reference for a working group at MSC 110 to establish cybersecurity requirements for ships and port facilities.
Strategic direction, if applicable:	2 and 5
Output:	2.8
Action to be taken:	Paragraph 15
Related documents:	MSC 109/22, paragraphs 7.1 to 7.7 and 19.53.3, MSC 109/7; MSC 109/7/1, MSC 109/7/2; MSC 108/20, paragraph 6.1 to 6.11, MSC 108/6, MSC 108/6/1; MSC-FAL.1/Circ.3/Rev.3; resolution A.1110(3); resolution MSC.428(98); MSC.1/Circ.1526; MSC-MEPC.7/Circ.1; MSC 107/20, paragraphs 17.26 to 17.28; MSC 107/17/9, MSC 107/17/28, MSC 107/INF.11, MSC 107/INF.17; MSC 104/7/1; FAL 48/20, paragraphs 5.17 to 5.18, FAL 48/5/5, FAL 48/17; and FAL 46/23/2

Introduction

1 The Maritime Safety Committee at its 108th session (MSC 108) approved the revised *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3/Rev.3) and forwarded them to the Facilitation Committee's forty-ninth session (FAL 49) for concurrent approval. The second part of the item, focusing on the identification of next steps to enhance maritime cybersecurity, was included in the agenda at MSC 109 (MSC 109/1/1). The Committee agreed there was a need for further in-depth discussion and agreed to extend the target completion of the output to 2026 (MSC 109/22, paragraph 7.7).

2 This document identifies key points of discussion and proposes a process to facilitate the identification of next steps to enhance maritime cybersecurity through structured terms of reference. This document builds on previous decisions of the Committee while considering the evolving nature of maritime cyber threats and the critical need for harmonized international standards.

Background

3 At MSC 109, the Committee considered documents MSC 109/7 (INTERPORTPOLICE), which emphasized key aspects of cyber incident response, as well as MSC 109/7/1 (Antigua and Barbuda et al.) and MSC 109/7/2 (United Arab Emirates), which highlighted the urgent need for robust and unified cybersecurity measures. However, due to the shorter duration of MSC 109 and working group capacity constraints, the Committee agreed on the need to further develop cybersecurity standards for ships and port facilities and considered the possibility of establishing a working group at MSC 110, subject to submissions and taking into account the limit on the number of working groups (MSC 109/22, paragraph 7.7.1).

4 Furthermore, the Committee invited Member States and international organizations to submit proposals on next steps to enhance maritime cybersecurity for consideration (MSC 109/22, paragraph 7.7.2).

5 The Committee also agreed to extend the target completion year of the output to 2026 (MSC 109/22, paragraph 7.7.3).

Discussion

6 The maritime industry faces increasing cybersecurity challenges due to rapid technological advancement and digitalization. The convergence of information technology with operational technology systems has created new vulnerabilities requiring immediate attention.

7 As highlighted in document MSC 109/7/1 (Antigua and Barbuda et al.), critical maritime infrastructure remains susceptible to cyber threats as the industry continues to increase its reliance on automated and interconnected systems. This vulnerability is compounded by gaps in cybersecurity awareness and training across the maritime workforce, legacy hardware and software that may lack current security features, and complex network architectures with multiple access points.

8 The consequences of cyber incidents in the maritime industry can be severe and far-reaching. Disruptions to critical supply chains can have global economic impacts, while compromised ship or port facility operations directly threaten maritime safety. Environmental damage may result from accidents or incidents triggered by cyberattacks, and significant economic losses can occur from system downtime or data breaches. Additionally, loss of control of ships or port facility operations in the vicinity of critical waterways and infrastructure could lead to loss of life, a national level safety incident, and severe disruption to national security. These catastrophic consequences underscore the urgency of developing robust cybersecurity standards.

9 The United States recently updated its domestic maritime transportation security regulations by establishing minimum mandatory cybersecurity requirements. These new requirements apply to U.S.-flagged ships, and facilities that are subject to the United States' implementing regulations for the Maritime Transportation Security Act of 2002.[*]

[*] 33 Code of Federal Regulations (CFR) Part 101 Subpart F, 101.600 – 101.670.

These updates address current and emerging cybersecurity threats to key segments of the United States' maritime infrastructure to help detect risks and respond to and recover from cybersecurity incidents. These include requirements to develop and maintain a cybersecurity plan, designate a cybersecurity officer, ensure cybersecurity training for personnel, and take various risk-based measures to maintain cybersecurity.

10 The United States is of the view that the development of mandatory cybersecurity requirements is warranted. It is critical for Member States to establish internationally agreed-upon standards that address the commonly shared cybersecurity threats to maritime trade. Through global consensus, development of a harmonized regulatory approach can mitigate the risks of any exploitable security vulnerabilities, especially any gaps between flag and port States requirements in the context of ship to port interfaces. The Committee should consider whether the development of cybersecurity requirements should remain voluntary or be made mandatory.

11 The Committee should also evaluate different regulatory approaches, including prescriptive standards that specify detailed requirements, goal-based standards that focus on desired outcomes while allowing flexibility in implementation, and risk-based approaches that scale requirements based on assessed threat levels and potential impacts.

12 The United States notes that the implementation of cybersecurity requirements could be achieved through various regulatory instruments. Existing frameworks, such as the International Safety Management (ISM) Code and the International Ship and Port Facility Security (ISPS) Code, could be expanded to address cybersecurity alongside existing related physical security measures. Alternatively, a new dedicated instrument could be developed, such as a stand-alone cybersecurity code, or a new chapter could be added to SOLAS specifically addressing cybersecurity requirements. The Committee should consider how enhanced maritime cybersecurity requirements would be implemented.

13 To facilitate these efforts, the United States proposes terms of reference in the annex as a structured approach, providing a process for identifying and evaluating the next steps in developing maritime cybersecurity requirements. This would allow the Committee to assess current measures, identify gaps, and develop appropriate recommendations among Member States and international organizations.

Proposal

14 The Committee is invited to consider next steps as proposed in the annex through the establishment of a working group. If a working group cannot be established at MSC 110, establish a correspondence group to report to MSC 111.

Action requested of the Committee

15 The Committee is invited to consider the information provided in paragraphs 6 to 13 and the proposal in paragraph 14, and take action, as appropriate.

***

ANNEX

DRAFT TERMS OF REFERENCE FOR THE FURTHER DEVELOPMENT OF CYBERSECURITY STANDARDS FOR SHIPS AND PORT FACILITIES

1 Determine a standardized approach for the further development of cybersecurity requirements (i.e. risk-based/goal-based/prescriptive).

2 Determine if cybersecurity requirements should be made mandatory or voluntary.

3 If mandatory, consider the IMO instrument that would be the most appropriate mechanism for implementing new cybersecurity requirements for ships, port facilities and ship-port facility interfaces (e.g. SOLAS – amending ISM Code or ISPS Code, establishing a Cyber Code, establishing a cyber chapter within SOLAS/etc.).

4 Consider interim measures, such as thorough audits, to enhance maritime cybersecurity while associated standards are under development.