INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
110th session
Agenda item 7

MSC 110/7
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

A goal-based approach to the development of maritime digital-ecosystem cybersecurity standards

Submitted by Canada, Indonesia, Republic of Korea, United Arab Emirates, United Kingdom, IACS and IAPH

SUMMARY

Executive summary:	This document proposes the development of a goal-based approach to maritime digital-ecosystem cybersecurity standards, capturing cyber risk management for port facilities, shipping and logistical systems that support global networks. This provides a next step in the development of a global approach following MSC 109 where the need for further development of cybersecurity standards for ships and port facilities at MSC 110 was agreed.
Strategic direction, if applicable:	2 and 5
Output:	2.8
Action to be taken:	Paragraphs 17 and 18
Related documents:	MSC 109/7; MSC 108/6 and MSC 108/6/1, MSC 108/20, paragraphs 6.1 to 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 to 17.28, MSC 107/INF.11 and 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.3; MSC.1/Circ.1526 and MSC-MEPC.7/Circ.1

1 This document is submitted in accordance with the *Organization and method of work of the Maritime Safety Committee and the Marine Environment Protection Committee and their subsidiary bodies* (MSC-MEPC.1/Circ.5/Rev.5) and proposes the creation of a set of goal-based standards for maritime cybersecurity.

Introduction

2 At its 109th session the Maritime Safety Committee agreed to:

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

.2 potentially establish a working group at MSC 110 to develop these standards while engaging with Member States.

3 This decision followed agreement at MSC 107 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". It is essential that IMO proactively leads efforts to establish unified cybersecurity standards that support the global supply chains essential for the prosperity of all Member States in its role of providing machinery for cooperation among Governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade.

4 Developing and adopting goal-based standards is a proportionate, incremental method to developing a global approach. It enables Member States and industry to follow an approach suited to local requirements and aspirations. The methods of achieving a goal can be supported through guidance submitted by Member States and collated on the IMO website under "Maritime cyber risk", as agreed at MSC 108; and through the use of the IMO *Generic Guidelines for Developing Goal-Based Standards* (MSC.1/Circ.1394/Rev.2)

5 In setting standards, IMO should not set explicit conditions, but foster confidence, by ensuring the maritime digital-ecosystem of ships, port facilities, and associated logistical networks are able to meet an agreed minimum cybersecurity level.

6 This document intends to:

.1 set out an initial proposal for the development of international goal-based standards to support cybersecurity risk management within the maritime sector; and

.2 posit that this proposal should be further discussed and developed by Member States during a working group of MSC.

Background

7 As highlighted by document MSC 109/7/1 (Antigua and Barbuda et al.), the maritime industry has an urgent need for enhanced cybersecurity measures to protect commercial ship and port facility operations from increased cyber threats and risks.

8 Ships and port facilities are becoming increasingly interconnected, expanding the traditional view of maritime from one focused on ports and ships. In contrast, the modern maritime digital-ecosystem now covers a range of interconnections. Supporting ship operations, safety, and security with effective cybersecurity throughout the maritime digital-ecosystem is now essential.

9 The co-sponsors greatly appreciate all the work that has preceded MSC 110 including the discussions to develop the global debate. The most substantial piece of work completed was at MSC 108 which approved the revised *Guidelines on Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.3). This objective was to set a uniform approach on board ships for surveys and inspections surrounding cyber risk management. This work has facilitated

increased engagement at the global level on maritime cybersecurity, with a range of bilateral and multilateral events taking place that have raised awareness and facilitated a global approach to the challenges.

10 MSC 109 agreed that unified cybersecurity standards would be the most effective mechanism to instil confidence that ships and port facilities meet a minimum cybersecurity level. Such an approach should also consider 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.

11 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. Developing and adopting international standards can support all nations and set effective baseline goals. This demonstrates the need for IMO to take a central role in providing consistency and coherence in the global understanding of the challenge being faced. To do this, the co-sponsors believe in an incremental approach to developing the global approach to maritime cybersecurity, to ensure all parts of the maritime sector progress in tandem.

Proposal

12 The co-sponsors propose the development of goals based maritime digital-ecosystem cybersecurity standards (MDECSS). MDECSS should be developed as a global community, including Member States and industry, and should be underpinned by comprehensive guidance to assist Member States in application of the standards.

13 There are many cybersecurity frameworks in existence across Member States, setting out goal-based standards, The proposed starting point for these discussions is based around four core objectives, with Member States being invited to work with IMO to develop a set of agreed, unified standards.

14 MDECCS four starting objectives are:

.1 managing cybersecurity risk;

.2 protecting against cyberattacks;

.3 detecting cybersecurity events; and

.4 minimising the impact of cybersecurity incidents.

15 Principles underpinning these objectives can be found in the annex.

16 The MDECSS development should consider relevant cybersecurity frameworks, standards and legislative frameworks already in existence. MDECSS should support Member States by providing a clear baseline, they should not supersede legislative frameworks at a higher level.

Action requested of the Committee

17 The Committee is invited to consider the information provided in paragraphs 7 to 11 and the proposal in paragraphs 12 to 16 (including the annex), and take action, as appropriate.

18 The co-sponsors invite the Committee to:

.1 agree to the developments of goal-based Maritime Digital-Ecosystem Cybersecurity Standards based on the proposed framework; and

.2 encourage Member States to submit guidance to the IMO Secretariat for collation to support adherence to globally agreed standards.

***

ANNEX

Proposed Maritime Digital-Ecosystem Cybersecurity Standards

Objective A - Managing Security Risk

Principle: A1 Governance
Putting in place the policies, processes and procedures which govern your organization's approach to the security of network and information systems.

Principle: A2 Risk Management
Identification, assessment and understanding of security risk including the establishment of an overall organizational approach to risk management.

Principle: A3 Asset Management
Determining and understanding everything required to deliver, maintain and/or support essential functions.

Principle: A4 Supply Chain
Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.

Objective B – Protecting against cyber attacks

Principle: B1 Service Protection Policies, Processes and Procedures
Defining and communicating appropriate organisational policies, processes and procedures to secure systems and data that support the operation of your essential function(s).

Principle: B2 Identity and Access Control
Understanding, documenting and controlling access to networks and information systems supporting essential functions.

Principle: B3 Data Security
Protecting stored or electronically transmitted data from actions that may cause an adverse impact on essential functions.

Principle: B4 System Security
Protecting critical network and information systems and technology from cyber attack.

Principle: B5 Resilient Networks and Systems
Building resilience against cyber attack.

Principle: B6 Staff awareness and training
Appropriately supporting staff to ensure they make a positive contribution to the cybersecurity of essential functions.

Objective C – Detecting cybersecurity events

Principle: C1 Security Monitoring
Monitoring to detect potential security problems and track the effectiveness of existing security measures.

Principle: C2 Proactive Security Event Discovery
Detecting anomalous events in relevant networks and information systems.

Objective D – Minimizing the impact of cybersecurity incidents

Principle: D1 Response and Recovery Planning
Putting suitable incident management and mitigation processes in place.

Principle: D2 Lessons Learned
Learning from incidents and implementing these lessons to improve the resilience of essential functions.