INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
110th session
Agenda item 5

MSC 110/5/7
11 April 2025
Original: ENGLISH
Pre-session public release: ☒

DEVELOPMENT OF A GOAL-BASED INSTRUMENT FOR MARITIME AUTONOMOUS SURFACE SHIPS (MASS)

Proposed amendments to chapter 22 (Special measures to enhance maritime security)

Submitted by Canada, Indonesia, Japan, United Arab Emirates, United Kingdom and IACS

SUMMARY

Executive summary:	This document proposes a new draft text and restructuring of chapter 22 (Special measures to enhance maritime security). Proposed amendments to the existing draft include functional requirements addressing the security of the remote operations centre (ROC), autonomous vessel, automated security technologies, and the expansion of the applicability of the ISPS Code to include remote operators and ROCs. In addition, the co-sponsors suggest that a review of cyber security provisions within the MASS Code is conducted upon completion to ensure that this topic is adequately addressed.
Strategic direction, if applicable:	2, 5
Output:	2.23
Action to be taken:	Paragraph 12
Related documents:	MSC 107/WP.9; MSC 108/4, MSC 108/J/5; MSC 109/WP.8; MSC/ISWG/MASS-3/VP chapter 22 – Security

1 This document is submitted in accordance with MSC-MEPC.1/Circ.5/Rev.5 on the *Organization and method of work of the Maritime Safety Committee and the Marine Environment Protection Committee and their subsidiary bodies,* taking into account resolution A.1174(33) on the *Application of the Strategic Plan of the Organization*.

Introduction

2 MSC 105 established the intersessional MASS Correspondence Group (CG) for the development of the draft MASS Code, and MSC 106 agreed to allocate this work to participating Member States and observer organizations under the CG. MSC 107 agreed to continue the review of the draft MASS Code, based on document MSC 107/WP.9, in the CG.

3 Chapters of the draft MASS Code were developed in detail during this time by several volunteering Member States, as was reported in document MSC 108/4 (Marshall Islands). Directly prior to MSC 108, a further review of the draft MASS Code was performed, which was reflected in MSC 108/J/5. This document aims to provide input on chapter 22 (Special measures to enhance maritime security) which has not yet been discussed in detail by the MASS Working Group.

Special measures to enhance maritime security chapter

4 The co-sponsors would like to express sincere gratitude to those individuals and Member States whose expertise and efforts have already contributed to the development of this chapter, including the Liberian delegation for development of the previous version of this vital chapter.

5 Through analysis of the Hazard Identification (HAZID) tables, developed as a basis for the different MASS Code chapters,* the ISPS Code, and review of the previous works conducted by this group, the co-sponsors believe that additional inclusions are needed in order to ensure the security chapter encompasses all relevant considerations with regard to the security of MASS.

6 The co-sponsors have developed the annex with the aim to progress the MASS Code as a whole.

7 The co-sponsors believe that the security chapter should attempt to cover several distinct security goals, and have structured the annex as such. These security goals are:

.1 use of autonomous security systems to replace actions conducted by seafarers, e.g. automated CCTV monitoring for intrusion detection;

.2 security of autonomous systems to replace actions conducted by seafarers e.g. navigation systems;

.3 security of seafarers on board an autonomous ship and on board other ships;

.4 security concerns of a remote facility in control of a ship;

.5 security concern of, and caused by, an unmanned autonomous ship, e.g. hijacking, or the use of a ship as a weapon; and

.6 security of data within networked systems, and the need for these systems to communicate and operate securely.

8 This document, while specifically addressing chapter 22 of the MASS Code, seeks to provoke discussion on wider security provisions included within the MASS Code as a whole. The co-sponsors are aware that there is potential overlap between provisions suggested here and other parts of the MASS Code. However, it is our opinion that other chapters may not have adequately considered the possibility of incidents brought about by malign actors. The continued inclusion of the relevant functional requirements (FRs) and expected performances (EPs) in this draft Code is a suggestion that either the specific security concerns of these provisions should be addressed in this chapter, or that the provisions elsewhere in the Code be amended to include additional security considerations.

* Available via IMO Virtual Portal for MSC/ISWG/MASS.

9 In this document, the co-sponsors wish to reiterate that the requirements of the ISPS Code continue to apply to MASS, and we believe that these requirements should also apply to personnel such as remote operators and the ROCs that they work from, where they are fulfilling functions normally undertaken by seafarers (as noted in chapter 5).

10 The co-sponsors have not explicitly discussed the concept of cyber security in this chapter, as it is currently included in provisions throughout the MASS Code. However, it is the co-sponsors' opinion that autonomous ships, by their nature, will require a higher level of cyber security than traditional ships to achieve comparable safety and security outcomes due to the removal or reduction of the physical presence of seafarers on board, and greater reliance on networked operational technology (OT) systems and information technology (IT) systems. As such, the co-sponsors suggest that, upon completion, the Working Group, if established, conduct an assessment of cybersecurity provisions throughout the Code to ensure that it is sufficiently addressed throughout a ship's lifecycle.

11 The annex sets out a proposed revised draft of chapter 22 to be used as the base text.

Action requested of the Committee

12 The Committee is invited to consider the proposals highlighted above in reference to chapter 22 for further development of the Code, in particular, to:

.1 use the annex as the base text for chapter 22 of the MASS Code to be further developed and finalized in the Working Group, if established; and

.2 upon completion, undertake a review of the provisions within the MASS Code related to cybersecurity in order to ensure that it is adequately addressed across the Code,

and to take action, as appropriate.

***

ANNEX

PROPOSED REVISED BASE TEXT FOR CHAPTER 22

22.1 Goal

The goal of this chapter is to ensure adequate security.

22.2 Functional Requirements

To achieve the above-mentioned goal, the ship and ROC should comply with the requirements of the special measures to enhance maritime security in SOLAS chapter XI-2 "Special Measures to Enhance Maritime Security" and the ISPS Code, as supplemented by the functional requirements of this chapter.

22.2.1 Means should be provided to enable the assessment of security effectiveness for autonomous and remotely controlled systems.

22.2.2 The ship should be able to communicate and exchange security-related information with the ROC and, where appropriate, to flag State authorities, Contracting Governments, and port Authorities upon request taking into account the sensitivity of the information and authorization to access security-sensitive information.

22.2.3 The use of autonomous security systems should not negatively impact on the:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies including the Ship Security Plan (SSP);

.5 radio and telecommunication systems including computer systems and networks; and

.6 any other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship.

22.2.4 In the event of the security of a ROC being compromised, measures and procedures should be in place to ensure that this does not subsequently impact the security of a remotely operated or autonomous ship.

EP 1 There should be a mechanism for safely shutting communications down when the security of the ROC has been compromised.

EP 2 The vessel should enter a predefined fallback state until secure communication can be established with a secure ROC.

EP 3 Communication between a ROC experiencing an incident, or having experienced an incident, and an automated vessel should only be reestablished once the security of the ROC has been ensured and validated.

EP 4 Procedures should be documented in the SSP, with plans in place to state where communications will failover to, and how communication will be reestablished.

22.2.5 Measures and procedures should be in place on board a remotely operated or autonomous vessel to ensure continuity of outcomes to manned vessels in the event of a security incident, considering the safety of any crew, other shipping and the environment.

EP 1 An appropriate level of communication between the ship and the ROC should be maintained during and following a security event on board, or impacting upon, a ship.

EP 2 Systems should allow for coordination between the ship and third party responders, and should provide sufficient information to ensure the safety of external responders, other shipping, and the ship's environment.

EP 3 Sufficient redundancy should be included in the design and implementation of communication systems such that a reasonably foreseen attack scenario would not result in damage to all systems.

EP 4 In the event communication is lost following a security event the ship should enter an appropriate fallback state and be capable of maintaining that state during and following the event to the degree necessary.

22.2.6 Means should be provided to implement the requirements of the Ship Security Plan meeting the requirements laid out in the ISPS Code. The security of the ship should not be compromised by the use of autonomous systems.

EP 1 Sufficient processes should be in place to ensure that the vessel can respond appropriately to a change in ISPS Security Levels.

EP 2 The role of remote operators, and those with responsibilities that have been transferred from the vessel, shall be required to be addressed in the SSP requirements under ISPS Code, section A/9.4.

EP 3 The role and responsibilities of the ship security officer must be maintained and an SSP must include measures of how the duties of this role will be carried out.

EP 4 The SSP must be stored such that agents required to take action are able to access it at any time.

EP 5 Record of activities addressed in the SSP must be stored such that stakeholders required to access and amend them are able to do so at any time.

22.2.7 Means should be implemented to prevent unauthorized access to autonomous and remotely controlled ships, to ensure the security of the vessel, their cargo, and to prevent the introduction of unauthorized weapons, incendiary devices or explosives.

EP 1 Systems should be sufficient to detect physical intrusion by unauthorized personnel.

EP 2 Systems should be sufficient to detect physical attacks on the ship during its voyage.

EP 3 Systems and processes should be sufficient to detect cyber intrusion or interference.

EP 4 Means should be provided to control access to the ship, as well as the embarkation of persons and their effects.

EP 5 Systems deployed to serve security purposes must themselves be secure, resilient to attempts to compromise them, and exchange information in such a way that it does not compromise the security of the data.

22.2.8 Where responsibilities are transferred from seafarers to remote operators, these personnel shall be considered to be bound by the requirements of the ISPS Code, including but not limited to:

EP 1 Land-based persons shall be required to take part in training drills and exercises as laid out in ISPS Code.

EP 2 Records of the activities laid out ISPS Code, section A/10.1, shall include the involvement of remote operators.

EP 3 When conducting ship security assessments, identification of weaknesses, including human factors, in the infrastructure, policies and procedures shall consider remote operators.