Council of the
European Union

Brussels, 26 March 2024
(OR. en)

8304/24

MAR 58
OMI 40

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	1 March 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2024) 52 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Union submission to the International Maritime Organization's 108th Maritime Safety Committee proposing next steps to enhance maritime cybersecurity

Delegations will find attached document SWD(2024) 52 final.

Encl.: SWD(2024) 52 final

EUROPEAN
COMMISSION

Brussels, 1.3.2024
SWD(2024) 52 final

COMMISSION STAFF WORKING DOCUMENT

Union submission to the International Maritime Organization's 108th Maritime Safety Committee proposing next steps to enhance maritime cybersecurity

Union submission to the International Maritime Organization's 108th Maritime Safety Committee proposing next steps to enhance maritime cybersecurity

PURPOSE

This Staff Working Document contains a draft Union submission to the International Maritime Organization's (IMO) 108th Maritime Safety Committee (MSC 108). The IMO has scheduled MSC 108 from 15 to 24 May 2024.

The draft submission highlights the importance of further cybersecurity measures for ships and port facilities and proposes next steps to enhance maritime cybersecurity. It notably proposes to develop mandatory cybersecurity requirements for ships and port facilities and to establish a working group on the topic at the next session of the Maritime Safety Committee. This submission has been prepared by the United States of America which has reached out to several parties to the IMO, including the European Commission, asking for a possible co-sponsorship.

EU COMPETENCE

Regulation (EC) No 725/2004 on enhancing ship and port facility security[1] and Directive 2005/65/EC on enhancing port security[2] implement the maritime security regime agreed by the IMO in December 2002 in the International Convention for the Safety of Life at Sea (SOLAS) chapter XI/2 and the International Ship and Port Facility Security (ISPS) Code.

Regulation (EC) No 725/2004 also renders some provisions of Part B of the ISPS Code mandatory. Several sections under the ISPS Code are relevant to cybersecurity, notably the requirement to take computer systems and networks into account for both ships and ports facilities: Regulation (EC) No 725/2004, Annex III, paragraphs 8.3.5 and 15.3.5.

Cybersecurity was first horizontally regulated in the EU by Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union[3]. On 16 January 2023, Directive (EU) 2022/2555[4] (known as NIS2) entered into force replacing Directive (EU) 2016/1148. NIS2 Directive strengthens security requirements with a list of focused measures and streamlines incident reporting obligations. It significantly expands the scope of sectors and introduces a size threshold to define which entities fall in its scope, including in the water transport subsector. The EU Member States have until 17 October 2024 to transpose the Directive into their national legislative systems.

On 30 November 2023, a provisional political agreement was reached on the EU Cyber Resilience Act between the co-legislators, the European Parliament and the Council. The Cyber Resilience Act (CRA) mandates that products with digital elements, will only be made available on the market if they meet specific essential cybersecurity requirements. According to the provisional political agreement, the CRA shall not apply to marine equipment that falls within the scope of Directive 2014/90/EU. The CRA's cybersecurity requirements for hardware and software, including components, will significantly contribute to ensuring security of supply chain, including for the maritime sector. The CRA will help organisations defined as essential and important entities under the NIS2 Directive, such as critical infrastructure providers, including in the water transport subsector, meet their supply chain security obligations by providing them with assurance that the products they deploy exhibit a high level of cybersecurity and that their manufacturers will take the provision of security updates throughout their deployment time seriously. Once formally adopted, the CRA will enter into force on the 20th day following its publication in the Official Journal. The transition period agreed by the co-legislators for the CRA cybersecurity essential requirements is of 36 months. The CRA will also be followed by European harmonised standards to be developed by European Standardisation Organisations.

[1] OJ L 129, 29.4.2004, p. 6
[2] OJ L 310, 25.11.2005, p. 28
[3] OJ L 194, 19.7.2016, p. 1
[4] OJ L 333, 27.12.2022, p. 80

In light of all of the above, the present draft Union submission falls under EU exclusive competence, pursuant to article 3(2) TFEU.[5] This Staff Working Document is presented to establish an EU position on the matter and to transmit the document to the IMO prior to the required deadline of 12 March 2024.

[5] An EU position under Article 218(9) TFEU is to be established in due time should the IMO Maritime Safety Committee eventually be called upon to adopt an act having legal effects as regards the subject matter of the said draft Union submission. The concept of '*acts having legal effects*' includes acts that have legal effects by virtue of the rules of international law governing the body in question. It also includes instruments that do not have a binding effect under international law, but that are '*capable of decisively influencing the content of the legislation adopted by the EU legislature*' (Case C-399/12 Germany v Council (OIV), ECLI:EU:C:2014:2258, paragraphs 61-64). The present submission, however, does not produce legal effects and thus the procedure for Article 218(9) TFEU is not applied.

MARITIME SAFETY COMMITTEE
108th session
Agenda item 6

MSC 108/6/x
12 March 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 Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands (Kingdom of the), Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the European Commission[6], acting jointly in the interest of the European Union

SUMMARY

Executive summary:	This document discusses the importance of further cybersecurity measures for ships and port facilities and proposes next steps to enhance maritime cybersecurity.
Strategic direction, if applicable:	2
Output:	2.8
Action to be taken:	Paragraph 16
Related documents:	MSC-MEPC.1/Circ.5/Rev.5; MSC 107/20 paragraph 17.26-17.28; MSC 108/6; MSC-FAL.1/Circ.3/Rev.2; resolution A.1110(3); resolution MSC.428(98); MSC.1/Circ.1526; MSC-MEPC.7/Circ.1; MSC 107/17/9; MSC 107/INF.11; MSC 107/INF.17; MSC 107/17/28; MSC 104/7/1; FAL 48/5/5; and FAL 46/23/2

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".

2 This document aims to identify the next steps to enhance maritime cybersecurity.

Background

3 As highlighted by document MSC 107/17/9 (Australia et al.) along with MSC 107/17/28 (IAPH), MSC 107/INF.11 (Republic of Korea), and MSC 107/INF.17 (Brazil) the

[6] United States of America has drafted this submission and enquired several parties to the IMO, including the European Commission, if there is interest in being co-sponsors.

maritime industry has an urgent need for enhanced cybersecurity measures to protect commercial ship and port facility operations from increased cyber threats and risks.

4 As a co-sponsor for [MSC 108/6 (Australia et al.)], which provides an update to the guidelines for cyber risk management, we greatly appreciate all the work that was done to revise the guidelines on cyber risk management, 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 United States [and co-sponsors] are of the view that mandatory cybersecurity requirements 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 cyber threats.

Discussion

7 The rapid advancement in technology, including digitalization, autonomous, and remote-control technologies, 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.

8 These innovations and technologies, while beneficial, also introduce increased vulnerabilities in the marine transportation system. This includes the increasing threat of cyber attacks by terrorist organizations and cyber criminals.

9 Converging information technology and operational technology systems, combined with hardware and software onboard which is often outdated increases a ship's susceptibility to viruses. Additionally, a lack of visibility over vast and complex networks, and a lack of crew cyber training, hygiene, and awareness leave innumerable entry points for cyber criminals.

10 These vulnerabilities are becoming increasingly problematic due to increased incentives to target the maritime sector. Cyber incidents 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 foreseeable effects of a cyber incident. The opportunity for global disruption through an easy, simple access point makes the maritime domain the perfect target.

11 While the main focus at IMO to date has been on ship cyber risk management, port facilities are also at risk of cyber incidents. 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 cyber incident on a port facility or multiple port facilities may have an exponentially greater crippling effect on the marine transportation system and supply chain resiliency. Therefore, port cyber risk management is as critical as ship cyber risk management.

12 Member states have recognised 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, they may create unclear expectations for ships and seafarers sailing internationally.

13 In its crucial role as the primary international forum for addressing technical matters of all kinds impacting global shipping, the IMO should proactively lead efforts to establish unified and mandatory cybersecurity requirements for ships and port facilities. 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 cyber threats.

[14 Such 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.][7]

Proposal

15 The co-sponsors invite the Committee to:

.1 agree to develop mandatory cybersecurity requirements for ships and port facilities;

.2 encourage interested delegations to submit proposals to the next session of MSC; and

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

Action

16 The Committee is invited to consider the information provided in paragraphs 7 to 14 and the proposal in paragraph 15, and take action, as appropriate.

[7] Subject to the approval by the United States of America.