Council of the European Union

Brussels, 5 February 2026
(OR. en)

6080/26

MAR 19
OMI 5
DIGIT 34
FRONT 28
MIGR 37
RELEX 164

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2026) 31 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Union submission to the 50th session of the International Maritime Organization's Facilitation Committee proposing a new output to develop a non-mandatory maritime cyber code

Delegations will find attached document SWD(2026) 31 final.

Encl.: SWD(2026) 31 final

EUROPEAN
COMMISSION

Brussels, 4.2.2026
SWD(2026) 31 final

COMMISSION STAFF WORKING DOCUMENT

Union submission to the 50th session of the International Maritime Organization's Facilitation Committee proposing a new output to develop a non-mandatory maritime cyber code

Union submission to the 50th session of the International Maritime Organization's Facilitation Committee proposing a new output to develop a non-mandatory maritime cyber code

PURPOSE

This Staff Working Document contains a draft Union submission to the International Maritime Organization's (IMO) 50th session of the Facilitation Committee (FAL 50). The IMO has indicatively scheduled FAL 50 from 23 to 27 March 2026.

The draft submission proposes a new output to develop a non-mandatory maritime cyber code. The co-sponsors build on work to date and discussions at previous MSC meetings. Noting the urgency of this matter, the co-sponsors have worked together to propose a new output on development of a goal-based, non-mandatory Maritime Cyber Code to be under the remit of the FAL Committee.

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 (NIS Directive)[3]. On 16 January 2023, Directive (EU) 2022/2555[4] (known as NIS2) entered into force replacing Directive (EU) 2016/1148 with effect from 18 October 2024. The NIS2 Directive strengthens security requirements with a list of focused cybersecurity risk-management 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. As threats to the security of network and information systems can have different origins, the NIS2 Directive prescribes that cybersecurity risk-management measures are based on an all-hazard approach, which aims to protect network and information systems and their physical environment from any event, including from system failures, human error, malicious acts or natural phenomena.

Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)[5] mandates that products with digital elements, will only be made available on the market if they meet specific essential cybersecurity requirements. 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. The CRA will also be followed by European harmonised standards to be developed by European Standardisation

[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
[5] OJ L, 2024/2847, 20.11.2024

Organisations.

In light of all of the above, the present draft Union submission falls under EU exclusive competence, pursuant to article 3(2) TFEU.[6] The non-mandatory maritime cyber code should be developed in full coherence with the existing EU legal framework on cybersecurity.

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 19 December 2025.

[6] An EU position under Article 218(9) TFEU is to be established in due time should the IMO Facilitation 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.

FACILITATION COMMITTEE
50th session
Agenda item XX

FAL 50/X
19 December 2025
Original: ENGLISH

Pre-session public release: ☒

WORK PROGRAMME

Proposal for a new output to develop non-mandatory maritime cyber code

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, acting jointly in the interest of the European Union

SUMMARY

Executive summary:	This document proposes a new output for the development of a non-mandatory maritime cyber code.
Strategic direction, if applicable:	2, 5, 7
Output:	Not applicable
Action to be taken:	Paragraph 42
Related documents:	FAL 49/22; FAL 49/22/Add.1; MSC.428(98); MSC.1/Circ.1639; MSC 109/22; MSC-FAL.1/Circ.3/Rev.; MSC 110/21; MSC 110/WP.10; MSC 110/7; MSC 110/7/1, MSC 110/7/2 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); MSCFAL.1/Circ.3/Rev.3; MSC.1/Circ.1526 and MSC-MEPC.7/Circ.1

Introduction

1 This document, is submitted in accordance with paragraph 4.6 of the *Organization and method of work of the Facilitation Committee* (FAL.8/Circ.1).

Background

2 The maritime sector has continued to evolve, adopting a range of new technologies and communications methods to support the movement of cargo and people through the global supply chains. The adoption of these advanced technologies and communication methods gives rise to new security challenges which pose significant risks to the safe operations of the modern maritime sector.

3 Member States and industry acknowledge the importance of cyber resilience and have taken steps to safeguard the sector from current and emerging threats and vulnerabilities

related to digitalization, integration and automation of processes and systems used across the sector. However, there is a lack of consistency in the how these issues are approached. It is important that the global community have an agreed framework supported by provisions and guidance that facilitates protecting against and preventing current and future risks.

4 The IMO has taken a number of steps to address this through; MSC-FAL.1/Circ.3/Rev.3 on *Guidelines on Maritime Cyber Risk Management,* resolution MSC.428(98); *Maritime Cyber Risk Management in Safety Management Systems*, IMO Guidelines for setting up a maritime single window (FAL.5/Circ.42/Rev.4); and initiatives such as the MASS Code and the digitalization strategy, both of which contain a cyber component.

5 MSC 109 noted relevant outcomes at FAL 48 and 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 be consistent with relevant horizontal cybersecurity frameworks and standards, such as legislative frameworks setting out cybersecurity requirements for critical infrastructure, related interconnected systems, operators and the digital supply chain. It was also noted that a broad spectrum of cybersecurity experts should be included.

6 MSC 110 established, a Working Group on Cybersecurity and Maritime Security to identify next steps to enhance maritime cyber security. The committee agreed that it should be a goal-based non-mandatory Maritime Cyber Code (the Code).

7 Some Member States have recognized the direction of activity within the global system and have begun to set national frameworks for cybersecurity requirements for port facilities, shipping and the ship to shore interface within their jurisdiction. Developing and adopting an international framework within the IMO with baseline goals can support all nations to work together in alignment.

8 Noting the agreement at MSC 110, not to establish a correspondence group, but recognising urgency of this matter, the co-sponsors have informally worked together to propose a new output on development of a goal-based, non-mandatory Maritime Cyber Code. The co-sponsors believe that the FAL Committee should be the appropriate body for commencing a relevant discussion. However, considering the Committee's remit and relevance to the MSC, a joint working mechanism should be agreed.

9 Building on work to date and discussions at MSC110, the co-sponsors agree that an incremental approach to developing the global approach to maritime cyber security is needed. This should be based on a Maritime Cyber Code being:

.1 goal-based in line with MSC.1/Circ.1394/Rev.2;
.2 non-mandatory, leading to an Experience Building Phase with further work undertaken in the future;
.3 respective of regional and national jurisdictions and authorities;
.4 scalable, being based upon a broader risk assessment which should take into account regional risk assessments and the risk appetite of individual operators informed by their size and complexity;
.5 inclusive of the scope of ports, shipping and ship to shore interface; and
.6 reflective of other work taking place across IMO as part of wider digitalization strategy work.

10 This paper provides details on the proposed output and requests upon FAL50, supported by MSC, where appropriate.

IMO's Objectives

11 The development of an internationally recognised non-mandatory Maritime Cyber Code covering the Computer Based Systems (CBS) of port facilities, shipping and the ship to shore interface constituting an as yet undefined 'Maritime Digital Ecosystem', aligns with the IMO's mission, vision and strategic direction as set out in the IMO's *Strategic Plan for the Organization for the six-year period 2024-2029* (resolution A.1173(33)).

12 The IMO's mission to promote "safe, secure and environmentally sound, efficient, and sustainable shipping through cooperation.

13 The vision:

.1 IMO will uphold its leadership role as the global regulator of shipping, promote greater recognition of the sector's importance to world trade, and enable the advancement of shipping. In this regard, IMO will address the challenges and opportunities presented by ongoing developments in technology, the protection and preservation of the marine environment, tackling climate change, improving the well-being and competence of seafarers, and strengthening the resilience of the maritime industry and global supply chains.

.2 To achieve this, IMO will focus on the review, development, implementation of, and compliance with, IMO instruments in its pursuit to proactively identify, analyse and address emerging issues. IMO will support Member States in achieving the goals of the 2030 Agenda for Sustainable Development, including through capacity development, taking into account the Organization's Capacity-Building Decade 2021-2030 Strategy.

14 The IMO's strategic directions set out its areas of specific focus for addressing during the period 2024 to 2029. Of these eight area of focus, three would be addressed by the development of a goal-based, non-mandatory Maritime Cyber Code that covers ports, shipping and the ship to shore interface; including: SD 2 (Integrate new, emerging, and advancing technologies in the regulatory framework), SD 5 (Enhance global facilitation, supply chain resilience and security of international trade), SD 7 (Ensure the regulatory effectiveness of international shipping).

15 A globally agreed Code would strengthen the Organization's leadership role in safeguarding international shipping, enhance Member States' and industry's capability to respond to evolving cyber threats, and ensure that digital transformation supports, rather than undermines the safety, security, and sustainability of maritime operations.

Need

16 The maritime sector is experiencing a rapid transformation driven by digitalization, decarbonisation, and the integration of advanced and emerging technologies. While these developments aim to enhance operational efficiency and environmental performance, they also introduce new vulnerabilities. Ports, ships and the ship to shore interfaces are now interlinked through digital platforms, creating complex cyber-physical dependencies. Disruption to any component can result in cascading impacts on safety, supply chain continuity, and international trade flows.[7,8]

[7] United Nations Conference on Trade and Development (UNCTAD). (2025). Review of Maritime Transport 2025

[8] International Maritime Organization (IMO). (2017). Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems

17 Recent industry reporting confirms a marked escalation in the sophistication, speed and organisation of maritime cyber threats that hostile actors employ. In particular, artificial intelligence (AI) enabled tools, credential theft and "hands-on-keyboard" intrusions, that can achieve lateral movement across networked systems rapidly. The widespread exploitation of vulnerabilities in remote access systems and legacy operational technology (OT) further demonstrates the growing capacity of both criminal and other hostile actors to disrupt maritime operations.[9]

18 The risks arising from cyber incidents in the maritime domain are multifaceted. Compromise of navigational, propulsion, or cargo-handling systems can endanger human life, disrupt port operations, and cause significant economic and environmental harm. Increasing cases of GPS jamming, spoofing and data manipulation affect global navigation and logistics. In addition, the 2023 IMO GHG Strategy drives advancement in the reliance on real-time data exchange, automation, and digital monitoring systems. On the other hand, this has expanded the potential attack surface of the maritime sector.[1,10]

19 The maritime workforce, both onboard and ashore, is also facing acute skills shortages amid concurrent digital and green transitions. Effective cyber resilience depends not only on technical systems but on competent, trained personnel, capable of identifying, managing and responding to cyber threats. These missions imply skills, knowledge and competences that must be developed and maintained, in particular to address the shortage in the sector. A coherent international framework supported by national regulatory policy, coordinated industry action, and sustained investment in training and infrastructure can support bridging the skills needs in the maritime sector.

20 In this context, there is a clear and urgent need for the development of a Maritime Cyber Code.

Analysis of the issue

21 The IMO is the recognised entity for addressing issues related to international shipping and the associated infrastructure that facilitates operations, such as port facilities and the ship to shore interface. As such it is the appropriate body to address the need for a consistent approach to cybersecurity

22 As Outlined in MSC 110/7 as part of the work to address next steps to improve Maritime Cybersecurity, there is a desire to agree a new output on the production of the Code.

23 Existing IMO instruments were drafted prior to the proliferation of the digital technologies we see in the sector today; and as such consensus does not exist on where cybersecurity should be addressed within these existing instruments.

24 In developing the Code the IMO is requested to consider essential CBS that support safe operations of port facilities, shipping and ship to shore interface. These should take into account the modern realities of ships and ports being interconnected and interdependent, via logistical systems and services that facilitate maintenance, safety and general operations. The co-sponsors consider the scope of the Code should consider a holistic 'Maritime Digital Ecosystem' that should be discussed as part of a Correspondence Group.

25 The Code needs to cover the range of activities and ambitions the IMO has in ensuring the maritime sector modernises in a clearly understood manner, while ensuring that the scope of a new Code does not become overly complex or burdensome on industry, Member States or the IMO's functions.

[9] Marlink. (2025). Global Maritime Cyber Threat Report H2 2024
[10] Allianz Global Corporate & Specialty. (2025). Safety and Shipping Review 2025

26 As such the Code should cover digital technologies, including CBS that are essential to the operation and management of numerous systems critical to the safety and security of port facilities, shipping and the ship to shore interface. In some cases, these systems are to comply with international standards and the national requirements. However, the vulnerabilities created by accessing, interconnecting or networking with these systems can lead to vulnerabilities and risks which need to be addressed.

27 As defined in MSC-FAL.1/Circ.3/Rev.3 *Computer Based System (CBS)* means a programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBSs include Information Technology and Operational Technology systems. A CBS may also be a combination of subsystems connected via a network. CBSs may be connected directly or via public means of communications.

28 Cyber risks are presented by malicious actions (e.g. hacking or introduction of malware),the unintended consequences of benign careless actions (e.g. software maintenance or user permissions), system failure or any other source. In general, these actions can expose or exploit vulnerabilities (e.g. outdated software or ineffective firewalls) in CBSs. Understanding these systems, their vulnerabilities and the threats posed to them can enable effective cyber risk management.

29 Vulnerabilities can result from inadequacies in design, integration and maintenance of systems, as well as lapses in cyber hygiene. In general, where vulnerabilities in CBSs are exposed or exploited, either directly (e.g. weak passwords or careless password management that enables unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for the confidentiality, integrity and availability of data, as well as implications for the safety and security of a port facility or a ship, particularly where critical systems are compromised.

30 Risk management processes should also consider how threat actors might take advantage of emerging technologies like; MASS, AI or others that affect the CBS, disrupting safe operations of port facilities, shipping or the ship to shore interface.

Analysis of implications

31 As the proposed Code is non-mandatory; there would be no required costs for industry associated with the output. It is anticipated that the Code may reduce the costs and administrative burden through the creation of a clear, common approach to cybersecurity, and standardising the expectations and provisions when interfacing with various external organisation.

32 The output would not place any immediate additional requirements on Member States to act, resulting in no additional administrative or legislative burdens. Once the Code is developed and future intentions are identified a more in-depth analysis of potential future costs should be undertaken.

Benefits

33 The average cost of a cyberattack is roughly US$550,000 in 2023, with an average ransom payment for the release of data being around US$3,200,000. Such costs could potentially increase in the future.[11] For ports the daily financial losses from a cyberattack are

[11] Cyber Owl. 2023. Shifting Tides, Rising Ransoms and Critical Decisions: Progress on maritime cyber risk management maturity

not fully understood. However, given the vital nature of maritime supply chains to the import/export of goods that other industrial sectors are reliant upon, cyberattacks have significant cascading effects that are difficult to properly identify.

34 Having a single Code that supports Member State and Industry understanding of a harmonised framework can help to ensure:

.1 a maritime sector resilient to 21st century risks exposed by the adoption of technologies and processes that have been implemented without consideration for cyber risks;
.2 a maritime sector able to securely adopt new technologies and processes that supports safe and secure operations;
.3 a maritime sector able to take a comprehensive approach to interconnected and interdependent technologies and processes that facilitate maritime operations;
.4 improved safety and security of seafarers and maritime personnel;
.5 improved protection of commercial and personal data essential to modern maritime operations;
.6 greater mitigation of financial losses, by increasing industry's ability to understand and protect itself from cyber incident, respond to an incident more rapidly and restore services quickly following an incident;
.7 improved stability of global trade by ensuring that vessels and their supporting systems are able to respond to threats to new and emerging technology; and
.8 continued movement of both cargo and passengers through the maritime sector, as well as accurate and timely data that support maritime operations.

35 A comprehensive framework leads to reduced costs, the ability to develop improved training and skills retention, enhancing consistency and quality, better internal and external oversight, and the sharing of best practices across industry to achieve common goals.

Industry standards

36 The IMO maintains a list of existing industry and national standards, and guidance on the Maritime Cyber Risk section on its website and encourages the submission of additional resources by IMO members.[12]

37 IMO Circular MSC-FAL.1/Circ.3/Rev.3 *Guidelines on Maritime Cyber Risk Management* includes a non-exhaustive list of standards from its time of publications, from both national and industry bodies.

38 Several industry organisations have developed clear standards that underpin a certain part of the sector. For instance, IACS UR26 and UR27 aim to enhance the cyber resilience of ships. Some Member States have developed national legislation to ensure cyber resilience of port infrastructure. While other Member States leverage the ISPS Code, interpreting select clauses as relevant to cyber systems.

39 The proposed output, does not intend to supersede these existing industry standards, but instead aims to highlight the key outcomes that the global community would expect industry to achieve. The output aims to codify the provisions of many existing standards, while identifying other areas that require consideration or improvement in future, bringing a holistic approach to maritime cybersecurity.

[12] https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx

40 The non-mandatory nature of the proposed output and the subsequent experience building phase will allow for sufficient time for engagement between industry, Member States and the IMO to identify any further improvements to goals, and to address any potential conflicts that may arise.

Output

41 It is requested that the committee:

.1 approves a new work output to prepare a non-mandatory Maritime Cyber Code for approval at FAL52;

.2 invites the Maritime Safety Committee to participate as an associated organ in the development of this Code and consider a joint working mechanism with the MSC that guarantees continuous interaction;

.3 approves the provisional roadmap set out in annex 3;

.4 approves the formation of an Intersessional Correspondance Group to develop the Maritime Cyber Code; and

.5 approves the proposed Terms of Reference for a Correspondence Group to develop the Maritime Cyber Code annex 4.

Human element

42 This proposal has been developed in line with Resolution A.947(23) on the human element vision, principles and goals. It recognizes that maritime cyber security is inseparable from human, organizational and cultural factors influencing safety, security and environmental protection. The proposed IMO Maritime Cyber Code aims to strengthen these dimensions by ensuring that human-centred principles, such as communication, competence, and error management are systematically incorporated into cyber risk prevention and response across ship and shore operations.

43 While existing IMO instruments, including the ISM Code, STCW Convention and MSC-FAL.1/Circ.3, provide references to cyber risk management, they do not establish a structured or mandatory framework for addressing human factors in this context. There is no consistent mechanism to evaluate or mitigate vulnerabilities related to human performance, training, organisational culture or fatigue in cyber incident management. This proposal addresses these gaps by integrating human element considerations as a core component of cyber resilience.

44 A checklist identifying key human element considerations has been completed and attached as annex 3. It demonstrates how the new regulatory framework could embed human factor analysis in cyber risk management, promote effective communication and training, and strengthen safety culture to ensure that digital transformation enhances, rather than undermines, the human contribution to maritime safety and security.

45 If the proposed work output is adopted, it is recommended that HTW Sub-committee be invited when necessary to provide relevant expertise, in particular any associated training requirements.

Urgency

46 The maritime sector faces real threats and challenges to its resilience now. These threats and risks continue to increase so it is important to give clarity and coherence to the sector as soon as practicable.

47 The co-sponsors propose that the output be included in the Committee's biennial agenda with two sessions needed to complete the work.

48 As the proposed work output would be non-mandatory there would be no regulatory obligations required of administrations or the maritime industry. Following the creation of the Code, the proposal would be for the maritime industry to enter into an Experience Building Phase, upon such a time the existing Code should be reviewed and amended, and the Member States of the IMO should again consider whether mandatory implementation is the desire of Member States.

Action required

49 The committee is invited to consider the proposals in paragraph 41 and to take action, as appropriate.

***

Annex 1

Checklist for Identifying Administrative Requirements

This checklist should be used when preparing the analysis of implications required in submissions of proposals for inclusion of outputs. For the purpose of this analysis, the term "administrative requirement" is defined in accordance with resolution A.1043(27), as an obligation arising from a mandatory IMO instrument to provide or retain information or data.

Instructions:

(A) If the answer to any of the questions below is **YES**, the Member State proposing an output should provide supporting details on whether the requirements are likely to involve start-up and/or ongoing costs. The Member State should also give a brief description of the requirement and, if possible, provide recommendations for further work, e.g. would it be possible to combine the activity with an existing requirement?

(B) If the proposal for the output does not contain such an activity, answer **NR** (Not required).

(C) For any administrative requirement, full consideration should be given to electronic means of fulfilling the requirement in order to alleviate administrative burdens.

1. Notification and reporting? Reporting certain events before or after the event has taken place, e.g. notification of voyage, statistical reporting for IMO Members	**NR** ☑	Yes □ Start-up □ Ongoing
Description of administrative requirement(s) and method of fulfilling it: (if the answer is yes)		
2. Record keeping? Keeping statutory documents up to date, e.g. records of accidents, records of cargo, records of inspections, records of education	**NR** ☑	Yes □ Start-up □ Ongoing
Description of administrative requirement(s) and method of fulfilling it: (if the answer is yes)		
3. Publication and documentation? Producing documents for third parties, e.g. warning signs, registration displays, publication of results of testing	**NR** ☑	Yes □ Start-up □ Ongoing
Description of administrative requirement(s) and method of fulfilling it: (if the answer is yes)		
4. Permits or applications? Applying for and maintaining permission to operate, e.g. certificates, classification society costs	**NR** ☑	Yes □ Start-up □ Ongoing
Description of administrative requirement(s) and method of fulfilling it: (if the answer is yes)		
5. Other identified requirements?	**NR** ☑	Yes □ Start-up □ Ongoing
Description of administrative requirement(s) and method of fulfilling it: (if the answer is yes)		

Annex 2

Checklist for Considering the Human Element

	1 Question	2 Yes/ No	3 IMO References	4 Considerations	5 Instructions
Workload			*Other relevant references may be added* *Strike out references that are not relevant*	*If answer to question is "yes" identify considerations. If answer is "no" make proper justification*	*Identify how human element considerations should be addressed in the output*
1	**Does the "output" affect workload?**				
1.1	**On board, especially in the already intensive phases of the voyage and port operations to:**	**Yes**	*Revised guidelines for the operational implementation of the International Safety Management (ISM) Code by Companies* (MSC-MEPC.7/Circ.8) *Guidelines on fatigue* (MSC.1/Circ.1598) *Principles of minimum safe manning* (Resolution A.1047(27)) *Guidelines for the investigation of accidents where fatigue may have been an issue* (MSC/Circ.621)	Additional cyber monitoring, reporting and incident response tasks across ship and shore; coordination during cyber events; documentation and audit workload; potential fatigue from alerts.	**Phase-in workload with risk-based prioritisation; schedule windows; streamline forms; define ship/shore roles; include fatigue safeguards.**
1.1.1	Operations including navigation, cargo and engineering	**Yes**		Digital navigation, ECDIS, engine monitoring and cargo	

				systems require continuous cyber vigilance; alarms and patch windows add time pressure.	
1.1.2	Maintenance of the ships structure and its equipment	**Yes**		Software updates and configuration control increase maintenance workload; segregation of duties and verification steps lengthen tasks.	
1.1.3	Onboard administration in support of the ships' management systems	**Yes**		Cyber logs, access reviews and vulnerability reporting expand admin workload and require accuracy under time constraints.	
1.1.4	Onboard administration related to regulation involving flag States, classification societies, port State and other bodies such as charterers and port authorities	**Yes**		Increased submissions (e.g., cyber incidents, attestations) to authorities/charterers; portal use and data validation add admin cycles.	
1.1.5	Increased workload or time pressure on personnel if involved in implementation of changes prior to the implementation date	**Yes**		Pre-implementation tasks (asset inventory, baselining, training, drills) peak workload prior to entry-into-force.	
1.2	**Ashore, in a manner that would affect the ships operation to:**	**Yes**		Additional cyber monitoring, reporting and incident response tasks across ship and shore; coordination during cyber events; documentation and audit workload; potential fatigue from alerts.	
1.2.1	Companies' administration			Company SOC/IT/OT coordination increases workload for shore teams	

				supporting vessels across time zones.	
1.2.2	Flag State, port State and classification societies administration such that certification and other processes are compromised or delayed			Surge in certification/verification cycles may slow approvals; coordination needed to avoid operational delays.	

	1 Question	2 Yes/ No	3 IMO References	4 Considerations	5 Instructions
Decision-making			*Other relevant references may be added* *Strike out references that are not relevant*	*If answer to question is "yes" identify considerations. If answer is "no" make proper justification*	*Identify how human element considerations should be addressed in the output*
2	**Does the "output" impact decision-making on board the ship?**			Cyber disruptions (compromise of integrity/availability/authenticity /confidentiality), multiple guidance sources and automation trust can hinder timely, accurate decisions under pressure.	
2.1	By confusion with existing requirements and regulations	Yes		Overlap between cyber risk procedures and existing safety/ISM processes may confuse prioritization during incidents.	Provide clear decision trees, communication templates, and pre-authorized actions; align with bridge/engine room procedures; train for degraded modes.
2.2	By changing responsibilities as laid out in the ISM Code	Yes		Clarify Master, DPA, CSO, ETO and watchkeeper roles for cyber decisions and authority to degrade/isolated systems.	
2.3	By creating complexity in its implementation and/or in the safety management systems	Yes		Integration into SMS may add layers; ensure simple, actionable checklists and escalation paths.	
2.4	By requiring increased mental effort, such as the need to find, transform and analyse data or result in the need to make	Yes		Incident triage demands data correlation under uncertainty; risk of cognitive overload.	

	judgements based on incomplete information				
2.5	By limiting the time available to establish situational awareness, decide, communicate (possibly across time zones) or check	Yes		Time-critical coordination with shore SOC across time zones; maintain backup comms and pre-authorized actions.	
2.6	By increasing reliance on judgement and administrative controls to manage major risks such as oil spills and collisions	Yes		Fallback to procedural and administrative controls when technical safeguards fail; ensure human-in-the-loop for safety-critical calls.	

	1 Question	2 Yes/ No	3 IMO References	4 Considerations	5 Instructions
Living and Working Environment			*Other relevant references may be added* *Strike out references that are not relevant*	*If answer to question is "yes" identify considerations. If answer is "no" make proper justification*	*Identify how human element considerations should be addressed in the output*
3	**Does the "output" affect the living and working environment?**		*Guidelines on the basic elements of a shipboard occupational health and safety programme* (MSC-MEPC.2/Circ.3) *Guidelines on fatigue* (MSC.1/Circ.1598)	Cyber alarms/drills add cognitive load; ensure alarms and procedures do not conflict with emergency arrangements; manage stress and privacy concerns from monitoring.	
3.1	By interfering with existing arrangements for abandonment, fire-fighting and other emergency plans or procedures	Yes		Cyber procedures must not delay abandon-ship/fire responses; avoid alarm conflicts; prioritize life-saving signals.	Integrate cyber alarms with existing emergency priorities; include stress management, rest policies and privacy notices in procedures.
3.2	By introducing new materials that could create an explosion, fire, environmental or occupational health risk	Yes		No new hazardous materials, but ensure handling of secure storage devices (e-waste) follows OH&S.	
3.3	By introducing new high energy sources such as high-voltage, high pressure fluids	Yes		Primarily informational/IT load; ensure added equipment (servers, UPS) does not introduce unsafe energy sources without safeguards.	

3.4	By affecting access or egress and causing lack of ventilation in working spaces	Yes		IT racks/cabling should not impede access/egress; maintain ventilation for equipment rooms.	
3.5	By affecting the habitability of accommodation spaces due to noise, vibration, temperatures, dust and other contaminants	Yes		Minimize nuisance alarms and screen fatigue; schedule drills to limit sleep disruption.	

	1 Question	2 Yes/ No	3 IMO References	4 Considerations	5 Instructions
Operation and Maintenance			*Other relevant references may be added* *Strike out references that are not relevant*	*If answer to question is "yes" identify considerations. If answer is "no" make proper justification*	*Identify how human element considerations should be addressed in the output*
4.	**Does the "output" affect the operation and maintenance of the ship, its structure or systems and equipment?**		*Revised guidelines for the operational implementation of the International Safety Management (ISM) Code by Companies* (MSC-MEPC.7/Circ.8) *Guidelines for bridge equipment and systems, their arrangement and integration (BES)* (SN.1/Circ.288) *Principles of minimum safe manning* (Resolution A.1047(27)) *Issues to be considered when introducing new technology on board ships* (MSC/Circ.1091) *Guideline on software quality assurance and human-centred design for e-navigation* (MSC.1/Circ.1512)	Cyber controls affect OT/IT operations, requiring new competencies, careful integration, and safe update/maintenance processes.	

			Guidelines for the standardization of user interface design for navigation equipment (MSC.1/Circ.1609)		
4.1	By introducing equipment that the user may find difficult to operate or maintain or may be unreliable			Security appliances and network tools may be complex; risk of misconfiguration impacting operations.	Adopt change management, user-centred HMI reviews, staged rollouts, and competence-based training; validate interfaces and recovery steps.
4.2	By introducing new and/or novel technology, or technology that changes the role of the person			Role shifts (e.g., watchkeepers performing basic cyber checks) and increased reliance on automation.	
4.3	By introducing requirements for new competencies and roles			Competencies in access control, patching, backup/restore, and incident response needed ship/shore.	
4.4	By overloading existing infrastructure such as power generation and ventilation systems			Servers/UPS/network gear add heat/power load; plan capacity and ventilation.	
4.5	By poor integration with existing systems and controls			Ensure cyber measures do not degrade HMI usability (bridge/engine consoles); validate in trials.	
4.6	By introducing new and unfamiliar operations/procedures			New procedures for removable media, remote access, configuration control, and backups.	

4.7	By introducing new and unfamiliar operating interfaces?			New security dashboards/interfaces require training and standardization.	
4.8	By introducing risks to the ship during any modifications required prior to the implementation date of the output			Change windows and testing required; risk of downtime or degraded safety if poorly planned.	

	1 Question	2 Yes/ No	3 IMO References	4 Considerations	5 Instructions
Measures to address the human element			*Other relevant references may be added* *Strike out references that are not relevant*	*If answer to question is "yes" identify considerations. If answer is "no" make proper justification*	*Identify how human element considerations should be addressed in the output*
5.	**Does the "output" require changes to:**		*Shipboard technical operating and maintenance manuals* (MSC.1/Circ.1253) *Revised guidelines for the operational implementation of the International Safety Management (ISM) Code by Companies* (MSC-MEPC.7/Circ.8)	To embed cyber resilience, updates are required across training, procedures, manuals, and shore support.	
5.1	Training	Yes		Role-based cyber awareness and incident response training for shipboard and shore personnel; regular drills.	Amend SMS, manuals and training matrices; schedule drills; define shore support arrangements; maintain version-controlled documentation.
5.2	Practical skill development and competences	Yes		Hands-on skills: backup/restore, isolation, safe patching, log capture, and comms during incidents.	
5.3	Operating, management and/or maintenance procedures	Yes		Integrate cyber steps into bridge/engine room checklists and SMS; clear escalation paths.	

5.4	Information/manuals for operation and maintenance	Yes		Update manuals with asset inventories, diagrams, recovery playbooks, and contact lists.	
5.5	Spares outfit	Yes		Spares for secure storage media, network equipment, and backup devices as appropriate.	
5.6	Occupational safety requirements including guarding and PPE	Yes		Safe handling of IT equipment (e.g., ESD, battery safety) and ergonomic considerations.	
5.7	Shore support	Yes		24/7 shore SOC/IT/OT support to assist Masters/DPAs; clear service levels and contact protocols.	

Annex 3

Proposed Roadmap

The following timetable is being put forward as a possible roadmap for the approval of the Maritime Cyber Code

Year	Committee & Activity	Outcome
2026	FAL 50: Output submission and approval; invite MSC to become an associated organ. Consideration of invitation to form an intersessional correspondence group MSC 111: Consideration of outcome of FAL 50 including invitation to associate on the output Council, 137th session: Endorsement of new output Intersessional Correspondence Group: Hazard identification workshops (see as an example Revision SOLAS chapter III and LSA Code) Report of the Correspondence Group submitted to FAL 51	List of hazards, ranked
2027	FAL 51: Consideration of the Report of the Correspondence Group, additional paper submissions on the topic, establishment of a working group. FAL 51 Working Group: Agreement on document structure, Chapters and associated goals. Begin work on functional requirements. Establish terms of reference for an intersessional correspondence and working group. Intersessional Correspondence Group: Development of functional requirements for outstanding chapters. Begin work on expected performances for functional requirements. Intersessional Working Group: Agreement on functional requirements and expected performances. Preparation of a draft. Report of the Correspondence / Working Group submitted to FAL 52	
2028	FAL 52: Consideration of the Report of the Correspondence Group, additional paper submissions on the topic, establishment of a working group. FAL 52 Working Group: Discussion on the draft non-mandatory Cyber Code. Agreement on finalised version for FAL 52.	

	Invite MSC to approve code. Following MSC: Approval of code.	

Annex 4

DRAFT TERMS OF REFERENCE FOR THE CORRESPONDENCE GROUP ON THE DEVELOPMENT OF NON-MANDATORY MARITIME CYBER CODE

The Correspondence Group, taking into account the comments and decisions made in plenary, and documents FAL 50/XX is instructed to:

.1 develop a roadmap for development of a Maritime Cyber Code;
.2 define the scope of a Maritime Cyber Code, considering a Maritime Digital Ecosystem that incorporates Computer Based Systems that support safe operations of port facilities, shipping and ship to shore interface;
.3 organise and conduct virtual Hazard Identification Workshops;
.4 further develop the text of a goal based, non-mandatory Maritime Cyber Code; and
.5 submit a report for consideration at FAL 51.