`

INTERNATIONAL MARITIME ORGANIZATION

MARITIME SAFETY COMMITTEE
111th session
Agenda item 7

MSC 111/7/1
06 October 2025
Original: ENGLISH
Pre Session Public Release: ☑

PROPOSALS TO THE MARITIME SAFETY COMMITTEE FOR DEVELOPMENT OF A NON-MANDATORY CYBERSECURITY CODE

Submitted by Team: B4, Category: B

Institute: Indian Maritime University (DMET), Kolkata

SUMMARY

Executive summary: This paper summarizes the cybersecurity challenges and opportunities in the maritime sector, emphasizing the need for a non-mandatory, goal-based cybersecurity framework for ships and port facilities. The increasing digitalization of maritime operations has exposed ships and ports to vulnerabilities such as malware, spoofing and ransomware attacks.

The proposed framework advocates for risk-informed, interoperable and scalable measures to strengthen maritime cybersecurity capacity, especially for Role B nations with advanced fleets but limited cybersecurity research capacity. The approach aligns with the NIST Cybersecurity Framework 2.0 and IMO's existing guidelines (MSC-FAL.1/Circ.3/Rev.2), while emphasizing flexibility and capacity building rather than rigid compliance.

Strategic direction, if applicable: *2*

Output: *3*

Action to be taken: *4*

Related documents: *Ref.* MSC 111/7

`

1 CONTEXT AND RATIONALE

Maritime operations are increasingly dependent on digital networks and automation systems. While these advancements enhance operational efficiency, they also introduce complex vulnerabilities that can compromise safety and trade continuity.

The recent rise in global cyber incidents demonstrates that cyber threats are transnational and are capable of disrupting global supply chains through a single weak link. Current IMO cyber risk guidelines (MSC-FAL.1/Circ.3/Rev.2) provide general principles but lack a structured, capacity based compliance model.

Hence, we propose the development of a non-mandatory, goal-based Cybersecurity Code. A framework designed for flexible implementation across diverse Member States while providing a path for gradual capacity building and harmonization of the standards.

2 GUIDING PRINCIPLES OF THE CODE

1. Goal-Based and Risk-Informed Approach: The focus should be on achieving cybersecurity outcomes and not compliance with rigid checklist. Integrating cybersecurity management into Safety Management Systems (SMS) and Port Facility Security Plans (PFSP) under SOLAS and ISPS frameworks should be considered.

2. Harmonization and Interoperability: Alignment with internationally recognized frameworks such as NIST Cybersecurity Framework 2.0 and ISO/IEC 272700. Further ensure its interoperability and consistency with IMO's own cyber guidelines as the final step towards harmonization.

3. Scalable Implementation: Recognize diverse national capacities and allow its progressive adoption. Further, introducing a tier based compliance model adaptable to varying technical and economic capabilities will ensure scalability of the method.

3 PROPOSAL FOR A TIER BASED IMPLEMENTATION FRAMEWORK VIA PILOT PROGRAM

This structure ensures equitable participation, avoids overburdening developing States and encourages leadership roles for Role B nations as pilot implementers.

Tier	Nation Profile	Primary Focus	IMO/Partner Support
Tier 1	High-capacity nations with strong R&D and cyber workforce	Innovation, global best practices	Lead pilot projects, share research and tools
Tier 2	Developed nations with modern fleets but limited cyber R&D (Role B)	Regional leadership, workforce training	Targeted technical assistance, shared intelligence
Tier 3	Developing maritime nations	Foundational infrastructure, awareness	Full support package, extended timelines

The Committee is invited to consider a pilot program using modern fleets from Role B nations to:

- Test and validate cybersecurity procedures and readiness indicators
- Develop standardized implementation templates for future adoption
- Establish a Maritime Cyber Readiness Index (MCRI) for benchmarking progress.

Implementation Phases:

- **Phase I :** Foundation Phase - Self-assessment, cyber hygiene, appointment of Cyber Risk Officers.
- **Phase II :** Integration - ISM linked audits, anonymous reporting, training under STCW.
- **Phase III :** Cooperation - Launch of a Maritime Cyber Readiness Index (MCRI), incentives for high performing operators and mentoring of emerging economies.

`

4 ACTIONS TO BE TAKEN

The Committee is invited to inculcate the following capacity building proposals:

1. Endorse the development of a non-mandatory, goal-based Maritime Cybersecurity Code as a new output under the IMO work program.
2. Approve the establishment of a tiered compliance and capacity building framework as described above.
3. Encourage Member States to participate in pilot programs and contribute to the creation of the Maritime Cyber Readiness Index (MCRI).
4. Facilitate cooperation through the Maritime Cybersecurity Resource Hub (MCRH) and regional centers for cyber excellence and Peer Exchange/ Cyber Shadowing Programs.
5. Form a Collaborative Investment Pool for Digital Infrastucture development.
6. Facilitate a Cyber Resilience Fellowship Scheme to address manpower demands for cyber security infrastructure.
7. Support continued dialogue for eventual transition from a non-mandatory to a goal based mandatory code as global readiness improves.

5 CONCLUSION

Maritime cyber threats evolve continuously with advancing technology, making static regulations ineffective. The proposed goal based Cybersecurity Code offers a dynamic and adaptive framework that evolves alongside emerging risks. Its flexible, tier based structure allows nations to progress at their own pace while maintaining global alignment. Through pilot programs and regular capacity building, it ensures continuous improvement, keeping maritime cybersecurity resilient, relevant and future-ready.