Merchant Marine Circular

Panama Maritime Authority
General Directorate of Merchant Marine
Control and Compliance Department

MERCHANT MARINE CIRCULAR MMC-354

To: Recognized Organizations, ship-owners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime.

Subject: Guidelines on Maritime Cyber Risk Management.

Reference:

a- Resolution No. 106-OMI-15-DGMM of December 13, 2007 (Resolution A. 741(18) of November 4, 1993)

b- MSC-FAL.1-Circ.3-Guidelines on Maritime Cyber Risk Management **(Only as recommendation)**

c- MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems Guidelines on Cyber Security on board Ships (Version 3) ISO/IEC 27001 **(Only as recommendation)**

d- Implementing the NIST Cybersecurity Framework Cyber Security-Code of Practice for Ships Rec. No.127 - A Guide to Risk Assessment in Ship Operations **(Only as recommendation)**

e- Rec.No.166 – Cyber Resilience. **(Only as recommendation)**

---

1. Purpose

1.1 The purpose of this Merchant Marine Circular is to inform that the Facilitation Committee (FAL) and Maritime Safety Committee (MSC) of the International Maritime Organization approved the Guidelines on Maritime Cyber Risk Management thorough MSC-FLA.1/Circ.3 as well as the Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems (SMS) on June 16, 2017 (for both documents visit Maritime Security link, IMO Documents).

2. Introduction

2.1 These Guidelines provide high-level recommendations for maritime cyber risk management. For the purpose of these Guidelines, maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential

circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

2.2 Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

2.3 For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices application of the ISM Code should support and encourage the development of a safety culture in shipping. Success factors for the development of a culture that promotes safety and environmental protection are, inter alia, commitment, values, beliefs, and clarity of the safety management system.

2.4 Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

2.5 Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by the International Maritime Organization on ISM/ISPS Code.

3. Definitions

3.1 Access control: Selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.

3.2 Computer based system: Combination of interacting programmable devices and/or cyber systems organized to achieve one or more specified purposes. Computer based System may be a combination of subsystems connected via network. Onboard computer based System may be connected directly or via public means of communications (e.g. Internet) to ashore based computer based Systems, other vessels' computer based System and/or other facilities

3.3 Contingency Plan: The plan which provides essential information and established procedures to ensure effective response and recovery in case of a cyber- incident affecting computer-based system providing essential contribution.

3.4 Critical System: The technical systems that the sudden operational failure of may result in hazardous situation.

3.5 Cyber-attack: any type of offensive maneuver that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access company and ship systems and data.

3.6 Cyber incident: an occurrence, which actually or potentially results in adverse consequences to an on-board system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

3.7 Cyber resilience: means capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

3.8 Cyber risk management: The process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level by taking into consideration the costs and benefits of actions taken by stakeholders.

3.9 Cyber safety: The condition of being protected against vulnerabilities resulting from inadequate operation, integration, maintenance and design of cyber related systems, and from intentional and unintentional cyber threats.

3.10 Information Technology (IT): Devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).

3.11 Operational Technology (OT): Devices, sensors, software and associated networking that monitor and control onboard systems. In a vessel these systems include devices, sensors, software and associated networking that monitor and control onboard systems, plant and machinery, communications, on and off board sensors and navigation systems.

3.12 OT system: Computer based systems, which provide control, alarm, monitoring, safety or internal communication functions.

3.13 Security Information Event Monitoring (SIEM): Application that provides the ability to gather security data from IT and OT system components and present that data as actionable information via a single interface.

3.14 Service provider: A company or person, who provides and performs software maintenance.

3.15 Virus: A hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.

3.16 Wi-Fi: All short-range communications that use some type of electromagnetic spectrum to send and/ or receive information without wires.

3.17 International Safety Management (ISM) Code: means the International Management Code for the Safe Operation of Ships and for Pollution Prevention as adopted by the International Maritime Organization, as may be amended.

3.18 Company: means the Owner of the ship or any other organization or person such as the Manager, or the Bareboat Charterer, who has assumed the responsibility for operation of the ship from the Shipowner and who on assuming such responsibility has agreed to take over all the duties and responsibility imposed by the ISM Code.

3.19 Safety Management System (SMS): means a structured and documented system enabling Company personnel to implement effectively the Company safety and environmental protection policy.

3.20 Document of Compliance (DOC): means a document issued to a Company which complies with the requirements of the ISM Code.

3.21 Company Security Officer (CSO): means the person designated by the Company for ensuring that a Ship Security Assessment (SSA) is carried out; that a Ship Security Plan (SSP) is developed, submitted for approval, and thereafter implemented and maintained and for liaison with Port Facility Security Officers (PFSO) and the Ship Security Officer (SSO).

3.22 Ship Security Officer (SSO): means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the Ship Security Plan (SSP) and for liaison with the Company Security Officer (CSO) and Port Facility Security Officers (PFSO).

3.23 Port Facility Security Officer (PFSO): means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

3.24 Cyber Security Officer (CySO): is the person or persons tasked to manage and coordinate the cyber security of a ship. For larger fleets the CySO is likely to report to the Company's Chief Information Security Officer (CISO) or CSO, for smaller fleets the role is likely to report to the Company's Head of Security.

3.25 Ship Security Plan (SSP): means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

3.26 Security level: is the qualification of the degree (probability and impact) of risk that a security incident will be attempted or will occur.

3.27 Security level 1: means the level for which minimum appropriate protective security measures shall be maintained at all times.

3.28 Security level 2: means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

3.29 Security level 3: means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

3.30 Security Incident: means any suspicious act or circumstance threatening the security of a ship, including a Mobile Offshore Drilling Unit and a High Speed Craft, or of a Port Facility or of any Ship/Port interface or any Ship to Ship activity.

3.31 Security-sensitive information: Information, the disclosure of which would compromise the security of the ship, including, but not limited to, ship operational data, information contained in any personnel-related file or privileged or confidential information that would compromise any person, system or organization.

3.32 Sensitive Ship Systems: These systems will vary according to the type and function of a ship, but are likely to include:

a) critical systems;

b) systems required for the safety of life and safe operation of the vessel;

c) systems holding personal information; and

d) the VDR.

3.33 Ship: A passenger ship carrying more than 12 passengers or a cargo ship engaged in an international voyage and includes high-speed craft and mobile offshore drilling units (MODUs). Generally, the provisions of the SOLAS Convention apply to cargo ships of, or over, 500 gross tonnage. The Maritime Security Measures apply to passenger ships, as above, and to cargo ships over 500gt.

3.34 Threat: A potential cause of an incident or hazardous situation that may result in harm to an asset, person, system or organization.

3.35 Vulnerability: A weakness (for example, systematic, procedural, physical or technical) of an asset, or group of assets, that can be exploited by one or more threats.

4. Background

4.1 Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

1. Bridge systems;
2. Cargo handling and management systems;
3. Propulsion and machinery management and power control systems;
4. Access control systems;
5. Passenger servicing and management systems;
6. Passenger facing public networks;
7. Administrative and crew welfare systems; and
8. Communication systems.

5. Application

5.1 These Guidelines are primarily intended for all organizations in the shipping industry and are designed to encourage safety and security management practices in the cyberdomain.

5.2 Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

5.3 These Guidelines are recommendatory.

6. Elements of Cyber Risk Management

6.1 For the purpose of these Guidelines, cyber risk management means the process of identifying, analyzing, assessing, and communicating a cyber- related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

6.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

6.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

6.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

6.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential –all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

1. Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
2. Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
3. Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
4. Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
5. Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

7. Best Practices for Implementation of Cyber Risk Management

7.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

7.2 Additional guidance and standards may include, but are not limited to:

1. The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, IINTERMANAGER, NTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL.

2. ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

3. United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

8. MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems (SMS).

8.1 According to this Resolution MSC.428 (98), an approved Safety Management System (SMS) should take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code.

8.2 The objectives of the ISM Code include the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment.

8.3 Cyber risks are appropriately addressed in Safety Management Systems (SMS) no later than the first annual verification of the company's Document of Compliance (DOC annual verification audit) on or after **1 January 2021.**

9. Recommendations:

9.1 This Administration recommends to the all ship-owners and operators to take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance (DOC) after **1 January 2021**.

9.2 This Administration recommends to the company’s current procedures for cyber risk management should be seen as complementary to existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.

9.3 This Administration recommends to all duly authorized Recognized Organizations duly authorized for the verification and certification of the ISM/ISPS Codes, to brings this information and support to ship-owners, operators and interested parties.

Merchant Marine Circular

December, 2023 – *The references were updated and the numbers of paragraphs 3.19 and 3.24 were corrected.*
July, 2020 *- Whole review of the Circular.*
June, 2019*- Including in paragraph 1, 5 and 6 reference to MSC-FAL.1/Circ.3, Resolution MSC.428 (98) and Guidelines on Cyber Security on board Ships (Version 3).*
December, 2018 *– Modification of paragraph 6 and inclusion of the 'Guidelines on Cyber Security on board Ships (Version 3)'.*
August, 2017

Inquiries concerning the subject of this Merchant Marine Circular or any other request should be forward to:

Maritime Ship's Security Department and SEGUMAR Panama
General Directorate of Merchant Marine
Panama Maritime Authority

Phone: (507) 501-5037 / 501-5085
E-mail: isps@amp.gob.pa and segumar.headoffice@segumar.com
Website: https://panamashipregistry.com/circulars/