INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
104th session
Agenda item 7

MSC 104/7/1
2 July 2021
Original: ENGLISH
Pre-session public release: ☒

MEASURES TO ENHANCE MARITIME SECURITY

IAPH Cybersecurity Guidelines for Ports and Port Facilities

Submitted by IAPH

SUMMARY	
Executive summary:	With this document IAPH presents to the Committee the recently finalized first edition of its Cybersecurity Guidelines for Ports and Port Facilities. IAPH calls for the Committee's support towards the promotion and dissemination of these guidelines as appropriate.
Strategic direction, if applicable:	5
Output:	Not applicable
Action to be taken	Paragraph 13
Related documents:	Resolution MSC.428(98); MSC-FAL.1/Circ.3/Rev.1 and Circular Letter No.4204/Add.20

Background

1 With submission MSC 103/9/2, IAPH informed the Committee on its different activities in the field of enhancing cybersecurity in ports and port facilities.

2 Specifically, IAPH informed the Committee on the development of Cybersecurity Guidelines for Ports and Port Facilities, with the intention to submit those for consideration by MSC 104.

3 The same information was submitted to the IMO Facilitation Committee (FAL 45/21/1) with both MSC 103 and FAL 45 noting with appreciation.

4 The mentioned guidelines are now finalized (see annex) by a dedicated IAPH team of experts from ports and port facilities around the globe. The scope and key elements of the IAPH Cybersecurity Guidelines for Ports and Port Facilities[1] are summarized below.

[1] https://bit.ly/IAPHCyberGuide1

Cybersecurity Guidelines for Ports and Port Facilities

5 Ports and port facility stakeholders from around the world are reporting significant increases in cyber-threat activities, particularly since the outbreak of the COVID-19 pandemic. Between February and May of 2020 alone, the maritime industry overall suffered a fourfold increase in cyber-attacks and those attacks against Operational Technology (OT) systems specifically increased by 900 percent since 2017. The risk of a cyber-attack has become the top risk for port authorities and the wider port community.

6 The accelerated pace of digitalization in the port and port facilities community only intensifies the urgency for executives to focus on organizational cyber resilience in order to safeguard the integrity and availability of critical data, ensure service delivery and protect maritime infrastructure. Doing so will increase the overall cybersecurity capabilities of the global maritime supply chain.

7 The IAPH Cybersecurity Guidelines for Ports and Port Facilities are developed to support the global port and port facility community in a manner consistent with IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1). The guidelines are intended for use by the Chief Executive Officer and C-suite executives of ports to recognize the importance of managing cyber risk and to instill an understanding that it is a responsibility that starts at the top of their organization.

8 The guidelines address the need for executives to develop a cyber risk management strategy and plan to achieve and sustain a defense-in-depth posture, provide key insights into the 21st century cyber threat landscape, and include insights into the impacts of cyber-attacks against integrated port systems. Specific considerations address organizational structures, the identification of key stakeholders, reporting mechanisms, data flow and network mapping, characterizations of critical activities that are performed, and the identification and analysis of critical data, systems, assets, and infrastructures.

9 The guidelines further illustrate how executives should consider cyber risk in the context of their own operations. Insights are provided for executives on how to assess risk and vulnerabilities in their port operations and how to adopt a holistic approach that will enable them to organize and manage their cybersecurity program by implementing customized cybersecurity protection, detection, and mitigation measures. Best practices for cybersecurity information sharing, communication and coordination are also provided. General recommendations are provided throughout.

10 Equally important, is the establishment of an organizational cyber awareness to address the human as the pivotal element. Therefore, general and technical training is highlighted for accomplishing the design and implementation of the emergency management plan, which is vital for maritime organizations to respond quickly and effectively to improve the resiliency of port and port facilities, as well as the broader port ecosystem.

11 Since cybersecurity represents a collective responsibility, that it is not solely limited to the IT department, the guidelines demonstrate how cybersecurity capability can drive cyber resilience. It is essential that C-suite port executives take the lead in allocating resources to deal with cyber security, actively managing governance and building an organizational culture to support cybersecurity operations, and developing leadership strategies for driving cyber resilience including the creation of a port ecosystem cybersecurity workforce.

12 Finally, the guidelines provide the designated cybersecurity lead with practical assistance in developing their port and port facility security assessment and plans.

Action requested by the Committee

13 The Committee is invited to take note of the first edition of the IAPH Cybersecurity Guidelines for Ports and Port Facilities, and to consider promoting them as appropriate, including referencing them in the next version of circular the MSC-FAL.1/Circ.3/Rev.1 Guidelines on Maritime Cyber Risk Management under additional detailed guidance and industry standards.

***

ANNEX

The full text of the *IAPH Cybersecurity Guidelines for Ports and Port Facilities Version 1.0* is available at https://bit.ly/IAPHCyberGuide1.