iaph
international association
of ports and harbors

IAPH Data Collaboration Committee brief on Cybersecurity developments and submissions to the IMO

We are glad to share with you the recent cyber security activity related to IMO by the IAPH Data Collaboration Committee

As MSW is mandatory since January 1st, it becomes a critical information infrastructure and as such it is paramount assure the availability of this systems. If they will be compromised by a cyber-attack the port will not be able to operate.

For that reason, At IMO's 48th Facilitation Committee meeting (FAL 48), held 8-12 April, IAPH introduced a submission that called for new output that would require Member States to develop and operate Maritime Single Windows in a cyber-secure and resilient way. IAPH's proposal met with positive response from the floor by sixteen Member States and the Committee agreed that a proposal for a new output should be presented to the next FAL Committee meeting (FAL 49), which will be held in spring next year.

In coordination with IMO secretariat and IAPH cybersecurity expert group, we are currently in the process of preparing the proposal for new output, which will consist of the introduction of a new paragraph to the FAL Convention which requires Member States to introduce a mandatory legal framework aimed at safeguarding the cybersecurity of the MSW.

In addition, as there are countries that don't have any legal framework today for cybersecurity requirements for critical information infrastructure, in our submission to FAL 48 we also recommended to develop a model law on cybersecurity with an explanatory note, which would facilitate governments in need of such a legal framework, to get their Maritime Single Window systems managed and operated in a cyber-secure way.

Because it can't be a model law only for the MSW but for all the critical information infrastructure we are exploring the possibility to cooperate in this project with other

NGO Consultative Status: ECOSOC, ILO, IMO, UNCTAD, UNEP & WCO organizations such as WBG, United Nations Office for Disarmament Affairs (UNODA) and WEF.

IAPH is also co-sponsoring USCG led submission to IMO MSC109 for 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

Another activity of IAPH cybersecurity expert group is the development of the next version of IAPH cybersecurity guidelines for ports that was published at the end of 2021.

We are planning to develop a new guideline that will be focused in two aspects of emerging technologies:

1. How these technologies can help us to improve cybersecurity in ports and
2. Which new challenges these technologies might bring to the ports industry and how to overcome them. This is an important tool to implement "cybersecurity by design".

If as a member of IAPH you wish to join the IAPH Data Collaboration Committee, please contact:

Antonis Michail, Technical Director, IAPH (antonis.michail@iaphworldports.org)