|  |  |
| --- | --- |
| From: ENAV & ARM committees | ENAV26-12.1.2 |
| To: All IALA technical committees | 06 10 2020 |

LIAISON NOTE

Work on Cyber Security within IALA

# INTRODUCTION

Cyber Security is increasingly a topic being discussed within IALA. There have been several input papers with regards to the subject and an IALA Cyber Security workshop is planned for October 2021.

The Policy Advisory Panel (PAP) has decided in February 2020 that Cyber Security activities should be coordinated by the ARM committee. This liaison note aims to provide guidance on the way of handling Cyber Security related subjects and documents within IALA.

# COORDINATION OF WORKSHOP

The ARM committee will coordinate all initiatives regarding Cyber Security, although the subject may be discussed in all committees. The cyber security workshop steering committee will gather topics for the workshop to be held in October 2021 in Quebec, Canada.

The preliminary workshop programme has 3 main topics to be worked on in working groups;

* Risk Management – Topics are standards, human awareness and cyber risk management
* Preventive Technical Measures – Topics are technical measures in the IALA domains VTS, AtoN and Maritime Services
* Incident Response and Recovery – Topics are business continuity incident handling and recovery planning

Expected output on the of the workshop is a guideline on the management of cyber security and a recommendation on cyber security measures.

# ACTION REQUESTED

All IALA technical committees are requested to:

1. Inform ARM working group 2 on the results of work being done on Cyber Security
2. Provide input to the cyber security workshop steering committee regarding any (additional) subjects for the workshop
3. Although the Cyber Security workshop is still a year away, committees should not wait to apply preventive measures where appropriate to enhance cyber security protection in the short term; some standards offering suitable preventive measures for the maritime domain are IEC 62443, IEC 61162-460 and IEC 63154. For IT environments, ISO 27001 and ISO 27002 may be suitable, as well as the NIST cyber security framework. IALA members are encouraged to review these standards and take appropriate action with their digital infrastructures.
4. Committees are invited to provide inputs to ENAV28 and ARM13 of any other pertinent standards which we might have overlooked or are unaware of.