|  |  |
| --- | --- |
| From: VTS Committee | ARM-8.7.2  (VTS50-13.1.2.1) |
| To: ENAV and ARM Committee(s) | 31 March 2021 |

LIAISON NOTE

Response to Work on Cyber Security within IALA

# INTRODUCTION

The VTS Committee welcomes the initiative on getting a broader overview on work being done within IALA on this topic. The workshop to be arranged in Canada in November 2021 will be a good starting point for further work, and also a good arena to portion responsibilities between committees who will create what guidance, as there might be different needs between the different committees on areas that need guidance. There could also be a need for coordination between committees on who should be responsible for different Guidelines.

Therefore the expected output of the workshop should be a *draft* guideline on the management of cyber security and a *draft* recommendation on cyber security measures for the relevant committees to further develop and send to Council for approval.

# RESPONSE TO REQUESTED ACTION

The answer follows the actions and numberings from received input paper VTS50-10.4.1 (ENAV26-12.1.2).

1. Producing Cyber Security Documents for VTS is on hold until after Workshop on Cyber Security.
2. We suggest that a GAP analysis is carried out prior to the Workshop using the principles described in documentation such as IMO Guideline MSC-FAL.1/Circ.3 – 2017 as a reference. The analysis should cover where we are, where to go, how do we know when we arrive, and what committee should be responsible for getting us there. This will set a baseline for where we are in regards of Cyber Security within IALA, and, more significantly, where we need to go.

An additional subject for the WS should also be to consider some metrics to measure progress and procedures to continuously upgrade the need for Cyber Security guidance within IALA committees

1. Noted. Preventive measurements are carried out within the different IALA members already, and many are considering the referenced standards from both IEC and ISO as well as national regulations.
2. Relevant standards and more information could be found in guidance from each national member´s authority for cyber security. It should be noted that VTS might be considered as critical infrastructure for national administrations and should follow national requirements for critical infrastructure.

# ACTION REQUESTED:

1. Secretariat is requested to forward this liaison note response to ARM and ENAV Committees.
2. ARM is requested to consider carrying out or arranging a GAP analysis in advance of the Workshop.
3. ENAV is requested to note the response from VTS.