61ST CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGION

Kuala Lumpur, Malaysia
7 – 11 September 2026

AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION

MALAYSIA'S COMPREHENSIVE APPROACH IN THE IMPLEMENTATION OF MEASURES RELATING TO CYBER THREATS

(Presented by Malaysia)

INFORMATION PAPER

SUMMARY

This Information Paper aims to provide a general overview of Malaysia's comprehensive approach to the implementation of measures relating to cyber threats, through the established legal framework and collaboration between State, Government Agencies and Entities.

MALAYSIA'S COMPREHENSIVE APPROACH IN THE IMPLEMENTATION OF MEASURES RELATING TO CYBER THREATS

1. INTRODUCTION

1.1 Recent trends and developments have shown an increase in awareness and necessity in mitigating the risks relating to cyber threats. Particularly under the SARPs of Annex 17, Malaysia, as a Contracting State, is required to ensure the implementation of measures relating to cyber threats within the context of civil aviation. This is crucial in ensuring the prevention of any rapidly evolving acts of unlawful interference that may jeopardise the safety of passengers, crew, ground personnel and the general public.

1.2 This Information Paper aims to provide a general overview of Malaysia's comprehensive approach through the established legal framework and collaboration between State, Government Agencies and Entities.

2. DISCUSSION

2.1 Brief Overview on Cyber Security Code of Practice and its Legal Framework

2.1.1 Cyber Security Code of Practice (CoP) is a document that establishes cyber security measures, standards and processes for the identified civil aviation entities within the regulatory functions of the Civil Aviation Authority of Malaysia.

2.1.2 CoP is mandatory in nature and a part of a legal framework established by virtue of the Cyber Security Act 2024 [Act 854], regulations under Act 854, directives of the Chief Executive of the National Cyber Security Agency (NACSA) and the National Cyber Security Baseline.

2.1.3 Extensive collaboration has been undertaken between the NACSA, CAAM, subject-matter experts and identified civil aviation entities to ensure that CoP is fit and tailored for civil aviation operations. Under the same framework, CAAM is responsible for monitoring the implementation and compliance with the approved CoP by the identified civil aviation entities.

2.2 Salient Features of the CoP

2.2.1 To ensure the comprehensiveness of the CoP, several crucial elements have been incorporated for compliance purposes. The following is intended to highlight a few salient features of the CoP: -

a) Resources and Facilities

Each identified civil aviation entity is expected to ensure the designation of cybersecurity-related roles and responsibilities within its organisation. Adequate resources and facilities shall be allocated towards capacity building, necessary tools and continuous internal assessments. The allocation of resources and facilities must be reviewed within the organisation to ensure the continuous development of cybersecurity.

b) Cyber Security Assurance

The resources and facilities for security measures allocated within the identified civil aviation entities shall operate effectively. This shall be achieved through the governance of the usage policy for IT infrastructure, regular audits and monitoring, including the resolution of deficiencies and supply chain management.

c) Risk Assessment

Cybersecurity risk assessment shall be conducted by identified civil aviation entities. This process is to support informed decision-making and the management of cybersecurity risks. The assessment is mandatory to be made in line with industry best practices to ensure the consistency of the approach.

d) Operational Efficiency

Identified civil aviation entities shall ensure structured and controlled changes to IT infrastructure. Any changes shall be accounted for and authorised by the designated owners within their organisation.

2.3 **Way Forward**

2.3.1 In-line with the CAAM's role as aviation appropriate authority, CoP is continuously monitored to ensure its implementation by the identified aviation security entities. Additionally, CAAM is working closely with NACSA and other relevant Government Entities in ensuring the rapid identification of threats related to cybersecurity.

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to note the information contained in this Paper.

— END —