60th CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGIONS

Sendai, Japan
28 July - 1 August 2025

AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION

CYBER SECURITY LEGAL FRAMEWORK AND NACSA – CAAM COORDINATION TO ACHIEVE EFFECTIVE IMPLEMENTATION OF MEASURES RELATED TO CYBER THREATS

(Presented by Malaysia)

INFORMATION PAPER

SUMMARY

This paper is intended to provide the Conference with information about the Malaysia aviation cyber security framework under the National Cyber Security Agency (NACSA) and how its implementation assist CAAM as regulatory body for civil aviation to achieve the effective implementation of measures related to cyber threats under Annex 17 ICAO.

CYBER SECURITY LEGAL FRAMEWORK AND NACSA – CAAM COORDINATION TO ACHIEVE EFFECTIVE IMPLEMENTATION OF MEASURES RELATED TO CYBER THREATS

1. INTRODUCTION

1.1 National Cyber-Security Agency (NACSA) is a regulatory body incorporated in Malaysia. It's the national lead agency for cyber security matters, with the objectives of securing and strengthening Malaysia's resilience in facing the threats of cyber-attacks, by co-ordinating and consolidating the nation's best experts and resources in the field of cyber security.

1.2 Civil Aviation Authority of Malaysia (CAAM) is a regulatory body incorporated in Malaysia as an appropriate authority for civil aviation. Its functions under the Civil Aviation Authority Act 2017, inter alia, is to regulate the safety and security of the civil aviation including establishment of standards and their enforcement and to safeguard the civil aviation against any acts of unlawful interference.

1.3 Standard 4.9 of Annex 17 requires the State to ensure that the stakeholders identify critical information related to civil aviation and establish risk-based measures to protect the critical information.

1.4 Cyber Security Act 2024 is an act to enhance the cyber security by providing the establishment of powers and duties of Chief Executive of NACSA, functions and duties of national critical information infrastructure sector leads (NCII Sector Lead) and national critical information infrastructure entity (NCII Entity) and including the management of cyber security. Cyber Security Act 2024 come into force on 26 August 2025.

1.5 In the context of Cyber Security Act 2024, national critical information infrastructure means is defined as critical system that includes information assets (electronic), networks, functions, processes, facilities and services in an information and communications technology (ICT) environment that is important to the country where any disruption or destruction to it can have an impact on national defense and security, national economic stability, national image, the Government's ability to function, public health and safety as well as individual privacy.

1.6 This Information Paper is intended to provide information on the basic legal framework of cyber security and the coordination between NACSA – CAAM for the implementation of Cyber Security Act 2024 and how it assists the State to achieve the effective implementation of measures related to cyber threats under Annex 17 ICAO.

2. DISCUSSION

2.1 Duties and Functions of Chief Executive of NACSA

2.1.1 In exercising the functions under Cyber Security Act, the Chief Executive of NACSA have the power to make the recommendation to the Minister in appointing NCII Sector Lead. More on the NCII Sector Lead is provided under para 2.2.

2.1.2 Chief Executive of NACSA has the authority to issue directives related to cyber security. Currently, the directives issued under power are as per the following: -

a. identify to NCII Sector Lead the NCII Entity's national critical information infrastructure;

b. for the NCII Entity to conduct cyber-security baseline self-assessment;

c. for the NCII to conduct cyber-security risk assessment;

d. for the NCII to report any information related to cyber security to NCII Sector Lead and NACSA.

2.2 **Duties and Functions of NCII Sector Lead**

2.2.1 CAAM, as the national appropriate authority, is the NCII Sector Lead for civil aviation. The main obligation for CAAM as NCII Sector Lead is to designate the stakeholder which owns or operate national critical information infrastructure as NCII Entity.

2.2.2 CAAM in designating NCII Entity, has the obligations to establish of Code of Practice, which is then endorsed by the NACSA and shall have the binding regulatory effects for the NCII Entity. The purpose for Code of Practice to establish clear guidelines and minimum security standards in ensuring that NCII Entity adopt and implement a cyber security framework that aligns with regulatory requirements and industry best practices.

2.2.3 In addition to the NCII Entity designation and establishment of Code of Practice, CAAM also have the following functions under the Cyber Security Act 2024: -

a. monitor the NCII Entity's identification of national critical information infrastructure related to civil aviation;

b. monitor the NCII Entity's cyber-security baseline self-assessment;

c. monitor the cyber-security risk assessment by the NCII Entity, including its regular maintenance; and

d. ensure the implementation of the risk-based measures by the NCII Entity in accordance with the Code of Practice.

2.3 **CONCLUSION**

2.3.1 The Cyber Security Act 2024 is a welcomed addition to the current existing legal framework for civil aviation security in Malaysia. It introduces a more comprehensive source of power and resources for the CAAM, as the Sector Lead for civil aviation in the effort to strengthening the measures related to cyber threats and to increase the effective implementation of the Standard related to cyber-threats under ICAO Annex 17.

2.3.2 The directives issued by the Chief Executive of NACSA specifically relating to the obligation to identify national critical information infrastructure by the NCII Entity, establishment of NCII Entity's cyber-security baseline self-assessment and the risk assessment. Such directives, are in-line with the Annex 17 requirements. In addition, the power of Chief Executive to appoint experts in cyber security to assist with the implementation of Cyber Security Act 2024 ensures the possibilities to get best practices.

3. ACTION BY THE CONFERENCE

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

— END —