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

ENHANCING CYBERSECURITY IN CIVIL AVIATION THROUGH NATIONAL AND INTERNATIONAL COLLABORATION

(Presented by the Republic of Indonesia)

DISCUSSION PAPER

SUMMARY

In compliance with ICAO Annex 17 – Aviation Security, the Directorate General of Civil Aviation (DGCA) Indonesia has developed measures addressing cyber threats, which are incorporated into the National Civil Aviation Security Programme (NCASP). To strengthen the national cybersecurity framework, DGCA Indonesia and the National Cyber and Crypto Agency (BSSN), in collaboration with the Australian Government, conducted a series of cybersecurity initiatives. These initiatives included workshops on regulatory frameworks and a table-top exercise on aviation cybersecurity. The two consecutive workshops aimed to enhance national regulations and guidance, while the table-top exercise was designed to simulate cybersecurity incidents, review existing policies and procedures, identify gaps, and propose improvements.

ENHANCING CYBERSECURITY IN CIVIL AVIATION THROUGH NATIONAL AND INTERNATIONAL COLLABORATION

1. INTRODUCTION

1.1 Aviation is a complex system that relies increasingly on digital technology and information for all aspects of its operations, from supply chains and manufacturing, airport operations and ground systems, maintenance, to air traffic control.

1.2 The interrelationships, dependencies, and complexities within the aviation ecosystem create vulnerabilities that make the aviation ecosystem susceptible to cyberattacks.

1.3 This threat is reflected by the growing number of cyber actors targeting aviation systems with the intention of carrying out malicious intrusions, extracting data, destruction, and disruption.

1.4 To protect aviation operations from cyberattacks, states must take strategic steps in regulation, strengthening of technological infrastructure, strengthening cooperation and exchange of information, strengthening human resources and raising cybersecurity awareness, and ensuring preparedness in facing cyberattacks.

2. DISCUSSION

2.1 In compliance with ICAO Annex 17 – Aviation Security, addressing cyber threats, which are incorporated into the National Civil Aviation Security Programme (NCASP). Operators shall establish and implement protective measures for aviation electronic data and systems that are critical from cyber-attacks in order to maintain confidentiality, integrity, authenticity, accessibility and availability.

2.2 The Indonesian NCASP is currently being revised. Operators will be categorized in the development of cyber protective measures, based on their varying levels of capability in handling cyber incidents. DGCA Indonesia has encouraged operators to establish a Cyber Incident Response Team (CSIRT) registered with the National Cyber and Crypto Agency (BSSN). It is important for each operator to establish a CSIRT responsible for managing cyber incidents, escalating issues to the leadership level, and reporting to DGCA and BSSN. Having a CSIRT is also beneficial as BSSN continues to monitor identified critical infrastructures.

2.3 BSSN through the National CSIRT has provided ISACS (Information Sharing and Analysis Centers) services and the Ministry of Transportation has joined this forum in 2025. Currently, the Directorate of Aviation Security serves as the CSIRT Liaison specifically for the Air Transport sector.

2.4 In the purpose of enhancing cyber security in aviation, DGCA Indonesia collaborate closely with the National Cyber and Crypto Agency (BSSN) to identify of critical electronic systems, measure cybersecurity maturity levels and assess cybersecurity risk.

2.5 To strengthen the national cybersecurity framework, DGCA Indonesia and the National Cyber and Crypto Agency (BSSN), in collaboration with the Australian Government, conducted a series of cybersecurity initiatives. These initiatives included workshops on regulatory frameworks and a table-top exercise on aviation cybersecurity.

2.6 The two consecutive workshops were aimed at enhancing national regulations and guidance in cyber security. The first workshop was conducted to update operators on emerging cyber threats and to gather feedback on the draft revision of the regulation from stakeholders, including airport operators, airlines, air traffic service providers, and ground handling companies. The second workshop

focused on formulating the final regulation and guidance, taking into account the feedback received during the first session.

2.7 Cyber security in aviation table-top exercise (TTx) was carried out with the aim to:

a. assess and strengthen collaborative incident response capabilities of aviation sector stakeholders in Indonesia in the event of a significant cyber incident;
b. evaluate crisis communication, decision-making under pressure, and coordination between government and private agencies;
c. identify gaps in policies, procedures, and capabilities for handling cyber incidents that impact aviation safety and operations; and
d. develop recommendations to improve incident response, crisis management, and future cybersecurity capabilities based on the results of the exercise.

2.8 The TTX on aviation cybersecurity involved stakeholders from the national and airport levels. The outcome of the last activity was that the Indonesian aviation community would be better prepared for potential future cyber crises through cybersecurity incident simulations, reviewing existing policies and procedures, identifying gaps, and finding opportunities for improvement. The table-top exercise covered the phases of detection, mitigation, response and recovery.

2.9 Enhancing cybersecurity in aviation requires a comprehensive, multi-layered, and collaborative approach from both regulators and operators. The aforementioned activities have not only increased the capacity and the capability of the stakeholders to respond to cyber threat, but have also strengthened the relationship between the regulators and the operators in managing the incidents of cybersecurity. These efforts foster coordination in a cyber crisis, and even enable the development of a resilient ecosystem of aviation cybersecurity in Indonesia.

2.10 Continuous collaboration both national and internationally, regular exercises, and information sharing are essential to ensure readiness and adaptability in the face of evolving cyber risks. Indonesia is ready to collaborate with other states to conduct cybersecurity in aviation table-top exercise.

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to:

1) note Indonesia's initiatives and progress contained in this Paper;

2) encourage States to:

   a. share best practices in aviation cybersecurity;

   b. consider collaborating both nationally and internationally to conduct a cybersecurity in aviation tabletop exercise to effectively address the growing cybersecurity threats.

— END —