International Civil Aviation Organization
ICAO South American Regional Office
Eighteenth Meeting of the Civil Aviation Authorities of the SAM Region (RAAC/18)
(Sao Paulo, Brazil, 24- 26 February 2025)

Agenda Item 5A: Effectiveness of plans

Cybersecurity in Civil Aviation and Regional Cooperation in South America

(Presented by Brazil)

SUMMARY

This paper provides a background on how the issue of cybersecurity has evolved and gained importance in international civil aviation, and how ICAO has organized itself to address it. It then presents the vision and organization adopted by Brazil to address the issue, in the context of Brazilian civil aviation, emphasizing that an integrated approach is essential to tackling cyber challenges in the aviation sector.

Action by the RAAC18 is proposed in section 3

***ICAO Strategic Objectives*:**	*A: Safety* *B: Air navigation capacity and efficiency* *C: Aviation security and facilitation*

1. Introduction

1.1 Cybersecurity in civil aviation has evolved significantly over the past decades, becoming an increasingly relevant topic on the global stage. With the rise of digitalization and interconnectivity of aeronautical systems, the threat of cyberattacks has become a critical risk to operational safety, aviation security, operational efficiency, and public trust in the aviation sector. Recognizing the magnitude of these challenges, the International Civil Aviation Organization (ICAO) has been leading efforts to support States and stakeholders in implementing effective cybersecurity measures.

1.2 Among ICAO's initiatives, the works of the Cybersecurity Panel (CYSECP) and the Trust Framework Panel (TFP) stand out, developing strategies, action plan, guidelines and trust framework to strengthen cybersecurity resilience in the sector, while continuing to innovate and grow. In 2019, ICAO published its Aviation Cybersecurity Strategy based on seven pillars addressing the following topics: development of international cooperation; creation of governance practices; creation of effective legislation and regulation; implementation of cybersecurity policy; methodology for information sharing; mechanisms for incident management and emergency planning; and topics for capacity building, training and cybersecurity culture. In 2020, ICAO published the Cybersecurity Action Plan (CyAP), which was updated in 2022, with the purpose of enabling member states and civil aviation stakeholders to work together to develop principles, measures and actions to achieve the objectives of the pillars of the Civil Aviation Cybersecurity Strategy.

1.3 In recent years, working together, ICAO member States and civil aviation stakeholders, through CYSECP Working Groups (Working Group on Cyber Threat and Risk - WGCTR and Working Group on Cybersecurity Guidance Material - WGCGM), manuals have been published on various topics such as policy, culture, and cyber information sharing. The CYSECP plans to expand its activities with a focus on international cooperation and the development of additional guidance materials.

1.4 Brazil, through the National Civil Aviation Agency (ANAC) and the Department of Airspace Control (DECEA) recognizes the strategic importance of cybersecurity in aviation and aligns its actions with ICAO's guidelines. To this goal, they have accompanied and assisted in the implementation of CyAP. ANAC has been actively working to strengthen its regulatory and operational framework to address cyber threats effectively. In the same way, DECEA has many Instructions to guide the airspace control activities and protect it against cyber threats and other malicious activities.

1.5 As a product certification authority, ANAC is also engaged with collaborative efforts in international industry committees, such as: EUROCAE, RTCA and ARAC as well as working closely with other civil aviation authorities such as the FAA, EASA, and Transport Canada, aiming at regulatory harmonization in cybersecurity.

2. Discussion

2.1 To address the challenges in cybersecurity, a series of actions have been carried out, including the development of various governance mechanisms to implement and foster cybersecurity in Brazilian civil aviation, within its responsibilities.

2.2 Internally, ANAC established the Cybersecurity Committee, which acts as a forum for discussing and implementing strategies related to this topic. This committee has continued previous initiatives and promoted significant ones over the past three years, including:

a) Implementation of the Civil Aviation Sector Computer Security Incident Response Team (Aviation Sector CSIRT);

b) Development of the Sectoral Cyber Incident Management Plan for Civil Aviation.

2.3 Publication of Manuals: Development of guidance materials for air operators, airport operators and other regulated entities, such as: Civil Aviation Cybersecurity Awareness Manual, Civil Aviation Cybersecurity Assessment User Manual, Civil Aviation Cybersecurity Information Sharing Manual. All with the collaboration and active participation of civil aviation stakeholders (industry: airlines, airports and associations; and aviation authorities: ANAC and DECEA).

2.4 Working Groups: establishment of specialized groups to address specific cybersecurity issues, such as: management of cyber incident notifications, promotion actions for the regulated sector, development of a sectoral cyber incident management plan.

2.5 Cyber Guardian Exercise: coordination of the civil aviation sector in the simulated cyber incident exercise promoted by the Brazilian Army's Cyber Defense Command, in collaboration with DECEA, other government agencies and industry stakeholders.

2.6 Implementation of CyAP: recognizing the importance of monitoring the evolution of the implementation of the ICAO CyAP by stakeholders, ANAC monitors the actions to be developed, which is a responsibility of the Brazilian State.

2.7 Regulatory Oversight: development and testing mechanisms for continuous oversight of air operators and airport operators, focusing on cybersecurity practices.

2.8 It is important to highlight that currently the Aviation Security and Facilitation *Regional Group (AVSEC/FAL/RG)* deals with cybersecurity aspects. Thus, it is important Members States contribute with participation in the Regional Group not only with AVSEC and Facilitation but also with cybersecurity aspects.

2.9 In the product certification sector, through its involvement in organizations such as ICAO, EUROCAE, RTCA, and ARAC, ANAC contributes to the establishment of harmonized certification criteria, ensuring that aviation products comply with globally recognized safety and performance standards, including cybersecurity. This participation enables Brazil to align its regulatory framework with international best practices, fostering mutual recognition agreements and reducing barriers to certification and validation processes. Some of the standards resulting from this cooperation are: DO-326 Airworthiness Security Process Specification; DO-356 Airworthiness Security Methods and Considerations; DO-355 Information Security Guidance for Continuing Airworthiness; and DO-392 Information Security Event Management. As work in progress, we can list reports for handling data security, ISMS and an FAQ containing instructions on how to use DO-356.

2.10 ANAC also engages in collaborative efforts with other civil aviation authorities to enhance regulatory harmonization in cybersecurity. By working closely with agencies such as the FAA, EASA, and Transport Canada, ANAC ensures that certification requirements are consistent across different jurisdictions, thereby facilitating seamless acceptance of aeronautical products in international markets. These coordinated efforts contribute to a robust and reliable certification ecosystem, ultimately enhancing the safety, security, cybersecurity and operational efficiency of the global aviation sector.

2.11 In Brazilian Airspace Control, DECEA has implemented actions to promote cybersecurity in the systems that support the civil airspace control, like the implementation of a MISP instance to sharing information about malwares and prevent cyberattacks.

2.12 Cybersecurity is a cross-cutting action that transcends borders. Therefore, Brazil emphasizes that an integrated approach is essential to tackling cyber challenges in the aviation sector. Information sharing between States and operators is fundamental to identifying common vulnerabilities/threats and developing effective solutions. In this context, Brazil is willing to share its experience with other countries in the SAM region in order to strengthen cybersecurity in civil aviation in the region.

3. Suggested action

3.1 The Meeting is invited to participate in a joint project focused on cooperation in cybersecurity for civil aviation. With the support of ICAO SAM Office, under the umbrella of the Aviation Security and Facilitation *Regional Group (AVSEC/FAL/RG),* this initiative aims to:

a) Establish a regional network for sharing information about cyber threats, vulnerabilities and incidents;
b) Develop regional guidelines aligned with global best practices;
c) Encourage regional agreements to boost cybersecurity in civil aviation by sharing processes, regulations, and knowledge; and
d) Develop a framework for cybersecurity oversight in civil aviation adapted to the specific characteristics of the region.

- - - - - - - - -

- END -