



ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security – Policy

CURRENT PRACTICES AND IMPROVEMENTS IN CYBERSECURITY FOR
INTERNATIONAL CIVIL AVIATION

(Presented by El Salvador on behalf of the Member States of COCESNA²)

EXECUTIVE SUMMARY

Technology plays a vital role in the aviation sector, facilitating tourism, trade and global connectivity, driving economic growth and improving the quality of life. Advances in avionics have made possible significant improvements in navigation management, the safety of aeroplanes, and operational efficiency. Technological innovation in the sector is essential for maintaining competitiveness and responding to the growing demands of air transport.

Civil aviation cybersecurity has become a cornerstone for guaranteeing safety and air navigation efficiency. Industry is currently facing a dynamic environment with ever-evolving cyber threats, which requires a strategic and coordinated approach to ensure the protection of critical infrastructures.

This working paper presents an analysis of current cybersecurity practices in the aviation sector and proposes key aspects to be considered for their improvement and future implementation with a view to enhancing aviation system resilience to emerging cyber threats.

Action: The Assembly is invited to:

- a) Take note of the information presented;
- b) Request that ICAO assess and enhance cybersecurity strategies, adopting approaches based on international best practices, information exchange and new technologies; and
- c) Request that ICAO continue to support States in establishing and implementing regulatory frameworks for cybersecurity regulation, in training and enhancing staff competencies in this area, and in creating cyber resilience plans that incorporate cybersecurity into the National Aviation Security Plans (NASPs).

*Strategic
Goals:*

*Every Flight is Safe and Secure
No Country Left Behind
The Economic Development of Air Transport Assures the Delivery of Economic
Prosperity and Societal Well-Being for All*

*Financial
implications:*

References:

National Institute of Standards and Technology (NIST) Regulatory Framework

¹ Spanish version provided by El Salvador

² Belize, Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua

	ICAO Doc 9985, <i>Air Traffic Management Security Manual</i> ICAO Doc 10075, <i>Assembly Resolutions in Force (as of 6 October 2016)</i> ICAO Doc 10161, <i>Global Aviation Safety Roadmap</i> Annex 17 – <i>Aviation Security</i>
--	---

1. INTRODUCTION

1.1. Technology plays a vital role in the aviation sector, and technological advances have generated great benefits for air navigation services provision. Systems such as performance-based navigation (PBN), automatic dependent surveillance (ADS-B) and air traffic management (ATM) systems have transformed the way flights are managed, improving accuracy, safety and efficiency. These systems allow for better route planning, the reduction of delays, and airspace optimization.

1.2. Civil aviation cybersecurity has become fundamentally important, as operations depend increasingly on interconnected digital systems in which technological resources are critical for the safe and efficient operation of civil aviation. Technological evolution has brought with it significant challenges, including cyberattacks targeting air traffic control systems, airports and air operators. Thus it is strategic and critical to protect them from cyber threats. The integrity and availability of these systems must be maintained in order to avoid interruptions that may affect operational safety and air transport continuity. Cybersecurity in this context not only protects data and systems, but also shores up trust in the global air navigation infrastructure.

1.3. In response to such threats, States have implemented a variety of cybersecurity measures based on international standards, such as those developed by ICAO, IATA and EASA. However, there are still gaps that need to be addressed to ensure comprehensive protection of the aviation ecosystem.

1.4. This paper has been drafted in keeping with ICAO Assembly Resolution **A39–19**, which constitutes a recognition by the international community that cybersecurity is an urgent priority for civil aviation; Resolution **A40–10** on the ICAO Aviation Cybersecurity Strategy, with its collaborative and multidisciplinary approach; and Resolution **A41–19**, which reaffirms the urgency of addressing cybersecurity and cyber resilience.

2. CURRENT CYBERSECURITY PRACTICES AT COCESNA

2.1 The importance of implementing an ICAO Cybersecurity Framework has been taken into account for identifying, protecting against, detecting, responding to and recovering from cyber incidents. Coordination for the sharing of best practices is underway in and beyond the region with international organizations such as IATA, EUROCONTROL and EASA.

2.2 As for cyber risk management, COCESNA is in the process of laying the foundations for the application of risk analysis methodologies (ISO 27001, NIST, and MITRE ATT&CK). The implementation of these methodologies will allow for continuous assessments of aviation system vulnerabilities and for cybersecurity integration into the air navigation services systems for the Central American region. Similarly, COCESNA intends to establish a Security Operations Center (SOC), permitting the organization to strengthen its security posture through continuous surveillance, advanced threat analysis and rapid incident response. Through this service, we seek to implement a strategic and efficient approach to the protection of systems, data and users, minimizing risks and guaranteeing business continuity and regulatory compliance.

2.3 In the area of training and awareness raising, we are currently developing basic cybersecurity training for all Corporation personnel, and specialized courses will be created to train specific personnel in cybersecurity best practices and trends.

3. ASPECTS TO CONSIDER FOR THE IMPROVEMENT OF CYBERSECURITY IN AVIATION

3.1 Cooperation and information exchange with other air navigation service providers can be established by creating secure platforms for sharing information on threats and vulnerabilities in real time. This can be achieved by strengthening regional collaboration on cybersecurity through multilateral agreements.

3.2 A regulatory framework to regulate cybersecurity should be defined and implemented. Such a framework should provide clear guidelines and standards that organizations can follow to protect their digital assets and safeguard data confidentiality. The implementation of a robust regulatory framework will help to mitigate risks, prevent security incidents and ensure operational continuity.

3.3 Cybersecurity training programs should include technical and practical aspects, such as incident management, risk analysis, and the implementation of protective measures. Additionally, it is important to foster communication and collaboration skills so that staff can work as a team and share knowledge about cybersecurity. Investing in training is a cost-effective strategy that strengthens the organization's resilience to cyber threats.

3.4 Promoting cybersecurity awareness among staff helps reduce human error, which is a leading cause of security incidents. According to studies such as the World Economic Forum *Global Risks Report 2022*, 95% of cybersecurity problems are caused by human error. Threat awareness and cybersecurity best practices help create an organizational culture focused on digital security.

3.5 We should develop a cyber resilience plan that allows cybersecurity to be integrated into National Aviation Security Plans (NASPs). Such a plan will need to include cyberattack recovery strategies to minimize operational impact.

3.6 We must proactively identify and address vulnerabilities to protect technology infrastructure and ensure data security.

3.7 Cooperation with cybersecurity experts from various industries such as technology, banking, and other sectors can give rise to valuable knowledge and specialized resources that enhance protection for aviation systems.

3.8 The adoption of emerging technologies such as artificial intelligence and cloud computing offers opportunities to improve efficiency and safety in civil aviation. However, it is crucial that these technologies be implemented with robust cybersecurity measures to protect against potential vulnerabilities and threats. Secure integration of these technologies could transform the industry but will require careful planning and proper risk management.

4. CONCLUSIONS

4.1 Cybersecurity is a key element of operational safety and efficiency in civil aviation. Protecting aviation systems from cyber threats is essential to ensuring operational safety and air transport continuity. While significant progress has been made in the implementation of protective measures, challenges requiring immediate attention still remain.

4.2 Strengthening international cooperation and information exchange among organizations in the aviation sector through secure platforms and multilateral agreements is vital to improving cybersecurity, while also integrating advanced technologies and adopting proactive approaches to cyber risk management in international civil aviation.

4.3 The implementation of international standards such as ISO/IEC 27001 and NIST CSF will provide clear guidelines for protecting digital assets and ensuring data confidentiality, helping to mitigate risks and prevent incidents.

4.4 Training staff and promoting cybersecurity awareness reduces human error, improving threat response capacity and strengthening organizational resilience.

4.5 In order to protect technology infrastructure, it is crucial to proactively identify and address vulnerabilities through risk assessment, upgrades, penetration testing, and continuous monitoring.

4.6 Collaborating with cybersecurity experts from various industries and contracting specialized services such as SOC and MSSP makes possible continuous monitoring and rapid incident response, ensuring better protection for aviation systems.

4.7 Integrating technologies such as AI and cloud computing with robust cybersecurity measures offers opportunities for improvements in civil aviation safety and efficiency, ensuring the safe and effective adoption of such technologies.

— END —