International Civil Aviation Organization
North American, Central American and Caribbean Office

WORKING PAPER

NACC/WG/10 — WP/33
20/08/25

Tenth North American, Central American and Caribbean Working Group Meeting (NACC/WG/10)
Tulum, Mexico, from 8 to 12 September 2025

Agenda Item 5: NACC/WG Collaborative Task Forces Working Session

CURRENT PRACTICES AND IMPROVEMENTS IN CYBERSECURITY FOR CIVIL AVIATION

(Presented by the Central American Corporation for Air Navigation Services/COCESNA)

EXECUTIVE SUMMARY

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

Cybersecurity in civil aviation has become a fundamental pillar for ensuring operational safety and air navigation efficiency. Currently, the industry faces a dynamic environment with constantly evolving cyber threats, requiring a strategic and coordinated approach to protect critical infrastructure.

This study note presents an analysis of current cybersecurity practices in the aviation sector and proposes key aspects to consider for future improvement and implementation, with the aim of strengthening the resilience of aviation systems to emerging cyber threats.

Action:	Actions suggested in section 6 of the study note.
Strategic Objectives:	• Safety • Air Navigation Capacity and Efficiency • Economic Development of Air Transport • Environmental Protection
References:	• NIST Regulatory Framework • ICAO Documents 9985, 10161, 10075 • ICAO Annex 17

1. Introduction

1.1 Technology plays a vital role in the aviation sector, and the provision of air navigation services has benefited greatly from technological advances. 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 enable better route planning, reduced delays and optimised airspace.

1.2 Cybersecurity in civil aviation has become a fundamental issue, as operations increasingly depend on interconnected digital systems, where technological resources are critical for the safe and efficient operation of civil aviation. Technological developments have brought significant challenges, including cyber-attacks targeting air traffic control systems, airports and air operators, making it strategic and essential to protect them from cyber threats. The integrity and availability of these systems must be guaranteed to avoid disruptions that could affect operational safety and the continuity of air transport. Cybersecurity in this context not only protects data and systems but also ensures confidence in the global air navigation infrastructure.

1.3 In response to these 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 note is developed in line with resolutions: A39-19 of the ICAO Assembly, which recognises that cybersecurity is an urgent priority for civil aviation on the part of the international community, resolution A40-10 on the ICAO Aviation Cybersecurity Strategy with a 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 Implementation of a Regulatory Framework through the application of ICAO Circular 350 on cybersecurity in aviation. The importance of implementing an ICAO Cybersecurity Framework for the identification, protection, detection, response and recovery from cyber incidents has been taken into account. Likewise, coordination has taken place with international organisations within and outside the region, such as IATA, EUROCONTROL and EASA, to share best practices.

2.2 For cyber risk management, COCESNA is in the process of establishing the basis for the application of risk analysis methodologies (ISO 27001, NIST, MITRE ATT&CK). These implementations will enable us to carry out continuous assessments of vulnerabilities in aeronautical systems and integrate cybersecurity into the systems that provide air navigation services in the Central American region.

2.3 COCESNA intends to implement a SOC – Security Operations Centre (SOC), which will enable the organisation to strengthen its security posture through continuous monitoring, advanced threat analysis and rapid incident response. This service seeks to implement a strategic and efficient approach to protecting systems, data, and users, minimising risks and ensuring business continuity and regulatory compliance.

2.4 In the area of training and awareness, basic cybersecurity training is currently being developed to be provided to all Corporation staff, and training will also be developed to specialise specific personnel in cybersecurity best practices and trends.

3. Aspects to consider for improving cybersecurity in aviation

3.1 Cooperation and information exchange with other air navigation service providers through the creation of 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 Define and implement a regulatory framework governing cybersecurity. This framework should provide clear guidelines and standards that organisations can follow to protect their digital assets and safeguard data confidentiality. Implementing a robust regulatory framework helps mitigate risks, prevent security incidents and ensure operational continuity.

3.3 Cybersecurity training programmes should include technical and practical aspects, such as incident management, risk analysis and the implementation of protective measures. It is also 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 organisation's resilience to cyber threats.

3.4 Promoting cybersecurity awareness among staff reduces human error, which is one of the main causes of security incidents. According to studies such as “The Global Risks Report 2022” from the World Economic Forum's indicates that 95% of cybersecurity problems originate from human error. Raising awareness about threats and cybersecurity best practices helps create an organisational culture focused on digital security.

3.5 Develop a cyber resilience plan that allows us to incorporate cybersecurity into National Aviation Security Plans (NASPs). This should include cyber-attack recovery strategies to minimise operational impact.

3.6 Proactively identify and address these vulnerabilities to protect technological infrastructure and ensure data security.

3.7 Cooperation with cybersecurity experts from various industries, such as technology, banking and other sectors, can provide valuable insights and specialised resources that improve the protection of 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 are implemented with robust cybersecurity measures to protect against potential vulnerabilities and threats. The secure integration of these technologies can transform the sector but requires careful planning and appropriate risk management.

4. Conclusions

4.1 Cybersecurity is a key element for operational safety and efficiency in civil aviation. Protecting these systems from cyber threats is essential to ensure operational safety and the continuity of air transport. While significant progress has been made in implementing protective measures, there are still challenges that require immediate attention.

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

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

4.4 Training staff and promoting awareness of cybersecurity reduces human error, improving the ability to respond to threats and strengthening organisational resilience.

4.5 Proactively identifying and addressing vulnerabilities through risk assessment, updates, penetration testing and continuous monitoring is crucial to protecting technological infrastructure.

4.6 Collaborating with cybersecurity experts from various industries and contracting specialised services such as SOC and MSSP provides continuous monitoring and rapid incident response, improving the protection of aeronautical systems.

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

5. Recommendations

5.1 It is recommended that the proposal to strengthen cybersecurity in civil aviation be submitted for consideration by the various ICAO working groups, based on:

- Evaluating and strengthening cybersecurity strategies by adopting approaches based on international best practices, information sharing, and new technologies.
- Implementing a robust regulatory framework governing cybersecurity, providing clear guidelines and standards that organisations can follow to protect their digital assets and safeguard data confidentiality.
- Promoting cooperation and information sharing.
- Collaborating with cybersecurity experts from various industries and contracting specialised services such as SOC and MSSP to provide continuous monitoring and rapid incident response.
- Integrating emerging technologies such as artificial intelligence and cloud computing with robust cybersecurity measures to improve efficiency and safety in civil aviation.

6. Suggested actions

6.1 The Meeting is invited to:

a) Take note of the information presented
b) Request that ICAO, within the framework of the relevant regional working groups, evaluate and strengthen cybersecurity strategies, adopting approaches based on international best practices, information exchange and new technologies
c) ICAO, within the framework of the relevant regional working groups, to continue to support states in defining and implementing regulatory frameworks for cybersecurity, as well as in training and strengthening staff competencies in this area and in creating cyber resilience plans that incorporate cybersecurity into National Aviation Security Plans (NASPs).

— END —

— — — — — — — — — — —

or

— END —