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

WORKING PAPER

NACC/WG/10 — WP/24
01/09/25

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

Cybersecurity in Air Navigation Services

(Presented by the Secretariat)

EXECUTIVE SUMMARY

ICAO has recognized cybersecurity as an essential pillar to ensure the operational safety and continuity of air navigation services, especially in the face of the increasing digitalization and interconnection of ATS systems, airports and aircraft. AN-Conf/14 of 2024 highlighted that cyberattacks are a constant and evolving threat, requiring States to implement risk management mechanisms, recovery plans, specialized training, and robust regulatory frameworks, aligned with the ICAO Cybersecurity Strategy (2019) and the Global Aviation Security Plan (GASeP).

As a regional response, the NACC Office launched the NACC-2 pilot project in 2025, which includes the development of a Cybersecurity Assistance Plan in Trinidad and Tobago and COCESNA, with the aim of expanding it to other Caribbean States. The project seeks to strengthen the resilience of ANS systems through a multidisciplinary approach involving ATCO, ATSEP, ANSPs, airlines and manufacturers, promoting international cooperation. In conclusion, cybersecurity is key to protecting aviation from digital threats, ensuring public trust, and complying with ICAO global standards.

Action:	Suggested actions under item 4 of this working paper
Strategic Objectives:	• Safety • Air Navigation Capacity and Efficiency • Economic Development of Air Transport • Environmental Protection
References:	• NACC/WG/09 • The fourteenth AN-Conf/14 air navigation conference

1. Introduction

1.1 The increasing digitalization and connectivity of air navigation systems, airports and aircraft has increased the sector's exposure to cyber risks. ICAO recognizes cybersecurity as an essential pillar to ensure operational security, business continuity and public trust. Strategic documents such as the ICAO Cybersecurity Strategy (2019) and the Global Aviation Security Plan (GASeP), guide States and industry in the adoption of prevention, detection, response and recovery measures against cyber incidents.

1.2 At AN-Conf/14 of 2024, ICAO underlined that cybersecurity is an essential component of operational security, especially in the face of the increasing hyper-connectivity of air navigation systems. Several working papers, such as WP-125 submitted by LACAC States, highlighted the need to establish cyber risk management mechanisms, develop recovery procedures, and define specific competencies to deal with incidents affecting air traffic systems (ATS). The conference also recognized that cyberattacks are an ongoing threat that requires a global and coordinated approach, aligned with ICAO's cybersecurity strategy.

1.3 The debate was marked by discussion of the roles of different professionals in the face of cyber incidents: while some argued that air traffic controllers (ATCOs) should be prepared to respond, the International Federation of Technical Personnel (IFATSEA) emphasized that the immediate technical responsibility lies with electronic systems specialists (ATSEPs). In conclusion, the conference reinforced that cybersecurity must be addressed in a multidisciplinary manner, strengthening staff training, clarifying responsibilities and promoting international cooperation to ensure the resilience of air navigation systems.

2. Analysis

2.1 The following items that affect air navigation services in terms of cybersecurity are identified:

- Threats: denial-of-service (DDoS) attacks on air traffic management systems, manipulation of navigation data, malware in airport networks and vulnerabilities in the supply chain.
- Impact: Interruption of ANS/ATM services, loss of critical data and degradation of operational safety.
- Regulatory gaps: fragmentation in regulatory frameworks; not all States have developed specific aviation cybersecurity standards.
- Collaboration: ICAO promotes a coordinated and interoperable approach between States, NPAs, airlines and manufacturers.

3. ICAO Activity Summary – Assistance Plan

3.1 In 2025, the ICAO Talent Mobility Program included the NACC-2 allocation "Development of a Cybersecurity Assistance Plan for the States of the NACC Region". This initiative contemplates:

- Preparation of a State Cybersecurity Assistance Plan following the ICAO global guide.
- Cybersecurity analysis applied to air navigation services (SLA).
    - Evaluation in two Caribbean States through field missions.
    - Delivery of a technical report with findings and recommendations.
- The pilot project responds to express requests from Caribbean States, which have modernized their ANS systems, but still lack robust cyber protection mechanisms.

3.2 The Office will carry out this pilot project in the State of Trinidad and Tobago and in the COCESNA Organization. The results of this pilot project drive a much larger project covering the other CAR States.

3.3 It is also important to have the support of the States that are already working on the issue and that support this type of innovative projects in the region.

4. Recommendations

4.1 It is recommended that air navigation providers work hard to ensure:

- Integrate cybersecurity into National Civil Aviation Security Programmes.
- Apply cyber risk management methodologies in critical systems.
- Strengthen training and simulations for ANS/ATM personnel.
- Implement monitoring and technical redundancies (e.g. GNSS/ADS-B authentication).

4.2 Promote international cooperation in regional forums (NACC/WG, GREPECAS).

5. Conclusion

5.1 Cybersecurity in aviation requires robust regulatory frameworks, resilient technical measures, and strengthening of the human factor. Threats are persistent and evolving, requiring a proactive and coordinated approach.

5.2 Cybersecurity in air navigation services is essential because it protects operational safety, ensures continuity of service and preserves public confidence in aviation. Air traffic management, communications, navigation, and surveillance systems rely on digital networks vulnerable to attacks that can disrupt critical data, disrupt operations, and create direct risks to flight safety.

5.3 In addition, cyber threats are intentional, dynamic and constantly evolving, requiring ongoing vigilance, international cooperation and compliance with ICAO standards. Integrating cybersecurity into national programs not only strengthens the resilience of air navigation services but also ensures that States and providers comply with global standards, avoiding serious technical, economic, and reputational consequences.

6. Suggested actions

6.1 The meeting is invited:

a) Work with their national organizations to develop a National Aviation Cybersecurity Plan.
b) Carry out periodic vulnerability assessments at CNS/ATM and airports.
c) Establish a Regional Cybersecurity Coordination Centre.
d) To implement awareness and training programs at all levels.
e) MCAAP members request the application for funds for the development of the project that covers this need.
f) Include cyber-incident exercises in contingency plans.
g) (g) Strengthen international cooperation to share alerts and lessons learned.
h) Assign contact personnel to work in this area.

— END —