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

WORKING PAPER

NACC/DCA/11 — WP/04
06/06/23

Eleventh North American, Central American and Caribbean Directors of Civil Aviation Meeting (NACC/DCA/11)

Varadero, Cuba, 28-30 June 2023

Agenda Item 5: NAM/CAR Regional Aviation Security/Facilitation Implementation

ASSISTANCE ON CYBERSECURITY MATTERS

(Presented by the Secretariat)

EXECUTIVE SUMMARY

Cybersecurity involves mainly two main areas of expertise: aviation security (AVSEC) and Air Navigation Services (ANS). This paper presents cybersecurity activities in which ICAO has been involved and provides an overview of future developments.

Action:	Suggested actions are presented in Section 5.
Strategic Objectives:	• Strategic Objective 1 – Safety • Strategic Objective 2 – Air Navigation Capacity and Efficiency • Strategic Objective 3 – Security & Facilitation
References:	• Annex 17 – Aviation Security (22nd Edition) Amendment 18 • Aviation Cybersecurity Strategy (October 2019) • Cybersecurity Action Plan (January 2022) • ICAO Aviation Security Manual (Doc 8973) • Air Traffic Management Security Manual (Doc 9985)

1. Introduction

1.1 Aviation is a sector characterized by its extensive interconnectivity and, like most of the leading-edge sectors, has been profoundly affected by technological development. The deployment of digital infrastructure is allowing global interconnectivity of civil aviation systems and networks which redound in efficiency and capacity and in steady growth.

1.2 However, these digital advances expose the sector to cybersecurity threats across all stakeholders, where a successful cyber-attack might have negative impacts on financials, reputations, continuity of services, and even on the safety and security of people and facilities.

1.3 Aware of these threats, ICAO has been aligning efforts and fostering international cooperation to address aviation cybersecurity comprehensively, ensuring the participation of States and all concerned stakeholders.

1.4 The ICAO Assembly further highlighted the importance of addressing cybersecurity in civil aviation. Being ICAO's work programme shaped by ICAO Assembly resolutions, three of them refer precisely to cybersecurity:

- Resolution A39-19 – Addressing Cybersecurity in Civil Aviation, 2016;
- Resolution A40-10 – Addressing Cybersecurity in Civil Aviation, 2019 (superseding A39-19); and
- Resolution A41-19 – Addressing Cybersecurity in Civil Aviation, 2022.

2. Cybersecurity developments at ICAO Headquarters

2.1 ICAO's work on cybersecurity is driven by a comprehensive approach that encompasses different vectors:

- Developing Standards and Recommended Practices (SARPs). Currently, Annex 17 – Aviation Security contains the following references to cybersecurity:

  4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

  4.9.2 ***Recommendation. —*** *Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity, and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.*

- Developing procedures and guidance material. To date, several documents and guidance materials have been published by ICAO:

  - Chapter 18 in the ICAO Aviation Security Manual (Doc 8973 – Restricted);
  - Air Traffic Management Security Manual (Doc 9985 – Restricted);
  - Guidance on Traffic Light Protocol;
  - Cybersecurity Policy Guidance; and
  - Cybersecurity culture in Civil Aviation.

  Non-restricted material is available at www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx.

- Ensuring the international air law framework is adequate to address cyber-attacks against civil aviation;
- Raising awareness in different fora on the importance of addressing cybersecurity in civil aviation. As part of the ICAO training programme, in partnership with Embry-Riddle Aeronautical University, the course *"Foundations of Aviation Cybersecurity Leadership and Technical Management"* is now being delivered globally;
- Supporting aviation cybersecurity discussions on the national, regional, and global levels; and
- Developing aviation cybersecurity capacity building and implementation support initiatives for States and the wider aviation community.

2.2 In 2022 the Cybersecurity Panel (CYSECP) was established in order to engage State's experts in the subject and advance in the lines of work presented above. The CYSECP also provides advice to the ICAO Council as required and work closely with the Secretariat.

3. ICAO NACC Regional Office's work on cybersecurity

3.1 Following ICAO guidelines, and supported by its States, the ICAO NACC Regional Office developed a working plan on cybersecurity and participated in several fora with the aim of raising awareness among States and producing adapted guidance material. The main events and activities in which the ICAO NACC Regional Office was involved are listed below:

- FAA Civil Aviation Cybersecurity Tabletop Exercise (Washington D.C., 16-20 July 2018);
- ICAO NAM/CAR and SAM Workshop on Cybersecurity in Aviation (Mexico City, 4-6 December 2018), funded by the Multi-Regional Civil Aviation Assistance Programme (MCAAP);
- Workshop on Civil Aviation Cybersecurity (Buenos Aires, 19-22 February 2019), funded by OAS-CICTE;
- Joint AFAC, SENEAM and FAA Mexico Cybersecurity Tabletop Exercise (Mexico City, 9-10 September 2020);
- ICAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation (Online, 1 December 2020);
- 2nd ICAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation (Online, 16-18 March 2021);
- Integral Approach to Cybersecurity Risks in Aviation: the EU Strategy (Online, 21 September 2021), organized under the framework of the European Union-Latin America and Caribbean Aviation Partnership Project (EU-LAC APP);
- Cybersecurity Webinar on Air Traffic Management (ATM) and Communications, Navigation and Surveillance (CNS) Activities (Online, 6 October 2021); and
- OAS Airport Cybersecurity (Online, 18 November 2021).

3.2 Part of the work on cybersecurity has been articulated through a specific task fore integrated by the ICAO NACC Regional Office, the Civil Air Navigation Services Organization (CANSO) and AIRBUS. Having as reference the guidance material mentioned in the previous section, the task force developed on December 2020 the "Air Traffic Management (ATM) Cybersecurity Policy Template", specifically oriented to the protection of States' ATM systems.

4. Upcoming regional activities on cybersecurity

4.1 ICAO is investing more resources in cybersecurity and the subject has been pointed out as one of the ICAO work programme's priorities at A41. In coordination with Headquarters, the ICAO NACC Regional Office will continue to raise awareness among States and stakeholders and provide assistance as demanded. Indeed, AVSEC Technical Assistance Missions (TEAMs) already incorporate the review of cybersecurity measures (e.g., Cuba in September 2022), in line with the last version of the Universal Security Audit Programme (USAP)-Continuous Monitoring Approach (CMA) protocol questions.

4.2 The next activity contemplated is the organization of a cybersecurity workshop in 2024, in which latest developments at CYSECP meetings, training and guidance material (e.g. review of ICAO Cybersecurity Action Plan) will be shared.

4.3 Since one of the main areas related to the implementation of cybersecurity measures is ANS, several Multi-Regional Civil Aviation Assistance Programme (MCAAP) initiatives contemplate this subject. Strengthening of ANS cybersecurity measures is included in the analysis of ANS facilities in two NACC States, scheduled for 2023.

4.4 Particular details regarding these activities will be shared in due course.

5. Suggested actions

5.1 States are invited to:

a) consider in their work plans the implementation of cybersecurity measures in accordance with ICAO SARPs and available guidance material;

b) allocate resources for cybersecurity matters; and

c) support ICAO cybersecurity activities.

— END —