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

WORKING PAPER

NACC/WG/7 — WP/34
30/08/22

Seventh North American, Central American and Caribbean Working Group Meeting (NACC/WG/7)
ICAO NACC Regional Office, Mexico City, 30 August - 1 September 2022

Agenda Item 4: **NACC/WG Work Programme Update to 2024**
4.5 Emerging technologies and regional challenges

CYBERSECURITY IN AIR NAVIGATION SERVICES

(Presented by the Secretariat)

EXECUTIVE SUMMARY	
This working paper provides a summary on the available information on cybersecurity in air navigation services.	
Action:	Suggested actions are presented in Section 3.
Strategic Objectives:	• Safety
References:	• ICAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation, December 2020 https://www.icao.int/NACC/Pages/meetings-2020-aci.aspx • Second ICAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation-Cybersecurity Policy Manual https://www.icao.int/NACC/Pages/meetings-2021-canso02.aspx • Sixth North American, Central American and Caribbean Working Group Meeting (NACC/WG/6), online, 25 – 27 August 2021 https://www.icao.int/NACC/Pages/meetings-2021-naccwg6.aspx.

1. Introduction

1.1 Air navigation services have evolved in the last decade, implementing highly digital and automated technologies that require the implementation of other security mechanisms than those we have known to date.

1.2 Cyber technology and systems have become essential to modern society, being a component of many activities that have become dependent on information technology. Along with the benefit of cyber technologies, insecurities arise that affect all systems and infrastructures.

1.3 The cyber-threat and cyber-attack have a transnational component and effect, since global systems are interconnected. In addition, the complexity of the action has implications for various actors at the national, regional and international levels.

1.4 It is in this environment of cyber-insecurity that civil aviation carries out its activity. Civil aviation relies heavily on cyber technology that is used to increase the safety and efficiency of air transport. However, the interconnectivity of systems and the dependence on technology have created the optimal premises for new risks to emerge.

1.5 The aviation sector uses a wide range of interconnected computer-based systems, ranging from air navigation systems, aircraft on-board communication and control systems, airport ground systems, flight information, security checks and many others that are used on a daily basis and for all aviation-related operations. The trend in the aviation sector is to become increasingly digital. Digitization brings new dangers, as interactions between people and systems make risk more difficult to predict.

1.6 Recognizing the urgency and importance of protecting critical civil aviation infrastructure, information and communication technology systems and data against cyber threats, ICAO is committed to developing a robust cybersecurity framework. The 40 Session of the ICAO Assembly adopted *Resolution A40-10 - Addressing cybersecurity in civil aviation*. The resolution addresses cybersecurity through a horizontal, transversal and functional approach, reaffirming the importance and urgency of protecting critical infrastructure systems and civil aviation data against cyber-threats, and calls on States to apply the ICAO Cybersecurity Strategy.

1.7 Aviation cybersecurity strategy encompasses rests on seven pillars:

1. International cooperation
2. Governance
3. Effective legislation and regulations
4. Cybersecurity policy
5. Information sharing
6. Incident management and emergency planning
7. Capacity building, training and cybersecurity culture

1.8 The full document is available at the following link:

https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf#search=Aviation%20cybersecurity%20strategy

1.9 Since 2020, the ICAO NACC Regional Office has made an alliance with CANSO and AIRBUS and focused on the development of guidance documentation that allows States to evaluate air navigation systems and, based on this, develop their own cybersecurity policy customized to their operations. The document is a manual called: Air Traffic Management Cybersecurity Policy Template.

1.10 The manual is prepared following the recommendations of resolution *A40-10 - Addressing cybersecurity in civil aviation*, and under the ICAO Cybersecurity strategy, based on pillar number 4 "Cybersecurity Policy".

1.11 The NACC/WG is requested to adopt the document so that it can be used by the CAR region.

2. Cybersecurity Policy Template for Air Traffic Management

2.1 The objectives of this document are:

1. Contribute to the resilience of the State aviation system.
2. Provide support for the integrity, availability, and confidentiality of information.
3. Protect the hardware/software that supports the aviation system infrastructure to reduce risks for all State services.
4. Support the implementation of cybersecurity procedures and processes for all infrastructure and services.
5. Support cybersecurity and resilience of civil aviation.

2.2 The document lists a series of requirements that States must assess regarding their architecture and operations. Identifies the infrastructure and systems that are the core of its operations and implements mechanisms that ensure its protection and, most importantly, the continuity of its operations.

2.3 The document is in the **Appendix** to this working paper. This second version incorporates comments from the ICAO Air Navigation and Air Transport Offices.

2.4 A checklist has also been integrated into this new version that serves as a guide for the State to evaluate the requirements that it meets or does not meet according to its operations.

2.5 The ICAO NACC Regional Office has held a series of events aimed at understanding what cybersecurity means, and identifying threats to aviation operations, but it is necessary for States to take very seriously the activities that must be carried out in regarding this area.

2.6 Cybersecurity requires a commitment from States to allocate resources in all areas, from human to financial. However, prior to the development of projects aimed at this area, it is necessary for States to carry out an analysis of their operations and the Air Traffic Management Cybersecurity Policy Template supports this activity.

2.7 Projects in this area require an investment that must be supported by data that supports decision-making and the evaluation of their operations. The staff will support the State in defining the activities that it needs to develop.

2.8 The ICAO NACC Regional Office thanks CANSO and AIRBUS for this joint work. It is important to emphasize that the joint work between the organizations allows them to take advantage of the experts, experience and work more effectively on tasks of common interest and for the benefit of the States.

3. Suggested Actions

3.1 The meeting is invited to:

a) approve the adoption of the document as a Regional Guide for States;

b) designate Point of Contact (PoC) personnel by States to work directly with them;

c) work with the ICAO Regional Office in the scheduled activities to deal with cybersecurity issues addressed to air navigation services; and

d) other applicable action.

— — — — — — — — — — —