*International Civil Aviation Organization*

**MIDANPIRG/20 and RASG-MID/10 Meetings**

*(Muscat, Oman, 14-17 May 2023)*

---

**Agenda Item 2.2:** **Updated from States and International Organizations**

## CYBERSECURITY IN AIR NAVIGATION SERVICES

*(Presented by CANSO)*

| 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:* | • CAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation, December 2020 https://www.icao.int/NACC/Pages/meetings-2020-aci.aspx<br>• Second ICAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation-Cybersecurity Policy Manual https://www.icao.int/NACC/Pages/meetings-2021-canso02.aspx<br>• 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　　　　　CANSO, ICAO NACC office and AIRBUS prepared the *Air Traffic Management Cybersecurity Policy Template* to help states implement cybersecurity mechanisms and culture across entire ATM systems and security operations. The template aims to guarantee aviation system resilience, safeguarding information integrity, availability, confidentiality, and hardware/software protection, and support civil aviation security, national security and defence and law enforcement.

The *Air Traffic Management Cybersecurity Policy Template* is a living document that will adapt to the changing environment we live in. Implementing a cybersecurity policy protects your organisation while increasing safety.

Below you can download the document:

https://canso.org/publication/air-traffic-management-cybersecurity-policy-template/

1.8　　　　　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".

1.9　　　　　 The NACC/WG adopted the document to be used by the CAR region.

## 2.　　CYBERSECURITY POLICY TEMPLATE FOR AIR TRAFFIC MANAGEMENT

2.1　　　　　The objectives of this document include:

- Contribute to the resilience of the State aviation system.
- Provide support for the integrity, availability, and confidentiality of information.
- Protect the hardware/software that supports the aviation system infrastructure to reduce risks for all State services.

- Support the implementation of cybersecurity procedures and processes for all infrastructure and services.
- 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 can be downloaded via the link in point 1.7 above. The second version is completed and will publish in the second quarter of 2023. The new version incorporates comments from the ICAO Air Navigation and Air Transport Offices.

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

2.5        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.

2.6        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.

2.7        It is important to emphasize that the joint work between the organizations allowed to take advantage of professionals, experience and work more effectively on tasks of common interest and for the benefit of the States. The template is one of many examples of a joint cooperation.

**3.        SUGGESTED ACTIONS**

3.1        The meeting is invited to encourage States to:

a)  use the template as guidance material; and

b)  work with the ICAO Regional Office in air navigation services cybersecurity activities.


— END —