



WORKING PAPER

FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

- Agenda Item 4: Hyper-connectivity of air navigation system**
4.2: Cybersecurity and information system resilience

COMPUTER INCIDENT SECURITY RESPONSE TEAM (CSIRT) FOR CIVIL AVIATION

(Presented by Colombia)

EXECUTIVE SUMMARY

Computer incident security response teams (CSIRTs) offer IT security response solutions to entities taking real-time decisions in anticipation of or in response to a cyber incident, enabling them to act immediately and recover as quickly as possible. Most countries have critical infrastructure CSIRTs that work under the national authorities on matters of cybersecurity. However, national air transport sectors often lack this facility. It is urgent to create a CSIRT specifically for civil aviation.

The civil aviation sector has the responsibility to ensure the safety of operations and passengers. It rests on a layer of technological infrastructure for information and operations that is considered critical and requires 24/7 monitoring to anticipate cyberthreats.

For this reason, a reference framework should be established by ICAO to provide guidance and establish procedures for countries to set up a civil aviation CSIRT.

A CSIRT for civil aviation should have an appropriate governance structure and comply with international cybersecurity standards. It should support States as they develop the civil aviation cybersecurity strategy proposed by ICAO using the tools, staff and processes that are instrumental to the purpose.

In view of the foregoing, we propose that ICAO issue guidance for the creation of a CSIRT specifically for civil aviation, and associated procedures, that brings together the human and technological cybersecurity resources of stakeholders in the civil aviation sector in each country.

Action: The Conference is invited to recommend that ICAO develop guidance and procedures for all Member States to establish a civil aviation CSIRT and assign its functions, under the leadership of the Organization.

¹ Spanish version provided by Colombia.

1. INTRODUCTION

1.1 The ICAO Cybersecurity Strategy recognizes the increasing dependency on IT systems and the importance of ensuring the integrity, confidentiality and availability of information for the safe development of the sector. Cyberthreats to civil aviation are constantly evolving, and jeopardize the safety and continuity of operations. Threats can be motivated by political, financial, terrorist or other objectives. In response to this threat landscape, a reference framework has been established that is founded on seven pillars:

- a) international cooperation;
- b) governance;
- c) effective laws and regulations;
- d) cybersecurity policies;
- e) information-sharing;
- f) incident management and emergency planning;
- g) capacity building and training; and
- h) cybersecurity culture.

2. DISCUSSION

2.1 The civil aviation sector and its stakeholders comprise airports, communications, navigation, and surveillance (CNS), air traffic management (ATM), unmanned aircraft system traffic management (UTM) and meteorological (MET) providers, equipment manufacturers and distributors, maintenance organizations and airlines, all of whom are interconnected by information and communication technologies. This complicates the safe handling and management of data and information, posing a potential risk to the safety of life. For that reason, teamwork, coordination and threat intelligence sharing should take place among the stakeholders and among sovereign States.

2.2 Sovereign States have agencies and/or entities in charge of cybersecurity policy at the most strategic level, and their work is carried out by computer emergency response teams (CERTs). At the lower levels, sectoral CSIRTs coordinate and adopt protocols for responding to cyber incidents, especially in entities and/or sectors with critical infrastructure. Civil aviation is one such sector, and so it would be logical to develop a dedicated CSIRT.

2.3 In view of the foregoing, we propose that ICAO develop guidance for the creation of a civil aviation CSIRT, together with procedures, in each State with the common goal of improving the cyber-resilience posture of civil aviation.

3. **CONCLUSION**

3.1 The Conference is invited to agree to the following recommendation:

Recommendation 4.2/x – Guidance for the creation of a civil aviation computer incident security response team (CSIRT) and associated procedures

That ICAO develop guidance and procedures for all Member States to establish a civil aviation CSIRT and assign its functions, under the leadership of the Organization.

— END —