*International Civil Aviation Organization*
South American Regional Office
**Eleventh Multilateral Meeting of the SAM Region for the Transition of AIS to AIM (SAM/AIM/11)**
Lima, Peru, 23 to 27 April 2018



**Agenda Item 8: Other business**

# Civil aviation cybersecurity awareness and training

(Presented by the Secretariat)

**SUMMARY**

This working paper presents information on actions that should be considered for adoption to protect AIM data from cyber attacks.

**REFERENCES**

- Doc 8973/10th edition - Security Manual, Chapter 18, *Cyber threats to critical aviation information and communication technology systems.*
- Doc 9985 - Air traffic manual security manual, Chapter 5, *Information communication and technology (ICT) security system (including cybersecurity*).
- Assembly Resolution A39-19: *Addressing cybersecurity in civil aviation.*

## 1. Introduction

1.1 The 39th ICAO Assembly adopted Resolution 19, on ways to address cybersecurity.

1.2 While technology and information technology evolve at very high speed, cybercrime has grown worldwide, affecting different vital areas of organisations, companies, financial institutions, even social networks, not to exclude the aeronautical sector. Accordingly, cyber attacks have become one of the emerging threats to information technology systems, critical communications and data, and other civil aviation data.

1.3 Aeronautical information services/aeronautical information management are the focal point for the collection, verification and distribution of aeronautical information of the States. Therefore, they are subject to cyber threats that could affect the safety of aeronautical operations.

## 2 Discussion

2.1 The ICAO 39th Assembly, through Resolution A39-19: *Addressing cybersecurity in civil aviation,* urged States, *inter alia,* to:

- Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents.

- Encourage the development of a common understanding among member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected.

- Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed.

- Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts.

- Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out.

2.2 The aeronautical industry, air navigation service providers (ANSPs) and civil aviation authorities (CAAs) increasingly rely on communications and network-based operations. Accordingly, States must endeavour to modernise IT and network infrastructure, connecting users, systems and data in order to provide seamless and secure access, protected from cybersecurity incidents.

2.3 Cyber incidents may affect the global aeronautical community or individual systems at many levels. These incidents may jeopardise communications and information exchange among the different aviation stakeholders, affecting safety and security, and aeronautical business continuity.

2.4 It is important that States develop training material on cybersecurity and that information be shared among aviation stakeholders, such as regulatory authorities, air navigation service providers, aircraft and airport operators, IT support experts and other aviation industry collaborators with basic awareness on cybersecurity risks.

2.5 It should be noted that not all cybersecurity issues affecting civil aviation safety are related to unlawful and/or intentional acts. Accordingly, they should be resolved through the implementation of safety management systems. However, it is important to protect critical civil aviation infrastructure systems and data from cyber threats. AIS/AIM, as aeronautical information and data managers in the State, should start sensitising their personnel on information management measures that could be implemented to mitigate threats.

2.6 Work should be closely coordinated with network and IT personnel for the protection of information and implementation of other contingency measures that might help in case of cyber attacks.

2.7 The ICAO/LACAC NAM/CAR and SAM Regional Aviation Security and Facilitation Group (AVSEC/FAL/RG) started to work on this issue in 2014. It would be important to identify the focal points of this group in your States and start working with them in order to agree on actions to mitigate cyber attacks in an area as sensitive as AIM.

3. **Suggested action:**

3.1 The Meeting is invited to:

a) take note of the contents of this working paper; and

b) incorporate cybersecurity into the AIM work agenda.

- END -