



**Twentieth Meeting of the CAR/SAM Regional Planning and Implementation Group  
 (GREPECAS/20)**

Salvador, Brazil, 16 – 18 November 2022

- Agenda Item 3: Second GREPECAS-RASG-PA Joint Meeting**  
**3.2 CAR/SAM Regions Air Navigation Priorities, Targets and Emerging Risks**

**CYBERSECURITY IN CIVIL AVIATION**

(Presented by the Secretariat)

<b>EXECUTIVE SUMMARY</b>	
<p>This information paper provides information on the resolutions taken at the 41st ICAO Assembly regarding the updating of cybersecurity issues that need to be addressed by States in our regions.</p>	
<i>Strategic Objectives:</i>	<ul style="list-style-type: none"> <li>• Air Navigation Capacity and Efficiency</li> </ul>
<i>References:</i>	<ul style="list-style-type: none"> <li>• ICAO ASSEMBLY -41ST SESSION            Montreal, September 27 – October 07, 2022  <a href="https://www.icao.int/Meetings/a41/Pages/default.aspx">https://www.icao.int/Meetings/a41/Pages/default.aspx</a></li> </ul>

**1. Introduction**

1.1 During the day of the 41st ICAO Assembly, discussions were held on emerging aviation issues and Resolution A41-19: Addressing cybersecurity in civil aviation was agreed.

1.2 The global aviation system is a highly complex and integrated system comprising systems that are critical to the safety and security of civil aviation operations that are increasingly dependent on the reliability, integrity and availability of systems, data and information.

1.3 That there is a growing awareness that cyber threats to civil aviation are evolving rapidly and continuously, that aviation remains a target for criminals, both cyber and physical, and that cyber threats can mutate to affect critical civil aviation systems worldwide and that cyber security events affect safety.

## 2. Resolution A41-19: Addressing Cybersecurity in Civil Aviation

2.1 Urges Member States to adopt and ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) as a means for dealing with cyberattacks against civil aviation and calls upon States and industry stakeholders to take the following actions to address cyber threats to civil aviation:

- a) implement the ICAO Aviation Cybersecurity Strategy, and make use of the ICAO Cybersecurity Action Plan as a tool to support the implementation of the Aviation Cybersecurity Strategy;
- b) designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies;
- c) define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;
- d) develop and implement a robust cybersecurity risk management framework that draws on relevant safety and security risk management practices, and adopt a risk-based approach to protecting critical civil aviation systems, information, and data from cyber threats;
- e) establish policies and instruments, and allocate resources to ensure that, for critical aviation systems: system architectures are secure by design; systems are protected and resilient; data is secured and available in storage and while in transfer; system monitoring, and incident detection and reporting, methods are implemented; incident recovery plans are developed and practiced; and forensic analysis of cyber incidents is carried out;
- f) 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;
- g) encourage civil/military cooperation with regard to identifying, protecting, and monitoring common vulnerabilities and data flows at interfaces between civil and military aviation systems, and collaborate in response to common cyber threats and recovery from cyber incidents;
- h) 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;
- i) design and implement a robust cybersecurity culture across the civil aviation sector;
- j) encourage States to continue contributing to ICAO in the development of international Standards, strategies, and best practices to support advancing aviation cybersecurity and cyber resilience; and
- k) Continue collaborating in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving aviation safety, aviation security, facilitation, air navigation, communication, surveillance, air traffic management, aircraft operations, airworthiness, and other relevant disciplines.

2.2 Finally invited to ICAO to continue to promote the universal adoption and ratification of the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) and continue to ensure that cybersecurity and cyber resilience matters are considered and coordinated in a cross-cutting manner through the new mechanism in ICAO to address aviation cybersecurity

### **3. Conclusion**

3.1 The meeting is invited to take note of the information provided and begin to implement the measures it applies to its aviation system to ensure that cybersecurity threats do not affect its operations.