



ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

NEED TO STRENGTHEN HUMAN FACTOR AND CYBERSECURITY MANAGEMENT MEASURES IN AVIATION SECURITY

(Presented by Cuba and supported by 17 LACAC Member States²)

EXECUTIVE SUMMARY

This paper reflects on human factors and their impact on aviation security personnel development and performance, an essential area where strategies can be developed and further steps taken to attract aviation security professionals and, in general, provide stability for those trained in these roles. A concerted effort is needed to continue strengthening aviation security, a key element for the sustainable development of air transport, by recruiting and retaining qualified and skilled personnel to manage and maintain the system's effectiveness and efficiency.

Action: The Assembly is invited to:

- a) note the information presented; and
- b) urge States to strengthen measures for human factor and cybersecurity management in aviation security, such as:
 - developing comprehensive human factors and cybersecurity management plans aligned with Annex 17 to the Chicago Convention and the ICAO Aviation Cybersecurity Strategy;
 - conducting periodic risk assessments and updating protective measures;
 - promoting national and international cooperation for sharing information and best practices;
 - providing continuous cybersecurity and human factors training to personnel; and
 - fostering an organizational culture focused on digital security and resilience.

<i>Strategic Goals:</i>	This working paper relates to Strategic Goal <i>Every Flight is Safe and Secure</i>
<i>Financial implications:</i>	Resources for personnel recruitment and training, and investment in technology.
<i>References:</i>	Doc 10118, <i>Global Aviation Security Plan (GASeP)</i> , Second Edition Resolution A41-18, <i>Consolidated statement on continuing ICAO policies related to aviation security</i> Resolution A41-19, <i>Addressing Cybersecurity in Civil Aviation</i> Annex 17 – <i>Aviation Security</i> Doc 8973, <i>Aviation Security Manual</i> <i>Aviation Cybersecurity Strategy</i> <i>Muscat Declaration on Aviation Security and Aviation Cybersecurity</i>

¹ Spanish version provided by Cuba

² Belize, Bolivia (Plurinational State of), Brazil, Chile, Colombia, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay, Venezuela (Bolivarian Republic of)

1. INTRODUCTION

1.1 Aviation security is key to the sustainable and efficient development of air transport worldwide. This vital sector for global connectivity and economic growth requires robust security standards to ensure safe and reliable operations. In this context, human factors play a decisive role, as the prevention of incidents and accidents largely depends on personnel training, performance, and decision-making in all phases of air operations. In addition, the successful implementation of international standards and procedures can only be achieved through effective human factor management, an area that requires further study and application to strengthen security and ensure the resilience of the aviation system.

1.2 The increasing complexity of aviation, driven by technological development and the emergence of new threats, has led the international community to establish robust regulatory frameworks. In this regard, ICAO Annex 17 is the primary regulation to protect civil aviation from acts of unlawful interference, including both physical and cyber threats. The Annex recognizes that aviation security entails not only physical barriers and procedures, but also comprehensive human factors and cybersecurity management. Both elements have become essential for ensuring aviation resilience in the face of current and future challenges.

2. DISCUSSION

2.1 Human factors comprise all aspects of the behavior, performance, skills, and limitations of security personnel. This includes selection and training, stress and fatigue management, communication, and decision making in critical situations. Security personnel should have a sound technical and professional background, specific certifications and experience in managing such situations. Continuous training is essential to keep pace with constantly evolving threats and security technologies.

2.2 Present challenges include:

- a) **Shortage of qualified personnel:** The industry is facing challenges in attracting and retaining specialized talent, which can compromise the effectiveness of security measures and limit incident response capabilities.
- b) **Fatigue and excessive workload:** Shortage of human resources can lead to long working hours, fatigue and diminished performance, which increases the risk of errors and hazardous situations.
- c) **Technological adaptation:** The rapid adoption of new technologies requires personnel to adapt and develop digital skills to operate complex systems and protect sensitive information.
- d) **Sensitive information management:** Staff must be able to handle confidential data and respond to security incidents, including cyber threats.
- e) **Diversity and teamwork:** Multicultural and generationally diverse teams require strong communication and leadership skills to prevent misunderstandings and foster collaboration.

2.3 Shortage of security personnel can lead to errors, process delays and reduced incident response capabilities. It can also affect the implementation of security measures and increase the workload, which can lead to hazardous situations. This can result in increased operational risks and a failure to identify threats.

2.4 Strategies to prevent and mitigate human resource shortages include:

- a) human resources planning;
- b) recruitment and retention;
- c) continuous training;
- d) technological support;

- e) improved working conditions;
- f) supervision and continuous improvement.

2.5 The digital environment has introduced new security risks and challenges. ICAO Annex 17 recognizes the importance of cybersecurity in the protection against acts of unlawful interference. To be prepared to identify, prevent, and respond to cyber threats, security personnel should be provided with:

- a) **Cybersecurity training:** Specific training on digital threat identification and response protocol implementation.
- b) **Cyber incident management:** Development of skills to respond to incidents that can compromise safety.
- c) **Cybersecurity awareness and culture:** Promotion of best practices and awareness among personnel at all levels.

2.6 Annex 17 sets out the requirement to identify critical information and communication technology systems and to implement risk assessment-based measures for their protection. This requires the integration of cybersecurity into national security programs, cross-sector collaboration and continuously monitoring the measures in place.

3. CONCLUSIONS

3.1 Aviation security is a complex and dynamic system, where human factors are the backbone supporting the effectiveness of all measures and procedures in place. The ability of States and organizations to anticipate, prevent and respond effectively to conventional and emerging risks and threats, including cyber threats, largely relies on the appropriate management of these factors.

3.2 Cybersecurity is a new challenge in human factors management. The digital environment has broadened the spectrum of security threats. Personnel need to be prepared to face not only physical risks, but also cyber risks. This requires a robust cybersecurity culture, specific training, and clear digital incident response protocols. Integrating cybersecurity into human factors management is now a prerequisite for the comprehensive protection of civil aviation.

— END —