



**WORKING PAPER**

**ASSEMBLY — 42ND SESSION**

**EXECUTIVE COMMITTEE**

**Agenda Item 13: Aviation Security – Policy**

**THE NEED FOR A SUSTAINED FOCUS ON SECURITY**

(Presented by Australia, and co-sponsored by Canada)

**EXECUTIVE SUMMARY**

The aviation sector faces a dynamic and evolving range of threats, which are becoming increasingly complex. While traditional threats such as terrorism persist, the global threat environment has significantly changed. Security contributes to productivity and prosperity, and must be a fundamental part of any aviation entity's core business. ICAO plays an important global leadership role in ensuring a sustained focus on aviation security.

**Action:** The Assembly is invited to:

- (a) recognize the importance of a sustained focus on aviation security;
- (b) encourage greater connections between security, cybersecurity, and facilitation; and
- (c) encourage the Aviation Security Panel, Cybersecurity Panel and Facilitation Panel to work in closer collaboration.

<i>Strategic Goals:</i>	This working paper relates to Strategic Goal of <i>Every Flight is Safe and Secure</i> .
<i>Financial implications:</i>	<i>The actions referred to in this paper will be subject to the resources available in the Regular Programme Budget and/or from extra budgetary contributions.</i>
<i>References:</i>	Annex 17 – <i>Aviation Security to the Convention on International Civil Aviation Global Aviation Security Plan (GASeP)</i> (Doc 10118) Muscat Declaration on Aviation Security and Aviation Cybersecurity

**1. INTRODUCTION**

1.1 The aviation sector faces a dynamic and evolving range of threats, which are becoming increasingly complex. While traditional threats such as terrorism persist, the global threat environment has significantly changed. The aviation ecosystem is facing new challenges from non-traditional threat actors.

1.2 Since the last Assembly, there has been an increase in the frequency of cyber attacks on aviation. Ransomware, data theft, distributed denial of service attacks, and other cyber disruptions

are all becoming more frequent, and their impacts more significant and disruptive. This trend is likely to continue – and can only be answered by a concerted focus on cybersecurity.

1.3 2024 saw acts of sabotage in the air cargo supply chain, conducted by sophisticated actors. While air cargo has been recognised as a potential attack vector, these incidents using improvised incendiary devices (IID) highlighted new challenges and are a reminder that we cannot be complacent.

1.4 Globally, we have also seen increasing concerns around malicious use of unmanned aircraft systems (UAS), and airport security breaches, including runway and aircraft incursions, while bomb threats and hoaxes are surging globally.

1.5 These threats have been exacerbated by rapid technological advances as well as geopolitical issues and events. These threats are pervasive, multifaceted and, if unmitigated, could do serious harm to a State's sovereignty, security, prosperity and national interests. Despite all of this, and in the absence of a catastrophic aviation security incident or act of unlawful interference, our community runs the danger of becoming complacent and overly confident in existing security measures.

## **2. SECURITY SUPPORTS PRODUCTIVITY AND PROSPERITY**

2.1 Aviation security does not exist for security's sake. Rather, the goal of aviation security is to ensure the safe, efficient and sustainable operation of global civil aviation, which in turn contributes to productivity, prosperity, and drives economic growth, global connectivity and innovation.

2.2 As such, security considerations should be part of the DNA of all aviation entities. Security must be an ingrained way of thinking, as a fundamental part of doing business, rather than a burden, whether financial or otherwise. Security, cybersecurity, safety and facilitation are core to an effective, efficient and sustainable aviation sector.

2.3 Aviation security is a complex, multi-layered effort that requires coordination and collaboration across ICAO, Member States, industry partners, and the travelling public. A sustained security focus is key to addressing these shared challenges and to achieving our common goal of a strong and effective global aviation security system. There is no single measure that can fully mitigate current and emerging threats. Instead, a layered, risk-based approach anchored in ICAO's Annex 17 – *Aviation Security to the Convention on International Civil Aviation* is essential.

## **3. A SUSTAINED SECURITY FOCUS IS NEEDED**

3.1 Vigilance and proactive measures are essential to maintaining safe and secure aviation travel. As the threat environment evolves, it is critical that ICAO and Member States regularly assess the approach to aviation security and take action where necessary to ensure that the global response remains effective in countering evolving threats.

3.2 The need for a sustained security focus is echoed in ICAO's *Global Aviation Security Plan* (Doc 10118) and its call for Member States and industry to continue collaborating through ICAO, and to deliver aviation security at national, regional and global levels.

3.3 This call was reinforced by the Muscat Declaration on Aviation Security and Aviation Cybersecurity (11 December 2024). This Declaration recognises that aviation security and cybersecurity are critical for the sustainable development of air transport and, therefore, urges Member States, ICAO and industry to strengthen efforts in addressing new and existing threats to international civil aviation.

3.4 ICAO plays an important role in recognising security changes and promoting information sharing amongst Member States. This was evidenced in ICAO's coordination of efforts and engagement to address the issue of IIDs, and in initiating work on mail and cargo security with the Universal Postal Union, along with Member States. It is essential that ICAO continue to provide this global leadership.

3.5 A continued, sustained focus on aviation security, from both ICAO and Member States, is critical to mitigating evolving threats and operational challenges and building a culture of vigilance, innovation and collaboration.

— END —