

**60th CONFERENCE OF
DIRECTORS GENERAL OF CIVIL AVIATION
ASIA AND PACIFIC REGIONS**

*Sendai, Japan
28 July - 1 August 2025*

**AGENDA ITEM 5: AVIATION SECURITY AND
FACILITATION**

**DEVELOPMENTS IN AVIATION SECURITY AND
AVIATION CYBERSECURITY**

(Presented by the ICAO Secretariat)

INFORMATION PAPER

SUMMARY

This paper highlights recent developments in the global aviation security and aviation cybersecurity policy framework.

1. GLOBAL AVIATION SECURITY PLAN (GASeP)

1.1. In June 2024, ICAO issued the Second Edition of the *Global Aviation Security Plan* (Doc 10118) to reaffirm the Aspirational Goal to achieve and sustain a strong global aviation security system that is underpinned by full and effective implementation of ICAO aviation security Standards in all Member States. The updated Plan was designed to enhance international aviation security by providing detailed guidance to governments, industry and other stakeholders.

1.2. Since the coming into effect of the Second Edition of GASeP, outreach efforts have taken place to promote it, such as the following international roundtable discussion events: 7 November 2024 in Dubai, United Arab Emirates¹; and during the Security Week 2024 on 10 December 2024 in Muscat, Sultanate of Oman². These events served as a useful and effective platform for collaboration and dialogue on the updated GASeP, and on advancing aviation security. Notifications will be sent for future events.

2. OUTCOMES OF SECURITY WEEK 2024 AND MUSCAT DECLARATION

2.1. In an effort to launch the new GASeP and also address emerging challenges in the aviation sector, a High-level Ministerial Segment was convened on 11 December 2024 during ICAO Security Week 2024 hosted by the Civil Aviation Authority of Oman, in Muscat, from 9 to 12 December 2024. Ten Ministers participated in this event, with seven of them delivering

¹ <https://www.icao.tv/global-aviation-security-symposium-avsec/season:8/videos/security-week-day-2-global-aviation-security-plan-gasep>

² <https://www.icao.tv/latest-videos/videos/roundtable-advancing-the-gasep-with-renewed-ambition-dubai-7-november-2024>

oral statements. The event reaffirmed the commitment of States to enhancing aviation security and aviation cybersecurity, and provided policy direction, advancing the new Strategic Goal - Every Flight is Safe and Secure. The High-level Ministerial Segment culminated in the adoption of the Muscat Declaration on Aviation Security and Aviation Cybersecurity. As indicated in State letter AS 8/1.5-25/53 dated 22 May 2025, States are requested to take steps, as necessary, to achieve the objectives set out in the Muscat Declaration.

3. CONFLICT ZONES AND OBLIGATION OF MEMBER STATES

3.1. Operating over or near conflict zones continues to present significant risks to civil aviation. In the past, civil passenger aircraft downed over or near conflict zones, include among others Malaysian Airlines Flight 17 in 2014, Ukraine International Airlines Flight 752 in 2020, and Azerbaijan Airlines Flight 8243 on 25 December 2024. Accordingly, the ICAO Council during its 235th Session underscored the critical importance of mitigating risks to civil aviation over and near conflict zones, highlighted the need for concerted efforts to address such risks, and proposes that the 42nd Session of the Assembly adopt a dedicated Assembly resolution to reaffirm States' and operators' responsibilities, and for them to take timely and decisive action in mitigating risks associated with conflict zones.

3.2. ICAO has continued to promote greater awareness on risks to civil aviation posed by flights operating over or near conflict zones, particularly during times of heightened military activity, including convening a session during the ICAO Security Week 2024 focused on civil-military coordination and collaboration and innovation for secure operations. The session emphasized the critical importance of fostering collaboration and coordination among civil aviation stakeholders, and cooperation between civil and military authorities as essential to maintaining safe and secure aviation operations in the face of escalating challenges. Since September 2024 and in cooperation with the Safer Skies Consultative Committee and the support of the European Civil Aviation Conference (ECAC) for activities in Europe and Africa, ICAO concluded six regional awareness seminars on Risk Assessment Processes and on Doc 10084.

4. GUIDANCE MATERIAL

4.1. New and updated guidance material was endorsed by the Thirty-sixth meeting of the Aviation Security Panel (AVSECP/36) and subsequently approved for distribution. The areas addressed by the guidance material include: hold baggage screening, handling and processing; as well as Automated Prohibited Items Detection Systems (APIDS) and Open Architecture, which aim to assist States in better understanding these emerging concepts. The guidance material on hold baggage is available on ICAO-NET (portal.icao.int) under "Publications" and "Others", and public guidance will be made available on <https://www.icao.int/Security/SFP/Pages/Guidance-Material.aspx>. Other guidance material documents on the application of security controls to vehicles entering security restricted areas, as well as on addressing the threat posed by MANPADS will also be published in the fourth Quarter of 2025 following their endorsement by the Panel through correspondence and as per relevant ICAO guidelines. Finally, a Human Factors and Technology Toolkit developed by ICAO, with the support from the AVSEC Panel Working Group on Training, will be made available in the following weeks.

4.2. The First Edition of the ICAO *Aviation Security Training Manual* (Doc 10207) is available on ICAO-NET (portal.icao.int) under "Publications" and "Documents". All other ICAO language versions will follow as they become available. The Manual is designed to assist Member States, industry and other organizations in delivering robust aviation security training (including design, delivery and quality assurance aspects) and to strengthen security culture and human capability in aviation.

4.3. As guidance material is an invaluable resource designed to assist stakeholders in effectively implementing the Standards and Recommended Practices (SARPs) outlined in Annex 17, accessibility is key in carrying out such efforts. That is why ICAO is committed to sharing guidance material on its public website whenever permissible. At the time of this information paper, guidance material on the recognition of equivalence of security measures (one-stop security); the protection of civil aviation infrastructure against unmanned aircraft; the implementation of a reporting system; the

disposal of screening equipment; and on the establishment, implementation and maintenance of aircraft operator security programmes (AOSP) and supplementary station procedures (SSP) can be found at <https://www.icao.int/Security/SFP/Pages/Guidance-Material.aspx>.

4.4. As the ICAO *Aviation Security Global Risk Context Statement* (Doc 10108, Restricted) is currently undergoing updates for the next edition, an Addendum to the Third edition of Doc 10108 is available in English with other languages to follow. The Addendum provides an update to both the global threat picture and the risk assessment results for different threat types. This Addendum is an interim document to ensure States have the latest information until the more detailed Fourth edition of Doc 10108 is published.

5. **AIR CARGO AND MAIL SECURITY – IMPROVISED INCENDIARY DEVICES (IIDs)**

5.1. In response to a series of incidents involving Improvised Incendiary Devices (IIDs) in July 2024, several States issued specific recommendations and temporary measures to mitigate risks posed by IIDs for international aircraft operators, including cargo express operators, and the Universal Postal Union (UPU). The ICAO Secretariat issued an information bulletin through the ICAO Point of Contact Network (POC) on 3 October 2024, calling for heightened vigilance across all entities involved in the acceptance, screening, and handling of air cargo and mail. The Secretariat has since worked closely with affected States and industry partners, engaging relevant groups of the Aviation Security Panel (AVSECP).

5.2. AVSECP/36 in May 2025 expressed strong support for the development of guidance material to mitigate the threat of IIDs. The Panel also emphasized the urgency of a coordinated and actionable response, and welcomed enhanced cooperation with the Universal Postal Union (UPU), IATA (International Air Transport Association) and WCO (World Customs Organizations). It also supported further exploration of screening technologies and algorithmic tools, while affirming that security controls and human factors remain central.

5.3. In line with the growing need for data and comprehensive insight into the practical implementation of secure supply chains, the Secretariat conducted a survey to assess the level of implementation of Annex 17 Standards 4.6.2 and 4.6.5. The survey was developed in close coordination with the AVSECP Working Group on Air Cargo Security (WGACS), and the Secretariat incorporated specific references to mail to ensure better alignment with ongoing discussions on air mail security. It was sent via the ICAO POC Network Message on May 7, 2025. The objective of the survey is to collect updated information from Member States on the application of security measures to air cargo and mail, with particular focus on the role and responsibilities of “other approved entities”, as well as on the broader implementation of secure supply chains.

6. **AVIATION CYBERSECURITY³**

6.1. The Ad Hoc Cybersecurity Coordination Committee (AHCCC) met three times since its establishment, the last meeting was held from 23 to 25 April 2025, and continues to refine the ICAO Aviation Cybersecurity Work Programme as the work on cybersecurity evolves, serving as a collaboration platform for expert groups to share information and support a harmonized and consistent approach to aviation cybersecurity in the context of their respective work areas.

6.2. The Cybersecurity Panel (CYSECP) was established in 2022. It held four meetings to-date, the latest of which was held from 2 to 6 June 2025.

6.3. The CYSECP organizes itself into two Working Groups and one Task Force:

6.3.1 The Working Group on Cyber Threat and Risk (WGCTR) developed an aviation cyber threat and risk assessment methodology that integrates cyber risk management into aviation safety, security, efficiency, and capacity risk management processes. The methodology is published in the

³ <https://www.icao.int/aviationcybersecurity/Pages/default.aspx>

Global Cyber Risk Considerations (*Doc 10213 – Restricted*) along with a global cyber threat landscape. The methodology part of the document (unedited), including implementation examples, is published on ICAO public website⁴.

6.3.2 The Working Group on Cybersecurity Guidance Material (WGCGM) is supporting the Secretariat in the development of guidance material. The guidance material is being published as stand-alone documents on ICAO public website, and the WGCGM is developing additional guidance, all of which will be consolidated into an Aviation Cybersecurity Manual that will be available towards the end of 2026 – early 2027.

6.3.3 The Secretariat developed a study in 2022 which identified areas of potential interest to aviation cybersecurity in 16 Annexes of the *Convention on International Civil Aviation* (Chicago Convention) by cross-referencing the Annexes with high-level information security management systems and with the ICAO Aviation Cybersecurity Strategy. The Task Force on Cybersecurity Standards and Recommended Practices (TF-CYSARPS) is building on this work to identify gaps that may exist in ICAO SARPs framework to adequately cyber threats and risks to civil aviation. The work on this topic is ongoing and is expected to continue throughout the upcoming triennium.

6.4. ICAO also produced [guidance material](#) to support States and stakeholders in addressing aviation cybersecurity (Cybersecurity Policy Guidance, and Guidance on Cybersecurity Culture in Civil Aviation, Guidance on Cyber Information Sharing, Guidance on Cyber Incident Reporting and Guidance on Cyber Considerations for Insider Threats).

6.5. In addition, ICAO continues to organize and participate in national, regional, and international conferences, meetings and webinars to promote cooperation between all stakeholders in aviation cybersecurity. Between October 2024 and May 2025, ICAO conducted a series of Regional Aviation Cybersecurity Seminars across ICAO Regions. The seminars gathered more than 450 participants from all aviation and non-aviation relevant disciplines. Discussions included topics such as the global, regional, national and organizational cyber threat landscape to civil aviation, as well as successes, challenges and opportunities at Member States and industry stakeholders in addressing cybersecurity in civil aviation. The seminars also included a deep dive into ICAO aviation cybersecurity frameworks, and a table-top exercise that simulated the response to a complex international cyber incident with potential impact on safety. In the APAC Region, the Regional Aviation Cybersecurity Seminar was held from 12 to 14 March 2025 at the ICAO APAC Regional Office in Bangkok – Thailand. The event was attended by 62 participants from 14 Member States, and was supported by ICAO HQ and APAC officers.

7. 42ND SESSION OF THE ICAO ASSEMBLY

7.1. For the 42nd Session of the Assembly, the Council will be presenting four working papers:

- a) Assembly Resolution A41-18 regarding *Consolidated statement on continuing ICAO policies related to aviation security* will contain proposed revisions;
- b) the Assembly will be invited to reaffirm the commitments made in the Muscat Declaration on Aviation Security and Aviation Cybersecurity that was adopted during the ICAO Security Week in December 2024 in Oman.
- c) considering the importance of the Muscat Declaration on Aviation Security and Aviation Cybersecurity, a paper regarding Conflict zones and obligations by States will also be presented; and
- d) the Assembly will invited to note the developments in aviation cybersecurity activities and adopt the updated Assembly Resolution on *Addressing Cybersecurity in Civil Aviation*.

⁴ <https://www.icao.int/aviationcybersecurity/Documents/Doc%2010213%20%28Unedited%29%20-%20Global%20Cyber%20Risk%20Considerations.EN.pdf>

8. **ACTION BY THE CONFERENCE**

- 8.1. The Conference is invited to note the information contained in this Paper.

— END —