



ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security – Policy

**INDUSTRY INITIATIVES FOR IMPROVING THE REGULARITY, THE EFFICIENCY AND
ECONOMIC BENEFITS WHEN IMPLEMENTING THE SECURITY STANDARDS
CONTAINED IN ANNEX 17**

(Presented by the International Air Transport Association (IATA))

EXECUTIVE SUMMARY

The International Air Transport Association (IATA) continuously improves its IATA Operational Safety Audit (IOSA) mandatory requirements and guidance materials, with the global objective of achieving effective, harmonized, and sustainable implementation of all security standards outlined in Annex 17 across all States.

This global industry security objective can only be achieved through close alignment of all relevant ICAO security reference documents and programmes. Continuous enhancement of Annex 17 provisions is essential for improving the effectiveness and economic sustainability of security measures implemented by industry stakeholders, and for strengthening the oversight functions carried out by regulators.

This working paper highlights potential areas for improvement in the work undertaken by ICAO bodies responsible for aviation security. It also presents relevant guidance materials, initiatives and position papers developed by IATA to support States and industry stakeholders in maintaining high-quality implementation of security standards.

Action: The Assembly is invited to:

- a) Encourage all Contracting States, particularly those actively involved in relevant ICAO bodies responsible for aviation security, to make extensive use of technical input from the industry to further develop provisions and to enhance safety and security, but also promote regular, efficient and economically sustainable international air transport operations.

<i>Strategic Goals:</i>	This working paper relates to Strategic Goals <i>Every Flight is Safe and Secure</i> and <i>Economic Development</i>
<i>Financial implications:</i>	It is not expected that there will be significant financial implications to ICAO, given this work can be developed by the existing working bodies. IATA is ready to support the developments required for addressing the proposed actions.
<i>References:</i>	

¹ English, Arabic, Chinese, French, Russian and Spanish versions provided by IATA

1. **EFFECTIVENESS AND ECONOMICAL SUSTAINABILITY OF SECURITY MEASURES**

1.1 Since the transition from the original ICAO Universal Security Audit Programme (USAP), launched in 2002, to the USAP Continuous Monitoring Approach (USAP-CMA) in 2013, the global sustainability indicators have fluctuated from 71,27% to 72,77%, with an average of 72,07% and a standard deviation of 0,53%. Furthermore, the latest USAP-CMA report (2024), in paragraph 3.3.2, highlights that fifteen (15) Standards from Annex 17 have not reached fifty (50) per cent of global indicative compliance. Notably, twelve (12) of these standards belong to Annex 17 Chapter 4 – *Preventive Security Measures*.

1.2 Albeit the USAP-CMA numbers, the operational fact is that most of preventive security measures have been successfully and sustainably implemented on a daily basis by most of the industry operators and entities, including External Service Providers (ESPs), across all States.

1.3 The foundational aims and objectives of ICAO, as outlined in Article 44 of the Chicago Convention, include not only the development of principles and techniques to enhance safety and security, but also the regular, efficient and economically sustainable development of international air transport. These goals can be effectively advanced through consideration of industry's proposals in relevant ICAO bodies. This is especially critical when advocating for the continuous updating of Annex 17 and associated guidance materials to address implementation challenges identified by both operators and regulators.

2. **AIRCRAFT OPERATOR SECURITY PROGRAMME (AOSP), SUPPLEMENTARY STATION PROCEDURES (SSPs) AND AVIATION SECURITY TRUST FRAMEWORK (ASTF)**

2.1 A key example of the need for continuous updates is the introduction of a distinction between Aircraft Operator Security Programme (AOSP) and Supplementary Station Procedures (SSPs) in Amendment 18 to Annex 17, which became effective in November 2022. AOSPs are developed by airlines to meet the national requirements of their State of the Operator. SSPs, on the other hand, should only be developed when the AOSP doesn't fully address the national requirements of the State(s) of the operations.

2.2 Although ICAO published public AOSP and SSPs guidance material² in June 2022, the relevant USAP-CMA Protocol Questions remained misaligned until their most recent adjustment in April 2025. This situation led to confusion in some States and the update of some provisions may still be required.

2.3 In parallel, IATA developed a range of guidance and position papers, including a video, all of which are available on IATA's public Aviation Security website³, particularly the Position Papers webpage⁴.

2.4 Beyond guidance material, IATA has also launched an initiative aimed at improving both the efficiency and security of the aviation industry by leveraging digital trust technologies, the Aviation Security Trust Framework (ASTF). It seeks to streamline the verification process of the authenticity and validity of aviation security documents, like the official acknowledgment of endorsement of AOSPs and SSPs by relevant authorities. Additional resources include a White Paper⁵, a dedicated IATA ASTF website⁶, and an Information Paper presented by IATA at the most recent Aviation Security Panel (AVSECP) meeting forecasting ASTF's scalable capabilities to other areas, ranging but not limited to, cargo security status, oversight auditing activities, or personnel / crew background checks.

² ICAO AOSP and SSP guidance: <https://www.icao.int/Security/SFP/Pages/AOSP-and-SSP.aspx>

³ IATA Aviation Security: <https://www.iata.org/en/programs/security/>

⁴ IATA Position Papers: <https://www.iata.org/en/programs/security/position-papers-press-releases/>

⁵ IATA White Paper on ASTF: <https://www.iata.org/contentassets/1998554ac6624b97a2de8418938eaade/aviation-security-trust-framework-whitepaper-2025.pdf>

⁶ IATA Aviation Security Trust Framework: <https://astf.iata.org/>

3. SECURITY INCIDENT REPORTING

3.1 Another example highlighting the need for ongoing updates to Annex 17 is Standard 5.1.6, introduced in 2018. This standard implies that any entity responsible for the implementation of the national civil aviation security programme must report, in a practical and timely manner, any “information concerning incidents of acts of unlawful interference and preparatory acts thereto” to relevant authorities.

3.2 In response, ICAO published public Incident Reporting Guidance and Taxonomy⁷, in June 2022, “on the implementation of a reporting system, and established a common taxonomy, in an effort to structure and harmonize the reporting processes of aviation security occurrences and incidents”.

3.3 The ICAO guidance clearly defines the types of “information” that should be reported. IATA complemented this effort by publishing position papers on its Position Papers webpage³. The most recent on the Reporting of Aviation Security Occurrences and Incidents⁸ outlines the expected reporting processes for industry stakeholders already engaged in occurrence and incident reporting for decades.

3.4 To avoid any potential confusion around Standard 5.1.6, specifically the distinction between the reporting acts of unlawful interference, including attempted or preparatory acts, normally performed by States to ICAO, and the reporting of security incidents by operators and entities to authorities, the wording of this standard needs to be revisited for ensuring effective implementation.

3.5 Globally effective, harmonized and economically sustainable systems for reporting security occurrences and incidents are essential. They not only enhance aviation security by enabling the detection of emerging threats and vulnerabilities through reporting, but also improve the timely sharing of critical information when serious incidents reported in one State could impact global supply chains or operations.

4. SECURITY MANAGEMENT SYSTEM (SeMS)

4.1 The examples outlined above reflect the broader, integrated approach to Safety and Security Management Systems as promoted by the IATA Operational Safety Audit (IOSA) program and the IOSA Standards Manual (ISM) applicable to all IOSA registered airlines. The Safety Management System (SMS) has gained strong international recognition, particularly with the creation of a new ICAO Annex 19 in 2013. Meanwhile, the Security Management System (SeMS) became a mandatory requirement for all IOSA registered airlines in the second edition of the ISM (ISM/2) in 2007.

4.2 In January 2025, the seventeenth edition (ISM/17) further advanced the SeMS framework by expanding its scope to include External Service Providers (ESPs) implementing most of the operational security measures via outsourcing arrangements. IATA shares extensive information and guidance material through its SeMS webpage⁹ and the SeMS Aviation Community¹⁰ created in 2022 to assist ESPs.

4.3 Finally, IATA has launched a formal SeMS Certification Program¹¹ designed to offer a structured framework that enables all aviation entities and organizations to proactively manage regulatory compliance, security risks, threats and vulnerabilities, while improving their security management system.

— END —

⁷ ICAO Incident Reporting Guidance and Taxonomy: <https://www.icao.int/Security/SFP/Pages/Incident-Reporting-Guidance-and-Taxonomy.aspx>

⁸ IATA Position Paper on the Reporting of Aviation Security Occurrences and Incidents: <https://www.iata.org/contentassets/1998554ac6624b97a2de8418938eaade/2025-reporting-of-aviation-security-occurrences-and-incidents-april-2025.pdf>

⁹ IATA SeMS webpage: <https://www.iata.org/en/programs/security/security-management-system-sems/>

¹⁰ SeMS Aviation Community (contact aviationsecurity@iata.org)

¹¹ IATA SeMS Certification Program: <https://www.iata.org/en/services/certification/operations-safety-security/security-management-systems-sems/>