POSITION PAPER

The Use of Surveillance in Civil Aviation Aircraft Cabin, Hold, and Body-Worn Systems

Version 1 – January 2026

Executive Summary

This paper seeks to establish a harmonized global understanding for the responsible and proportionate use of surveillance technologies in the specific context of international civil aviation operations. The intent is to balance the legitimate needs of safety, security, protection of staff and assets, and operational efficiency with the broader considerations of privacy, cost, human rights, and technological implementation and challenges.

The paper recognizes that surveillance systems are already widely deployed in many States and installed in various public transportation infrastructures. Surveillance systems are installed in airports, catering and cargo facilities, in some cases directly in aircraft holds, or as body worn devices designed to protect staff and overseas operations while on the ground.

For all these configurations, surveillance systems must be assessed not only for their technical and detection capabilities but also for their impact on people, the airline crew who operate in these environments, ground and airport staff who support daily operations, passengers and customers whose privacy rights must be safeguarded according to the local and national regulations in place.

Not forgetting the local authorities responsible for oversight and compliance of all measures implemented in the States of the operations (local stations), including the measures that may be included in operators' security programmes endorsed by the authorities of the State of the Operators.

By embedding these diverse technical, operational and legal perspectives, the paper promotes a holistic and integrated approach to what can be conceptually termed as a "*Surveillance Policy or Responsible Use of Monitoring Technologies Framework in the context of international civil aviation operations*", ensuring that implementation remains risk based, transparent, efficient and interoperable across jurisdictions while applied to civil aviation operations.

It further outlines the principles, governance structures, and recommended policy positions for States, regulators, and industry stakeholders to adopt when evaluating or deploying such technologies maintaining consistency with ICAO foundational aims and objectives as outlined in the Article 44 of the Chicago Convention (1944)[1], the goals of the UN Resolution 2309 (2016)[2], in particular for "the protection of the safety of their own citizens and nationals against terrorist attacks conducted against international civil aviation, wherever these may occur, in accordance with international laws", and with existing Standards and Recommended Practices (SARPs), data protection obligations, and the overarching goal of enhancing aviation safety and security without compromising fundamental rights or public trust.

[1] https://www.icao.int/convention-international-civil-aviation-doc-7300
[2] https://digitallibrary.un.org/record/842640?v=pdf

This paper does not address technologies installed by aircraft manufacturers or aircraft operators for the sole purpose of meeting ICAO Annex 6 flight deck access control requirements. Specifically, it excludes Flight Deck Door Monitoring Systems of Cockpit Door Surveillance Systems, which are proprietary technologies implemented to provide flight crew with a means to verify and identify individuals requesting entry before the cockpit door is opened. As these systems serve a defined safety and security access control function, not broader surveillance or monitoring purposes, they fall outside the scope of this policy discussion.

Background

Recent years have seen renewed proposals by certain States to mandate onboard surveillance systems, including continuous video recording within passenger cabins, galleys, and cockpits. These initiatives highlight significant safety, technical, and legal concerns*:*

- **Airworthiness and Certification** - Retrofitting surveillance systems on aircraft requires design and certification approval by the State of Registry, consistent with Articles 17, 33, and 37 of the Chicago Convention.

- **Safety Protections** - International rules restrict cockpit voice and image recordings to use only in accident investigation, prohibiting other uses.

- **Risk Based -** ICAO Annex 17 requires that national aviation security measures be founded on risk, and proportionality, and where urgent or additional in nature, pre-decisional consultation, coordinated and time sensitive. In addition, operators must "*conduct effective risk assessments relating to their operations*"[3], which could be identified as "operational risk assessments", that may force operators to deploy additional "operational security measures", including surveillance systems, with the approval of the local authorities of the States where operations are conducted.

- **Data Protection -** Video surveillance captures personal data of passengers and crew, invoking data-protection and privacy obligations under regimes such as the General Data Protection Regulation (GDPR).

- **Operational Feasibility** - Fleet rotation across multiple jurisdictions complicates compliance with divergent national requirements, in particular during the flight phase (jurisdiction of the State of the Operator), while overflying other territories (jurisdiction of the states being overflown), and during stops (jurisdiction of the State of the operations).

- **Operational Performance -** When equipment and systems that were primarily developed for surveillance applications on the ground are deployed outside their initial intended operational environments, such as in confined aircraft cabins in flight with limited light conditions mainly for safety-related cabin lighting requirements. The detection capabilities of such systems could be drastically reduced, thus generating unacceptable levels of false alarms that could be immediately responded to with disproportionate operational responses (diversions for example).

[3] ICAO Annex 17 Standard 3.1.5 - *Each Contracting State shall establish and implement procedures to share, as appropriate, with relevant airport operators,* ***aircraft operators****, air traffic service providers or other entities concerned, in a practical and timely manner, relevant information* ***to assist them to conduct effective security risk assessments relating to their operations****.*

These issues underscore the need for a consistent international understanding and frameworks that facilitate legitimate national security objectives while respecting and protecting efficient civil aviation safety and security operations, national sovereignty, and individual rights.

Policy Objectives

1. **Promote Global Consistency -** Prevent unilateral civil aviation surveillance mandates that undermine ICAO primary goals, international standards and bilateral Air Services Agreements.

2. **Ensure Safety and Airworthiness -** Require operational certification from appropriate competent authorities before any camera system installation in the civil aviation environment.

3. **Protect Privacy and Human Rights** - Apply privacy by design, transparency, and data minimization principles to all surveillance uses.

4. **Adopt a Risk Based Framework** - Civil aviation surveillance should be justified through documented national and operational risk assessments and used only when less intrusive alternative measures are insufficient or inadequate.

5. **Foster Cooperation and Mutual Recognition -** Encourage dialogue between States, ICAO, and industry to develop globally accepted standards, harmonized measures and guidance.

Policy Principles

a. Legality and Proportionality
Civil aviation surveillance measures deployed within a flight operations environment by aircraft operators must comply with applicable laws of all affected jurisdictions and serve a clearly defined, lawful purpose, and be safeguarded against use for any purpose other than that for which they were originally intended.

b. Safety Integrity
No measure shall compromise aircraft safety systems or conflict with aircraft certified configurations.

c. Data Governance and Retention
Collected data shall be encrypted, access controlled, and retained only for as long as necessary, typically no more than 30 days, unless linked to an active investigation by authorities.

d. Privacy and Transparency
Operators must inform passengers and crew through notices and ensure access rights consistent with applicable data protection laws.

e. Oversight and Accountability
Each deployment requires internal approval based on a risk assessment, Data Protection Impact Assessment (DPIA), and airworthiness validation.

Regulatory and Legal Context

- **Chicago Convention (Articles 17, 33, 37)** - Contracting States must recognize other States' certifications; extraterritorial mandates breach uniformity principles, including the provisions contained in related technical Chicago Convention Annexes (such as Annex 6 – Operation of Aircraft and Annex 17 – Aviation Security)
- **Data Protection Law (e.g., GDPR) -** Personal data from surveillance cannot be transferred or processed without legal basis and safeguards.
- **Human Rights Treaties -** Surveillance must respect rights to privacy and dignity.
- **United Nations Resolutions** - International resolutions such as the UNSCR 2309 (2016) should also be considered

Industry Position

IATA fully respects the sovereign right of each State to regulate aircraft operating solely within its own jurisdiction.

However, this respect for sovereignty does not extend to unilateral civil aviation surveillance mandates that impose configuration requirements, data obligations, or operational burdens on foreign operators. Any such measure constitutes an extraterritorial action incompatible with the mutual recognition provisions of Articles 17, 33, and 37 of the Chicago Convention, and creates direct conflicts with safety, certification, privacy, and data-protection regimes in other jurisdictions.

IATA therefore does not support the unilateral imposition or expansion of mandatory onboard surveillance technologies.

While opposing unilateral mandates, IATA supports the collaborative development of global guiding principles through ICAO and appropriate regional mechanisms, recognizing that any future consideration of surveillance technologies must be risk-based, proportionate, privacy protective, and technically and operationally feasible.

States and aircraft operators that elect to use such technologies on a voluntary basis must do so within a documented risk justification framework, with privacy protections embedded by design and subject to strict limitations on activation, data access, retention, and evidentiary use.

To prevent misuse or unlawful disclosure, IATA requests that any State exploring such technologies provide explicit and transparent rules governing data retention periods, access authorities, permitted investigative uses, and cross-border data transfer safeguards. Where technical, financial, legal, or certification barriers exist, IATA will advocate for exemptions, implementation delays, or alternative measures to avoid operational disruptions or regulatory fragmentation.

IATA's position is clear, sovereign choices remain the prerogative of individual States, but no State may impose civil aviation surveillance requirements on foreign aircraft without at least ICAO level consensus. Ideally, ICAO should be the forum of discussion wherever unilateral measures threaten

uniformity, undermine international legal obligations, or compromise the safety and rights of passengers and crew.

Implementation Framework

- **Governance -** Operators establish Surveillance Steering Groups with Security, Safety, Legal, and Engineering representation.
- **Documentation -** Maintain operational procedures, retention schedules, and audit logs.
- **Training** - Provide instruction on lawful use, privacy awareness, and data handling.
- **Audit** – Conduct annual reviews to ensure ongoing compliance with policy and regulation.

Jurisdictional and Regulatory Shifts: Doors Open, In Flight, and State Requirements

Civil aviation surveillance on board aircraft does not operate within a single legal or security regime. The same surveillance device, on the same flight, will pass through different legal environments as the aircraft moves from turn-around to taxi, to en-route and back to gate.

This complexity is not academic – it directly affects who can demand access to surveillance data, how data is collected and stored and by whom, how crew and passengers are protected, and how incidents are handled.

Doors Open – Territorial State Dominance

When an aircraft is on the ground with doors open (boarding, disembarkation, servicing), the State territorial jurisdiction, laws and authorities are in the strongest position:

Local police, border control, airport authority and national regulators can assert jurisdiction over:

- criminal conduct, data protection and workplace surveillance law, labor protection for ground staff and crew on duty within their territory.

Surveillance systems active in this phase can be:

- seized or accessed under local legal process,
- subject to local privacy rules and evidence law,
- exposed to local disclosure rules in criminal or civil proceedings.

Supply-chain actors (caterers, cleaners, maintenance, security contractors) operate under the territorial State's regime, increasing the risk of:

- covert access to equipment and data, tampering or substitution of devices, informal extraction of footage by local officials or contractors.

Note that all these operational elements should be reflected in the Aircraft Operators Security Programmes (AOSPs) or the Supplementary Station Procedures (SSPs) produced by aircraft operators. The AOSPs are endorsed, verified, and/or approved by the authorities of the States of the Operators, while the SSPs are only produced if the AOSPs don't not already cover the local

requirements, and are endorsed and/or approved by the authorities of the States of the operations. The legal implications, and responsibilities, with the use of civil aviation surveillance systems in different jurisdictions, should not be dismissed.

Doors Closed / In Flight – Tokyo Convention Regime

Once doors are closed and the aircraft is "in flight" under the Tokyo Convention (1963) definition (from the moment all external doors are closed after embarkation until one door is opened for disembarkation), the primary jurisdiction shifts to the State of registration of the aircraft.

- Primary criminal jurisdiction over offences and acts on-board rests with the State of Registration or the State of the Operator.
- The commander's authority to restrain, disembark, and report unruly or unlawful acts derives from this convention framework.
- Other States (State of landing, State of operator's principal place of business, etc.) may have limited rights to intervene, but the baseline remains - the aircraft is legally "under" the State of Registration (or State of the Operator) while in flight.

When surveillance is active in this phase

- Data generated in flight is, in principle, subject to the State of Registration's law, particularly:
    - criminal law,
    - data protection/privacy rules,
    - rules on use of recordings as evidence,
    - protections to Cockpit Voice Recorder (CVR) / Flight Data Recorder (FDR) confidentiality in some regimes.
- But, upon landing, territorial authorities will often assert claims over that same data, leading to:
    - conflicting demands (State of Registration or State of the Operator vs States of the operations with transfer/transit and arrivals),
    - pressure on crew and operators to release footage,
    - Procedural conflicts may lead to operational impacts, including delays if local authorities withhold aircraft clearance.
    - potential breaches of data-protection or labour rights if operators comply without lawful basis.

Conclusion and Recommendations

This paper calls for States and industry to pursue a harmonized, risk-based approach to onboard surveillance. Surveillance must never compromise safety, security, privacy, or international legal order. Any requirement for mandatory civil aviation surveillance measures going beyond the current cockpit monitoring standards should first undergo multilateral consultation within ICAO and through its respective safety, security and legal Panels. This ICAO process may lead to the introduction of new international standards in different Annexes, that then could drive the development of appropriate harmonized guidance material for States and industry stakeholders.

Annex

Proposed Definitions & Classification of Civil Aviation Surveillance Technologies in Civil Aviation

To ensure clarity, consistency, and appropriate governance across jurisdictions, surveillance technologies used in civil aviation operations are classified into four categories. Each category reflects an operational purpose, technical configuration, and the degree of governance required.

Cabin Monitoring Systems (Fixed)

- Fixed, aircraft installed imaging or recording devices located within passenger cabins. These systems support incident documentation, safety assurance, security event review, and post-incident investigation. They do not include cockpit image or audio recording as per ICAO Annex 6.

Cargo / Hold Monitoring Systems (Fixed)

- Permanently installed devices within aircraft cargo compartments intended to monitor cargo integrity, detect tampering/pilferage, identify anomalies, or support regulatory compliance. These systems must comply with airworthiness and installation requirements but do not require explosion-proof housing unless mandated by aircraft design criteria.

Body-Worn Monitoring Devices (Portable)

- Wearable recording devices used by authorized staff such as airline security officers, safety personnel, or customer-facing teams to document incidents or support evidence gathering in specific, predefined operational circumstances. Their use must be visible, limited to incident-triggered activation, and compliant with labour and privacy laws.

Temporary or Mobile Surveillance Devices (Non-Fixed, Battery-Powered)

- Portable, removable, and self-powered devices deployed for time-limited periods in response to a specific operational, safety, or security need. These devices are not integrated with aircraft systems and must be used in accordance with risk-based triggers, clearly defined deployment periods, and strict transparency and privacy safeguards. They are intended for flexible, short-term monitoring in select areas that do not require permanent installation.