# EXPIRED "IDENTIFICATION PERMITS" - IMPLICATIONS TO AIRLINE OPERATIONAL SECURITY

## The issue and position

Crew members performing aircraft access control are required to verify ground staff identification permits - prior to accessing the cabin of an aircraft - that grant access to the security restricted area of an airport. Aircrew are required to visually inspect the "identification permits", by performing at a minimum a photograph to face check and verification to the "expiry date".

Should crew members performing verification identify an "expired date" on the identification permit, they have a reason to believe that unauthorized access to the cabin of the aircraft is or has been conducted and appropriate mitigating actions should be undertaken.

As reported to IATA, member airlines have been repeatedly confronted with notifications from certain airport operators and/or issuing authorities, advising in advance of the extension to identification permits' expiry dates, without reflecting date changes to the expired identification permit.

In this context, aircrew are required to make a discretionary judgements based on perceived risk in order to not to compromise the timely aspect of ground operations. Moreover, in the event aircrew do permit aircraft cabin access to an expired identified permit holder, the level of visual supervision required by aircrew thereafter – contingent on-ground departure phase – displaces aircrew priority from other areas to delivery safety and service.

## Background information

ICAO Annex 17 requires the implementation of an identification system and access control to the security restricted area of an airport, and aircraft.[1]

These standards are supported by the relevant guidance contained in ICAO Doc. 8973 points 11.2.4.4, 11.2.6.9 and 11.2.6.18, as well as, Annex 1 – National Civil Aviation Security Program Model, Part D recommending "…*placing the expiry date on the identification permit"*.

In the context of the situation described, it is necessary to also reference, ICAO Doc. 8973 point 11.2.7.1 stating *"…good practice is to update a background check every time airport security identification permits need to be renewed".*

Additionally, the IOSA industry standard reflects ICAO Annex 17 in terms of aircraft protection.[2]

Both conditions, "expiry date" and "background check" are inextricably linked and thus provide a compliant level of security control when implemented appropriately. Renewal of the identification permit ought to be predicated on the basis that a successful background check has been carried out by the issuing authority.

In the context of association between identification permits' renewal and background checks', by implication member airlines are rightfully concerned that recurrent airport staff background checks' are not being carried out appropriately. This consequently may result in an increase of risk to airline operations when international standards aim to manage the vulnerabilities associated with "trusted persons" who carry out airside functions.

[1] **ICAO Annex 17, 4.2.3 Each Contracting State shall ensure that identification systems are established in respect of persons and vehicles in order to prevent unauthorized access to airside areas and security restricted areas. Identity shall be verified at designated checkpoints before access is allowed to airside areas and security restricted areas.**

**ICAO Annex 17 4.2.5 Each Contracting State shall ensure that the movement of persons and vehicles to and from the aircraft is supervised in security restricted areas in order to prevent unauthorized access to aircraft.**

[2] **IOSA SEC 3.1.2 The Operator shall ensure measures are in place to control and supervise personnel and vehicles moving to and from the aircraft in security restricted areas to prevent unauthorized access to the aircraft.**

The requirement to conduct recurrent background checks are codified in IOSA SEC 1.5.3 Standard and in ICAO Annex 17 4.2.4 Standard and 4.2.9. Recommendation.

Secondly, since an expiry date is indicated on the identification permit, airlines are required to oppose "extension practices" – as described above by airport and issuing authorities – as they prevent aircrew from effective implementation of aircraft access control.

## Proposed solution

Given the current threat landscape (especially the "insider threat" aspect) airports are requested to ensure recurrent background checks are successfully completed for every identification pass holder. If recurrent background check is performed as a part of identification permit renewal this process should be scheduled and performed enough in advance of the identification permits exchange (renewal). IATA recommends a set of additional practices in the scope of insider threats in its position paper.[3]

IATA to adopt a data-driven, risk-based intervention approach. Airline security incident taxonomy[4] has been updated to include specific event occurrence.

The points raised in this position paper may be used as an airline letter for intervention to identified risks and vulnerabilities to IATA member airline operations.

[3] IATA Position Paper on Insider Threat.

[4] IATA Security Group developed security reporting taxonomy which should be considered when reporting insiders. If no standardized report for reporting security occurrences exists IATA report form template may be used.