International Civil Aviation Organization

THE FIRST MEETING OF THE ANS INFORMATION ASSURANCE (ANSIA) TASK FORCE (ANSIA TF/1)

(Bangkok, Thailand, 28 – 30 January 2026)

Agenda Item 5: Trust Framework implementation practices sharing by States

Agenda Item 6: Issues and Challenges in implementation

ADVANCING TRUST IN DIGITAL AVIATION SYSTEMS THROUGH NATIONAL IMPLEMENTATION PRACTICES, POLICY ALIGNMENT, AND IMPLEMENTATION CHALLENGES

(Presented by The Philippines)

SUMMARY

This paper presents national implementation practices and identifies key issues and challenges in establishing trust in digital aviation systems. It describes how national mandates, policies, and ongoing modernization initiatives support the objectives of the ICAO Trust Framework for digital aviation services. It also outlines policy alignment, strategies, institutional measures to enhance trust, and practical challenges encountered during implementation. It aims to contribute to regional knowledge-sharing and support harmonized Trust Framework development within the APAC region.

1. INTRODUCTION

1.1 The increasing digitalization of aviation systems and the expansion of cross-border information exchange have made trust a foundational requirement for safety, security, and operational continuity. Initiatives such as SWIM, digital aeronautical information management, and integrated surveillance and meteorological services rely on confidence in the identity of participants, integrity of data, availability of systems, and effectiveness of governance arrangements.

In the Philippines, trust in digital systems is established through a clear national mandate led by the concerned department. The National Cybersecurity Plan provides the strategic framework for protecting cyberspace, securing critical information infrastructure, and strengthening national and international cooperation. These policies are particularly relevant to aviation, which is recognized as a safety-critical and mission-critical sector.

This paper presents how the Philippines operationalizes Trust Framework concepts through national policy, regulatory instruments, and coordinated programs, and how these practices align with ICAO cybersecurity and safety management expectations.

2. DISCUSSION

2.1 National Policy and Regulatory Alignment

At the national level, Trust Framework implementation is supported by cybersecurity and digital governance mandates. A key reference is the National Cybersecurity Plan (NCSP), which establishes strategic pillars for protecting critical information infrastructure, strengthening governance, and enhancing cyber resilience across government and essential sectors, including aviation.

Complementing the NCSP are the department circulars and memoranda, which provide implementing guidance on areas such as:

- Information security management systems (ISMS),
- Network and system hardening,
- Identity and access management,
- Incident reporting and coordination.

These policies collectively provide the governance foundation necessary to support Trust Framework principles, particularly in identity assurance, data protection, accountability, and risk-based security management.

2.2 Institutional Trust Framework Implementation Practices

From an operational perspective, the aviation authority has initiated a series of measures that contribute to a national Trust Framework posture, even in the absence of a formally declared Trust Framework Instance (TFI). These measures include:

- Enabling consistent security policy enforcement across critical systems through enhanced endpoint protection management,
- Patching and vulnerability management programs,
- Improving visibility, incident detection, and analysis,
- Strengthening identity control, access governance, and accountability across operational systems.

These initiatives directly support Trust Framework objectives related to system integrity, identity trust, and continuous monitoring, and are particularly relevant to interconnected environments.

2.3 Issues and Challenges in Implementation

Despite ongoing progress, several challenges have been identified during implementation:

- Legacy systems and infrastructure constraints, which were not originally designed for modern trust-based architectures,
- Resource and skills limitations, including the need for specialized cybersecurity and PKI expertise,
- Coordination across stakeholders, especially where trust relationships span multiple organizations or sectors.

These challenges show the importance of phased implementation, regional cooperation, and continued engagement with ICAO-led Trust Framework development activities.

2.4 Conclusion

The establishment of trust in digital aviation systems is a progressive process that relies on strong policy foundations, practical cybersecurity controls, and institutional commitment. National alignment with

cybersecurity strategies such as the NCSP, supported by the assigned department and regulatory instruments, provide a solid basis for Trust Framework readiness. While challenges remain, ongoing system upgrades and governance improvements demonstrate tangible progress. Continued sharing of implementation practices and challenges within the APAC region will be essential to achieving harmonized, interoperable, and resilient Trust Frameworks in support of future aviation digitalization.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matter as appropriate

– – – – – – – – – – – – –