



**WORKING PAPER**

**THIRTEENTH AIR NAVIGATION CONFERENCE**

**Montréal, Canada, 9 to 19 October 2018**

**COMMITTEE A**

**Agenda Item 5: Emerging issues**

**5.4: Cyber resilience**

**CONSIDERATIONS ABOUT CYBERSECURITY IN AVIATION**

(Presented by the Civil Air Navigation Services Organisation (CANSO),  
International Coordinating Council of Aerospace Industries Associations (ICCAIA),  
the International Federation of Air Traffic Controllers' Associations (IFATCA) and  
the International Federation of Airline Pilots' Associations (IFALPA))

**EXECUTIVE SUMMARY**

This working paper presents the CANSO, ICCAIA, IFATCA and IFALPA positions regarding the need, as one of the necessary means to increase civil aviation cybersecurity resilience, to develop a global framework, harmonized between all aviation stakeholders, for trusted and secure digital information exchange in aviation (an Aviation Trust Framework), in support of global aviation modernization. Specifically, this paper supports the strategic principles proposed in the ICAO Secretariat paper AN-Conf/13-WP/27 and the need to develop the policy and governance requirements to enable a secure, capable and affordable implementation. It is understood that the technical implementation details will be worked out once a formal ICAO forum is established.

**Action:** The Conference is invited to agree to the recommendation in paragraph 3.2.

**1. INTRODUCTION**

1.1. The civil aviation sector as a whole is rapidly changing with the adoption of new operational concepts supported by extensive connectivity and new technology to improve air traffic safe and orderly operations. These modernization efforts that seek to improve aviation operations promise to yield significant benefits through airspace optimization. As the demand grows for more interconnected, dynamic and reliable data exchange, the associated benefits also come with added cybersecurity risks and potential for cyber-attacks to safety, air navigation capacity, efficiency, and operational capabilities.

1.2. In response to these changes, a new and globally harmonized end-to-end approach, supporting the needs to increase cyber resilience of the civil aviation system, must be pursued, and it must be done in a manner that supports all civil aviation stakeholders. This approach should consider governance and technical aspects, and should leverage commercially available technologies and methods to meet the demands of speed and affordability for the industry. As future aviation systems become increasingly

<sup>1</sup> Arabic, Chinese, English, French, Russian and Spanish versions provided by ICCAIA.

complex, modern methods and strategies will be required to operate as a global environment integrating all the regional or local specificities. This challenge cannot be functionally decomposed into the classic elements of aircraft/air navigation services (ANS)/aerodrome, but must be treated as an end-to-end integrated solution, considering the horizontal and crosscutting capabilities and cybersecurity risks.

1.3. Civil aviation should adopt, amongst other elements, a global framework, harmonized and agreed between all aviation stakeholders, for trusted and secure digital information exchange in aviation (an Aviation Trust Framework) considering the geo-political and financial sensitivities of the aviation community.

## 2. DISCUSSION

2.1. In the context of extensive connectivity between civil aviation system actors, the objective of resilience identified in the Global Aviation Security Plan (GASEP) and identified in the Secretariat paper on the subject, will not be upheld without the development of a trust framework identifying the key principles to enable trust in the aviation infrastructure and the information exchanged over that infrastructure (identity, integrity, confidentiality and availability). A trust framework is a key enabler to implement an effective and efficient end-to-end integrated solution across all connected stakeholders. Today stakeholders expend significant time and money to manage external interfaces, and in many cases, have limited understanding of the risk each external connection presents. The following considerations highlight critical dimensions of trust and inter-operability that should be discussed and decided upon in order to capture the benefits while managing the risks:

### Governance Considerations:

#### a) Establish minimum cybersecurity compliance requirements

Identify the minimum level of acceptable cybersecurity requirements and common standards to ensure greater integrity. A cybersecurity risk management system must be at the core to the approach, and needs to be complemented with open industry standards and a compliance approach to achieve a trustworthy framework.

#### b) Establish inspection or methods of validation

Cybersecurity needs a complementary approach to the physical security compliance evaluations performed today. Cybersecurity risk continually evolves, and so continual validation of compliance to cybersecurity operating standards will be needed. Mutual cooperation between connected partners to validate and manage both individual and joint end-to-end risk will be required as stakeholders become more integrated.

#### c) Legal Policies

Today, industry follows physical security standards. Cybersecurity risk evaluation and compliance validation should be added to existing processes, and organizations should maintain acceptable cybersecurity compliance.

Technical Considerations:

All stakeholders need to be able to build and operate their system in ways that are most effective and efficient. As the community becomes more integrated, technical solutions can become complex and costly. Modernizing the technical structure and standards implemented by all stakeholders should be tailored to each individual operating environment, with standardization enabling interoperability and connectivity between these stakeholders. The framework should:

- a) Support growing demand for interconnectivity utilizing newer technology, promoting commonly used technical methods, like digital certificates, and agreed upon attributes to establish mutual trust.
- b) Foster a foundation for trust between stakeholders following a common framework with modern standards, protocols and commercial technologies.
- c) Support the establishment of a common operating environment for inter-connectivity and digital information exchange. Leverage concepts like the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network used by banks worldwide and lessons learned from the financial industry.
- d) Reduce operating cost across the global community for many stakeholders and create opportunities for other markets.
- e) Consider adaptability and modularity of capabilities as a means to rapidly update and adjust the framework according to technology evolutions and to keep pace with cyber attackers.

2.2. Standardization creates a common level of trust in aircraft operations and air traffic services across the globe. The civil aviation community does not currently have the necessary standards in place for the future to ensure mutual trust and protection for digital information exchange, the methods of interconnectivity, or the process to protect against mutual risk. Establishing a common framework for information exchange using standards that are validated by all parties, will help ensure risks are managed and provide the needed level of confidence.

2.3. With a common trust framework, the enabling key civil aviation initiatives identified in the ICAO *Global Air Navigation Plan* (GANP, Doc 9750) should be achieved quicker, through reduced complexity and cost, while enabling the needed future capabilities:

- a) global integration (e.g. SWIM, FF-ICE, etc.) of secure and trusted digital communications between civil aviation actors;
- b) modernization of the existing trust frameworks to interoperate with legacy frameworks;
- c) federate control of new entrants from onerous legacy infrastructure; and
- d) leverage identity, integrity and confidentiality for other capabilities (e.g. operational and mission data supporting greater efficiency).

2.4. The trust framework must take into account all stakeholders, who may be at different levels of maturity in governance structure or technical capabilities. When implemented, stakeholders must be able to smoothly transition traditional elements over time, while new market entrants will need to implement quickly and affordably with unique operational and business objectives. The method of transition must provide a common foundation that all stakeholders can build towards and implemented in phases to reduce the impact to stakeholders based upon the maturity of the organization. All must support safe and seamless integration within the air space.

### 3. CONCLUSION

3.1. The Civil Air Navigation Services Organisation (CANSO), International Coordinating Council of Aerospace Industries Associations (ICCAIA), International Federation of Air Traffic Controllers' Associations (IFATCA) and International Federation of Air Line Pilots' Associations (IFALPA) promote the need for the development of a globally coordinated aviation trust framework for digital information exchange as a key enabler for developing a future cyber-resilient civil aviation ecosystem. Considering the horizontal and crosscutting capabilities and cybersecurity risks, this challenge cannot be functionally decomposed into the classic elements of airplane/ANS/aerodrome, but must be developed as an end-to-end integrated solution.

3.2. The Conference is invited to agree to the following recommendation:

#### **Recommendation 5.4/x – Cyber resilience**

That the Conference:

- a) request ICAO to establish a formal project involving States and international organizations in the development a globally harmonized and accepted trust framework addressing the objectives detailed in this paper; and
- b) request ICAO to develop a roadmap, with industry engagement and inclusion within the GANP, for the development of emerging technology enablers to address the future evolving cybersecurity needs of civil aviation (e.g. blockchain, cloud services, and other evolving technologies).

— END —