International Civil Aviation Organization

WORKING PAPER

A41- WP/64[1]
EX/33
22/7/22

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

INTEGRATION AND COORDINATION OF ICAO CYBERSECURITY STRATEGIES AND WORKPLANS

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

EXECUTIVE SUMMARY

Cybersecurity in civil aviation remains an incremental area of pointed interest for ICAO, States and industry. The focus remains not only on identifying and reducing cyber threat and risk that aims to interfere with digital systems but provide an international framework in the provision of safe technology innovation that adopts key principles such security by design for the aerospace supply chain.

This paper presents the need for an integrated and coordinated approach in the provision of cybersecurity by the new formed Ad-Hoc Cybersecurity Coordination Committee (AHCCC). Noting that the proposals stemming from technical Panels and sub groups, which may impact Standards and Recommend Practices (SARPs), and other requirements, are reflective of the transversality of this discipline, within the multitude of ICAO Annexes, Documents and Manuals.

Action: The Assembly is invited to request that the Council:

a) request the Council to ensure all ICAO working bodies, to jointly create a cross-discipline and multi-step concerted approach in the integration of cybersecurity provisions and other requirements, based on Security by Design; and
b) request the Council to recognize the potential impact of the introduction of new generation of interconnected and innovative technologies and associated supply chains that are not bound by civil aviation regulations and SARPs.

Strategic Objectives:	This working paper relates to the Strategic Objectives: *Safety*, *Security and Facilitation*, and *Air Navigation Capacity and Efficiency*.
Financial implications:	The cost of developing, coordinating and processing new provisions and guidance materials that would be delivered by industry to ICAO.
References:	Doc 10140, *Assembly Resolutions in Force (as of 4 October 2019)* Doc 10108, *Aviation Security Global Risk Context Statement* Resolution A40-10 on *Addressing Cybersecurity in Civil Aviation* *Aviation Cybersecurity Strategy* *Cybersecurity Action Plan*

[1] Submitted by IATA in English, Arabic, Chinese, French, Russian and Spanish.

1. INTRODUCTION

1.1 At the 40th Session of the ICAO General Assembly (2019) Resolution A40-10 was adopted – *Addressing Cybersecurity in Civil Aviation*. In essence the Resolution empowered the Secretary General to continue to ensure that cybersecurity matters are considered and coordinated in a crosscutting manner through the appropriate mechanisms in the spirit of the ICAO Aviation Cybersecurity Strategy (2019).

1.2 The ICAO Aviation Cybersecurity Strategy proposes a series of principles, measures and activity's and pragmatically identified clear coordination actions through the follow up ICAO Cybersecurity Action Plan (CyAP) (2019), for addressing cyber threats and the elements required to increase the posture of international civil aviation resilience towards digital safety, security and trust.

1.3 In 2022, the ICAO Council adopted the creation of the Ad-Hoc Cybersecurity Coordination Committee (AHCCC) and two separate Panels, under two different Committees. This notably underscores ICAO and the Council's focus on the criticality of strategic aviation cybersecurity. The new Cybersecurity Panel (CYSECP), as approved by the Aviation Security Committee during the 225th Session on 24 January 2022, held its first meeting in May 2022. The previous achievements of the SSGC were noted by the CYSECP, and a workplan was proposed, supplementing the need for internal and international coordination. Furthermore, the Air Navigation Commission (ANC) created the Trusted Systems Panel (TSP) reinforcing perspectives of cross-coordination between ICAO Bureaus, Committees and technical Panels.

2. DISCUSSION

ICAO Coordination on Cybersecurity

2.1 It is widely noted that aviation cybersecurity is a transversal and an integrated discipline by nature. As such the role of the AHCCC going forward is critical to ensure coordinated strategic direction tying together the work plans and activities of several ICAO related efforts to ultimately safeguard aviation against all forms of digital interference whilst supporting safe technological innovation.

2.2 Inherently, SARPs and guidance derived from Documents often relate to States achieving compliance against international obligations laid out across the 19 Annexes'. Therefore, it is paramount that the AHCCC ensure coordination via structured and efficient governance.

2.3 The below describes a number of efforts in connection to the AHCCC:

a) trusted Systems Panel activities are based on the foundations for next generation of air mobility and touch the development of a concept of operations and governance of such a framework;

b) the Cybersecurity Panel establishes activities that consider the introduction or proposals to change/modify existing Annexes, Documents, and Manuals in the provision of cybersecurity;

c) information Management Panel in its Procedures for Air Navigation Services – Information Management (PANS-IM) are expressing certain information security requirements, as well as other efforts, like the current drafting of the Document 9896 rev. 3, on the implementation of Internet Protocol Services on Aeronautical Telecommunication Network, which also introduces cybersecurity requirements in its manual;

d) modifications are also proposed to the Safety Management Manual (Doc 9859);

e) noting the coordination of Universal Security Audit Programme (USAP) results for Annex 17 cybersecurity related SARP as referenced by A41-WP/22 presented by the Council of ICAO; and

f) noting the work of the Research Sub-Group on Legal Aspects (RSGLA) and the Secretariat coordination with the Legal Committee, as reference by A41-WP/22 presented by the Council of ICAO.

2.4 Over time, integrating cybersecurity requirements and provisions across different Annexes and Documents will be complex. As a result, there may be a need to evaluate the creation of a new Annex to lower the complexity of integration and ensure SARPs are developed transversally to address measures that mitigate intentional and/or non-intentional events and even more so, threats that may lead to secondary/cumulative safety or security affects not necessarily immediately known as a form of digital interference.

Digital Transformation integration

2.5 Ongoing evolution of Digital Transformation in several areas is taking place resulting in more connected technologies such as predictive aircraft maintenance, artificial intelligence and/or machine learning based decision making, edge-computing, open architecture, and, “Over-The-Air” updates of critical telecommunication systems.

2.6 The latest Air-Mobility concepts are resulting in new and efficient technologies. However, aerospace supply chains are not necessarily regulated by traditional national civil aviation regulations and standards. The new supply chains introduce opaque opportunities for potential vulnerabilities to be introduced to an already complex operating environment, where the cyber-attack surface, once limited to legacy systems, is now extended to unknown interlinked technologies. Overall, emerging interconnectivity and increasing dependencies require clear aerospace regulatory structure that supports ongoing airworthiness and aircraft certification.

2.7 Principles in security by design is a part of a cybersecurity policy approach that was noted by the ICAO Aviation Cybersecurity strategy. In this connection, work plans that aim to digitally safeguard industry and support next generation technologies, innovative products and services need to be agnostic and address the whole-of-civil aviation system. It is not only limited to supporting a Trust Framework concept or proposing Amendments to Annexes and Documents, but also an overall cross-discipline workplan in a multi-stage approach.

3. CONCLUSION

3.1 International aviation cybersecurity policies and obligations that enable regulated operators and their supply chains to achieve an efficient return on investment is critical to the sustainability of the aviation sector. Additionally, so is the need for ICAO and States to support international efforts that enable industry to innovate and increase the resilience of civil aviation over new supply chains. It is imperative to promote a Secure by Design approach, that is cross-discipline and multi-phased in nature and thus integrate provisions and requirements in a universal workplan, under the purview of the AHCCC, across the ICAO Panels, Work and Study Groups.

3.2 A secure by Design led workplan would establish the essential baseline of an integrated cyber-resilient, agile and innovative ecosystem, in order to reduce the frequency and impact of cyber-attacks against States and industry that could have an impact on safety, and the wider international civil aviation industry.

— END —