



WORKING PAPER

FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

- Agenda Item 4: Hyper-connectivity of air navigation system**
4.2: Cybersecurity and information system resilience

**USING AGILE METHODOLOGIES TO TIGHTEN
THE CYBERSECURITY POLICY GAP**

(Presented by the United States)

EXECUTIVE SUMMARY

The discipline of cybersecurity has crosscutting implications across every aspect of the system as it has implications across every aspect of the system, including people, processes and technologies. New technologies are emerging that will have a profound effect on the capacity and efficiency of civil aviation. The benefits of these new technologies exacerbate the challenges to cybersecurity defenses as threat actors will also take advantage of them to improve their means and methods of attack. Considering the nature of cybersecurity, innovative and more agile ways are needed to accelerate how ICAO Cybersecurity guidance material is provided to ICAO Member States and aviation stakeholders.

Action: The Conference is invited to agree to the recommendation in paragraph 3.

1. INTRODUCTION

1.1 The aviation ecosystem is a unique global operational system of systems, services, processes, technologies, and people that are holistically connected to transport passengers and cargo safely and securely non-stop. A compilation of contributors who collectively comprise this ecosystem is shown in **Figure 1**.

1.2 Cybersecurity, like safety and physical security, is a crosscutting discipline that stretches across the aviation ecosystem to protect and preserve its ability to function. Cybersecurity goes further to provide urgent protections to defend aviation systems and services against threats that are dynamic (e.g. malware), unpredictable (e.g. zero-day events) and able to rapidly proliferate impact across the ecosystem (e.g. distributed denial of service attacks). **Figure 2** shows that cybersecurity is embedded in all components of the aviation ecosystem. When all these components, including cybersecurity are integrated seamlessly, safety and efficiency are achieved.



Figure 1. The components of systems, services and technologies forming the aviation ecosystem

1.3 New and advanced technologies, like generative artificial intelligence (AI), quantum computing (QC) and biometrics are being integrated into the aviation ecosystem to improve its capacity and efficiency. Cybersecurity threats to aviation systems and services are also evolving and adapting to leverage new technologies to develop more sophisticated and capable means of damaging critical infrastructure and proprietary data. Threat actors are also broadening the landscape by using emerging technologies to develop new ways to exploit old vulnerabilities once thought to be mitigated long ago.

1.4 In consideration of prevailing threats to the aviation ecosystem and the speed at which new technologies are emerging to increase inherent risks, the speed at which guidance materials are developed and made available to ICAO member states and aviation stakeholders is more important than ever before.



Safety and Efficiency

Figure 2. Cybersecurity protections embedded throughout the aviation ecosystem

2. DISCUSSION

2.1 Cybersecurity is an enabler of aviation core functions (e.g., communication, navigation and surveillance) and is comprised of an enterprise set of infrastructure, systems and services that forms a holistic barrier of protections against local, regional and/or global threats. These threats are rapidly evolving in their sophistication, destructive capacity and ability to inflict harm anytime and anywhere in the ecosystem.

2.2 Emerging technologies like generative AI, QC, biometrics and others are also creating unique opportunities for threat actors to leverage more sophisticated methods and means to disrupt civil aviation systems and data, imposing new challenges to aviation stakeholders, ICAO Member States and civil aviation regulators to implement countermeasures to continuously improve their protections.

2.3 Rapidly emerging threats drive the need to apply ever more innovative and time-sensitive approaches to developing and delivering cybersecurity guidance materials to aviation stakeholders and ICAO member states to assure the protection and resiliency of our aviation ecosystem.

2.4 Initiatives, such as the ICAO direct submission process, recognize the need for expediting the speed at which materials are released, however, its scope is limited to entities that have topics related to ICAO's Strategic Objectives of Safety, Air Navigation Capacity and Efficiency. Guidance materials intended to strengthen the cybersecurity posture of the aviation ecosystem need to be developed and released using more time-sensitive and agile processes while maintaining quality and configuration control.

2.5 In view of the above paragraphs, ICAO is invited to investigate means and methods to accelerate how cybersecurity guidance materials are developed, reviewed, released and distributed to aviation stakeholder and ICAO Member States commensurate with the needs of cybersecurity.

3. CONCLUSION

3.1 The Conference is invited to agree to the following recommendation:

Recommendation 4.2/x – Assess the viability of adopting Agile Methodology principles

That ICAO:

- a) recognize that cybersecurity guidance materials require timely, relevant, and actionable approaches to delivering them to ICAO Member States and aviation stakeholders; and
- b) investigate means and methods to accelerate how cybersecurity guidance materials are developed, reviewed, released and distributed to aviation stakeholder and ICAO Member States commensurate with the needs of cybersecurity.

— END —