**Keynote Address
by the President of the Council
of the International Civil Aviation Organization (ICAO)
Mr. Salvatore Sciacchitano
to the UAE High Level Conference
on Cybersecurity in Civil Aviation**

(Dubai, UAE – 29 March 2022)

Your Excellences, Colleagues, Ladies and Gentlemen,

Good afternoon.

It is my great honour to join you here in Dubai for this important and very timely event. I would like to express my deepest thanks and gratitude to the Government of the United Arab Emirates, and its General Civil Aviation Authority, for the warm welcome, exceptional arrangements, and very generous hospitality accorded to us.

After almost two years of virtual meetings, it is a real pleasure to restart meetings in person. Thanks to the effective health measures put in place, we can begin to see the light at the end of the tunnel.

Cybersecurity is a key priority for major public and private organizations all over the world today, but we also need to ask ourselves why it is especially crucial to civil aviation.

Consistent with the preamble to the *Convention on International Civil Aviation* (Chicago Convention) the safe and secure growth of civil aviation has been, and continues to be, a foundational priority for the nations of the world.

Air transport is vital as a catalyst for the sustainable socio-economic development of civil societies, and plays an essential role in helping people, cultures, and businesses to connect and unite by air to their wide-ranging mutual benefit.

Technology and innovation are at the very heart of these core benefits of powered flight, and together they have allowed this sector to increase its capacity and efficiency at the service of humanity for many decades now, while at the same time enhancing system safety, security, and sustainability.

When considering and appreciating these achievements, we can sometimes forget that the investment and actions supporting this technological progress have largely taken place in distinct domains.

This process over time has left us with a backbone comprised of both new and legacy systems, or an information architecture more commonly referred to as a 'system of systems'.

Legacy systems most especially can contain outdated hardware and software that is not always easy to replace. They also can pose inherent security vulnerabilities, being unable to accommodate latest security and encryption best practices.

Recalling that civil aviation has always been an attractive target for terrorists and other bad actors due to its high media exposure and key roles in national and global economic development, these vulnerabilities can pose serious and difficult-to-remedy concerns.

When COVID-19 struck, it brought international aviation virtually to a standstill. However, in spite of this sharp decline in traffic and operational activity worldwide, it is noteworthy that cyber-attacks targeting civil aviation continued to increase during the pandemic period.

The pandemic has also fostered a significant public expectation for touchless technologies to make their future traveller experience healthier and safer, meaning that we face an entire new wave of compartmentalized digitalization, and still further system-of-systems vulnerabilities arising.

Recognizing the seriousness of these threats to our network, and to safety and security of the billions of people who operate and connect with it, ICAO has been at the forefront of addressing cyber threats to civil aviation since 2005.

During this time we have led the development of international cybersecurity Standards, Recommended Practices, and guidance material, and we have supported engagement of States for example through the adoption of several important international declarations on aviation cybersecurity, including the one adopted here in Dubai in 2017.

The 40th Session of the ICAO Assembly, held in 2019, acknowledged that cyberattacks can simultaneously affect a wide range of aviation areas.

Assembly States therefore highlighted the need for global adoption of the Beijing Convention and Protocol of 2010, adopted a new global *Aviation Cybersecurity Strategy* and related *Roadmap*, and called on ICAO to develop a mechanism for addressing cybersecurity in civil aviation that ensures a holistic and overarching approach to the topic.

This took extensive deliberations and consultations between the ICAO Council, the Air Navigation Commission, and the Secretariat, and resulted in the design of an innovative, and I must say unprecedented solution in ICAO.

In fact, this work led to the establishment of a dedicated cybersecurity governance. This includes the recently established Cybersecurity Panel consisting of 23 experts with international organizations and industry invited to participate in an Observer capacity.

Reporting to the ICAO Council's Aviation Security Committee, which is a newly established body, the Cybersecurity Panel will conduct periodic reviews of the Aviation Cybersecurity Strategy and Cybersecurity Action Plan, assess and report on the evolution of aviation cybersecurity threats and risks, assist in the development and review of guidance material and technical requirements, in addition to other tasks.

Going forward this will now assure convergence into a unified work programme of all cybersecurity and cyber resilience initiatives undertaken by the different expert groups in ICAO, thus enhancing the accountability, transparency, efficiency, and coordination of ICAO's work in all related areas.

The ICAO Council receives updates each Session on the progress of ICAO's work in this area, and it is my pleasure to report that, in spite of the resource challenges we are facing as a result of the pandemic, the organization during the past couple of years has been increasing its cybersecurity-related activities and outputs, in step with monitored threat levels.

In addition, ICAO has been developing an international aviation trust framework to support the cybersecurity and cyber resilience of civil aviation in the air navigation domain.

This is a very important project, probably the most important of recent years, to support the secure global exchange of digital aviation information, and will include procedures, technical specifications, and guidance material supporting current and future global network requirements.

In next few months ICAO will be in the position to outline the governance of this international aviation trust framework.

Although a lot has been done, however, a lot still remains to be done. In closing, I would therefore like to thank all States and partners who have supported, and continue to support, ICAO's work on cybersecurity and cyber resilience. Ensuring a harmonized, consistent, and holistic approach to aviation cybersecurity and cyber resilience has never been more important.

I also encourage all States to adopt the Beijing Convention and Protocol of 2010, and enhance the global legal framework for dealing with cyberattacks on international civil aviation as crimes.

Finally, I wish to reiterate my sincere thanks and appreciation to the United Arab Emirates for hosting this important leadership summit, while wishing all participants very successful and fruitful deliberations.

Thank you.