Opening Remarks by the Secretary General
of the International Civil Aviation Organization (ICAO)
Mr. Raymond Benjamin,
to the Conference on Civil Aviation Cyber Security

(Singapore, 9-10 July 2015)

Mr. Pang Kin Keong, Permanent Secretary, Ministry of Transport, Singapore;
Mr. Yap Ong Heng, Director General, Civil Aviation Authority of Singapore;
Mr. Tony Tyler, Director General and Chief Executive Officer of IATA;
Ladies and gentlemen,

It is an honour for me to be among you today. I would like to thank the Ministry of Transport of Singapore for hosting this very timely conference on civil aviation cyber security, and for reaffirming its strong commitment to addressing this important topic.

While no catastrophic cyber security event has been reported to ICAO to this point in time, we know that terrorists, criminals and 'hacktivists' are generally set on exploiting vulnerabilities in civil society.

The events involving LOT Polish Airlines and United Airlines, to cite very recent examples, resulted in the cancellation and delay of a number of domestic and international flights. And while these cyber events posed no serious threat to safety or security of the air carrier's services, the implications arising from the inconvenience created for LOT and United passengers and freight customers should not be under-estimated.

We must recognize then that various actors, whether individuals or organized groups, may seek to interfere with aviation-related systems for mischief, notoriety, activism, commercial gain or other motivations. Their collective determination knows no limit, and neither should our resolve to work together to mitigate the threats they pose.

I am therefore especially pleased by the initiative of the Ministry of Transport of Singapore to hold this conference in the full spirit of international cooperation, and that it features a significant level of collaboration between State authorities and industry.

In any discussion on civil aviation security, whether about baggage, access control or cyber systems, the necessary starting point must be an objective and substantiated risk assessment.

ICAO is therefore grateful that our Aviation Security Panel's Working Group on Threat and Risk has recently expanded the scope of its analytical work to include cyber threats. This forms part of its continuous review of risks facing civil aviation security, and impacts its recommendations for updating the *ICAO Global Risk Context Statement*.

Among the many cyber security issues being reviewed by the AVSEC Panel's Working Group, a number of key initiatives are seeking to identify and assess credible building block scenarios for possible cyber attacks. Included in these scenarios are aircraft cockpit, cabin and maintenance systems, the inter-related information and communications technologies (ICTs) which support modern air traffic management (ATM) capabilities, and airport-based systems for requirements such as departure control and flight information display.

We should also not lose site of the fact that, with new developments such as Electronic Flight Bags (EFBs) or in-flight passenger Wi-Fi, every new ICT-based capability brings with it potential new cyber security vulnerabilities.

Over the last two ICAO triennia, several major international civil aviation events have identified cybersecurity as a high priority, and delivered strong recommendations for ICAO and its Member States. But while intentions are laudable, actions speak louder.

Back in 2011 for instance, a provision on measures relating to cyber threats was introduced by ICAO into Annex 17 to the Chicago Convention. It recommended that States develop measures to protect information and communications technology systems used for civil aviation from interference that may endanger the safety of our network.

Later that year, new guidance material on cyber threats to critical aviation ICT systems was introduced in the ICAO *Aviation Security Manual* (Doc 8973 - restricted). It was followed a year later by the First Edition of the ICAO *Air Traffic Management Security Manual* (Doc 9985 - restricted), which provided further technical guidance. And in February of 2014, the adoption by the ICAO Council of Amendment 14 to Annex 17 further strengthened measures relating to cyber security.

Another important development in this area occurred last December, when ICAO, the International Air Transport Association (IATA), the Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), and the International Coordinating Council of Aerospace Industries Associations (ICCAIA), as members of the ICAO Industry High Level Group, signed the *Civil Aviation Cyber Security Action Plan*.

The Action Plan established clear commitments and related targets with respect to developing a common understanding of cyber threats and risks, and the mechanisms needed to promptly share and communicate these between government and industry stakeholders.

The High-level Group's work will be invaluable as our sector seeks to present to the public a consistent and coherent approach to the management of cyber threats and risks.

It will also aid cooperation between States and industry, as well as promote the development of a robust cyber-security culture in all organizations involved in international civil aviation, while additionally identifying and sharing best practices. Specific near-, mid- and long-term targets have been set, with "long-term" in this instance being no later than the end of 2016.

Fortunately, ICAO and the Industry High-level Group are not alone in these endeavours. Many States and stakeholders have been hard at work in addressing cyber security by developing their own frameworks and guidance. ICAO is currently assembling these into a series of reference materials to provide further support.

And let us also not forget that better coordination within States can also bring great benefit to this work. ICAO therefore strongly urges all States to include their local civil aviation authorities (CAAs)

and other relevant civil aviation entities when they develop or assess their national cyber security frameworks.

In concluding today, ladies and gentlemen, let me please wish you a highly productive Conference. I am confident that civil aviation will benefit from your participation in this event, and ICAO will certainly look forward to receiving your recommendations.

— — — — — — —