CIVIL AVIATION CYBERSECURITY ACTION PLAN

Whereas:

The safety and security of the global aviation system is vulnerable to attacks on its information and data systems. Today's cyber threat actors such as hackers, cyber criminals, "hacktivists" and terrorists are focused on malicious intent, the theft of information, profit and disruption.

As one of the most complex and integrated systems of information and communications technology (ICT) in the world, the global aviation system is a potential target for a large-scale cyber-attack, or for attack on one or some of its elements. Possible impacts of a cyber-attack range from endangering the safety of an aircraft to affecting operational reliability, financial health and business continuity.

With the continual and rapid integration of new technologies, the aviation industry is becoming increasingly inter-connected and reliant on systems. As technologies rapidly evolve, however, so too can the threats. Without the appropriate cybersecurity measures in place for this evolving threat, civil aviation may be at risk.

Therefore, we, the undersigned organizations (the "Participants"), declare that we:

- recognize the need to work together, guided by a shared vision, strategy and roadmap to strengthen the aviation system's protection and resilience against cyber-attacks;
- will jointly make the necessary effort to prepare civil aviation against future challenges from cyber threats;
- will cooperate on the following commitments:
    - Develop a common understanding of cyber threats and risks ;
    - Share assessments of risks;
    - Agree common language and terminology;
    - Develop joint positions and recommendations;
    - Present a coherent approach to the public;
    - Promote cooperation among State-level appropriate authorities and industry to establish coordinated aviation cybersecurity strategies, policies, and plans;
    - Promote a robust cybersecurity culture in all organizations in civil aviation;
    - Promote the use of existing information security and cyber protection best practices, standards and design principles, and establish new ones, where necessary;
    - Establish the mechanisms and means to share and communicate information including identification of threats, reporting of incidents and developments in defenses;
    - Communicate threat-related information and assure situational awareness;
    - Refine best practices, operational principles and defensive systems, as appropriate.
- Support the actions defined in the roadmap attached to this document.

CIVIL AVIATION CYBERSECURITY ACTION PLAN

Principles of Cooperation

This Action Plan does not create any legally binding obligations by or amongst the Participants. Cooperation pursuant to this Action Plan remains subject to any domestic laws and international obligations applicable to the Participants. Nothing in this Action Plan obliges Participants to provide confidential or sensitive information. While this Action Plan sets out concrete steps to further cyber security cooperation in the context of civil aviation, it is intended to be flexible and expected to be refined or changed by consensus amongst the Participants, as new issues arise. Participation in this Action Plan does not preclude participation in any other efforts to combat cyber security in civil aviation whether among any Participant(s) or other organization(s).

Montreal, 05 December 2014

Angela Gittens
Director General
Airport Council International (ACI)

Jeff Poole
Director General
Civil Air Navigation Services Organisation (CANSO)

Tony Tyler
Director General and Chief Executive Officer
International Air Transport Association (IATA)

Raymond Benjamin
Secretary General
International Civil Aviation Organization (ICAO)

Jan Pie
Chairman
International Coordination Council of Aerospace Industries Associations (ICCAIA)
Secretary General
The Aerospace and Defence Industries Association of Europe (ASD)

CIVIL AVIATION CYBERSECURITY ACTION PLAN

Roadmap

Commitment	Short Term (0-6 months)	Mid Term (6-12 months)	Long Term (12-18 months)
Develop a common understanding of cyber threats and risks	Task: Develop and provide input to common risk and threat matrices. Deliverable: First draft input to threat and risk analysis.	Deliverable: 2015 Aviation Security Panel Paper. Deliverable: Input to ICAO Working Group on Threat and Risk and ECAC Risk Assessments.	Task: Continue to review and communicate threats, update threat and risk analysis.
Share assessments of risks	Task: Compare risk assessment processes from different stakeholders.	Task: Identify mechanism or platform for ongoing sharing of information. Task: Share risk assessments (at the system type level). Deliverable: Input to ICAO Aviation Security Panel Working Group on Threat and Risk.	Task: Continue to review and communicate threats, update threat and risk analysis. Deliverable: Process/platform for sharing of high level risk assessments across industry.
Agree common language and terminology	Deliverable: Industry High Level Group (IHLG) commitment to promote use of existing standards and frameworks. Task: IHLG organizations and their members provide input to a Glossary of Terms.	Deliverable: Glossary of terms for ICAO guidance material.	
Develop joint positions and recommendations	Deliverable: Agree, sign and announce Cybersecurity Action Plan. Task: Identify key areas where regulation is emerging. Task: Industry stakeholders to develop joint positions and recommendations for appropriate regulation.	Task: Prepare joint paper on key issues for regulation during 2015 AVSEC Panel. Task: Identify key areas where regulation is emerging. Task: Industry stakeholders to develop joint positions and recommendations for regulation.	Task: Provide input to development of regulation including standards, recommended practices and guidance material. Deliverable: New and updated guidance material.
Present to the public a joint, consistent and coherent approach to the management of cyber threats and risks	Deliverable: Agree the format and means of communication to the public of a joint position to be used by all signatories Publish the first such communication(s).	Publish refined and updated communication(s)	Publish refined and updated communication(s)

CIVIL AVIATION CYBERSECURITY ACTION PLAN

Commitment	Short Term (0-6 months)	Mid Term (6-12 months)	Long Term (12-18 months)
Promote cooperation among State-level appropriate authorities and industry to establish coordinated aviation cybersecurity strategies, policies, and plans	Deliverable: Agree, sign and announce Cybersecurity Action Plan. Task: Determine/promote mechanisms for regional and State-level appropriate authority/industry coordination.	Deliverable: Joint workshops in each region Task: Determine/promote mechanisms for regional and State-level appropriate authority/industry coordination.	Deliverable: Commitment from States for coordinated action during the 39th Assembly, September/October 2016.
Promote a robust cyber-security culture in all organizations in civil aviation	Deliverable: IHLG commitment to promote use of existing standards and frameworks.	Task: Raise awareness of cyber security and the need for a cyber-security culture, and provide guidance on implementation. Deliverable: Awareness program and guidance.	Deliverable: 80 percent of industry organization members commence implementation of cyber security culture.
Promote the use of existing information security, cyber protection standards and design principles, and establish new ones, where necessary	Deliverable: IHLG commitment to promote use of existing standards and frameworks.	Task: Compile and share best practices and standards such as International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST).	Deliverable: 80 percent of industry organization members agree to implement standards and best practices.
Establish the mechanisms and means to share and communicate information including identification of threats, reporting of incidents and developments in defenses	Deliverable: Agree confidentiality of information shared amongst IHLG members and at the working group level.	Task: Assess requirements for data sharing and identify possible solutions.	Deliverable: Implement means to share threat and incident information in a secure environment.
Communicate threat-related information and assure situational awareness	Task: Exchange information, develop a common understanding of specific issues as they arise and coordinate responses to potential or emerging threats. Deliverable: Establish communication channels between industry partners.	Task: Exchange information, develop a common understanding of specific issues as they arise and coordinate responses to potential or emerging threats.	Deliverable: Establish mechanism to more systematically and efficiently coordinate analysis and responses to potential or emerging threats.

CIVIL AVIATION CYBERSECURITY ACTION PLAN

Commitment	Short Term (0-6 months)	Mid Term (6-12 months)	Long Term (12-18 months)
Refine best practices, operational principles and defensive systems, as appropriate	Deliverable: IHLG commitment to promote use of existing standards and frameworks, 25 June 2014	Task: Continuous review and development of guidance material with ICAO and standard setting bodies. Task: Promote implementation of processes for quality assurance and continuous improvement of cyber security defenses and mitigations in all organizations. Deliverable: Share findings and best practices informally among industry stakeholders.	Deliverable: Implement mechanism to coordinate continuous improvement of operational and technical best practices across industry stakeholders.