



Aviation Partnership Project

Workshop on Cybersecurity in Aviation

draft AGENDA

05-07 February 2020, Colombo, Sri Lanka

This Workshop related to Cybersecurity in Aviation will introduce its international, regional, and local implications and facilitate discussions on a number of associated subjects. It will raise awareness of international, regional and national initiatives, both from states and industry and it will facilitate the discussion of a number of topics which are already part of those initiatives. Furthermore, it will encourage the identification and discussion of unexplored subjects, which could have an impact on the global aviation community. A broad exchange of opinions is sought, leading towards an international approach to increase the resilience, safety and security of aviation in the face of relentlessly evolving cyber threats.

DAY 1	Wednesday 5th February 2020
09:00 – 10:00	<i>Registration and Morning Tea</i>
10:00 – 10:15	<i>Keynote Speech – Introduction of the event</i>
10:15 – 10:30	<i>Speech by Chairman CAA SL</i>
10:30 – 11:00	<i>Group Photo and Tea Break</i>
11:00 – 12:30	<i>Workshop ONE: Cybersecurity From the Global Aviation Perspective</i> This workshop will discuss the cybersecurity risks faced by the international community and how it needs to take them into consideration. It will also discuss the role of ICAO in addressing those risks at a global level and how this can be supported by the creation of regional platforms, like it is the case of the ESCP (European Strategic Coordination Platform).
12:30 – 14:00	<i>Lunch Break and Networking</i>
14:00 – 15:15	<i>Workshop TWO: A Strategy for Cybersecurity in Aviation</i> This workshop will present and discuss the strategy that the international aviation community has already developed as part of the ICAO Secretariat Study Group on Cybersecurity (SSGC). It will explain its key subjects and will further refer to the first regional strategy, developed by the ESCP (European Strategic Coordination Platform).

15:15 – 15:45 **Tea Break**

15:45 – 16:45 **Workshop THREE: The Implementation Plan for the Cybersecurity Strategy**
This workshop will discuss possible detailed actions for the implementation of the Cybersecurity Strategy, and the ongoing related activities at ICAO and European level.

16:45 – 17.00 **Conclusions of the day**

19:30 – 22:00 **Networking Dinner (limited places available / upon invitation only)**

DAY 2 Thursday 6th February 2020

9:00 – 10:30 **Workshop FOUR: Introduction to Regulatory requirements for Organisations**
This workshop will discuss the need for the introduction of performance and risk-based regulatory requirements for the management of cybersecurity risks in all aviation domains, in proportion to their impact on aviation safety. It will also present the proposals being developed by EASA in coordination with the ESCP.

10:30 – 11:00 **Tea Break**

11:00 – 12:30 **Workshop FIVE: Information Security Management System (ISMS) and coordination with other Regulatory Frameworks**
This workshop will address a high-level approach to ensure that cybersecurity will be adequately taken into consideration during design, implementation, integration, operation, maintenance and end-of-life of products and services. It will further introduce the possibilities and benefits of integrating different management systems on an individual organisational basis.

In many countries, cybersecurity regulations have been put in place to protect certain critical stakeholders. In Europe, industrial operators, including aviation, have been mandated to additionally protect and report on attacks on services essential to the public. This session will address the attempt to align a number of co-existing regulatory frameworks such that both operators and oversight authorities will be able to minimise inconsistencies and overlaps in compliance and oversight.

12:30 – 14:00 **Lunch Break and Networking**

14:00 – 14:45 **Workshop SIX: Introduction to Risk Management Aspects**
This workshop will address the need to revise and extend the existing approach to safety risk management, as aviation is considered a System-of-Systems (SoS). It will focus on a community approach to reduce the risk exposure of the aviation community as a whole. Trans-organisational cyber risk management is the proposed tool to make this happen. The European Strategic Coordination Platform (ESCP) on Cybersecurity in Aviation has a dedicated work stream addressing key aspects of such coordinated risk management.

14:45 – 15:15 **Tea Break**

15:15 – 16:30 **Workshop SEVEN: Risk Assessment and Management Principles and Identification of Functional Chains**

In Eurocae Standard ED-201, concepts relating to sharing information pertaining to information security risk assessments have been documented. The objective was to allow users to meet requirements for the coherence of risk assessments between organisations, but also those requirements allowing for the comparability of risk evaluations and consequently those to assure a certain level of commonality of risk acceptability. This session will discuss these aspects.

This session will also address the concepts currently in development under the ESCP Shared Trans-Organisational Risk Management (STORM) work stream for the identification of shared risks.

16:30 – 16:45 **Conclusions of the day**

DAY 3 Friday 7th February 2020

9:00 – 10:30 **Workshop EIGHT: Introduction to the Sharing of Information**

This workshop will address a number of aspects related to sharing of information. Traditionally this is translated into “Information Sharing” between organisations such as Computer Emergency Response Teams (CERTs) or Information Sharing and Analysis Centres (ISACs). However, in a Systems-of-Systems environment, collaboration has to start much earlier, namely when assessing risks. Both areas are crucial and deserve consideration by this workshop.

10:30 – 11:00 **Tea Break**

11:00 – 12:30 **Workshop NINE: Sharing of Operational Information (SOC, CERT, CSC, ISAC)**

This session will discuss which types of information can be acquired, consolidated, evaluated and exchanged by organisations. The merits and challenges of various information sharing practices will be considered, along with the difference between concepts which restrict the circles among whom information is shared (e.g. “classification of information”, Traffic Light Protocol”).

12:30 – 12:45 **Summary and conclusions of the workshop**
