ESCP

The European Strategic Coordination Platform for Cybersecurity in Aviation

Charter

Version 2.0

February 2019

Contents

This document includes the following Annexes:

Annex I – Participating Organisations and Observers

1. Scope of this document

This charter document of the European Strategic Coordination Platform (ESCP) for Cybersecurity in Aviation describes the vision, identifies the stakeholders of the initiative and outlines values and underlying principles which are shared by the members of the platform. This document serves as a reference for the future of the ESCP.

2. Vision

The vision is to make the European Aviation System more **resilient** and more **secure** to cyber threats**,** by adopting a through-life tiered approach to security in design, production, operations and ultimately disposal of products, systems and services.

In order to drive this vision the aviation community (both civil and military) will join in a co-operative partnership, the ESCP, to define and coordinate the implementation of a European strategy for Cybersecurity in Aviation.

For the purpose of achieving adequate consistency and avoid duplications, this strategy shall consider the global context and include appropriate international coordination, taking into account, among other aspects, any relevant ICAO standards and initiatives, ECAC and EU initiatives, as well as any applicable EU regulation and Industry Standards.

3. Underlying Values

Members contribute **collaboratively**
The success of the *ESCP* relies on a collaborative effort involving all members of the platform.

Members engage **voluntarily**
Members of the platform engage, join, or leave on a voluntary basis following the membership rules described in section 5.

Members act **transparently**
Members of the platform shall act transparently in the interest of improving the safety and security of all aviation users. In doing so, the need for appropriate classification levels and handling of any security sensitive information must be ensured, both within the work streams and in communication with the public.

4. Governance

An Executive Committee is responsible for the governance of the ESCP, the achievement of the ESCP vision, and the definition of an underlying European Aviation Cyber Security Strategy.
The Executive Committee therefore is empowered to take decisions and steer the ESCP activities.

The ESCP governance ensures that the vision herewith described is pursued by the membership while respecting the basic platform principles detailed in this charter document endorsed by the ESCP Executive Committee.

A Technical Advisory Committee (TAC) will support the activities of the Executive Committee, substantiate the position of the ESCP and harmonize the contribution of the members. The TAC is tasked by the Executive Committee which may initiate a new activity called “Work Stream” to achieve a specific outcome in order to support the development of the ESCP position. The TAC will meet in Plenary coordination meetings and Work Stream meetings with different composition.

As an example Work Stream outcomes are: concepts for collaboration and engagement (such as this charter), strategy documents as well as policy papers.

Secretary:
EASA will act as the Secretary, being responsible for facilitating the organisation of meetings.

Chairmanship:
The Chairperson shall be elected by the members of the Executive Committee.

Decision-making process:
The decision-making process should be consensus-driven, since in most of the cases it will result in recommendations for EASA or the European Institutions. However, the Executive Committee may require 100% unanimity for certain decisions. In such a case only European organisations will be allowed to vote.

5. MEMBERSHIP

The membership of the ESCP will be as representative as possible of the public and private sector relevant to EU aviation. As such, it should include members from European Institutions, representing bodies, national civil and military authorities, industry associations and unions.

The membership of the ESCP comprises a maximum of 30 organisations, with each one nominating a person to represent them in the Executive Committee.

The initial membership of the ESCP comprises the European organisations listed in the Annex I to this document. New members for the ESCP will be assessed for relevance and agreed by the Executive Committee.

The Executive Committee may invite observers from other organisations. The initial observers are also listed in the Annex I.

The Technical Advisory Committee is composed of representatives, nominated by the Executive Committee members, in order to ensure the availability of relevant expertise. Representatives may be nominated to participate in the TAC Plenary meetings or to different work streams. The number of representatives will be limited as follows:

- For work streams: maximum of 3 delegates per organisation and per work stream.
- For the Plenary meeting: one delegate per organisation and per work stream.

6. Collaboration Modalities

The Executive Committee is expected to meet 3 times per year for face-to-face meetings, while the specific work streams of the TAC will convene when deemed necessary. To ensure an efficient process, the TAC's preferred mode of collaboration will be based on correspondence via email or teleconferences. To foster interpersonal interaction between the members of the TAC, a face-to-face meeting in the course of a kick-off event shall be organised per specific work stream.

The setup of a technical collaboration platform based on secure web-services shall further support the contribution to the overall ESCP objectives.

The proposed modalities shall adequately address the determining constraints of time and budget of the members. Given the voluntariness of the platform, the best endeavours will be made in order to provide the members of both the TAC and the Executive Committee with a reasonable advance notice prior to each meeting, with the view to ensuring the best possible attendance.

7. Basic Principles

The following principles will support the framing of the discussions at all levels by providing a rationale for the mutual legitimization of the community position:

I. Security is an evolutionary and continuous process.

II. Systems are comprised of technology, people and processes and each system is part of and contributes to the security of a System-of-Systems.

III. Resilience is the ability to prevent disruptions, to prepare for and adapt to changing conditions and to detect, respond and recover rapidly from disruptions to ensure the continuity, integrity and confidentiality of services at an acceptable performance level.

IV. A bespoke design of an aviation system does not guarantee resilience to cybersecurity threats.

V. Cybersecurity measures can only be effective if applied in a timely manner.

VI. Managing complexity is key to cybersecurity.

VII. The airborne platform is the last line of defence.

The *rationale* for each of the principles is:

I. Security is an evolutionary and continuous process:
Even if a system does not change, its security environment is undergoing constant changes. This especially applies to new challenges emerging from the cyber domain. In order to keep the aviation system secure, the aviation community shall keep a continuous and consistent effort to protect it against all identified and anticipated threats.

II. Systems are comprised of technology, people and processes and each system is part of and contributes to the security of a System-of-Systems:
Global Aviation is a system-of-systems which extends beyond the aviation industry. No one single element of a system should be dealt with in an isolated manner when it comes to cyber

security. It is important to apply appropriate security measures to each individual system of a system-of-systems and at the same time to consider the effects that multiple interrelated systems can have on each other. Only the consideration of all elements working together and being “interconnected” to a system ensures a holistic approach to its cyber security and supports an effective and efficient approach to reach an acceptable level of risk.
The human factor of a system deserves specific attention because of its crucial role in interacting with technology and execution of processes.

III. **Resilience is the ability to prevent disruptions, to prepare for and adapt to changing conditions and to respond and recover rapidly from disruptions to ensure the continuity of services at an acceptable performance level:**
Resilience implies minimising effects on a system’s overall performance to an acceptable level in the course of attempted and successful attacks. The system under consideration has to maintain an acceptable level of operational functionality at various levels of degradation during recovery, until effects of an attack have been assessed and mitigated.

IV. **A bespoke design of an aviation system does not guarantee resilience to cybersecurity threats:**
Aviation systems often rely on bespoke designs, of which many may not be available or accessible for a broader audience. However, the reliance on secret designs or closed source developments cannot ensure security of the system under consideration. Security relies on thorough and broad scrutiny of functionalities, architectures and implementations. Bespoke designs often lack the visibility of this level of scrutiny, providing a false sense of security and, potentially, safety.

V. **Cybersecurity measures can only be effective if applied in a timely manner:**
Applying cybersecurity measures in a timely fashion can significantly reduce the risk of vulnerabilities being exploited and therefore contribute to protect from breaches and related problems that come with it.

VI. **Managing Complexity is key to cybersecurity:**
As architectures become increasingly complex, it becomes more difficult to understand all possible interactions and interdependencies, be they internal or external.
It can ultimately lead to unidentified and exploitable vulnerabilities within a system-of-systems. Reducing and managing complexity on the other hand can improve the level of understanding of the system-of-systems, may simplify the process of identification of potential vulnerabilities, reduce the attack surface, and therefore allow for a higher level of system’s security.

VII. **The airborne platform is the last line of defence:**
An airborne platform is designed to operate for many decades and at the same time it is the least flexible to adapt to changes in its environment quickly. It is even more unlikely that an airborne platform will be able to adapt easily within given time constraints which are determined and imposed by the rapid pace of developments emerging from the cyber threat landscape. The system-of-systems in depth defence approach, which increases the required effort for an attack, with each layer of defence, positively contributes to the assurance of safety of flight.

8. CHANGE TO THIS CHARTER DOCUMENT

The Executive Committee will review this charter document after one year of activity. As a general provision, the Executive Committee may review the charter and initiate modifications to it at any point in time.

ANNEX I - PARTICIPATING ORGANISATIONS AND OBSERVERS

Here below are the lists of the European organisations participating to the ESCP (Table 1) and the non-European organisations taking part to the ExCom meeting as Observers (Table 2).

Table 1 - ESCP Participating European Organisations

Organisation	Acronym
Airports Council International - Europe	ACI
Airlines for Europe	A4E
AeroSpace and Defence Industries Association of Europe	ASD
Civil Air Navigation Services Organisation - Europe	CANSO
Computer Emergency Response Team for the EU Institutions	CERT-EU
Directorate-Gen. for Communications Networks, EU Commission	DG-CNECT
Directorate-Gen. for Internal Market, Industry, Entrepreneurship and SMEs	DG-GROW
Directorate-Gen. for Migration and Home Affairs	DG-HOME
Directorate-Gen. for Mobility and Transport	DG-MOVE
European Civil Aviation Conference	ECAC
European Cockpit Association	ECA
European External Action Service	EEAS
European Helicopter Association	EHA
European Union Agency for Network and Information Security	ENISA
EUROCONTROL	EUROCONTROL
European Defence Agency	EDA
European Independent Maintenance Group	EIMG
European Regions Airline Association	ERAA
European Transport Workers' Federation	ETF
European Union Agency for Law Enforcement Cooperation	EUROPOL
General Aviation Manufacturers Association	GAMA
International Air Transport Association - Europe	IATA
Single European Sky ATM Research Deployment Manager	SESAR DM
Single European Sky ATM Research Joint Undertaking	SESAR JU
Member State (Finland)	FIN
Member State (France)	FRA
Member State (Poland)	POL
Member State (Romania)	ROM
Member State (Sweden)	SWE
Member State (UK)	UK

Table 2 - ESCP Observer Organisations

Organisation	Acronym
Aerospace Industries Association of America Inc.	AIA
Aerospace Industries Association of Canada	AIAC
Federal Aviation Administration	FAA
International Civil Aviation Organization	ICAO
North Atlantic Treaty Organization	NATO
Transport Canada	TC