Workshop on Cybersecurity in Aviation

31 May 2017, Brussels, EASA

Presentation Session

EASA and EUROCAE organised the Workshop on Technical Standards to initiate the discussion about future rulemaking and standardisation for Cybersecurity in Aviation among stakeholders and NAAs and to facilitate the identification of key subjects of interest to the parties. It was the first time that the public part of the draft rulemaking concept was presented.

The workshop was introduced by Carlos Salazar, Head of the EASA Brussels Office. He welcomed the participants and opened the meeting by mentioning the Bucharest Declaration and the changing role EASA was asked to assume.

Christian Schleifer-Heingärtner, Secretary General of EUROCAE, introduced the subject. He underlined the importance of technical standards in the performance-based rulemaking and the role the standardisation bodies play in this context, as well as the complementarity of the two levels and the need for coordination. He also referred to the Bucharest Declaration in which the reliance on industry standards had been specifically emphasised. He explained the EUROCAE process, which is open, transparent and member driven - by the industry for the industry.

Jean-Jacques Woeldgen, representing DG MOVE on behalf of the European Commission, pointed out that the subject is considered to be a very important one and that their strategic priorities are Resilience, Development of cyber defence policies and capabilities, Reduction of Cybercrime, Development of technology resources, and the Promotion of any international dialogue. Key pillars, on which the EC counts, are the NIS Directive, the cPPP, ENISA, and the industry.

The morning continued with presentations by industry stakeholders (ASD, CANSO and IATA), followed by EUROCONTROL, SJU, and standardisation bodies. EUROCONTROL suggested to define and develop regulations (framework) and minimum standards of mitigation to establish acceptable cyber-security risk for the global aviation community. SJU focussed on the SESAR programme which develops, validates, and delivers ***securable*** solutions, and the application of the SESAR security risk assessment methodology. Some standardisation bodies (ECAC, SAE, CEN and EUROCAE) also presented their ongoing and planned activities.

At the end of the morning EASA presented its Regulatory Framework proposal, which represents the way EASA will deal with cybersecurity following the anticipated change of the Basic Regulation. This framework will rely on all levels of regulatory instruments available to

the Agency, including Certification Specification Cybersecurity and increase reliance on industry standards.

All presentations were made available to the participants of the workshop.

Key messages

- Improve the European regulatory/oversight framework in the field of information security, taking into account all aviation stakeholders (airlines, ANSPs, airports, MROs,…) and the existing systems in operation
- Set a roadmap (including Means of Compliance) with regular milestones
- Develop consistent and harmonised standards in close cooperation between Standards Developing Organisations (SDOs), and avoidance of duplication of work
- Develop upgradeable horizontal security standards applicable to all sectors, based on a holistic approach and expanding to other interfacing areas of relevance (e.g. ATM, Supply Chain, Operations & Business)
- Combine Rulemaking and standardisation expertise of aviation security, aviation safety, air navigation and cybersecurity.

Cybersecurity workshop – breakout sessions

The afternoon was dedicated to four breakout sessions, which discussed what subjects need to be addressed as a technical standard in order to provide supporting material for a regulation, and what EASA and EUROCAE should work on.

The following topics were raised as potential items for further work

- Security Event Management
- Incidence Response Management
- Maintenance Security
- Development & Production Security
- Interorganisational security requirements and interfaces
- Civil-military interoperability
- Incidence and vulnerability management
- Risk assessment methodology
- Trusted environment
- Cyber resilience requirements (overarching & per domain)
- Training, Education, Awareness
- Cybersecurity Terminology
- Cybersecurity Testing.

It was stressed that the SDOs should avoid duplication of work and make use of existing standards as much as possible, eventually with specific adaptations of existing standards to suit the needs of the aviation sector.

EASA and EUROCAE will now evaluate the proposals for potential future work in order to develop a concrete regulatory and standardisation work programme and coordinate future activities with the relevant stakeholders.