EASA
European Aviation Safety Agency

ESCP Regulatory Process Work Stream

Juan Anton
Cybersecurity in Aviation & Emerging Risks Section Manager

ESCP High Level Meeting
Toulouse, 14/15 November 2018

Your safety is our mission.

An agency of the European Union

A robust and flexible regulatory framework

One of the main elements of a succesful aviation cybersecurity strategy is...

Create a robust and flexible regulatory framework supplemented by Industry Standards, covering all aviation domains

With this objective, EASA included in the 2018-2022 EPAS (European Plan for Aviation Safety) two rulemaking tasks:

- **RMT.0648 for aircraft, engines and propellers.**
- **RMT.0720 for organisations.**

RMT.0648 (for aircraft, engines, propellers)

Rulemaking Task RMT.0648 “Aircraft Cybersecurity”: ***The objective is to ensure a robust product design to avoid cybersecurity risks.***

Next Deliverable: Notice of Proposed Amendment (NPA) expected before end 2018

Key aspects:

- **Harmonised with the FAA. Takes into account the recommendations to the FAA of the ASISP (Aviation Systems Information Security/Protection) ARAC (Aviation Rulemaking Advisory Committee) group, where EASA participated.**
- **Include amendments to the Certification Specifications and Acceptable Means of Compliance (AMC).**
- **There will be references to Industry Standards (ED-202A and ED-203A).**

This task is not being discussed within the ESCP.

RMT.0720 (for organisations)

Rulemaking Task RMT.0720: ***Requirements for the management of cybersecurity risks for organizations in all aviation domains (design, production, maintenance, operations, aircrew, ATM/ANS, aerodromes).***

Next Deliverable: Notice of Proposed Amendment (NPA) expected first half 2019.

Key aspects:

- **The objective is to ensure that organisations are able to manage cybersecurity risks, including the need for an Information Security Management System (ISMS) and occurrence reporting.**
- **For organizations in all aviation domains, and for competent authorities (with some exceptions to ensure proportionallity to the risks).**
- **Including high-level, risk and performance-based requirements (flexibility, no frequent amendments).**
- **Complemented by AMC, Guidance Material and Industry Standards.**
- **The structure should facilitate to the organisations the future integration of ISMS with existing Safety Management Systems (SMS) and Security Management Systems (SeMS).**
- **Consistent with other EU security requirements imposed on the Member States.**

RMT.0720 (for organisations)

Current status of the proposed rule (ongoing discussions taking place in the ESCP “Regulatory Work Stream“)

- **Objective:** Requirements to be met by organisations in order to identify, protect, detect, respond and recover from those information security events which could potentially affect aviation safety or could affect the European Aviation Traffic Management Network (EATMN).
- **Applicable to:**
  - POA, DOA.
  - Part-145 orgs., future Part-CAMO orgs (Opinion 05/2016).
  - Commercial air transport operators (CAT), Commercial specialised operators, Non-commercial operations with complex motor-powered aircraft, Non-commercial specialised operations with complex motor-powered aircraft.
  - Training Organisations (ATO, ATCO), Aeromedical Centres and FSTD Operators.
  - ATS, MET, AIS, DAT, CNS, ATFM and ASM Providers and the Network Manager.
  - Aerodrome Operators and Apron Management Service Providers.
- **Not applicable to:** Future Part-CAO orgs (Opinion 05/2016), Part-147 organisations, private & SPO operators of non-complex aircraft, DTO (aircrew).

RMT.0720 (for organisations)

- **Structure of the rule:**
  - Specific Implementing Rule (for information security) applicable to all domains, at the same level as any other EASA Implementing Rule (stemming directly from the Basic Regulation).
  - Contains a Cover Regulation with Articles and an Annex (Part-AISS: Aircraft Information System Security).
  - **Cover Regulation contains:**
    - Objective and scope, Definitions, Agency Measures and Alternative Means of Compliance, Competent Authority, Entry into Force.
  - **Part-AISS contains:**
    - **Section A (organisations):** Information Security Management System (ISMS), internal reporting, occurrence reporting, subcontracted activities, personnel requirements, record keeping…
    - **Section B (authorities):** Information Security Management System (ISMS), allocation of tasks to qualified entities, personnel requirements, record keeping, oversight principles & programme, etc.

RMT.0720 (for organisations)

- **Interface issues (3 regulatory frameworks):**
  - **NIS Directive (2016/1148) on Security of Network and Information Systems:**
    - **Applies only to essential services (defined by each State), covering different sectors (not only aviation)**
    - **Focuses on preventing significant disruption of essential services to society and economic activities.**
  - **Regulation 2015/1998 on Aviation Security:**
    - **Applies to all aviation domains.**
    - **Currently being evaluated in order to transpose ICAO Annex 17 latest amendments.**
  - **Future EASA regulation (Part-AISS):**
    - **Focuses on safety (directly on the aircraft or in relation to the sudden collapse of the aviation network).**
    - **Applies across all aviation domains (aviation is a system-of-systems).**

RMT.0720 (for organisations)

- **Interface challenges:**
  - Consistency of regulatory requirements.
  - Standardisation of requirements imposed by each State on essential services through the NIS Directive.
  - Coordination between the different authorities within each State (NAA, security authorities, etc)
- **Current approach discussed to avoid conflicts with NIS Directive:**
  - Authority for Part-AISS: The NAA currently responsible for the organisation (they can delegate to a national security agency or equivalent, normally the one responsible for the NIS Directive).
  - Organisations defined as "Essential Services" by the State can replace Part-AISS requirements by the NIS Directive requirements imposed by the State. They will still have to comply with the occurrence reporting of Part-AISS (reporting to the NAA). The NAA will have to coordinate the oversight with the authority responsible for the NIS Directive.
  - EASA will do the oversight on the NAA and on how they coordinate with the authority of the NIS Directive.

EASA
European Aviation Safety Agency

Thank you

Your safety is our mission.

An agency of the European Union