EASA

European Union Aviation Safety Agency

Workshop 5: “Information Security Management System and coordination with other Regulatory Frameworks”

Juan Anton

Cybersecurity in Aviation & Emerging Risks Section Manager

5th – 7th February 2020

Workshop on Cybersecurity in Aviation

Aviation Partnership Project

Sri Lanka

Your safety is our mission.

An Agency of the European Union

Why we need to develop new rules

Information security risks are constantly increasing

- **Information systems are becoming increasingly complex and interconnected, and a more frequent target of cyber-crime.**
  - Weaknesses in one organisation, product or system can have an impact on different stakeholders, largely amplifying the impact of a cyber attack.
  - These weaknesses are not always known by the operators.
  - They can be combined and exploited with malicious intent:
    - Different attacker profiles:
      - Sponsored by certain States for political/economic reasons.
      - Activists seeking publicity for their cause.
      - Criminals looking for economic benefits.
    - Not always necessarily targeting aviation, but producing a collateral damage.

Current EASA rules only partially address information security risks

- **<u>The current EASA aviation regulatory framework is mostly focused on reducing the likelihood of accidents resulting from non-intentional acts:</u>**
  - Includes different safety layers.
  - Accidents would only occur when several simultaneous deficiencies/errors randomly align themselves: very remote and fortuitous event.

- **<u>Not enough focus on safety risks resulting from intentional acts.</u>**
  - Existing flaws are exploited with malicious intent. Not a random event.
  - Traditional safety layers may not be sufficient to address these risks.
  - Current requirements only in the following areas:
    - Technical requirements for aircraft/engine certification
    - Organisation requirements for ATM/ANS and Aerodromes

Two other EU frameworks partially address information security (NIS Directive 2016/1148, Aviation Security Reg. 2015/1998)

- **<u>They are not focused on the impact on aviation safety</u>**
  - **NIS Directive:** focus on preventing disruption of essential systems (social and economic impact).
  - **Reg. 2015/1998:** focus on aviation security.
- **<u>They do not cover all aviation domains and stakeholders</u>**
  - **NIS Directive:** Only the essential services defined by each Member State.
    - Only some aviation domains, and not all stakeholders within those domains.
    - Different in each Member State.
  - **Reg. 2015/1998:** Applies only to:
    - Airports or parts of airports.
    - Operators (including air operators) and entities that provide services or goods to or through those airports.

Why we do it now, without waiting to the full implementation of the NIS Directive

Addressing aviation information security risks is an urgent matter

- **NIS Directive applicability:**
  - **9 May 2018:** Member States to adopt and publish the national laws, regulations and administrative procedures to transpose the NIS Directive.
  - **9 November 2018:** Member States to identify the operators of essential services affected by those requirements.

- **Current state of implementation of the NIS Directive:**
  - Some Member States have still not transposed the NIS Directive.
  - Very different speeds of implementation across the Member States.

Waiting for full implementation of the NIS Directive would mean several years before we could start this rulemaking task.

There is a need to ensure a level playing field across Europe

→ **Non-standardised implementation of the NIS Directive:**

→ Different approaches to the definition of essential services.

→ Very different levels of implementation across the Member States.

Waiting for full implementation of NIS Directive would mean starting this rulemaking task when a fully non-standardised landscape is already implemented across the EU. Instead:

→ The discussions on this rulemaking task already started in July 2017.

→ This allows Member States to take into account the material being developed in this task in order to define their policies for implementation of the NIS Directive for the essential services in the aviation domain.

→ **This promotes standardisation and consistency of both frameworks.**

Competent Authority responsible for the implementation and oversight of the proposed requirements

Options considered

- **When EASA is the authority for the current approval of the organisation:**
  - EASA would be also the competent authority for the elements of the proposed rule.
  - Special case: For Pan-European organisations such as EGNOS, coordination measures between EASA and the SAB (Security Accreditation Board) will need to be defined.

- **When a competent authority of a Member State is currently responsible for the oversight of the organisation:**
  - **Option 1:** Leave to the Member State the decision of who will be the competent authority for the proposed rule (could be different from the one already responsible for the current EASA safety approval (or declaration) of the organization).
  - **Option 2:** The authority for the proposed rule would be the same as the one responsible for the current EASA safety approval (or declaration) of the organization.

Option selected

- **Option selected:** The authority for the proposed rule would be the same as the one responsible for the current EASA safety approval (or declaration) of the organization.

- **Reasons:**
  - Prevents disputes between 2 authorities responsible for the approval of the organisation, and avoids the need to create 2 approval certificates for the organisation.
  - Permits a consistent oversight approach for all aspects related to aviation safety (including cyber), in particular for the management systems held by the organisation.
  - Permits EASA to perform its audit activities on the competent authority (may not be possible if a national cybersecurity agency is responsible, because of information access restrictions)

Delegation of oversight activities

- **AISS.AR.400 “Qualified entities”:** This allows the competent authority to delegate tasks, for example, to a national cybersecurity agency (possibly responsible for the implementation of the NIS Directive).
  - This facilitates the access by the competent authority to additional information security expertise
  - This provides flexibility to the State in order to create a national safety and security organisational structure that fits their needs.

NOTE: The responsibility remains on the competent authority. Especially to ensure that the audits performed by the qualified entity take due account of the safety aspects.

EASA standardisation activities

→ **EASA will perform its oversight activities on the competent authority.** This oversight will include also the elements related to information security.

→ If the competent authority has delegated certain tasks on, for example, a national cybersecurity agency, EASA will check how they coordinate. EASA will not audit the national cybersecurity agency.

Consistency with the NIS Directive (EU) 2016/1148

Consistency with NIS Directive (for essential services)

- **NIS Directive, Article 14:**
  - **Point 1:** "Member States shall ensure that operators of essential services take……technical and organisational measures to manage the risks posed to the security of network and information systems….."
  - **Point 2:** "Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of network and information systems…..with a view to ensuring the continuity of those services."
  - **Point 3:** "Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide….."

- **NIS Directive, Article 1:**
  - **Point 7:** This point allows to replace the requirements contained in the NIS Directive by those of a sector-specific Union legal act if such requirements are at least equivalent to those in the NIS Directive.

Options considered

- **Option 1: requiring the essential services to comply both with the NIS Directive and the requirements proposed in this NPA:**
  - This would have meant a duplication of requirements, sometimes not fully compatible, as well as duplication of authorities and oversight activities.

- **Option 2: replacing the requirements of Article 14 of the NIS Directive by the future requirements proposed in this NPA:**
  - This would not happen until the proposed rules are adopted (not before 2021).
  - Would mean a change of regulatory framework for essential services who may have been already applying the NIS Directive since 2018.

- **Option 3: considering that meeting the requirements of Article 14 of the NIS Directive would be acceptable instead of complying with the requirements proposed in this NPA:**
  - **<u>This was the option initially selected in NPA 2019-07.</u>**

Option initially selected in NPA 2019-07

- **Option initially selected:** Meeting the requirements of Article 14 of the NIS Directive would be acceptable for essential services, instead of complying with the requirements proposed in this NPA. **With one condition:**
  - The competent authority responsible for the safety approval (EASA rules) and the competent authority for the NIS Directive shall establish an agreement to coordinate the aspects impacting aviation safety.

- **Benefits:**
  - Prevents duplication of requirements and permits essential services to continue with their established practices related to information security.
  - Ensures coordination between authorities.
  - Prevents interference on how the Member States implement the NIS Directive across the different sectors (energy, banking, transport, etc) and define their authority structures.

Option initially selected in NPA 2019-07

- **Drawback:**
  - **Lack of standardisation across the EU:** The requirements imposed on essential services as a result of the NIS Directive currently vary across the different Member States.
  - **Risk that in certain countries, the NIS Directive may have been implemented in a very relaxed manner.** The essential services would be complying with those relaxed requirements while the non-essential services would have to comply with the more strict requirements of the future EASA rules.

Option finally selected (after comments received to NPA 2019-07)

- **Option 2: replacing the requirements of Article 14 of the NIS Directive by the future requirements proposed in this NPA:**
  - This would not happen until the proposed rules are adopted (not before 2021).
  - Would mean a change of regulatory framework for essential services who may have been already applying the NIS Directive since 2018.

  - **Mitigating measures:**
    - For the upcoming Acceptable Means of Compliance (AMC) and Guidance Material (GM) associated to this rule, EASA and the ESCP will review existing policies used by those Member States which are more advanced in the implementation of the NIS Directive.
      - This will allow to the essential services to continue doing what they were doing (if considered robust enough).
      - This will also allow to use that material across all the EU Member States and for all stakeholders (not only for essential services)

Consistency with Regulation (EU) 2015/1998

Regulation (EU) 2015/1998

- **Focuses on aviation security.**
- **Applies only to:**
  - Airports or parts of airports.
  - Operators (including air operators) and entities that provide services or goods to or through those airports.
- **It has been recently amended to align with Amendment 16 to ICAO Annex 17:**
  - Point 4.9.1 of ICAO Annex 17 on measures relating to cyber-threats, has become a "standard" applicable since November 2018:

    > *"Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference."*
- **Contains a provision that allows the replacement of those requirements by other equivalent EU requirements (the future EASA rules).**

Conclusions

Conclusions

- → **The future EASA cybersecurity rule should serve as the standard for the management of cybersecurity risks and reporting of incidents for the full aviation domain.**

- → **The requirements contained in the NIS Directive and the Aviation Security Regulation 2015/1998 would become superseded by the future EASA rules** (unless there are specific issues related to continuation of services and security which have not been properly addressed by the safety perspective of the future EASA rules)

- → **The audits on the organisations should be performed in a consistent manner involving the different authorities of the country, without duplicating audits.**

- → **The organisational structures in the Member States will need to be adapted to this new framework.**

EASA

European Union Aviation Safety Agency

Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union