EASA
European Union Aviation Safety Agency

“How can we regulate to protect against cyber risks”

Juan Anton
Cybersecurity in Aviation & Emerging Risks Section Manager

4th / 5th March 2020
2020 High Level Cybersecurity Conference
Madrid (Spain)

Your safety is our mission.

An Agency of the European Union

Why we need to develop new rules

Information security risks are constantly increasing

- **<u>Information systems are becoming increasingly complex and interconnected, and a more frequent target of cyber-crime.</u>**
  - 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.

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)

- **They are not focused on the impact on aviation safety**
  - **NIS Directive:** focus on preventing disruption of essential services (social and economic impact).
  - **Reg. 2015/1998:** focus on aviation security.
- **They do not cover all aviation domains and stakeholders**
  - **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.

- **Very different speeds of implementation across the Member States.**

- **Waiting for full implementation of the NIS Directive would have meant 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 have meant 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.**

Key elements of the proposed rule

Key elements:

- → **Introduce common requirements for an Information Security Management System (ISMS) and reporting of incidents.**
- → **Focus on the impact of information security threats and events on safety** *(directly on the aircraft or on the European Traffic Management Network)*
- → **Need to cover all aviation domains and interfaces** *(system-of systems)*
- → **Consistency with NIS Directive and Reg. 2015/1998** *(no gaps, loopholes or duplications)*
- → **Compliance with ICAO standards.**
- → **Minimize the impact on existing EASA regulations.**
- → **Proportionality to the risks incurred by the different organisations.**
- → **High-level, performance/risk-based rules supported by AMC/GM and industry standards.**
- → **Make possible for organisations and authorities to integrate the Information Security Management System (ISMS) with other management systems.**

Entry into Force and transition measures

- **NPA 2019-07 published on 27 May 2019.**
  - Public Consultation on the EASA website ended on 27 September 2019.

- **Opinion expected by summer 2020.**

- **Entry into force: once adopted by the European Commission (not expected before end of 2021).**

- **Expected to include transition measures to facilitate implementation.** A phased approach could be followed depending on the different timing where authorities and organisations could be ready to apply the different requirements.

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

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, totally or partially, 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.

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

- **Apply the Part-AISS requirements to all domains and use the "lex specialis" provisions of the NIS Directive:**
  - This would not happen until the proposed rules are adopted (not before end 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.
      - <u>This will allow to the essential services to continue doing what they were doing (if considered robust enough).</u>
      - <u>This will also allow to use that material across all the EU Member States and for all stakeholders (not only for essential services)</u>

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 replacing, totally or partially, those requirements by other equivalent EU requirements (e.g. 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 <u>from the safety perspective.</u>**
- **It could be possible to use the "lex specialis" provisions of the NIS Directive and the AVSEC Regulation to replace, totally or partially, their requirements by those in Part-AISS** (in order to avoid duplication of audits in equivalent areas).
- **Organisations could still apply procedures they are using under the NIS Directive or AVSEC Regulation if they meet the intent of the future Part-AISS** (through Acceptable and Alternative Means of Compliance).
- **The audits on the organisations should be performed in a consistent manner involving the different authorities of the country, without duplicating audits, and taking into account the different perspectives.**
- **The organisational structures in the Member States may 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

More details about the proposed rule

Scope of applicability

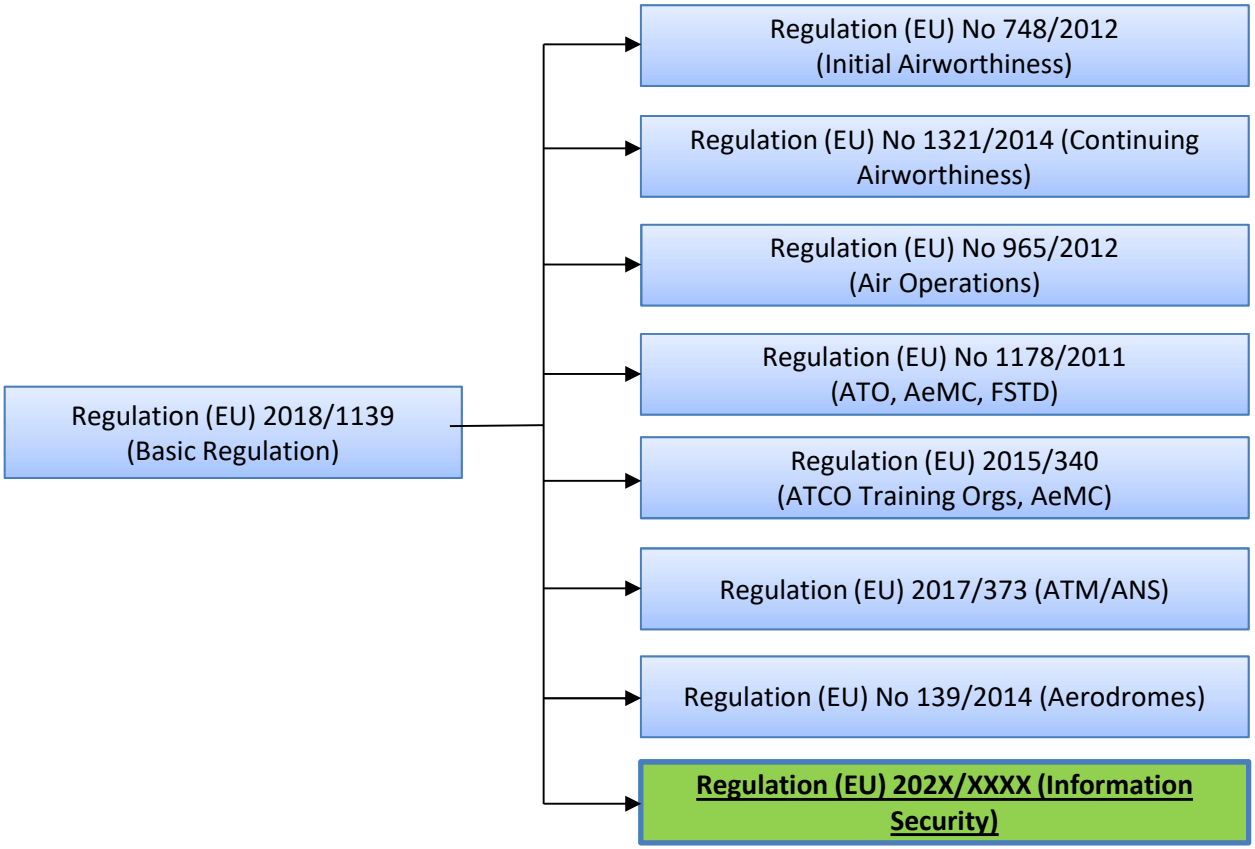
- Competent authorities.

- POA *(production)* and DOA *(design)* approval holders.
- Part-145 maintenance organisations.
- Part-CAMO continuing airworthiness management organisations.
- Air operators covered by Part-ORO *(commercial and/or larger aircraft).*
- Aircrew training organisations (ATOs) and aircrew Aeromedical Centres.
- ATCO training organisations and ATCO Aeromedical Centres.
- ATS, MET, AIS, DAT, CNS, ATFM and ASM providers and the Network Manager.
- Aerodrome operators and apron management service providers.

Exempted organisations

- Production and Design organisations not holding an approval (alternative procedures)
- Part-CAO organisations (they deal with lighter aircraft).
- Part-147 maintenance training organisations.
- Declared training organisations (for pilot licences of lighter aircraft)
- ATOs providing only theoretical training.
- Private operators of other than complex motor-powered aircraft.
- TCO operators (they will still be subject to national requirements resulting from point 4.9 "Measures relating to cyber threats" of ICAO Annex 17).
- Operators of UAS in the "open" and "specific" categories (in the future, for the "certified category", the exemption may not apply).
- POAs, DOAs, ATOs, FSTD operators and air operators, when solely dealing with ELA2 aircraft (most aeroplanes below 2000Kg MTOM, very light rotorcraft, sailplanes, balloons and airships).

The Cybersecurity rule within the EASA regulatory framework



Cross-references in the existing Implementing Rules

- **<u>AN EXAMPLE: Regulation (EU) No 1321/2014 (Continuing Airworthiness):</u>**
  - **In Part-145, Section A**:
    - **New point 145.A.72 "Information Security": The maintenance organisation shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-145, Section B:**
    - **Point 145.B.01 "Scope" amended to read:**

      This Section, **together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX,** establish the administrative and management system requirements to be followed by the competent authority that is in charge of the implementation and enforcement of Section A of this Annex.

Structure of the rule

- **Separate regulation with similar structure as other Implementing Rules:**
  - **Cover Regulation**, including:
    - Objectives, scope, definitions, competent authority and entry into force.
  - **Annex I "Part-AISS.AR — Authority Requirements"**
  - **Annex II "Part-AISS.OR — Organisation Requirements"**

Structure of the rule

ANNEX II

AERONAUTICAL INFORMATION SYSTEM SECURITY — ORGANISATION REQUIREMENTS

[PART-AISS.OR]

AISS.OR.005	Scope
AISS.OR.100	Personnel requirements
AISS.OR.200	Information security management system (ISMS)
AISS.OR.300	Information security internal reporting scheme
AISS.OR.310	Information security external reporting scheme
AISS.OR.400	Contracted activities
AISS.OR.500	Record keeping
AISS.OR.700	Information security management manual (ISMM)
AISS.OR.800	Changes to the organisation
AISS.OR.900	Findings

Some key elements of the ISMS (AISS.OR.200)

- **Establish, implement, maintain and continuously improve an ISMS. This ISMS shall (among other aspects):**
  - **Identify the organisation activities, facilities and resources, and the equipment, systems and services it provides, maintains and operates, which could be exposed to cyber risks.**
  - Identify the **interfaces with other organisations** with which it shares cyber risks.
  - Identify their **critical information and communication technology systems.**
  - Perform **information security risk assessments** (initially and when changes occur).
  - Develop and implement measures to **protect critical systems, data and processes.**
  - **Identify vulnerabilities and mitigate any unacceptable risks and vulnerabilities.**
  - Ensure that **personnel have the competences and skills** to perform their tasks.