EASA
European Union Aviation Safety Agency

NPA 2019-07 “Management of Information Security Risks”
Summary of Discussion: AMC & GM

Jean-Paul Moreaux
Principle Cybersecurity in Aviation Coordinator

2nd July 2019
EASA Workshop on NPA 2019-07

Your safety is our mission.

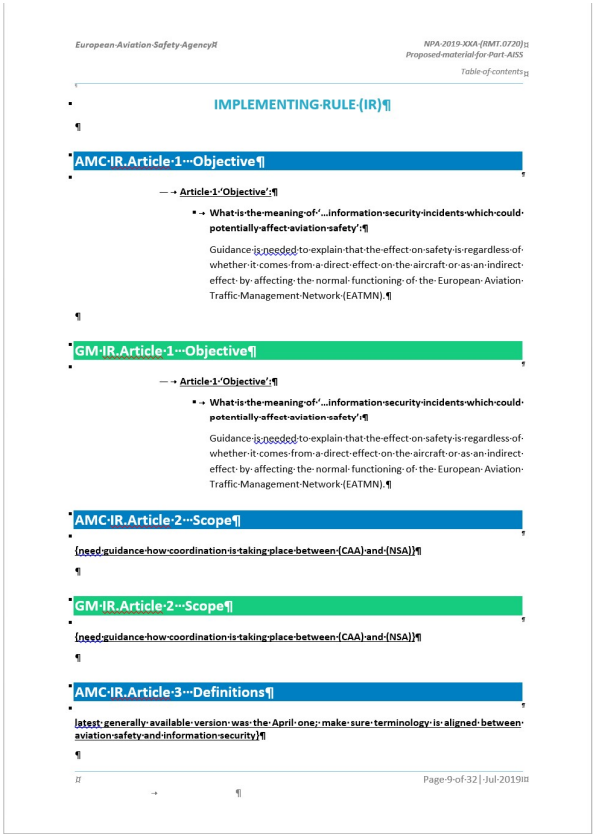
An Agency of the European Union

Summary of AMC & GM Discussions

- **First ESCP Regulatory Processes Work Stream Meeting related to AMC and GM Discussion:**

  27 & 28 May 2019

  - Based upon a first draft document, covering
    - General Discussion
    - Implementing Rule
    - Authority Requirements
    - Organisation Requirements
  - Should be ready early in 2021 to be considered by the European Commission and Member States before adopting the future rule.


European Aviation Safety Agency

NPA 2019-XXA (RMT.0720)
Proposed material for Part-AISS

Table of contents

IMPLEMENTING RULE (IR)

AMC IR.Article 1 … Objective

Article 1 'Objective':

What is the meaning of '…information security incidents which could potentially affect aviation safety':

Guidance is needed to explain that the effect on safety is regardless of whether it comes from a direct effect on the aircraft or as an indirect effect by affecting the normal functioning of the European Aviation Traffic Management Network (EATMN).

GM IR.Article 1 … Objective

Article 1 'Objective':

What is the meaning of '…information security incidents which could potentially affect aviation safety':

Guidance is needed to explain that the effect on safety is regardless of whether it comes from a direct effect on the aircraft or as an indirect effect by affecting the normal functioning of the European Aviation Traffic Management Network (EATMN).

AMC IR.Article 2 … Scope

{need guidance how coordination is taking place between (CAA) and (NSA)}

GM IR.Article 2 … Scope

{need guidance how coordination is taking place between (CAA) and (NSA)}

AMC IR.Article 3 … Definitions

{latest generally available version was the April one; make sure terminology is aligned between aviation safety and information security}

Page 9 of 32 | Jul 2019

Development of AMCs and GMs

- **Objective is to**
  - **Make use of Industry Standards, where possible**
  - **Align requirements from both, existing Aviation and IT related Standards and Best Practices, such as (but not limited to):**
    - ISO 27000 Series on 'information security management systems (ISMS)' standards;
    - ISO 31000 Series on 'risk management' standards;
    - CEN — EN 16495 on standards for 'Air Traffic Management — Information security for organisations supporting civil aviation operations';
    - ECAC Document 30 'Recommendations on cyber security and supporting Guidance Material'.
    - Eurocae, RTCA or SAE Industry Standards
  - **Adopt material available in the Member States for the implementation of the NIS Directive, and for the implementation of ICAO Annex 17, if found appropriate for the wider aviation sector (not just for Essential Services or Aviation Security).**

Main Subjects of Discussions held

- → Broader Principles to be used
- → Standardisation of Terminology
- → Information Security Management System (ISMS)
- → Audit and Oversight
- → Personnel Requirements (Skills, Background Checks)
- → Logging and Reporting
- → Shared Trans-Organisational Risk Management (STORM)
- → Roles and Responsibilities
- → Sharing of Information

A few more Details (1)

- → Broader Principles to be used
  - → Trustworthiness (CEN 16495), Capability Maturity (NPA Example), Operating Conditions (for Information Security, ANC/13 WP-160)
- → Standardisation of Terminology
  - → Alignment of Glossaries between ICAO, ECAC, EASA, Eurocae, SAE-IA, etc.
  - → Adopt what's globally available, and adapt to Aviation, where needed
- → Information Security Management System (ISMS)
  - → ISO27000 "too inward looking", need System-of System notion
  - → Applicability to Supply Chain?
  - → Security Event Management (Incidents, Vulnerabilities, Threats…)
  - → Asset and Config Management

A few more Details (2)

- → Information Security Management System (ISMS) – cont'd
  - → Assurance Requirements (see other OT Technical Standards, e.g. IEC62443)
- → Audit and Oversight
  - → One Organisation, One Audit only
  - → Harmonised Audit and Oversight Requirements between Aviation Safety, Security and Essential Services (as far as possible)
  - → Coordination between Competent Authorities
  - → Unified Accreditation of 3rd Party Audit Organisations
  - → Mutual Auditing System

A few more Details (3)

- Personnel Requirements
  - Skills needed
  - Who to background check? Based upon which regulation?
- Logging and Reporting
  - Reporting Objectives? Threshold of reporting?
  - Raw Data or confirmed safety related? Looking back for how long?
  - How to avoid duplication with NIS/AVSEC requirements?
  - To whom to report (Authority, ECCSA, EA-ISAC)
  - Safety reporting (376/2014) sufficient?

A few more Details (4)

- → Shared Trans-Organisational Risk Management (STORM)
  - → Identification of organisational relationships: Functional Chains
  - → Harmonisation of Risk Assessments, which information to share?
  - → Rules for Attribution of Information Security Requirements
  - → How to develop confidence in other organisations
- → Roles and Responsibilities
  - → How to connect organisations?
- → Sharing of Information
  - → Classification of Information or TLP?
  - → Operational Information (ECCSA, ISACs)
  - → Risk Information

EASA
European Union Aviation Safety Agency

EASA Workshop on NPA 2019-07

The End

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union