European Aviation Safety Agency

Terms of Reference

for rulemaking task RMT.0720

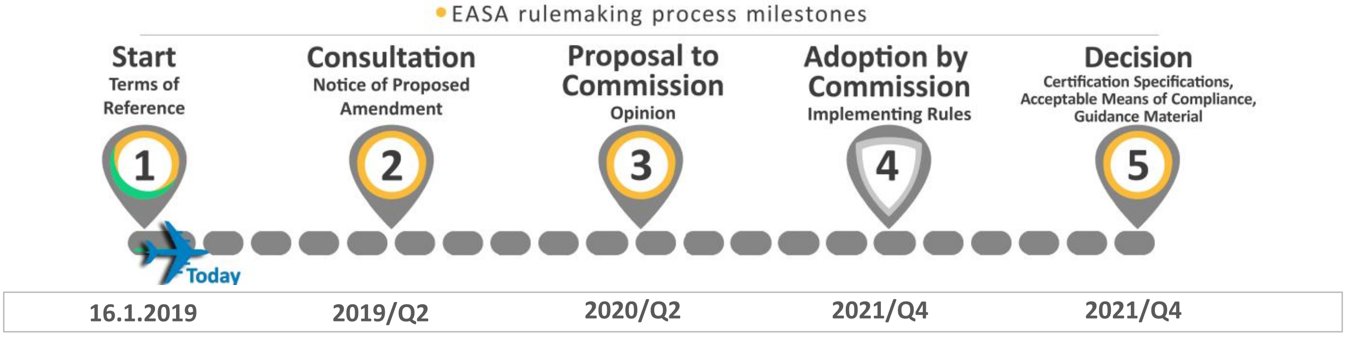
Cybersecurity risks

ISSUE 1

Issue/rationale

The specific objective of this task is to create a regulatory system that efficiently contributes to the protection of the aviation system from cyber-attacks and their consequences. To achieve this objective, it is proposed to introduce provisions for the management of cybersecurity risks by organisations in all the aviation domains (design, production, continuing airworthiness management, maintenance, operations, aircrew, ATM/ANS, aerodromes). These provisions would include high-level, performance-based requirements, and would be supported by AMC & GM material and industry standards.

Action area:	Emerging issues — safety and security		
Affected rules:	Regulations (EU) No 748/2012, No 1321/2014, No 1035/2011, 2017/373, 2015/340, No 139/2014, No 1178/2011, No 965/2012.		
Affected stakeholders:	manufacturers, airlines, maintenance organisations, CAMOs, training organisations, ATM/ANS providers, aerodromes, and Member States.		
Driver:	Safety	**Rulemaking group:**	No
Impact assessment:	Light	**Rulemaking Procedure:**	Standard



1. Why we need to change the rules — issue/rationale

The current European regulatory framework contains a series of requirements that would prevent an accident from happening. These requirements include, among other aspects:

- comprehensive requirements for the certification of aircraft and associated parts and components;
- comprehensive requirements for the continuing airworthiness of aircraft, including duplicated inspections for critical areas/systems;
- comprehensive requirements for the approval of organisations, complemented by periodic audits performed by their competent authority;
- independent quality systems or organisational reviews within all approved organisations;
- periodic airworthiness reviews performed on every aircraft to ensure the validity of the certificate of airworthiness;
- an aircraft continuing airworthiness monitoring programme implemented by the competent authority of the State where the aircraft is registered; and
- requirements for coordination between the competent authorities of the different Member States.

This combination of requirements allows that even if an error, mistake and/or deficiency happens, this should not create a hazardous situation that could result in an accident. As a consequence, an accident would only happen in the random event of several deficiencies happening simultaneously and, by chance, aligning themselves.

The concern, however, is that not enough focus may have been put in properly addressing the situation where existing flaws in different areas are aligned on purpose and exploited by individuals with a malicious intent, no longer being a random event. Such a risk is constantly increasing in the civil aviation environment as the current aviation information systems are becoming more and more interconnected, with several major elements interacting with the aircraft as well as with each other, such as:

- the original equipment manufacturer (OEM) and its supply chain;
- the operator (e.g. airlines), including the aircrew;
- the ground service providers;
- the aerodromes;
- the maintenance organisations;
- the passengers;
- the air traffic management (ATM) and aeronautical information services (AIS);
- communication service providers (CSP) and satellite service providers (SSP);
- third parties having access to non-protected aviation transmissions.

This is what we call cybersecurity risks, and addressing them is the objective of this rulemaking task.

It is important to note that, since a cyber event can have direct consequences on the safety of flight, interactions between information security and safety management systems (SMS) may be relevant for addressing cyber security risks. Nevertheless, certain adaptations will need to be made to take into account the differences which do exist, especially in relation to the concept of 'vulnerabilities' and the 'notion of intent', as well as the need to properly handle confidential and sensitive information.

These adaptations need to take into account that there is the intent and desire to damage aircraft systems, to disrupt operations, or to threaten human lives. In other words, there are entities that are intentionally looking for weaknesses in the system that can be exploited with the aim of creating maximum harm. These potential weaknesses are not always known to the operator. Furthermore, in some cases, weaknesses may be intentionally combined to obtain maximum damage, potentially having in such cases catastrophic effects, although, when assessed individually, they could appear harmless. In other cases, weaknesses could be inadvertently exploited by malware spreading beyond their intended target. Weaknesses can also be very different in nature, some related to hardware, some to software, and even some to physical security of a given system. When weaknesses can be exploited, they are called vulnerabilities. Timely reaction to known vulnerabilities adapted to the situation, as well as keeping critical systems away from unauthorised access, is essential to prevent potential attackers, who may have very different profiles and who can adapt quickly to the system, from exploiting them or combining them with other vulnerabilities.

In addition, the adaptations also need to consider those cases where attacks are performed for other purposes, not necessarily targeting aviation, but which may have a collateral damage on aviation safety.

Related safety issues

There are no safety recommendations (SRs) addressed to EASA pertinent to the scope of this RMT.

Exemptions[1] in accordance with Article 70 'Safeguard provisions' and Article 71 'Flexibility provisions' of Regulation (EU) 2018/1139[2]

There are no exemptions pertinent to the scope of this RMT.

Alternative means of compliance (AltMoC) relevant to the content of this RMT

There are no alternative means of compliance (AltMoC) having an impact on the development of this RMT content.

ICAO and third countries references relevant to the content of this RMT:

The Amendment 16 to ICAO Annex 17 adopted by the Council on 14 March 2018, and in particular its point 4.9 'Measures relating to cyber threats', will have to be considered during this RMT.

References to differences between the content of this RMT and ICAO SARPs, FARs, etc.

There are no relevant differences.

[1] Exemptions having an impact on the development of this RMT content and referring to:
- Article 70(1): Measures taken as an immediate reaction to a problem relating to civil aviation safety.
- Article 71(1): Exemptions from substantive requirements laid down in the Basic Regulation and its implementing rules in the event of urgent unforeseeable circumstances or urgent operational needs;

[2] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.08.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1139&from=EN)

EU requirement not having yet relevant reference — stemming from a comparison between the intended content of this RMT with ICAO SARPs, FARs, etc.

There are no current equivalent requirements at ICAO or the FAA to those that are intended to be introduced with this task.

2. What we want to achieve — objective

The overall objectives of the EASA system are defined in Article 1 of Regulation (EU) 2018/1139. This project will contribute to the achievement of the overall objectives by addressing the issues outlined in Chapter 1.

The specific objective is to propose requirements to be met by an organisation to identify, be protected from, detect, respond to and recover from those information security events that could potentially affect aviation safety or could affect the EATMN 'European Aviation Traffic Management Network' (composed of the systems listed in Annex I to Regulation (EC) No 552/2004).

These requirements should be consistent across the different aviation domains, and need to take into account the risks associated to:

— the organisation's facilities and activities;

— the products, systems and services it provides, maintains and operates;

— the products, systems and services received from other parties;

— its interactions with other organisations

3. How we want to achieve it

During the development of the draft rules and the RIA, the following activities will be considered:

— Review the legal basis of the task, taking into account the new Basic Regulation.

— Balance the urgency of the task with the need for promotion and harmonisation at international level.

— Review the scope of the task, in particular the aviation domains affected and the interfaces between safety and security.

— Review the different options for the structure of the proposed rules. In particular, whether the preferred approach is to develop a new horizontal rule for cybersecurity covering all domains or to develop further provisions related to cybersecurity in existing regulations.

— Ensure adequate proportionality of the proposed rules.

— Ensure consistency with other existing EU regulations, such as Regulation (EU) 2015/1998 on aviation security, and with the national security requirements stemming from Directive (EU) 2016/1148 of 6 July 2016[3] (also called 'the NIS Directive').

— Ensure compliance with ICAO requirements.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1527600196814&uri=CELEX:32016L1148

- Ensure adequate flexibility of the rule, taking into account a high-level, performance and risk-based approach.
- Review the need for associated AMC & GM and industry standards, identifying which existing best practices and material can be used as a source.
- Review the impact of the proposed changes.

4. What are the deliverables

- NPA with draft implementing rules, AMC & GM
- Opinion with draft implementing rules
- Decision with associated AMC & GM

5. How we consult

This rulemaking task has been established as an Agency task with consultation through the European Strategic Coordination Platform (ESCP).

Due to the complexity of the matter and the extremely wide scope of EU Institutions/Agencies/Organisations, competent authorities, stakeholders and international regulatory partners affected, this rulemaking task will be developed in full discussion, consultation and coordination with the ESCP. This platform is already discussing all the elements associated with the EU aviation cybersecurity strategy (not only regulatory matters), and it is seen as the best forum for these discussions.

This platform includes:

- An **Executive Committee (ESCP-EC)** at the higher, political level.
- A **Technical Advisory Committee (ESCP-TAC)** at the technical level, **with different work streams,** to discuss various matters **(ESCP governance matters, EU cybersecurity strategy, regulatory actions, coherence and consistency of risk management processes, etc.).**

This platform has been meeting since July 2017 and is composed of representatives from the following organisations:

- **Members:**
  - European Commission (DG-MOVE, DG-CNECT, DG-GROW and DG-HOME)
  - Other EU Agencies and Organisations:
- European External Action Service (EEAS)
- EUROPOL
- European Aviation Safety Agency (EASA)
- European Network Information Security Agency (ENISA)
- EU Computer Emergency Response Team (CERT-EU)
- EUROCONTROL
- SESAR Deployment Manager

- SESAR Joint Undertaking
  - European Defence Agency (EDA)
  - 6 Member States (Finland, France, Poland, Romania, Sweden, and the UK)
  - European Civil Aviation Conference (ECAC)
  - Aviation industry associations
- AeroSpace and Defence Industries Association Europe (ASD)
- Airlines for Europe (A4E)
- Airports Council International - Europe (ACI)
- Civil Air Navigation Services Organisation - Europe (CANSO)
- European Cockpit Association (ECA)
- European Helicopter Association (EHA)
- European Independent Maintenance Group (EIMG)
- European Regional Airlines Association (ERAA)
- European Transport Workers' Federation (ETF)
- General Aviation Manufacturers (GAMA)
- International Air Transport Association - Europe (IATA)
- **Observers:**
  - ICAO
  - FAA and TCCA
  - NATO
  - Aerospace Industries Association of America (AIA)
  - Aerospace Industries Association of Canada (AIAC)

6. Interface issues

The content of this rulemaking task should be coordinated with the ongoing rulemaking activities linked to safety management system (SMS). This will ensure proper consistency of requirements for safety risk management and information security risk management. It will also facilitate the integration of both systems by the industry.

In addition, it is essential to ensure consistency of regulatory requirements between the different frameworks (NIS Directive, Regulation 2015/1998 and the future EASA rules), as well as adequate coordination between the different authorities (European, NAAs, security authorities, etc.). This, while avoiding possible duplications and loopholes, coordinating with ENISA and the NIS Directive Cooperation Group to take into account the already on-going transposition by the States of the NIS Directive.

These regulatory frameworks may have different objectives (such as preventing disruption of essential services to society, addressing aviation security issues, or addressing the impact on safety), and may not cover the same scope of organisations. However, all of them are important and needed to address in a comprehensive, consistent, and standardised manner the security and safety of the aviation system.

In particular, the following interface areas need to be considered:

— At national level: interfaces between State Safety Programmes, National Aviation Security Programmes, National Cybersecurity Strategies and National Essential Services Protection policies.

— At organisation level: interfaces between security programmes/security management systems, information security management systems and safety management systems.

NOTE 1: RMT.0720 focuses on introducing provisions for organisations and does not intend to introduce requirements for the certification of products. This is, however, the objective of another rulemaking task (RMT.0648 'Aircraft cybersecurity'), that is intended to develop provisions for the certification of products in the corresponding certification specifications (CSs). Both tasks have 'safety' as the common driver, since both tasks have the objective to address cybersecurity risks.

NOTE 2: Currently there are no EU requirements for organisations in the area of unmanned aircraft systems (UAS). As a consequence, until such requirements exist, cybersecurity aspects for organisations dealing with UAS are beyond the scope of this rulemaking task.

7. Reference documents

7.1. Affected regulations

— Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations (OJ L 224, 21.8.2012, p. 1)

— Regulation (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks (OJ L 362, 17.12.2014, p. 1)

— Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 296, 25.10.2012, p. 1)

— Regulation (EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 311, 25.11.2011, p. 1)

— Regulation (EU) 2015/340 of 20 February 2015 laying down technical requirements and administrative procedures relating to air traffic controllers' licences and certificates pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council, amending Commission Implementing Regulation (EU) No 923/2012 and repealing Commission Regulation (EU) No 805/2011 (OJ L 63, 6.3.2015, p. 1)

— Regulation (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010 (OJ L 271, 18.10.2011, p. 23)

— Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011 (OJ L 62, 8.3.2017, p. 1)

NOTE: Future evolution of the current Regulation (EU) No 73/2010 of 26 January 2010 laying down the requirements on the quality of aeronautical data and aeronautical information for the single European sky (OJ L 23, 27.1.2010, p.6) will also be considered.

— Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 44, 14.2.2014, p. 1)

7.2. Affected decisions

— AMC & GM associated with the regulations listed in section 7.1.

7.3. Reference documents

The following list (not exhaustive) includes documents that will be considered during the developments of this rulemaking task:

— Amendment 16 to ICAO Annex 17 adopted by the Council on 14 March 2018.

— Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 104, 19.7.2016, p. 1)

— Regulation (EU) No 376/2014 of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 (OJ L 122, 24.4.2014, p. 18)

— Regulation (EU) 2015/1018 of 29 June 2015 laying down a list classifying occurrences in civil aviation to be mandatorily reported according to Regulation (EU) No 376/2014 of the European Parliament and of the Council (OJ L 163, 30.6.2015, p. 1)

— Regulation (EC) No 552/2004 of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26)

— Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72)

— Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015, p. 1)

— 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’