EUROPEAN
COMMISSION

Brussels, XXX
[…](2021) XXX draft

ANNEX III TO EASA OPINION 03 2021

COMMISSION DELEGATED REGULATION (EU) …/...

of XXX

amending Commission Regulations (EU) No 748/2012 and No 139/2014 as regards the introduction of requirements for the management of information security risks with a potential impact on aviation safety for organisations

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

The current European aviation safety regulatory framework contains a series of requirements which are aimed at reducing the likelihood of an accident happening.

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

The concern 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 information systems are becoming more and more interconnected.

As a consequence, it is necessary to introduce requirements for the management of information security risks which could have an impact on aviation safety.

In the particular case of this Delegated Act, the provisions introduced increase the robustness of the management systems and reporting processes and procedures required by Annex II 'Essential requirements for airworthiness' and Annex VII 'Essential requirements for aerodromes' to Regulation (EU) 2018/1139 ([1]) for design and production organisations, and for aerodrome operators and providers of apron management services.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

In accordance with Article 128(4) of Regulation (EU) 2018/1139, before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. The present draft delegated act was presented to the Air Safety experts group, which includes representatives from the Member States, at its meeting on […]. The present draft delegated act is based on EASA Opinion No 03/2021 whose contents had been publicly consulted through Notice of Proposed Amendment (NPA) 2019-07 'Management of information security risks' ([2]) (RMT.0720), published by EASA on 27 May 2019.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

Articles 19(1) and 39(1) of Regulation (EU) 2018/1139 empower the Commission to adopt delegated acts, in accordance with Article 128 of that Regulation, laying down detailed rules with regard to organisations responsible for the design and production of products, parts and

([1]) 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, 22.8.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

([2]) https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

non-installed equipment, and with regard to organisations responsible for the operation of aerodromes and for the provision of apron management services.

COMMISSION DELEGATED REGULATION (EU) …/...

of XXX

amending Commission Regulations (EU) No 748/2012 and No 139/2014 as regards the introduction of requirements for the management of information security risks with a potential impact on aviation safety for organisations

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 ([3]), and in particular Articles 19(1) and 39(1) thereof,

Whereas:

(1) In accordance with the essential requirements set out in Annex II to Regulation (EU) 2018/1139, design and production organisations shall implement and maintain a management system to manage safety risks.

(2) In addition, in accordance with the essential requirements set out in Annex VII to Regulation (EU) 2018/1139, aerodrome operators and organisations responsible for the provision of apron management services shall implement and maintain a management system to manage safety risks.

(3) The management systems implemented by those organisations to manage safety risks need to take into account not only those risks stemming for random events, but also those where existing flaws may be exploited by individuals with a malicious intent.

(4) This type of risks is constantly increasing in the civil aviation environment as the current information systems are becoming more and more interconnected, and increasingly becoming the target of malicious actors.

(5) The risks associated with these information systems are not limited to possible attacks to the cyberspace, but encompass threats which are both digital and analogue.

(6) A significant number of organisations already use international standards, such as ISO 27001, which deal with the management of information security risks.

(7) As a consequence, it is appropriate to introduce requirements for the management of information security risks, without limiting them to cybersecurity risks.

(8) It is essential that these requirements cover the different aviation domains and their interfaces since aviation is a highly interconnected system of systems. As a consequence, they shall apply to all the organisations and competent authorities that are already required to have a management system in accordance with the existing aviation safety regulations.

([3]) OJ L 212, 22.8.2018, p. 1.

(9) The measures provided for in this Regulation need to contribute to the creation of a seamless and consistent regulatory framework where the interfaces between security and safety are appropriately covered, and where special attention is paid at avoiding gaps, loopholes and duplications with other information security and cybersecurity requirements such as those contained in Commission Implementing Regulation (EU) 2015/1998 ([4]) and in the national requirements stemming from Directive (EU) 2016/1148 (NIS Directive) ([5]).

(10) The measures related to information security and cybersecurity stemming from the NIS Directive, Commission Implementing Regulation (EU) 2015/1998 and this Regulation should be coordinated at national levels to avoid gaps and duplications of obligations.

(11) It is therefore appropriate that, where organisations covered by this Regulation are subject to cybersecurity or information security requirements arising from other EU or national legislation, the competent authority defined according to this Regulation should have the possibility to replace compliance with the requirements of this Regulation by compliance with elements contained in other EU or national legislation, provided that such requirements are at least equivalent in effect to the obligations laid down in this Regulation. In such a case, the competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

(12) In addition, in the particular case of airport operators, air carriers and entities as defined in the national civil aviation security programmes of Member States, it is appropriate that the competent authority responsible for the certification and oversight of the organisation's compliance with this Regulation should have the possibility to replace compliance with the requirements contained in this Regulation, except those related to the information security external reporting schemes, by compliance with elements of the cybersecurity requirements contained in the Annex to Implementing Regulation (EU) 2015/1998. In such a case, the competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

(13) Furthermore, it is also appropriate that even if the competent authority decides not to use the options described in the previous two recitals, the affected organisations should still have the possibility to use compliance methods developed under the cybersecurity or information security requirements of those EU or national legislations as a means to comply with the requirements of this Regulation, In such a case, the organisation shall demonstrate to their competent authority that with those compliance methods the organisation fully meets the requirements and objectives of this Regulation.

(14) The measures provided for in this Regulation need to ensure a consistent implementation across all aviation domains, while creating a minimal impact on the existing rules already applicable to those domains.

(15) The measures provided for in this Regulation need to be proportional to the risks incurred by the different organisations.

(16) The measures provided for in this Regulation need to follow a performance- and risk-based approach.

([4]) Commission Implementing 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).

([5]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

(17) The measures provided for in this Regulation need to ensure that organisations can integrate any new management system requirements with other existing management systems they may have.

(18) A sufficient transition period should be provided for organisations to ensure their compliance with the new rules and procedures introduced by this Regulation.

(19) The measures provided for in this Regulation are based on Opinion No 03/2021 ([6]), issued by the European Union Aviation Safety Agency in accordance with Article 75(2)(b) and (c) and Article 76(1) of Regulation (EU) 2018/1139.

(20) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 127 of Regulation (EU) 2018/1139,

HAS ADOPTED THIS REGULATION:

Article 1

Annex I (Part 21) to Commission Regulation (EU) No 748/2012[7] is amended as follows:

(1) in the 'Contents', the following new points are added:

— '21.A.139A Information security management system'
— '21.A.239A Information security management system';

(2) in 'Section A', a new point 21.A.139A is added as follows:

'21.A.139A Information security management system

In addition to the production management system required by point 21.A.139, the production organisation shall establish, implement and maintain an information security management system in accordance with Delegated Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(3) in 'Section A', a new point 21.A.239A is added as follows:

'21.A.239A Information security management system

In addition to the design management system required by point 21.A.239, the design organisation shall establish, implement and maintain an information security management system in accordance with Delegated Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.'.

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) Commission 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).

Article 2

Annex III 'Part Organisation Requirements (Part-ADR.OR)' to Commission Regulation (EU) No 139/2014 ([8]) is amended as follows:

(1) a new point ADR.OR.D.005A is added as follows:

'ADR.OR.D.005A Information security management system

The aerodrome operator shall establish, implement and maintain an information security management system in accordance with Delegated Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.'

(2) point ADR.OR.D.007 is replaced by the following:

'ADR.OR.D.007 Management of aeronautical data and aeronautical information

(a) As part of its management system, the aerodrome operator shall implement and maintain a quality management system covering the following activities:

(1) its aeronautical data activities; and

(2) its aeronautical information provision activities.

(b) As part of its management system, the aerodrome operator shall establish a security management system to ensure the security of operational data it receives, or produces, or otherwise employs, so that access to that operational data is restricted only to those authorised.

(c) The security management system shall define the following elements:

(1) the procedures relating to data security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;

(2) the means designed to detect security breaches and to alert personnel with appropriate security warnings;

(3) the means of controlling the effects of security breaches and of identifying recovery action and mitigation procedures to prevent reoccurrence.

(d) The aerodrome operator shall ensure the security clearance of its personnel with respect to aeronautical data security.

(e) The aspects related to information security shall be managed in accordance with point ADR.OR.D.005A.';

(3) a new point ADR.OR.F.045A is added as follows:

'ADR.OR.F.045A Information security management system

The organisation responsible for the provision of AMS shall establish, implement and maintain an information security management system in accordance with Delegated

([8]) Commission 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).

Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.'.

Article 3

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [*OP please insert date: **1 year** after the date of entry into force*].

Organisations may correct any findings of non-compliance related to points 21.A.139A, 21.A.239A and ADR.OR.D.005A until ***[****OP please insert date: **2 years** after the date of entry into force****]*** or until the date established by the competent authority for the correction of the finding, whichever comes later.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President
Ursula VON DER LEYEN