Council of the
European Union

Brussels, 18 July 2022
(OR. en)

11468/22

AVIATION 171
DELACT 120

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	14 July 2022
To:	General Secretariat of the Council
No. Cion doc.:	C(2022) 4882 final
Subject:	COMMISSION DELEGATED REGULATION (EU) …/... of 14.7.2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and No 139/2014 and amending Commission Regulations (EU) No 748/2012 and No 139/2014

Delegations will find attached document C(2022) 4882 final.

Encl.: C(2022) 4882 final

EUROPEAN
COMMISSION

Brussels, 14.7.2022
C(2022) 4882 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 14.7.2022

laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and No 139/2014 and amending Commission Regulations (EU) No 748/2012 and No 139/2014

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 a potential 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 draft delegated act was presented to the Air Safety experts group, which includes representatives from the Member States, at its meetings on 17 February and 29 June 2022. The present delegated act is based on EASA Opinion No 03/2021 which 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 non-installed equipment, and with regard to organisations responsible for the operation of aerodromes and for the provision of apron management services.

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

COMMISSION DELEGATED REGULATION (EU) …/...

of 14.7.2022

laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and No 139/2014 and amending Commission Regulations (EU) No 748/2012 and No 139/2014

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) point (g) and 39(1) point (b) thereof.

Whereas:

(1) In accordance with the essential requirements set out in Annex II, point 3.1(b), to Regulation (EU) 2018/1139, design and production organisations are to implement and maintain a management system to manage safety risks.

(2) In addition, in accordance with the essential requirements set out in Annex VII, points 2.2.1 and 5.2, to Regulation (EU) 2018/1139, aerodrome operators and organisations responsible for the provision of apron management services are to implement and maintain a management system to manage safety risks.

(3) The safety risks referred to in recitals (1) and (2) may derive from different sources, including design and maintenance flaws, human performance aspects, environmental threats and information security threats. Therefore, the management systems implemented by the organisations as referred to in recitals (1) and (2), should take into account not only safety risks stemming from random events, but also safety risks deriving from information security threats where existing flaws may be exploited by individuals with a malicious intent. Those information security risks are 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.

(4) The risks associated with those information systems are not limited to possible attacks to the cyberspace, but encompass also threats which may affect processes and procedures as well as the performance of human beings.

3 OJ L 212, 22.8.2018, p. 1.

(5) A significant number of organisations already use international standards, such as ISO 27001, in order to address the security of digital information and data. These standards may not fully address all the specificities of civil aviation.

(6) Therefore, it is appropriate to set out requirements for the management of information security risks with a potential impact on aviation safety.

(7) It is essential that those requirements cover the different aviation domains and their interfaces since aviation is a highly interconnected system of systems. Therefore, they should apply to all the organisations that are already required to have a management system in accordance with the existing Union aviation safety legislation.

(8) The requirements laid down in this Regulation should be consistently applied across all aviation domains, while creating a minimal impact on the Union aviation safety legislation already applicable to those domains.

(9) The requirements laid down in this Regulation should be without prejudice to information security and cybersecurity requirements laid down in Point 1.7 of the Annex to Commission Implementing Regulation (EU) 2015/1998([4]) and in Article 14 of Directive (EU) 2016/1148 of the European Parliament and of the Council([5]).

(10) The definition on information security used for the purposes of this legal act should not be interpreted as divergent from the definition of security of network and information systems laid down in Directive 2016/1148.

(11) In order to avoid duplication of legal requirements, where organisations covered by this Regulation are already subject to security requirements arising from other Union acts referred to in recital (9), which are, in their effect equivalent to the provisions laid down in this Regulation, compliance with those security requirements should be considered to constitute compliance with the requirements laid down in this Regulation.

(12) Organisations covered by this Regulation that are already subject to security requirements arising from Regulation (EU) 2015/1998 should also comply with the requirements of Annex I (Part IS.D.OR.230 "Information security external reporting scheme") to this Regulation as Regulation (EU) 2015/1998 does not contain any provisions related to external reporting of information security incidents.

(13) Regulations (EU) No 748/2012([6]) and No 139/2014([7]) should be amended in order to establish the link between the management systems prescribed in the regulations listed above and the information security management requirements prescribed by this Regulation.

---

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).

6 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

7 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

(14) In order to provide organisations with sufficient time to ensure compliance with the new rules and procedures introduced by this Regulation, this Regulation should apply from 3 years after the date of entry into force.

(15) The requirements laid down by this Regulation are based on Opinion No 03/2021([8]), issued by the Agency in accordance with Article 75(2) points (b) and (c) and Article 76(1) of Regulation (EU) 2018/1139.

(16) In accordance with Article 128(4) of Regulation (EU) 2018/1139, the Commission consulted experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[9],

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation sets out the requirements to be met by the organisations referred to in Article 2 in order to identify and manage information security risks with potential impact on aviation safety which could affect information and communication technology systems and data used for civil aviation purposes and to detect information security events and identify those which are considered information security incidents with potential impact on aviation safety and respond to, and recover from, those information security incidents.

Article 2

Scope

1. This Regulation applies to the following organisations:

(a) production organisations and design organisations subject to Subparts G and J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012, except design and production organisations that are solely involved in the design and/or production of ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012;

(b) aerodrome operators and apron management service providers subject to Annex III 'Part Organisation Requirements (Part-ADR.OR)' to Regulation (EU) No 139/2014[10].

2. This Regulation is without prejudice to information security and cybersecurity requirements laid down in Point 1.7 of the Annex to Commission Implementing

8 https://www.easa.europa.eu/document-library/opinions

9 OJ L 123, 12.5.2016, p. 1.

10 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) 2015/1998[11] and in Article 14 of Directive (EU) 2016/1148 of the European Parliament and of the Council[12].

Article 3

Definitions

For the purpose of this Regulation, the following definitions shall apply:

(1) 'information security' means the preservation of confidentiality, integrity, authenticity and availability of network and information systems;

(2) 'information security event' means an identified occurrence of a system, service or network state indicating a possible breach of the information security policy or failure of information security controls, or a previously unknown situation that can be relevant for information security;

(3) 'incident' means any event having an adverse effect on the security of network and information systems as defined in Article 4(7) of Directive (EU) 2016/1148;

(4) 'information security risk' means the risk to organisational civil aviation operations, assets, individuals, and other organisations due to the potential of an information security event. Information security risks are associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets;

(5) 'threat' means a potential violation of information security which exists when there is an entity, circumstance, action or event that could cause harm;

(6) 'vulnerability' means a flaw or weakness in an asset or a system, procedures, design, implementation, or information security measures that could be exploited and results in a breach or violation of the information security policy.

Article 4

Requirements arising from other Union legislation

1. Where an organisation referred to in Article 2 complies with security requirements laid down in Article 14 of Directive (EU) 2016/1148 of the European Parliament and of the Council that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation.

2. Where an organisation referred to in Article 2 is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 of the European Parliament and of the Council[13], the cybersecurity requirements contained in Point

---

11 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).

12 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).

13 Regulation (EC) No 300/2008 of the European Parliament and of the Council 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).

1.7 of the Annex to Implementing Regulation (EU) 2015/1998 are considered to be equivalent to the requirements laid down in this Regulation, except as regards point IS.D.OR.230 of the Annex to this Regulation that shall be complied with.

3. The Commission, after consulting EASA and the Cooperation Group referred to in Article 11 of Directive (EU) 2016/1148, may issue guidelines for the assessment of the equivalence of requirements laid down in this Regulation and Directive (EU) 2016/1148.

Article 5

Competent authority

1. The authority responsible for certifying and overseeing compliance with this Regulation shall be:

   (a) with regard to organisations referred to in Article 2, point (a), the competent authority designated in accordance with Annex I (Part 21) to Regulation (EU) No 748/2012;

   (b) with regard to organisations referred to in Article 2, point (b), the competent authority designated in accordance with Annex III (Part-ADR.OR) to Regulation (EU) No 139/2014.

2. Member States, may for the purposes of this Regulation, designate an independent and autonomous entity to fulfil the assigned role and responsibilities of the competent authorities referred to in paragraph 1. In that case, coordination measures shall be established between that entity and the competent authorities, as referred to in paragraph 1, to ensure effective oversight of all the requirements to be met by the organisation.

Article 6

Amendment to Regulation (EU) No 748/2012

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

(1) the Table of Contents is amended as follows:

   (a) the following heading is inserted after heading 21.A.139:

   "21.A.139A Information security management system;

   (b) the following heading is inserted after heading 21.A.239:

   '21.A.239A Information security management system";

(2) the following point 21.A.139A is inserted after point 21.A.139:

"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 *[OP: Please insert reference number of this Delegated Regulation]* in order to ensure the proper management of information security risks which may have an impact on aviation safety.";

(3) the following point 21.A.239A is inserted after point 21.A.239:

‘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 *[OP: Please insert reference number of this Delegated Regulation]* in order to ensure the proper management of information security risks which may have an impact on aviation safety.’.

Article 7

Amendment to Regulation (EU) No 139/2014

Annex III (Part-ADR.OR) to Regulation (EU) No 139/2014[14] is amended as follows:

(1) the following point ADR.OR.D.005A is inserted after point ADR.OR.D.005:

“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 *[OP: Please insert reference number of this Delegated Regulation]* 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;

(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.

---

14 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).

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

(3) the following point ADR.OR.F.045A is inserted after point ADR.OR.F.045:

"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 Regulation (EU) 202X/XXXX *[OP: Please insert reference number of this Delegated Regulation]* in order to ensure the proper management of information security risks which may have an impact on aviation safety.".

Article 8

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 ***3 years*** *after the date of entry into force*.

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

Done at Brussels, 14.7.2022

For the Commission
The President
Ursula VON DER LEYEN