

## ANNEX

The Annex to Implementing Regulation (EU) 2015/1998 is amended as follows:

- (1) The following point 1.0.6 is added:
  - 1.0.6. The appropriate authority shall establish and implement procedures to share, as appropriate and in a practical and timely manner, relevant information to assist other national authorities and agencies, airport operators, air carriers and other entities concerned, to conduct effective security risk assessments relating to their operations.;
- (2) The following point 1.7 is added:
  - 1.7 IDENTIFICATION AND PROTECTION OF CIVIL AVIATION CRITICAL INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS AND DATA FROM CYBER THREATS
    - 1.7.1. The appropriate authority shall ensure that airport operators, air carriers and entities as defined in the national civil aviation security programme identify and protect their critical information and communications technology systems and data from cyber-attacks which could affect the security of civil aviation.
    - 1.7.2. Airport operators, air carriers and entities shall identify in their security programme, or any relevant document cross-referenced in the security programme, the critical information and communications technology systems and data described in 1.7.1.

The security programme, or any relevant document cross-referenced in the security programme shall detail the measures to ensure the protection from, detection of, response to and recovery from cyber-attacks, as described in 1.7.1.
    - 1.7.3. The detailed measures to protect such systems and data from unlawful interference shall be identified, developed and implemented in accordance with a risk assessment carried out by the airport operator, air carrier or entity as appropriate.
    - 1.7.4. Where a specific authority or agency is competent for measures related to cyber threats within a single Member State, this authority or agency may be designated as competent for the coordination and/or monitoring of the cyber-related provisions in this Regulation.
    - 1.7.5. Where airport operators, air carriers and entities as defined in the national civil aviation security programme are subjected to separate cybersecurity requirements arising from other EU or national legislation, the appropriate authority may replace compliance with the requirements of this regulation by compliance with the elements contained in the other EU or national legislation. The appropriate authority shall coordinate with any other relevant competent authorities to ensure coordinated or compatible oversight regimes.;
- (3) Point 11.1.2 is replaced by the following:
  - 11.1.2. The following personnel shall have successfully completed an enhanced or a standard background check:

---

**Changes to legislation:** There are currently no known outstanding effects for the Commission Implementing Regulation (EU) 2019/1583, ANNEX. (See end of Document for details)

---

- a) Persons being recruited to implement, or to be responsible for the implementation of, screening, access control or other security controls elsewhere than a security restricted area;
- b) Persons having unescorted access to air cargo and mail, air carrier mail and air carrier material, in-flight supplies and airport supplies to which the required security controls have been applied;
- c) Persons having administrator rights or unsupervised and unlimited access to critical information and communications technology systems and data used for civil aviation security purposes as described in 1.7.1 in accordance with the national aviation security programme, or having been otherwise identified in the risk assessment in accordance with 1.7.3.

Unless otherwise specified in this Regulation, whether an enhanced or a standard background check has to be completed shall be determined by the appropriate authority in accordance with applicable national rules.;

(4) The following point 11.2.8 is added:

- 11.2.8. Training of persons with roles and responsibility related to cyber threats
  - 11.2.8.1. Persons implementing the measures as laid down in point 1.7.2 shall have the skills and aptitudes required to carry out their designated tasks effectively. They shall be made aware of relevant cyber risks on a need-to-know basis.
  - 11.2.8.2. Persons having access to data or systems shall receive appropriate and specific job related training commensurate with their role and responsibilities, including being made aware of relevant risks where their job function requires this. The appropriate authority, or the authority or agency as laid down in point 1.7.4 shall specify or approve the content of the course..

**Changes to legislation:**

There are currently no known outstanding effects for the Commission Implementing Regulation (EU) 2019/1583, ANNEX.