

## CS-25 AMENDMENT 25 — CHANGE INFORMATION

EASA publishes amendments to the Certification Specifications for Large Aeroplanes (CS-25) as consolidated documents. These documents are used for establishing the certification basis for applications made after the date of entry into force of the applicable amendment.

Consequently, except for a note '[Amdt No: 25/25]' under the amended paragraph, the consolidated text of CS-25 does not allow readers to see the detailed changes introduced compared to the previous amendment. To allow readers to also see these detailed changes, this document has been created. The same format as for the publication of Notices of Proposed Amendments (NPAs) is used to show the changes:

- deleted text is ~~struck through~~;
- new or amended text is highlighted in blue;
- an ellipsis '[...]' indicates that the rest of the text is unchanged.

## BOOK 1 — CERTIFICATION SPECIFICATIONS

### SUBPART F — EQUIPMENT

CS 25.1319 is inserted as follows:

#### **CS 25.1319 Equipment, systems and network information protection**

- (a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.
- (b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained.

### APPENDICES

#### APPENDIX H — INSTRUCTIONS FOR CONTINUED AIRWORTHINESS

Appendix H25.6 is inserted as follows:

#### **H25.6 Information system security Instructions for Continued Airworthiness**

The applicant must prepare Instructions for Continued Airworthiness (ICA) that are applicable to aircraft information system security protection as required by CS 25.1319 (see AMC 20-42 Section 9).

**BOOK 2 — ACCEPTABLE MEANS OF COMPLIANCE****AMC – SUBPART F**

AMC to CS 25.1319 is inserted as follows:

**AMC to CS 25.1319****Equipment, systems and network information security protection**

In showing compliance with CS 25.1319, the applicant may consider AMC 20-42, which provides acceptable means, guidance and methods to perform security risk assessments and mitigation for aircraft information systems.

The term ‘adverse effects on the safety of the aeroplane’ limits the scope of this provision to security breaches that impact on the safety and airworthiness of the aeroplane and its operation, rather than security breaches that may impact on the systems that have no safety effect on the aeroplane. For example, while the manufacturer and the air operator may have real concerns about protecting a device that is used to process passenger credit cards and securing passenger information, EASA does not regard this as being subject to review and approval as part of the certification of the system, but instead as something that the air operator or manufacturer would address as part of their business practices and responsibilities to the customer.

The term ‘mitigated as necessary’ clarifies that the applicant has the discretion to establish appropriate means of mitigation against security risks.

The term ‘procedures and Instructions for Continued Airworthiness (ICA)’ clarifies that, while the ICA may be one mechanism for providing the necessary instructions to maintain airworthiness, the security protections may go beyond traditional ICA material, and also include other procedures provided to the air operator. This aligns with the existing practices among those applicants for which special conditions (SCs) have been issued to address the protection of the aircraft information systems’ security.