Annex III to ED Decision 2023/010/R

'AMC and GM to Part 21 — Issue 2, Amendment 15'

The text of the amendment is arranged to show deleted, new or amended text as follows:

— deleted text is ~~struck through~~;

— new or amended text is highlighted in cyan;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

Note to the reader

In amended, and in particular in existing (that is, unchanged) text, 'Agency' *is used interchangeably with* 'EASA'. *The interchangeable use of these two terms is more apparent in the consolidated versions. Therefore, please note that both terms refer to the* 'European Union Aviation Safety Agency (EASA)'.

The Annex to Decision 2012/020/R of 30 October 2012 of the Executive Director of the Agency is amended as follows:

AMC1 21.B.20A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

(a) To appropriately collect and analyse information related to information security incidents and vulnerabilities with a potential impact on aviation safety, the competent authority should implement means that ensure the necessary confidentiality.

(b) When disseminating information related to information security incidents and vulnerabilities with a potential impact on aviation safety, the competent authority should properly select the appropriate recipient(s) to prevent the content of a report from being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 21.B.20A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the information security event or incident and the availability of additional data that would require controlled and confidential distribution. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.

Therefore, the report should consist of two parts: one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. Wherever possible, reports should be based on an agreed taxonomy.