

中华人民共和国民用航空行业标准

MH/T 0058—2015

民用航空信息安全事件调查规范

Investigation specification for information security incidents of civil aviation

2015 – 12 – 31 发布

2016 – 04 – 01 实施

中国民用航空局 发布

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国民用航空局人事科教司提出。

本标准由中国民用航空局航空器适航审定司批准立项。

本标准由中国民航科学技术研究院归口。

本标准起草单位：中国民航大学。

本标准主要起草人：周景贤、吕宗平、王双、张礼哲、顾兆军、江志强、马勇、刘春波、王静、熊育婷。

MH

民用航空信息安全事件调查规范

1 范围

本标准规定了民用航空信息安全事件（以下简称事件）的调查启动、调查组织、调查过程和调查报告等要求。

本标准适用于民用航空信息安全事件调查及相关工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

MH/T 0028 民用航空信息系统应急管理规范

MH/T 0041 民用航空信息安全事件分类分级指南

3 术语和定义

下列术语和定义适用于本标准。

3.1

民航信息安全事件 information security incident of civil aviation

由各种原因导致民航行业信息系统出现关键业务中断、系统瘫痪、关键数据丢失或核心信息失窃密等现象，对公共安全、政治稳定、社会经济秩序等方面造成不良影响以及造成一定程度经济损失的事件。

3.2

信息安全事件调查 investigation of information security incident

对已经发生的信息安全事件组织调查，获取事件发生的原因、过程、影响程度及范围的过程。

4 事件调查

4.1 调查启动

4.1.1 事件发生后，事件发生单位应依据 MH/T 0028 迅速进行应急响应或者请求其他力量支援进行应急响应，并尽可能保存好原始证据。

4.1.2 符合下列情形之一的事件，应启动调查程序：

- a) MH/T 0041 规定的重大信息安全事件；
- b) 受到国家信息安全管理相关部门通报的事件；
- c) 民航信息安全主管部门认为需要进行调查的事件。

4.2 调查组织

4.2.1 事件的调查由民航局信息安全主管部门负责组织，民航各级行政管理机构及相关企事业单位协助、配合。

4.2.2 涉及国家法律、行政法规的事件调查由负责组织调查的部门与国家相关职能部门协商进行。

4.3 调查过程

4.3.1 负责组织调查的部门应成立事件调查组，并委派一名调查组组长，调查组组长负责管理调查工作。

4.3.2 事件调查组应按照以下程序展开调查：

- a) 采用远程或现场勘验的方式，迅速获取事件发生对象相关原始资料；
- b) 对事件发生单位相关人员进行质询，对相关记录和信息进行分析；
- c) 召开内部会议，讨论调查工作内容和方法，对调查情况进行会商；
- d) 召开证据确认会，对调查结论进行确认。

4.3.3 调查过程应当在接到事件报告后 30 天内完成，特殊情况下，经调查组织部门同意后可适当延长。

4.4 调查报告

4.4.1 调查组应当在调查过程完成后 10 天内，编制事件调查报告，调查报告中应包括查明的事实、事件原因分析及主要依据、调查结论、调查中尚未解决的问题等。

4.4.2 调查组织部门对调查报告进行审议批准后，调查组工作完成。

4.5 调查归档

事件调查结束后，事件调查组织部门应将有关资料归档。归档资料应完整，根据情况应包括：

- a) 事件调查报告；
 - b) 现场调查笔录、调查取证证据、会议纪要等资料；
 - c) 技术鉴定和测试报告；
 - d) 直接和间接经济损失材料；
 - e) 有关事件的通报、简报及成立调查组的有关文件；
 - f) 事件调查组的人员名单，内容包括姓名、职务、职称、单位等；
 - g) 事件暴露出来的问题及采取的整改措施。
-