ICS 03.220.50
CCS V54

MH

中 华 人 民 共 和 国 民 用 航 空 行 业 标 准

MH/T XXXX—XXXX

民用无人驾驶航空器航行服务系统数据安全技术要求

Technical requirements for data security of civil unmanned aircraft air navigation service system

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国民用航空局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国民航局空管行业管理办公室提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国民用航空总局第二研究所、中国民用航空局信息中心、深圳市大疆创新科技有限公司、深圳美团低空物流科技有限公司、粤港澳大湾区数字经济研究院（福田）、浙大城市学院滨江创新中心、珠海安擎科技有限公司、中移（成都）信息通信科技有限公司、工业和信息化部电子第五研究所(中国赛宝实验室)、中国民航大学、西安交通大学、北京航空航天大学。

本文件起草人：邹翔、唐滔、杨非、孙立超、陈明、贾佳、车海翔、刘莹、耿增显、杨泽渊、李子冀、王兆星、杨亮亮、张亮、石砾、刘欢、周小霞、苏州、周剑、谢拥军、刘怡良、秦正。

民用无人驾驶航空器航行服务系统数据安全技术要求

1 范围

本文件确立了民用无人驾驶航空器航行服务系统（以下简称“USS系统”）的业务组成和数据分类，并规定了USS系统进行数据收集、传输、存储、使用、提供、删除等数据处理活动的安全技术要求。

本文件适用于民用无人驾驶航空器航行服务提供方进行USS系统数据处理活动中的数据安全管理，也可为监管部门、第三方评估机构对USS系统数据处理活动进行监管、管理、评估提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 17901 信息技术安全技术 密钥管理

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 31500 信息安全技术 存储介质数据恢复服务要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 41479 信息安全技术 网络数据处理安全要求

MH/T 4058 民用无人驾驶航空器空中交通服务要求

MH/T XXXX 民航领域数据分类分级要求

3 术语和定义

GB/T 17901、GB/T 20988、GB/T 31500、GB/T 35273、GB/T 37988、GB/T 41479、MH/T 4058、MH/T XXXX界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

CA：证书颁发机构（Certificate Authority）

CRC：循环冗余校验（Cyclic Redundancy Check）

ETL：采集，转换，加载（Extract, Transform, Load）

TLS：传输层安全（Transport Layer Security）

SHA：安全哈希算法（Secure Hash Algorithm）

USS：民用无人驾驶航空器航行服务提供方（Civil Unmanned Aircraft Air Navigation Service Supplier）

UOM：民用无人驾驶航空器综合管理平台（Civil Unmanned Aircraft Operation Management Platform）

5 概述

5.1 业务组成

USS系统数据处理活动是围绕民用无人驾驶航空器航行服务的业务功能开展，包括：信息类服务、管控类服务、协同类服务。

USS系统参与主体包括：被服务方、监管方、第三方数据提供者。其中，被服务方包括：民用无人驾驶航空器（以下简称“无人机”）运行人、社会管理信息化平台等；监管方包括UOM等；第三方数据

提供者包括：无人机远程识别系统、其他第三方数据提供者等，主要为USS系统提供无人机远程识别数据和人口密度、气象、地面障碍物等运行环境数据。USS系统参与主体交互示意图见图1。

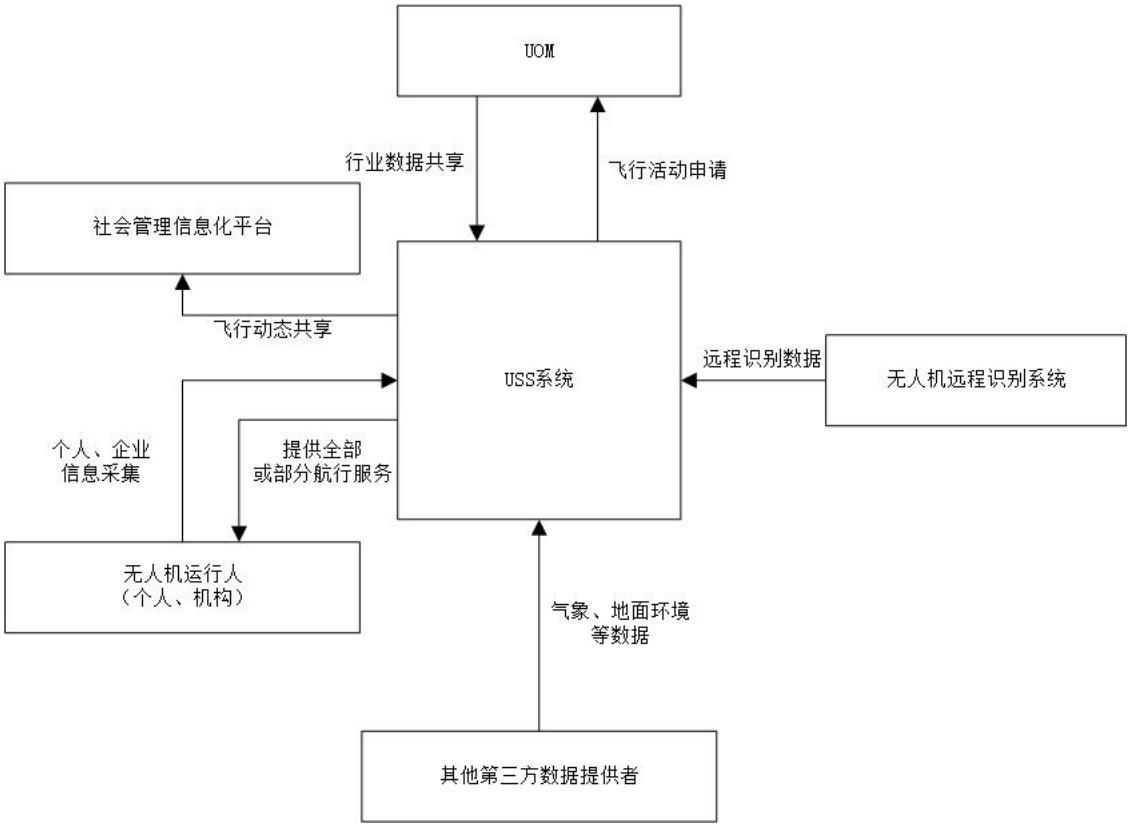


图1　USS 系统参与主体交互示意图

USS系统数据交互过程中涉及的数据处理活动及安全风险见附录A。

5.2　数据分类

USS系统数据包括如下。

a）　用户数据：USS 系统在提供服务过程中收集和产生的个人、企业用户数据，如姓名、身份证号、手机号、地址、邮箱、企业账号、营业执照、企业通信数据等。

b）　业务数据：USS 系统在提供服务过程中处理的各类用于支撑无人机安全、高效运行的业务数据，如空域数据、飞行活动数据、飞行动态、预警告警等。

按照MH/T XXXX（民航数据分类分级要求）中5.1的分类方法，对USS系统所涉及的业务数据进行分类，USS系统数据分类示例见表1。

表1 USS 系统数据分类示例

一级类别	二级类别	数据示例
空中交通管理域	空域规划	空域及航线数据、起降场数据、地形及地面障碍物数据等
	流量管理	飞行流量数据、空域容量数据、飞行计划数据、飞行申请审批数据、起飞确认数据等
	运行监控	飞行轨迹及状态数据、管制指令数据等
	通信导航监视	通导监信号覆盖数据、无线电干扰数据等
	气象服务	地面天气报告、空中风探测报告、气象卫星云图、气象雷达信息、雷电探测信息、天气预报、温度、气压、湿度、降水、低空风场信息等
安全监管域	航空安全	预警告警、人口密度等
	风险评估	风险评估报告、风险缓解措施等
	行政相对人	运营合格证数据、操控员执照数据、理论培训合格证明数据、生物识别数据等
生产运行域	航空器	民用无人驾驶航空器数据，包括生产序列号、唯一产品识别码、实名登记数据等等
宏观调控域	生产统计	运行统计与分析数据等

6 一般要求

USS系统数据安全的一般要求包括如下：

a) 数据处理活动应遵守 GB/T 41479 中规定的要求；
b) 个人信息处理活动应遵守 GB/T 35273 中规定的要求；
c) 应按照有关要求和标准进行数据分类分级保护,识别数据处理活动中的核心数据、重要数据、一般数据,对不同级别的数据采取不同的保护措施；
d) 应识别提供航行服务过程中涉及的一般个人信息、敏感个人信息,对个人信息进行标识和分类管理；
e) 数据安全能力应至少符合 GB/T 37988 中 2 级能力要求；
f) 应结合数据处理活动的实际情况,按照有关国家标准定期开展数据安全风险评估；
g) 应在开展对个人权益有重大影响的个人信息处理活动前,按照 GB/T39335 进行个人信息保护影响评估；

注：对个人权益有重大影响的个人信息处理活动,包括但不限于处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息,公开个人信息等。

h) 应符合 MH/T 4058 中 6.2.3 相关信息安全要求。

7 数据收集

7.1 告知同意

USS系统收集个人信息应在满足GB/T 35273—2020中5.4、5.5、5.6的要求基础上,遵守以下要求：

a) 用户使用飞行活动申请服务时，在收集个人信息前告知用户 USS 的名称、联系方式、个人信息的处理目的、处理方式、收集的个人信息种类、保存期限，用户行使权利的方式和程序,并取得用户同意；
b) 对用户进行实名认证时,向用户明示依据的法律法规具体规定,并且所收集的个人信息应仅用于完成实名认证目的。

7.2 范围最小化

USS系统收集数据的范围应满足以下要求：

a) 仅收集为提供航行服务所必需的信息；
b) 收集个人信息与实现业务功能有直接关联，获取个人信息的数量是实现业务功能的最小数量；
c) 对数据收集的时间、地点、对象、内容等情况进行日志记录；
d) 自动采集数据的频率是实现业务功能所必需的最低频率。

7.3 权限最小化

USS系统收集数据时申请的操作系统权限应满足以下要求：
a) 事先设计并公开声明收集数据所需的操作系统权限；
b) 获取的权限在实现业务功能所需的最低合理范围内，不应申请与业务功能无关的操作系统权限。

8 数据传输

8.1 保密性

USS系统传输数据时应在满足GB/T 35273—2020中6.3要求的基础上,遵守以下要求：
a) 使用数据传输安全性协议，建立加密的通信通道，例如 TLS1.3 及以上版本；
b) 向其他信息系统传输数据时，采取安全措施并以协议进行约定。

8.2 可用性

USS系统传输数据时，在数据可用性方面，宜采取以下措施：
a) 设计多条物理链路作为备份；
b) 根据数据传输需求，设计传输窗口大小、重传机制等；
c) 建立容错机制，包括错误检测和纠正；
d) 采用负载均衡技术分散数据流量；
e) 实施实时链路监测。

8.3 数据传输认证

USS系统在进行数据传输认证时，应采取下列措施：
a) 在数据传输前对数据传输双方进行身份认证和鉴权，例如使用基于分布式数字身份保证传输双方身份认证的可信性；
b) 在数据传输中，使用数据完整性校验技术，同时对数据传输和认证过程进行记录和同步。例如使用去中心化账本技术对传输的数据进行数据确权和存证；
c) 记录传输过程，可对数据传输的过程进行事后追溯，例如使用去中心化账本技术对传输过程进行追溯。

9 数据存储

9.1 存储和时效

USS系统进行数据存储时,应在满足GB/T 35273—2020中6.2、6.3、6.4要求的基础上，遵守以下要求：
a) 应对用户的个人身份信息、电话号码、地址等敏感个人信息采用加密等安全措施进行存储；
b) 密钥管理根据 GB/T 17901 密钥生成、存储、分配、使用、更换、销毁等全生命周期的管理要求进行管理；
c) 运行监控类数据至少保存 12 个月，其他类别数据至少保存 15 个月；
d) 加密数据的备份和恢复过程应受到保护；在发生故障或灾难情况下，加密系统应能支持快速恢复服务，同时不影响数据安全级别；
e) 加密数据备份应按照相关数据备份要求进行备份，根据数据重要程度使用备份介质、规定备份时间等，并具有在备份介质丢失或被盗的情况下，具有自保护功能，避免数据泄露；
f) 加密数据应按照相关数据备份要求，在发生数据错误或者损坏时，应具有恢复功能。

9.2 备份与恢复

USS系统数据的备份与恢复，应遵守以下要求：

a) 具有本地备份功能，根据系统的实际需求进行异地备份；
b) 数据库文件、重要日志等至少每周进行一次完全备份、每天做一次增量备份；
c) 按照GB/T 31500—2024中6.4规定的服务流程、技术手段、安全管理、服务质量等方面的要求进行数据恢复；
d) 按照GB/T 20988—2007中6.3规定的要求配置灾难恢复资源以及7.5规定的实现方式完成数据灾难恢复操作。

10 数据使用

10.1 访问控制

USS系统对数据的访问控制，应满足以下要求：

a) 对用户个人信息的访问控制，满足GB/T 35273—2020中7.1要求；
b) 建立审批流程，设置限制数据访问范围，限制批量查询、导出用户个人身份信息、电话号码、地址等的操作功能；
c) 对于查询用户个人身份信息、电话号码、地址等的操作，使用不同于用户登录的验证方式进行二次校验；
d) 根据使用人员的角色分配其最小所需数据访问权限。

10.2 数据展示

USS系统展示系统数据时，应遵守以下要求：

a) 展示用户个人信息时,满足GB/T 35273—2020中7.2要求；
b) 对飞行活动数据中的申请人、操控员等人员姓名，电话号码进行去标识化处理，因业务需要，确需查看未经去标识化处理的数据时，在展示界面中采用数字水印技术；
c) 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；
d) 在不影响正常提供航行服务情况下，展示空域、航路航线、起降场、无人机位置等空间坐标数据时，采用网格编码、加偏等模糊处理方式。

10.3 数据导出

USS系统进行数据导出时，应满足以下要求：

a) 具备对数据导出操作权限进行管理和控制的功能；
b) 对批量导出个人隐私数据的操作进行记录和监控，个人隐私数据包含且不限于身份信息、电话号码、家庭地址等数据；
c) 导出用户个人身份信息、电话号码、地址等操作前，进行多因子认证，核实用户身份信息。

10.4 日志记录

USS系统在记录数据使用日志时，应遵守以下规则。

a) 日志包括但不限于以下类型：
   1) 系统日志：记录系统运行状态、系统错误、系统安全事件等信息；
   2) 安全日志：记录用户认证、访问控制、系统安全警告等安全相关事件；
   3) 访问日志：记录用户或系统对资源的访问，包括协议信息、目的地址和源地址、会话持续时间等。
b) 所有类别的日志记录满足以下要求：
   1) 完整性：所有日志完整记录事件的所有相关信息；
   2) 准确性：日志记录的时间戳、事件类型、用户标识等信息准确无误；
   3) 一致性：不同应用模块的日志格式保持一致，便于日志分析和审计；
   4) 不可篡改性：日志记录一旦生成，保证其内容不被修改或删除。
c) 明确日志数据的存储期限，满足数据安全和隐私保护的要求。

d) 日志文件妥善保护，防止未经授权的修改和删除；实时监控日志，以快速检测并响应事件，同时配置告警系统，以便在检测到关键事件时通知相关人员，日志保护的内容包括：
   1) 分权管理：根据工作职责划分不同的角色，并分配访问权限；建立访问控制策略，实施控制措施，确保获得授权的角色才能进行日志的查看、管理和备份；对于访问敏感日志数据的用户实施多因素认证，增强安全性；定期审计用户权限，确保无过期或不必要的访问权限存在；
   2) 操作管理：对日志中的敏感操作（如删除、修改）实行必要的审批流程，确保操作的合法性和正当性，所有对日志进行的操作必须有记录，并能追溯到具体的个人，确保日志数据不可被未授权修改，采取如加密、散列等措施保护日志数据的完整性；
   3) 日志备份：定期进行全量备份，恢复所有日志数据；实现增量备份机制，保证自上一次全量或增量备份后所产生的日志更改能够被备份，设置周期性全量备份计划，以应对灾难恢复的需求。

11 数据提供

11.1 数据共享交换

USS系统进行数据共享交换时，应满足以下要求。

a) 与外部系统进行数据交换时，需明确交换的数据范围，且仅限于所提供服务范围内的必要交换。
b) 在数据共享和交换节点建立连接之前，对所有接入的用户进行身份认证，利用 APIkey、可信认证、数字证书等手段验证请求端用户和应用的真实性和合法性。
c) 在数据提供过程中，根据数据安全保护等级，利用 CA、加密和加签等技术，保证数据存储、传输、处理过程中的安全性，防止数据在传输过程中被窃取和篡改。
d) 服务系统内部进行数据共享交换时，进行私有协议加密传输、数据安全检查和安全完整性保护。

11.2 接口安全

USS系统应采取以下措施，以保障数据交换接口的安全。

a) 对于 API、数据库接口、消息队列、文件接口等数据交换方式，至少具备访问控制和身份鉴权的安全措施。
b) 具备接口访问的监控功能，实时监控接口的异常访问、识别攻击。
c) 具备接口状态的监控功能，针对不同时段、用户、不同报文类型、不同传输路径等各种条件下的数据量进行监控，并通过日志进行详细、准确、及时记录每一个接口交换过程的属性信息及状态信息。
d) 设计防重和防采集机制，防止接口被重复请求。

12 数据删除

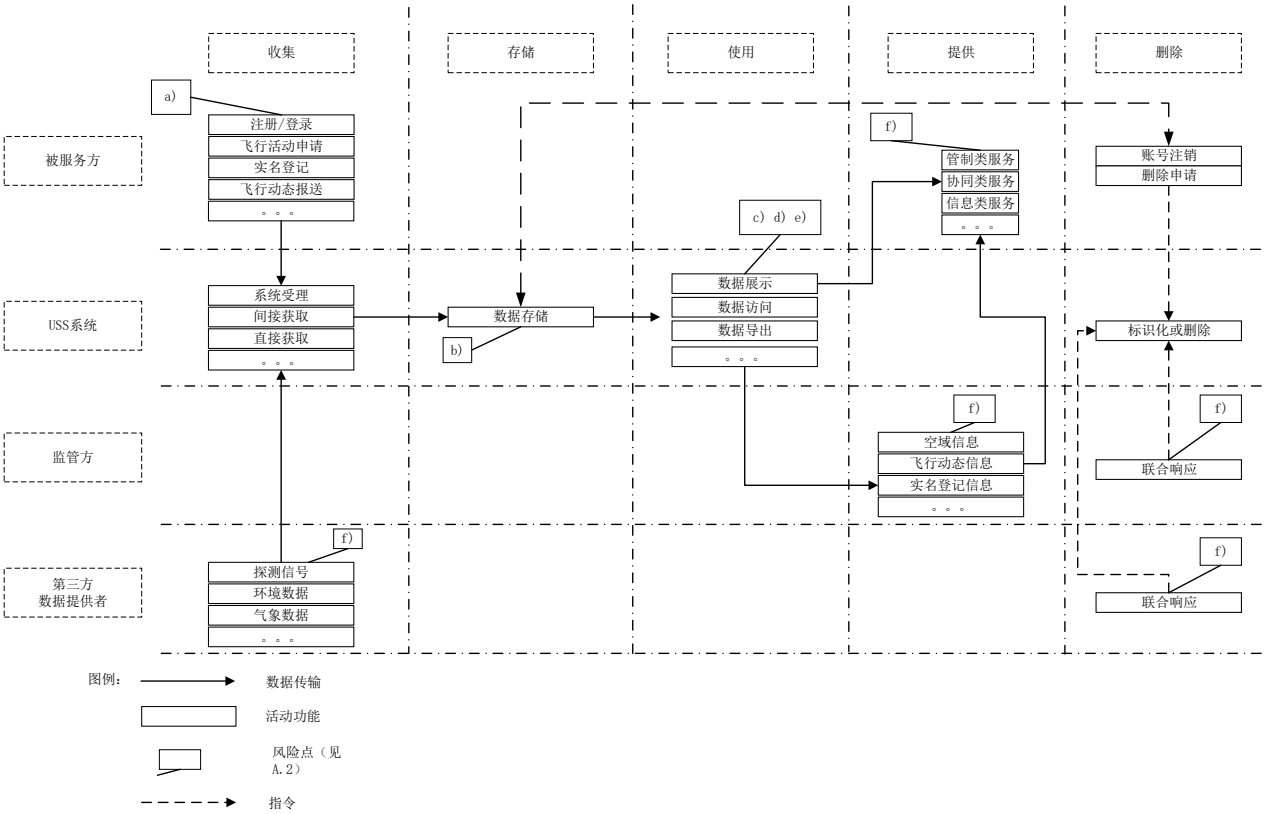
USS系统进行数据删除时,应遵守以下要求：

a) 个人信息删除满足 GB/T 35273—2020 中 8.3 的要求；
b) 保存数据删除的有关记录,记录内容包括但不限于删除的数据类型、方式、时间、责任人等。

附 录 A
（资料性）
数据处理活动及安全风险

A.1 数据处理活动

USS系统数据处理活动示意如图A.1所示。



图A.1 USS 系统数据处理活动示意图

A.2 数据安全风险

USS系统主要面临以下数据安全风险：

a) 在提供服务时,过度收集用户个人信息,或过度索取操作系统权限的风险；
b) USS 系统使用硬件设备进行数据备份,因设备丢失或设备保护措施不足等导致数据泄露的风险；
c) 无人机运行人在使用无人驾驶航空器进程中，因航空器租用、遗失、经手人员泄露等场景下带来的数据泄露风险；
d) 在第三方参与者数据传输过程中,接触用户个人信息的提供者内部人员多,且管理难度大,可能出现内部人员泄露用户个人信息、数据改动和数据损毁风险；
e) 以业务营销、业务风险控制、提升服务质量为目的分析个人信息,对用户进行画像和信息推送,未提供有效的拒绝个性化推荐和删除相关信息等功能,造成个人权益受损的风险和数据不正当使用的风险；
f) 系统服务器在正常使用过程中被恶意软件攻击，造成数据窃取、数据改动和损毁风险。

参 考 文 献

[1] GB/T 38152 无人驾驶航空器系统术语
[2] GB/T 42013 信息安全技术 快递物流服务数据安全要求