ICS 35.020
CCS L70

# 团　　体　　标　　准

T/HSPA XXXX—XXXX

# 文物安全综合信息应用平台
# 总体要求

**Comprehensive information application platform for cultural heritage security -- general requirements**

（征求意见稿）

2023－XX－XX 发布　　XXXX－XX－XX 实施

湖北省安全技术防范行业协会　　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。

T/HSPA XXXX《文物安全综合信息应用平台 总体要求》，与T/HSPA XXXX《文物安全综合信息应用平台　功能要求》、T/HSPA XXXX《文物安全综合信息应用平台　数据接口要求》、T/HSPA XXXX《文物安全综合信息应用平台　数据资源分类及编码》共同构成支撑文物安全综合信息应用平台建设的团标标准体系。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国文物保护标准化技术委员会（SAC/TC 289）提出并归口。

本文件起草单位：中国文物信息咨询中心、中南民族大学、湖北省安全技术防范行业协会、中国人民公安大学、武汉旗云高科工程技术有限公司、重庆声光电智联电子有限公司、湖北省智能识别产品质量监督检验中心等。

本文件主要起草人：张学文、李成华、刘为军、江小平、石鸿凌、夏天、刘晓栋、王奎、张伟、丁昊、孙斯。

# 引　言

从2017年的国务院办公厅《关于进一步加强文物安全工作的实施意见》（2017年81号文），到2018年中共中央办公厅、国务院办公厅的《关于加强文物保护利用改革的若干意见》（2018年10月发文），再到2022年4月国家文物局的《文物安全防控“十四五”专项规划》（2022年第12号文），这些文件都指出服务于文物安全保护的信息化系统建设刻不容缓。2020年7月针对目前文物安全保护领域信息化系统建设存在缺乏顶层设计、规范和标准长期缺位的问题，国家文物局发布了《文物安全监管平台建设指南(2020)》（文物督发〔2020〕24号）。该文件对文物安全监管平台建设起到了一定的指导作用，但未对建设全国互联的平台提供整体规范性指导，导致相关平台建设仍然各自为政、效益不高。2022年5月国家文物局印发《文物安全防控“十四五”专项规划》的通知（文物督发〔2022〕12号），进一步提出“出台文物安全监管平台建设技术指导标准，实现文物安全防护智能化和标准化”等要求。可见，指导信息化建设的相关标准规范迫在眉睫，亟需出台。

本文件以文物安全综合信息应用平台为标准化对象，目标是以科技手段辅助文物行政管理部门落实监管责任以及文物保护单位落实直接管理责任。本文件提供了平台的顶层设计方案，并提出了总体要求，且与《文物安全综合信息应用平台 功能要求》、《文物安全综合信息应用平台 数据接口要求》以及《文物安全综合信息应用平台 数据资源分类及编码》共同构成支撑文物安全综合信息应用平台建设的系列文件，涵盖了平台构成、技术框架、性能要求、安全要求、功能要求、数据接口要求以及数据资源分类和编码等内容，为服务于文物安全监督管理信息化平台的建设提供了较为完整的指导。文件的制定将促进相关系统的建设，促进形成“物理分散、逻辑互联、全国一体、协同工作”的文物安全监督管理工作模式，使得文物安全监督管理高效有力，更好地服务于文物安全工作国家战略。

文物安全综合信息应用平台主要围绕不可移动文物进行风险防控和安全监督管理而设置，博物馆单位可参考本文件开展建设。

# 文物安全综合信息应用平台　总体要求

## 1　范围

本文件界定了文物安全综合信息应用平台的术语和定义，规定了文物安全综合信息应用平台的平台架构、性能要求以及安全要求。

本文件适用于文物安全综合信息应用平台的设计、建设以及验收。

## 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 16571 博物馆和文物保护单位安全防范系统要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 32399 信息技术 云计算参考架构

GB/T 32922-2023 信息安全技术 IPSec VPN安全接入基本要求与实施指南

GB 50348 安全防范工程技术规范

## 3　术语和定义

GB 50348、GB/T 16571界定的以及下列术语和定义适用于本文件。

3.1

**文物安全综合信息应用平台**　comprehensive information application platform for cultural heritage security

以信息化数字化驱动，为各级文物行政管理部门落实文物安全监管责任以及为文物保护单位落实文物安全直接责任提供服务的信息系统。

3.2

**文物安全防护系统**　security system for cultural heritage

服务于文物安全风险防护的信息化应用系统的总称，具体包括安全防范系统、消防系统和防雷系统等。

3.3

**边缘数据接入系统**　edge data acquisition system for cultural heritage security

设置在文物保护单位，统一获取文物安全防护系统的报警类、故障类等数据，消除信息孤岛，为上层应用提供统一格式数据的服务。

3.4

**社会数据**　Social data

来自文物保护单位和文物行政部门单位信息系统以外，可用来预测包括对盗窃、盗掘、火灾以及法人违法等文物安全风险事件发生可能性的数据。

注：如网络舆情数据、天气数据、文物拍卖数据等。

## 4 缩略语

以下缩略语适用于本文件：

**AI**：人工智能（Artificial Intelligence）

**CA**：证书授权（Certificate Authority）

**GIS**：地理信息系统（Geographic Information System）

**HTTP**：超文本传输协议（Hypertext Transfer Protocol）

**HTTPS**：超文本传输安全协议（Hypertext Transfer Protocol over Secure Socket Layer）

**Kafka**：消息队列传输协议（Kafka Protocol）

**MQTT**：物联网传输协议（Message Queuing Telemetry Transport）

**VPN**：虚拟专用网络（Virtual Private Network）

## 5 平台架构

### 5.1 平台构成

5.1.1 文物安全综合信息应用平台（以下简称“平台”）由文物安全综合信息应用系统以及边缘数据接入系统构成，见图 1。

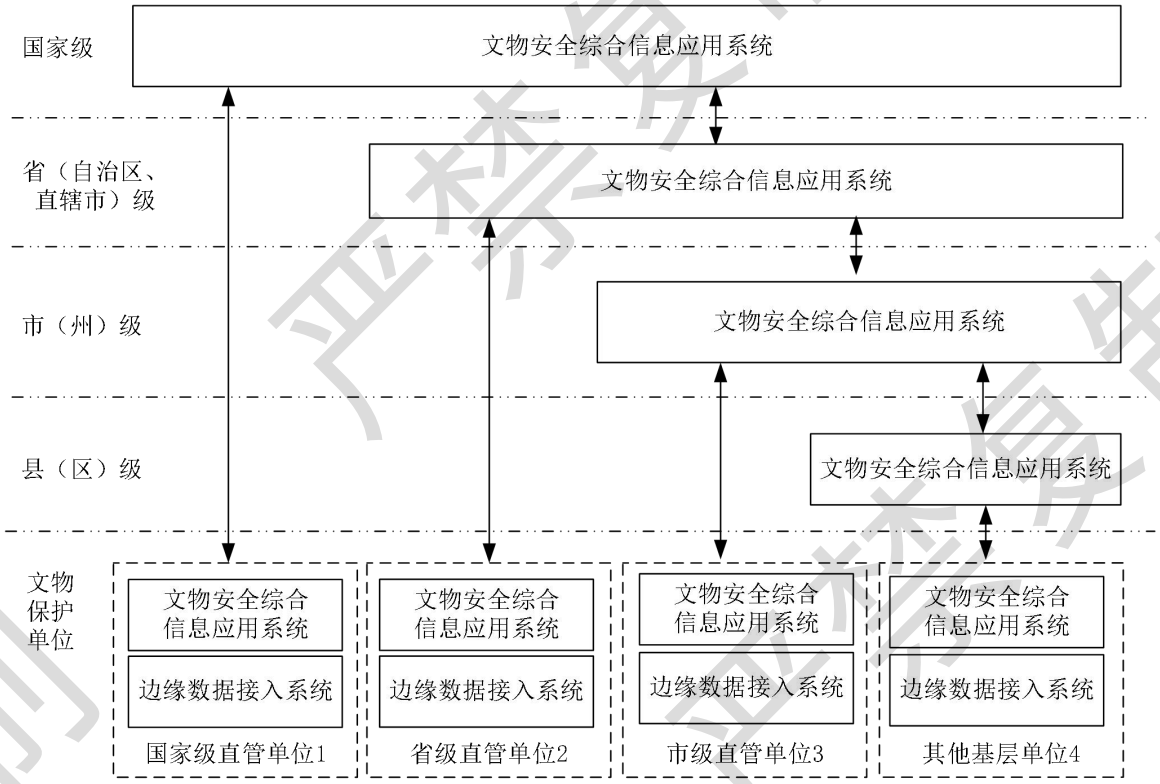


**图 1 平台构成**

5.1.2 文物安全综合信息应用系统的用户类型分成部门用户和单位用户。其中，部门用户包括国家级用户、省级用户、市级用户以及县级用户，实现对本级所直接管辖的文物保护单位履行文物安全监管责任。单位用户是指文物保护单位的用户，其履行文物安全直接管理责任。

5.1.3 部门用户的主要应用功能目标是实现监管要素全覆盖、监督管理业务流程化以及风险防控主动

化，使得文物监管有力、高效。

5.1.4 单位用户的主要应用功能目标是文物安全信息全息掌握、异常事件融合分析识别、风险分级预警及防控以及闭环处置管理可视化，使得文物安全直接管理措施得到有效落实。

5.1.5 部门用户的业务应用系统具有相同的业务应用功能模块，区别在于不同行政级别管辖文物保护单位不同，上级部门用户拥有访问下级系统的数据和应用的能力。

5.1.6 边缘数据接入系统设置在文物保护单位，其主要应用功能目标是屏蔽底层不同厂商提供的文物安全防护系统（如安防、消防系统）之间的技术架构和数据差异，以统一格式协议提供数据服务。

## 5.2 文物安全综合信息应用系统技术框架

文物安全综合信息应用系统功能主要包括数据服务，应用支撑，业务应用三个部分，其技术框架见图 2。

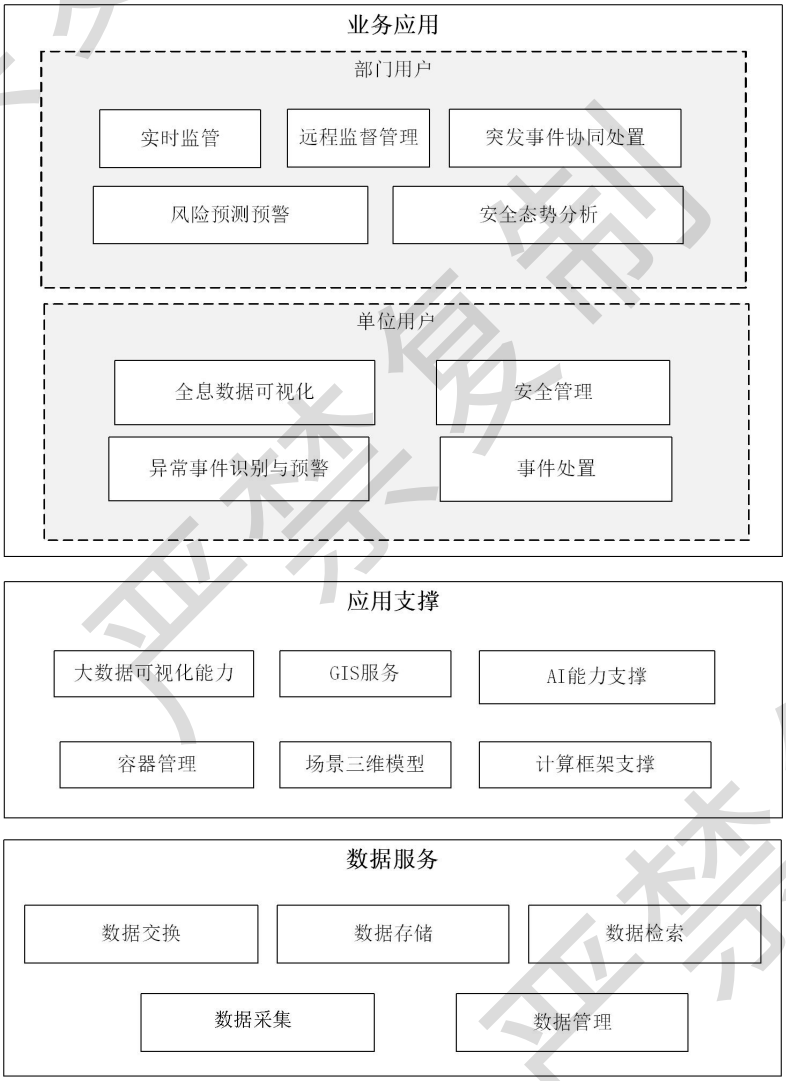


图 2 技术框架

## 5.3 数据服务

### 5.3.1 数据采集

数据采集包括但不限于以下内容：

a）应支持获取文物安全边缘数据接入系统的提供数据，其数据接口应符合T/HSPA XXXX《文物安全综合信息应用平台　数据接口要求》附录A的A接口的A.1-A.10要求；

b）宜支持采集社会数据，包括但不限于以下内容：

——文物拍卖交易数据；

——网络舆情数据；

——文物安全违法犯罪案件。

c）可支持采集横向部门的公共数据，包括但不限于以下内容：

——气象部门的天气数据；

——公共安全部门的公共安全数据；

——应急部门的公共数据；

——医疗部门的疫情数据；

——地震部门的公共数据。

### 5.3.2　数据交换

数据交换包括但不限于以下内容：

a）应支持下级单位的系统向上级部门系统开放数据访问权限；

b）宜具备向公安、海关、应急消防、医疗卫生等部门提供数据服务接口的功能。

### 5.3.3　数据管理

数据管理包括但不限于以下内容：

a）应支持元数据管理功能，实现数据定义、数据类型和数据格式的统一管理；

b）应提供数据资源目录管理功能；

c）应具备数据访问权限管理功能。

### 5.3.4　数据存储

数据存储包括但不限于以下内容：

a）应支持对结构化数据及非结构化数据的存储能力；

b）应提供包括基础数据库、主题数据库以及专题数据库等服务；

c）基础数据库、主题数据库以及专题数据库的数据库表的建立宜参考T/HSPA XXXX《文物安全综合信息应用平台 数据资源分类及编码》的描述。

## 5.4　应用支撑

### 5.4.1　AI 能力支撑

宜提供 AI 能力支撑，包括但不限于以下内容：

a）提供统计分析能力：提供应支持多维度数据统计分析算法；

b）提供大数据预测模型，包括以下内容：

——提供基于大数据分析算法的文物安全风险预测模型服务；

——提供模型管理服务，宜包括模型训练与评估、模型发布、版本管理、部署情况等；

——预测的风险类型宜涵盖盗掘、盗窃、火灾以及法人违法等。

c）提供视频数据的智能分析处理能力，包括以下内容：

——提供基于深度学习的视频智能分析模型服务；

——提供模型管理服务，宜包括模型训练与评估、模型发布、版本管理、部署情况等；

——宜采用容器化部署技术，将模型和其依赖项打包为独立的容器；

——视频智能分析的异常事件类型宜涵盖盗掘、盗窃、火灾以及法人违法等类型。

#### 5.4.2 场景三维模型

宜提供场景三维模型支撑功能，包括但不限于以下内容：

a）宜支持采用三维建模技术对重点文物防护对象实景进行建模；

b）宜支持对三维模型文件存储与管理。

#### 5.4.3 容器管理

宜具备容器管理能力，对基于容器化部署的视频智能分析模型，提供包括容器启动，容器运行状态监控，容器关闭，镜像文件管理等功能，以服务于基于视频智能分析模型开展异常行为识别。

#### 5.4.4 GIS 服务支撑

应具备二维地理信息系统服务能力，以支持基于 GIS 的信息可视化呈现。

#### 5.4.5 大数据可视化组件

应支持折线图、饼图、柱状图、雷达图、热力图等多种形式的数据展示方式。

#### 5.4.6 计算框架支撑

宜提供流式计算、批量计算、图计算、内存计算等多种计算框架。

### 5.5 业务应用

5.5.1 业务应用层分成部门用户功能和单位用户功能两个大部分。

5.5.2 部门用户具有实时监管、远程监督管理、风险预测预警、安全态势分析以及突发事件协同处置功能。

5.5.3 单位用户具有全息数据可视化、安全管理、异常事件识别与预警、事件处置功能。

5.5.4 业务应用功能的具体要求见T/HSPA XXXX《文物安全综合信息应用平台 功能要求》描述。

## 6 性能要求

### 6.1 文物安全综合信息应用系统性能要求

6.1.1 风险防控措施决策推理实时计算延迟指标：应不高于 1s。

6.1.2 资源利用率指标，满足以下要求：

——峰值内存应保持在 80%以下；

——峰值 CPU 占有率应保持在 75%以下。

### 6.2 边缘数据接入系统性能要求

6.2.1 获取系统数据时，误码率应为 0。

6.2.2 获取实时数据时，时延要求不宜低于 30ms。

6.2.3 应支持协议包括但不限于：MQTT、Websocket、https、http、Kafka、Modbus、Opc 等。

6.2.4 应具备采集数据库的数据能力，包括但不限于 GaussDB、mysql、oracle 和 Sql server 等数据库管理系统。

6.2.5 应具备实时采集文物保护单位的安全防范类信息系统的数据，采集的数据包括但不限于安全事件报警类和故障报警类数据，安全防范类信息系统包括但不限于安防管理系统、电子巡查系统、出入口控制系统。

6.2.6 应具备实时采集文物保护单位的消防类信息系统数据，采集的数据包括但不限于事件报警类和故障报警类数据。

6.2.7 应具备采集监控摄像头的实时视频数据的能力。

## 7 安全要求

### 7.1 设备安全

设备安全包括但不限于以下要求：

a）宜采用已获得安全许可认证的国产操作系统；

b）宜采用已获得安全许可认证的国产数据库管理系统；

c）宜部署在已获得安全许可认证的设备上；

d）文物安全综合管理系统的信息安全等级保护应达到GB/T 22239-2019第6章规定的第二级标准及以上；

e）文物安全边缘数据采集系统应具有双物理网卡，并使得内部网络与外部互联网隔离；

f）文物安全边缘数据采集系统的信息安全等级保护应达到GB/T 22239-2019第6章规定的第二级标准及以上。

### 7.2 应用安全

文物安全综合管理系统的web应用应符合GB/T 37931中的基本级要求。

### 7.3 传输安全

传输安全包括但不限于以下要求：

a）文物安全综合信息应用系统与文物安全边缘接入采集系统之间宜采用专线网络连接；

b）文物安全综合信息应用系统与文物安全边缘数据接入系统之间采用互联网连接时，应按照GB/T 32922-2023的第7章要求实施VPN安全接入，以建立起安全网络隧道。

### 7.4 数据安全

数据安全符合下列要求:

a）访问控制应满足GB/T 22239的8.1.3.2要求；

b）安全审计应满足GB/T 22239的8.1.3.5要求；

c）文物安全综合信息应用系统与文物安全边缘数据接入系统之间进行数据传输时，宜采用数字证书对上传的所有数据进行签名与加密；

d）密钥管理和证书管理宜由文物安全综合信息应用系统提供。

## 参 考 文 献

[1] 关于进一步加强文物安全工作的实施意见,国办,[2017]第81号.
[2] 关于加强文物保护利用改革的若干意见,中办、国办,2018年10月.
[3] 文物安全监管平台建设指南,国家文物局文物督发,[2020]第24号.
[4] 文物安全防控“十四五”专项规划,国家文物局文物督发,[2022]第12号.
[5] T/HSPA XXXX《文物安全综合信息应用平台 功能要求》
[6] T/HSPA XXXX《文物安全综合信息应用平台 数据接口要求》
[7] T/HSPA XXXX《文物安全综合信息应用平台 数据资源分类及编码》