ICS 35.100.01
L79

DB4403

深　圳　市　地　方　标　准

DB4403/T 37—2019

智慧监督平台数据接入规范

Data access specifications for intelligent supervision platform

2019-12-25 发布　　2020-02-01 实施

深圳市市场监督管理局　发布

目　　次

前　言

本标准依据GB/T 1.1-2009的规则起草。

本标准由中共深圳市纪律检查委员会、深圳市监察委员会提出并归口。

本标准主要起草单位：中共深圳市纪律检查委员会、深圳市监察委员会。

本标准主要起草人：郭钢、姚晓升、楼中元、陈景春、姜星、贾骅俊、贺晨阳、李良刚、李煜俊。

引　言

为提升城市治理体系和治理能力现代化水平，提高党风廉政和反腐败领域信息化程度，建设现代化的智慧监督平台，需要实现纪检监察信息系统与监察对象单位信息系统之间数据的互联互通，智慧监督平台数据接入标准是数据互联互通的基础，也是用现代化标准建设全面推进监督机制模式创新的积极探索。

本标准通过要求监察对象单位在信息化系统中建立和维护标准数据目录和接口，实现与深圳市智慧监督平台的数据互通，使全市纪检监察单位可运用大数据进行廉政建模分析和风险预警，帮助监察对象单位预防和发现廉政风险，减轻人工重复报送数据的压力，节约政府行政资源。

智慧监督平台数据接入规范

1 范围

本标准规定了监察对象单位信息系统数据接入智慧监督平台的模型及技术要求。

本标准适用于监察对象单位信息系统与智慧监督平台进行跨系统、跨平台的实时数据联通。

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。

GB/T 20271-2006 信息系统通用安全技术要求

GB/T 21063.4-2007 政务信息资源目录体系 第4部分：政务信息资源分类

GB/T 21063.5-2007 政务信息资源目录体系 第5部分：政务信息资源标识符编码方案

GB/T 36622.2-2018 智慧城市 公共信息与服务支撑平台 第2部分：目录管理与服务要求

GB/T 4754-2017 国民经济行业分类

SZDB/Z 159.1-2015 公共基础信息数据元规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧监督平台 intelligent supervision platform

通过新一代信息技术与监督职能相结合所建设的具有廉政风险防控、问题线索发现等功能的信息系统。

3.2

数据提供方 data provider

提供监督数据的监察对象单位。

3.3

数据获取方 data demander

从数据提供方获取监督数据的纪检监察部门。

3.4

统一数据接入系统 uniform data access system

智慧监督平台中实现数据接入过程管理的子系统。

4 缩略语

以下缩略语适用于本文件：

API：应用程序编程接口（Application Programming Interface）

JSON：JavaScript对象标记（JavaScript Object Notation）

XML：可扩展标记语言（Extensible Markup Language）

REST：表述性状态传递（Representational State Transfer）

URL：统一资源定位符（Uniform Resource Locator）

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

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket）

5 智慧监督平台数据接入模型

5.1 总体模型

实现智慧监督平台数据接入时，应按本标准总体模型接入流程及相关技术要求进行操作。

智慧监督平台实现数据接入的总体模型见图1，由元数据管理、数据目录管理、接口管理、认证与鉴权、数据对接管理、数据安全管理及数据应用管理等过程组成。数据接入流程参与对象分为数据提供方、数据获取方两种不同的角色，在本模型的各过程中分别描述了相应角色的职责与分工。

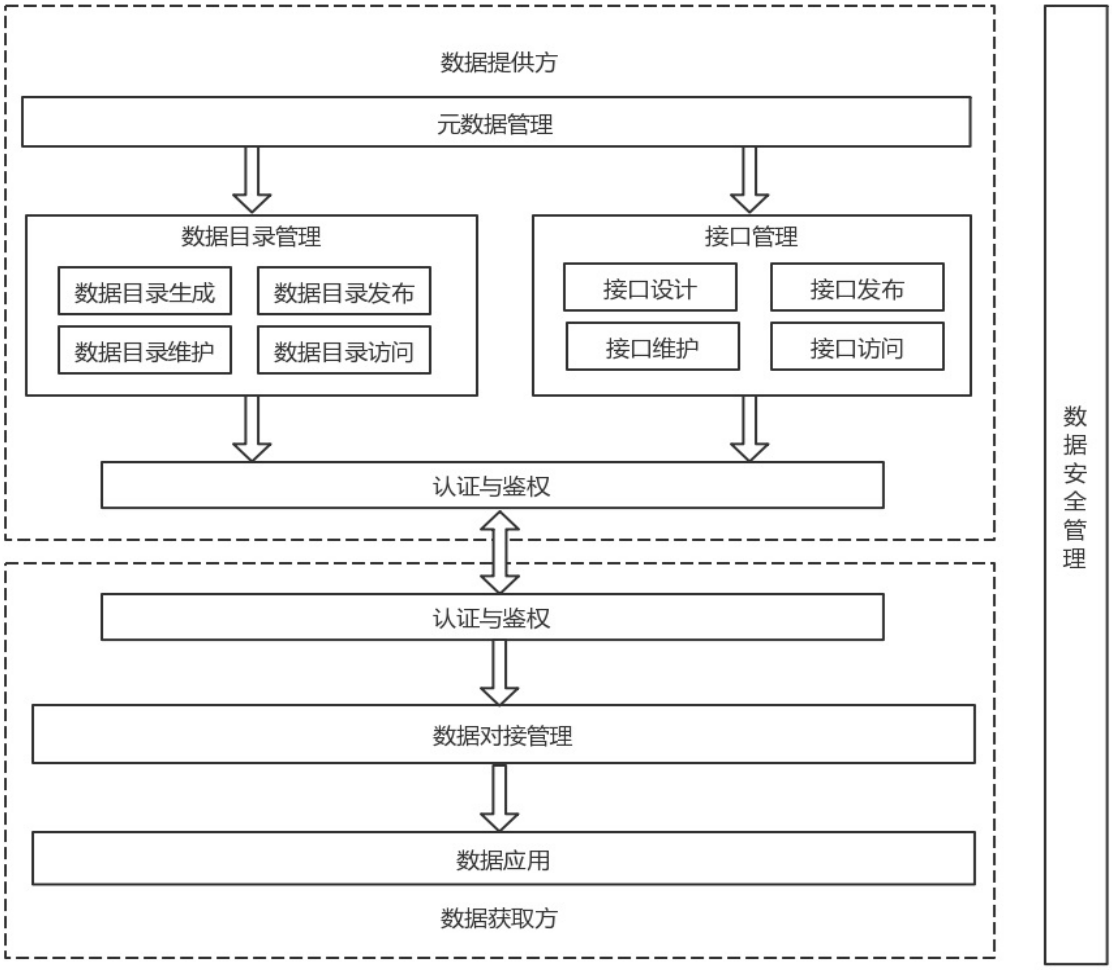

图1 智慧监督平台数据接入总体模型

5.2 数据接入过程

5.2.1 元数据管理过程

由数据提供方对自有的数据进行规范化和标准化管理，实现对数据进行准确描述，确保数据获取方能够快速识别字段级别的业务含义和技术含义。

5.2.2 数据目录管理过程

由数据提供方将已进行标准化处理的数据编制成数据目录，并对数据目录进行管理。

5.2.3 接口管理过程

由数据提供方生成用于监督的实时数据查询的接口，并对接口进行管理。

5.2.4 认证与鉴权过程

由数据提供方和数据获取方对访问己方系统的用户进行安全认证和身份鉴别，确保用户身份的合法性和用户权限的有效性，用户只能在已有权限范围内进行操作。

5.2.5 数据对接管理过程

由数据获取方提供统一数据接入系统，数据提供方在统一数据接入系统发布数据目录及接口，以供数据获取方进行数据查询、采集。

5.2.6 数据安全管理过程

由数据提供方与数据获取方在数据产生、存储、传输、应用过程中，对数据制定安全策略，保障数据安全。

5.2.7 数据应用管理过程

由数据获取方对接入数据进行处理，使其满足智慧监督平台的业务要求。

6 智慧监督平台数据接入技术要求

6.1 元数据管理

数据提供方负责元数据的维护与管理，元数据管理要求包括且不仅限于：

a）统一元数据管理过程，保证元数据完整性和实效性，元数据管理过程符合GB/T 36622.2-2018中4.2的要求；

b）统一数据类型和格式，具体数据类型和数据格式应满足SZDB/Z 159.1-2015中第5章要求；

c）统一常用数据值域，具体参照SZDB/Z 159.1-2015第5章相关要求。

6.2 数据目录管理

6.2.1 概述

数据目录管理应由数据提供方按以下要求，建立数据目录管理制度并管理数据目录的生成、发布、维护和访问等过程。

6.2.2 数据目录生成

a) 数据目录的内容，包括且不限于表 1 的内容：

表1 数据目录内容

编号	数据项	说明
1	数据目录编码	数据目录的编码
2	名称	数据的名称
3	摘要	对数据内容的整体描述或说明
4	主题分类	数据所属主题
5	关键字	对数据内容的简要概括
6	数据提供部门	数据目录来源部门
7	行业分类	数据对应的行业分类
8	发布时间	数据目录发布的具体时间
9	更新时间	数据目录更新的具体时间
10	更新频率	数据目录更新频率，如年、月、周、日等
11	所属行政区域	生成数据目录的部门所属行政区域
12	支持格式	数据格式，如 CSV、XLS（或 XLSX）、JSON 等格式
13	资源状态	数据目录的状态，如激活、废弃等
14	记录数量	目录中数据的数量
15	来源系统	数据库系统来源
16	时间范围	数据内容属于的时间范围
17	接入方式	接入数据的方式

b) 数据目录编码方式应符合 GB/T 21063.5-2007 的规定；
c) 数据目录主题分类应符合 GB/T 21063.4-2007 的规定；
d) 数据目录行业分类应符合 GB/T 4754-2017 的规定；
e) 对于结构化数据，应提供完整的数据目录；
f) 对于非结构化数据，应先从中抽取出主要特征存储到结构化关系表中，再生成相应的数据目录。

6.2.3 数据目录发布

数据提供方应负责发布数据目录信息，发布时应指定允许访问数据目录的用户列表及访问权限，数据获取方应被纳入在内，并且具有读取全局数据的权限。数据目录发布的要求包括且不限于：

a) 应包括数据目录内容说明；
b) 应保证数据目录的完整性和时效性。

6.2.4 数据目录维护

数据提供方应对数据目录进行维护，对数据目录变更流程进行统一管理。数据目录维护要求包括且不限于：

a) 数据目录变更管理流程应包括变更申请、变更审批、变更实施、变更记录等过程；
b) 应建立数据目录信息同步机制，数据目录变更后应及时更新至统一数据接入系统，并由数据获取方进行审核。

6.2.5 数据目录访问

数据提供方应为数据获取方提供具有访问全局数据权限的账号，以支持数据获取方读取对应的数据资源。

6.3 接口管理

6.3.1 概述

数据提供方应向数据获取方提供数据资源访问接口，并提供接口描述及调用方法。数据提供方对接口的设计和实现应遵循统一的技术规范要求，具体涉及接口设计、接口发布、接口维护和接口访问等过程。

6.3.2 接口设计

接口设计要求包括且不限于：

a) 接口命名应符合统一的编程语言规范，并且采用统一的命名风格；
b) 接口请求格式应根据接口格式设定，常用格式包括且不限于 JSON、XML、REST 等。具体接口请求格式示例参见附录 A；
c) 接口响应时应返回相应的状态码，具体状态码应遵循 RFC 2616 规范，参见附录 B；
d) 接口响应消息应采用固定格式进行封装，每条响应消息应包括：状态码（code）、消息内容（message）、数据内容（data）等。数据内容应包括审计字段，如创建人（creator）、创建时间(create_time)、更新人(update_person)、更新时间(update_time)、备注说明(remark)等；
e) 接口编码方式统一采用 UTF-8 编码。

6.3.3 接口发布

a) 接口生成后，数据提供方应及时通过统一数据接入系统向数据获取方发布接口信息；
b) 接口发布内容应包括且不限于以下信息：

——接口说明；
——状态码参照表；
——接口调用示例文档。

6.3.4 接口维护

数据提供方应对数据接口进行维护，对接口变更流程进行统一管理。接口维护要求包括且不限于：

a) 接口版本管理机制，将 API 版本号放入 URL，多版本并存，采用增量的方式发布；
b) 接口信息同步机制，接口的变更应及时更新到统一数据接入系统，并由数据获取方进行审核。

6.3.5 接口访问

a) 数据获取方访问数据提供方数据的接口，具备读取数据操作权限；
b) 数据提供方在进行信息系统建设时，应考虑满足数据获取方通过接口批量获取数据的需求，支持数据获取方通过接口对数据的实时调用。

6.4 认证与鉴权

6.4.1 概述

为保证数据的安全，数据的发布和调用应经过认证与鉴权。

6.4.2 数据发布的认证与鉴权

在数据发布过程中：

a) 数据提供方初次访问统一数据接入系统时应进行注册，并由数据获取方进行审核、授予相应权限；

b) 数据获取方应对数据提供方在统一数据接入系统中的身份进行认证，并对其操作进行鉴权。

6.4.3 数据调用的认证与鉴权

在数据调用的过程中：

a) 数据提供方应为数据获取方提供可实时获取全局数据权限的账号信息，并保证账号信息及其权限的有效性；

b) 数据提供方应对数据获取方调用数据过程中的身份进行认证，并对其操作进行鉴权；

c) 相关认证与鉴权流程参见附录C。

6.5 数据对接管理

6.5.1 概述

数据对接过程基于统一数据接入系统进行，数据提供方在统一数据接入系统上发布并维护数据目录及接口等信息；数据获取方基于统一数据接入系统上的数据目录和接口等信息，访问并调用数据资源。

6.5.2 统一数据接入系统功能要求

统一数据接入系统功能应包括且不限于：

a) 用户管理，包括用户注册、登录、注销等功能；

b) 权限管理，实现对用户权限的统一管理；

c) 数据目录管理，实现对数据目录发布、数据目录维护和数据目录访问等过程的管理；

d) 数据接口管理，实现对接口发布、接口维护和接口访问等过程的管理；

e) 数据预览，用户可通过在线预览方式迅速获取部分数据快照信息；

f) 系统审计，实现对用户在统一数据接入系统操作的监控。

6.5.3 统一数据接入系统对接流程

统一数据对接流程包括：

a) 注册：数据提供方通过已有账号和密码登录统一数据接入系统，将数据目录、接口等信息注册到统一数据接入系统；

b) 审核：数据获取方对数据提供方发布的数据目录、接口等信息进行审核，只有审核通过的信息才能正常发布；

c) 发布：数据提供方在统一数据接入系统上发布数据目录、接口等信息，应符合本标准6.1、6.2及6.3的要求；

d) 调用：数据获取方根据数据提供方在统一数据接入系统上提供的数据目录、接口等信息调用数据。

6.6 数据安全管理

6.6.1 概述

数据安全管理体系是支持数据产生、存储、传输、应用等过程的基础，主要分为数据存储安全、数据传输安全、数据防篡改等。

6.6.2 数据存储安全

数据提供方与数据获取方对数据存储安全应从物理安全、运行安全、数据安全等多方面进行考虑，具体可参考GB/T 20271-2006相关规定。

6.6.3 数据传输安全

数据获取方与数据提供方在数据交互过程中，要求采用HTTPS协议，或者其他具有同等或者更高安全级别的传输协议。

6.6.4 数据防篡改

数据提供方与数据获取方应加强数据安全保障体系建设，防止数据造假、篡改、窃取等事件发生。

6.7 数据应用管理

数据获取方在获取数据后，应在规定范围内使用数据，安全地保存数据，防止数据泄露和滥用。为保证数据完整性，数据获取方可定期对数据进行检查。

附 录 A
（资料性附录）
接口请求格式示例

表A.1 给出了接口请求格式示例。

表A.1 接口请求格式示例

请求 URL	https://ip:port/api/v{n}/resource?access_token=ACCESS_TOKEN		
请求方法	POST/GET		
请求参数	是否必传	数据类型	说明
page	否	int	页码
size	否	char(n)	分页大小
***	否	根据具体情况确定	业务参数
返回参数			
参数名	是否必传	数据类型	说明
code	是	int	状态码(200 表示请求正常，其它值异常)
message	否	char(n)	消息提示，n 为消息长度，其取值根据具体情况确定
data	否	根据具体情况确定	接口的主数据，即业务数据。可以根据实际返回数组或者特定格式数据对象（如 JSON 格式、XML 格式等）
total	否	int	记录总数，列表查询返回
page	否	int	当前页，列表查询返回
size	否	int	分页大小，列表查询返回
pages	否	int	总页数，列表查询返回

附 录 B
（资料性附录）
接口响应状态码

B.1 接口返回状态码

状态码的定义遵循RFC 2616规范，常见HTTP响应状态码及其含义如表B.1：

表B.1 接口返回状态码

状态码	含义
200	请求已成功
400	请求信息不完整或无法解析
401	访问令牌没有提供，或者无效
403	访问令牌有效，但没有权限
404	资源不存在
409	资源冲突
422	请求信息完整，但无效
500	服务器内部抛出错误

附 录 C
（资料性附录）
认证与鉴权流程示例

C.1 身份认证

数据获取方根据已有账号信息创建安全会话并获取access_token（访问令牌）。

C.1.1 请求示例：

POST 请求：https://ip:port/api/v{n}/auth/login

Content-Type: application/json

请求参数：

```
{
  "app_key":"APP_KEY",
  "app_secret":"APP_SECRET"
}
```

C.1.2 返回结果：

```
{
  "code":200,
  "message":"success",
  "access_token":"91440300792588888K ",
  "expires_in":"86400"
}
```

C.2 访问控制

数据获取方根据获取到的access_token调用接口。

C.2.1 请求示例：

GET请求：https://ip:port/api/v{n}/resource/get_data?access_token=ACCESS_TOKEN

C.2.2 返回结果：

a) 正常返回结果：

```
{
  "code":200,
  "message":"success",
  "data":[
          {
               "user_id":"1"
```

```
                "age":25
                "user_name":张三
        "creator":AAA
        "create_time": 2019-03-01 16:00:00
        "updater":null
        "update_time": null
        "remark":null
                }
                {
                "user_id":"2"
                "age":32
                "user_name":李四
        "creator":AAA
        "create_time": 2019-03-01 16:00:00
        "updater":null
        "update_time": null
        "remark":null
                }
                {
                "user_id":"3"
                "age":22
                "user_name":王五
        "creator":AAA
        "create_time": 2019-03-01 16:00:00
        "updater":null
        "update_time": null
        "remark":null
                }
          ],
        "total":5,
        "page_name":1,
        "size": 3,
        "pages":2
        }
```


b) 异常返回结果：


```
        {
          "code":401,
          "message":"用户信息不存在"
        }
```


C.3 权限注销

数据获取方调用安全会话接口的logout方法，设置access_token为无效。

C.3.1 请求示例：

POST 请求：https://ip:port/api/v{n}/auth/logout?access_token=ACCESS_TOKEN

Content-Type: application/json

C.3.2 返回结果：

```
{
  "code":200,
  "message":"success"
}
```

参 考 文 献

[1] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
[2] GB/T 20282-2006 信息系统安全工程管理要求
[3] GB/T 21063.1-2007 政务信息资源目录体系 第1部分：总体框架
[4] GB/T 21063.2-2007 政务信息资源目录体系 第2部分：技术要求
[5] GB/T 21063.3-2007 政务信息资源目录体系 第3部分：核心元数据
[6] GB/T 21063.4-2007 政务信息资源目录体系 第4部分：政务信息资源分类
[7] GB/T 21063.5-2007 政务信息资源目录体系 第5部分：政务信息资源标识符编码方案
[8] GB/T 24294-2009 信息安全技术 基于互联网电子政务信息安全实施指南
[9] GB/T 25058-2019 信息系统安全等级保护实施指南
[10] GB/T 25062-2010 信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范
[11] GB/T 25070-2019 信息系统等级保护安全设计技术要求
[12] GB/T 28827.1-2012 信息技术服务 运行维护 第1部分：通用要求
[13] GB/T 28827.2-2012 信息技术服务 运行维护 第2部分：交付规范
[14] GB/T 28827.3-2012 信息技术服务 运行维护 第3部分：应急响应规范
[15] GB/T 29245-2012 信息安全技术 政府部门信息安全管理基本要求
[16] 中华人民共和国监察法
[17] 中华人民共和国计算机信息系统安全保护条例
[18] 计算机信息网络国际联网安全保护管理办法
[19] 广东省电子证照系统数据规范