ICS 03.160
CCS A 00

DB33

浙 江 省 地 方 标 准

DB33/T 1420.1—2025

跨部门大数据办案平台通用规范 第1部分：总体要求

Specification for cross-departmental case-handling platform based on big data—Part 1: General requirement

2025－02－19 发布　　2025－03－21 实施

浙江省市场监督管理局　发布

目　　次

前　言

本部分按照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。

本部分是DB33/T 1420《跨部门大数据办案平台通用规范》的第1部分。DB33/T 1420分为以下五个部分：

——第 1 部分：总体要求；

——第 2 部分：协同共享；

——第 3 部分：数字卷宗；

——第 4 部分：音视频证据随案移送；

——第 5 部分：涉案财物在线管理与处置。

请注意本部分的某些内容可能涉及专利。本部分的发布机构不承担识别专利的责任。

本部分由中共浙江省委政法委员会提出、归口并组织实施。

本部分起草单位：浙江省政法信息管理中心、浙江省高级人民法院、浙江省人民检察院、浙江省公安厅、中共金华市委政法委员会、中共义乌市委政法委员会、义乌市人民检察院、义乌市司法局、浙江省质量科学研究院。

本部分主要起草人：周川玲、周泰石、陈模科、姜政、陈伊文、高扬、杜科、林纪平、吴媛波、陈骥浩、金隽婷、王亦斌、孙雅和、孟一丁、应珊婷、王雅梦。

引　言

为深入贯彻落实习近平法治思想、习近平总书记关于政法工作重要论述和考察浙江重要讲话精神，浙江全面推进跨部门大数据办案平台提质增效工作，探索建立与现代科技深度融合的执法办案新方式，通过构建跨部门大数据办案平台，打破政法机关的网络隔阂、数据壁垒，形成贯穿联通的高速通道和流转共享体系，有效推动政法工作质量变革、效率变革、动力变革，促进实现更高水平的公平正义。DB33/T 1420《跨部门大数据办案平台通用规范》为多部分标准，旨在规范跨部门大数据办案平台的总体要求、协同共享、数字卷宗、音视频证据随案移送和涉案财物在线管理与处置，拟由五个部分构成。

——第 1 部分：总体要求。目的在于提出跨部门大数据办案平台建设的基本原则、平台架构、应用功能、运行和安全等要求。

——第 2 部分：协同共享。目的在于提出公安机关、检察机关、审判机关、司法行政机关办案协同共享的技术路径。

——第 3 部分：数字卷宗。目的在于提出跨部门大数据办案过程中数字卷宗的立卷、生成制作、检查、移送与签收、归档、安全、使用与管理等技术要求。

——第 4 部分：音视频证据随案移送。目的在于提出跨部门大数据办案过程中音视频证据随案移送的基本要求、总体架构、音视频证据汇聚、音视频证据协同、音视频证据使用与管理等技术要求。

——第 5 部分：涉案财物在线管理与处置。目的在于提出跨部门大数据办案过程中涉案财物在线管理与处置的系统架构、交接入出库、保管维护、财物流转、拍卖、销毁等技术要求。

跨部门大数据办案平台通用规范
第1部分：总体要求

1 范围

本部分规定了跨部门大数据办案平台的基本原则、平台架构、应用功能、运行要求和安全要求等内容。

本部分适用于跨部门大数据办案平台的建设和应用，其他部分与本部分联合使用。

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部分必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本部分；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本部分。

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—2022 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 29765 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 34110 信息与文献文件管理体系基础与术语

GB/T 35274 数据安全技术 大数据服务安全能力要求

GB/T 43697 数据安全技术 数据分类分级规则

GM/T 0132 信息系统密码应用实施指南

DB33/T 2487 公共数据安全体系建设指南

DB33/T 2488 公共数据安全体系评估规范

DB33/T 1420.2 跨部门大数据办案平台通用规范 第2部分：协同共享

DB33/T 1420.3 跨部门大数据办案平台通用规范 第3部分：数字卷宗

DB33/T 1420.4 跨部门大数据办案平台通用规范 第4部分：音视频证据随案移送

DB33/T 1420.5 跨部门大数据办案平台通用规范 第5部分：涉案财物在线管理与处置

3 术语和定义

GB/T 34110界定的以及下列术语和定义适用于本部分。

3.1

跨部门大数据办案平台 cross-departmental case-handling platform based on big data

政法机关在刑事诉讼等办案活动中，以数字卷宗为载体，以单轨制办案为核心，通过业务协同、数据交换、流程再造，打通公检法司执法办案系统，实现案件线上流转，提升案件办理效率和准确性。

注1：政法机关指公安机关、检察机关、审判机关和司法行政机关。

注2：相较于线上和线下分别移交案件卷宗的双轨制，单轨制办案是指通过线上数字卷宗移交取代线下纸质卷宗移交的办案模式。

3.2

办案源头数字化 original digitization of handling cases

依托电子签名捺印、跨系统交互等数字技术和工具，开展文书材料制作、讯（询）问、调取证据等执法办案活动的工作模式。

3.3

数字卷宗 digital archive

政法机关在诉讼活动中形成，以数字化的形式存储，具备有序结构的法律文书和各类证据材料的电子文件合集。

注1：包括案件受理或办理过程中收集、制作的数据、文档、图像、音频、视频等电子文件，以及将纸质案卷材料依托数字影像、文字识别等技术形成的电子文件。

注2：暂不包括政法机关的副卷（内部卷宗）。

3.4

音视频证据随案移送 transfer of audio and video evidence with case

在刑事诉讼活动中，公安机关将证明案件事实的视听资料，通过跨部门大数据办案平台移送至检察机关、审判机关的过程。

3.5

涉案财物 property involved in cases

公安机关、检察机关、审判机关在刑事诉讼活动中查封、扣押、冻结、提取、调取或从其他办案机关、个人处接收的与案件有关的财物。

3.6

云上专有域 virtual private cloud

政法机关在云计算平台上专有的网络区域，专有网络环境之间物理上相互隔离。

4 基本原则

4.1 高效便利

通过大数据、云计算等现代信息技术手段，实现无纸化办案，以及案件信息的实时共享、自动流转和智能分析，优化办案流程，提高办案效率。

4.2 安全保密

采用先进的数据加密技术，对跨部门大数据办案平台相关数据进行加密存储和传输，确保数据在传输过程中不被非法截获和篡改。

4.3 共享兼容

充分考虑政法机关内部业务系统之间的技术差异，选择可靠、兼容的技术改造或新建方式，确保各系统之间的数据交换、信息共享的通畅，各系统平稳升级。

5 平台架构

5.1 体系架构

跨部门大数据办案体系采用多层架构，由跨部门大数据办案平台（以下简称平台）、政策制度体系、标准规范体系、安全保障体系以及运行维护体系5个子体系构成，并通过安全可控的网关、接口和交换平台，与其他相关业务系统对接拓展，见图1，政法元数据信息实体见附录A。

a) 平台：通过数字基础底座、协同平台和业务应用场景集成的综合平台，实现政法信息共享、业务协同及决策智能化。
b) 政策制度体系：跨部门大数据办案应遵循的法律法规、政策文件等监督制约机制。
c) 标准规范体系：跨部门大数据办案平台建设运行应遵循的业务、数据、技术、安全、研发、运维等相关标准和规范。
d) 安全保障体系：跨部门大数据办案平台建设运行应建立的安全措施保障、安全技术保障和安全管理保障，确保系统物理安全、网络运行安全、信息安全保密。
e) 运行维护体系：跨部门大数据办案平台运行应建立的运维管理体系，包括信息化组织建设、系统维护管理、监控等。

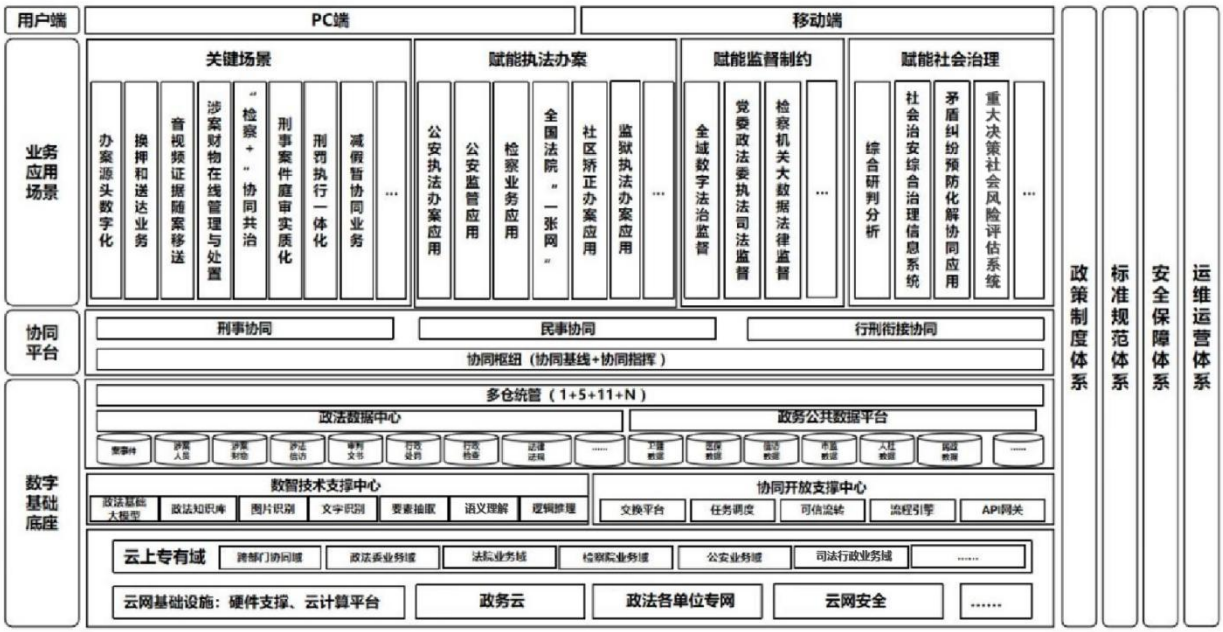

图 1　跨部门大数据办案平台体系架构

5.2　平台组成

5.2.1　数字基础底座

数字基础底座包括云网基础设施、云上专有域、数智技术支撑中心、协同开放支撑中心、多仓统管数据中心等。

a) 云网基础设施：
   1) 硬件支撑：服务器、存储设备、网络设备、安全设备等物理硬件；
   2) 云计算平台：采用云计算、雾计算和边缘计算等技术，适配政法云环境，运用政法云提供的存储、负载均衡、弹性扩展等能力构建统一的计算资源池和存储资源池。
b) 云上专有域：通过绑定弹性网际互连协议(Internet Protocol, IP)和配置网络地址转换（Network Address Translation, NAT）网关的方式，将专有网络与互联网连接。通过一对路由器链接其他专有域，建立高速、安全的私网通信。通过物理专线将云上专有域与本地数据中心连接起来：
   1) 专有域之间物理上隔离，用户可以管理和定义自有的专有网络；
   2) 每个专有域应包含至少一个私网网段、一个路由器和一个交换机；

3) 定义上包含网络名称、描述、无类别域间路由（CIDR）、是否支持 IPv6 等关键元素，具备创建、修改、权限控制等开放接口；
4) 具备虚拟路由器能力，可以连接专有网络内各个交换机以及其他网络设备；
5) 具备虚拟交换机能力，连接不用的云资源；
6) 具备虚拟边界路由器能力，提供关联至物理专线的功能和接口；
7) 具备高可用虚拟 IP 能力，可以独立创建和释放私网 IP 资源，支持搭建高可用主备服务。

c) 数智技术支撑中心：基于政法云统一算力底座及政法大模型平台，建设统一知识中心和模型中心，赋能辅助决策分析、监督制约体系、统一信息检索等业务场景。
d) 协同开放支撑中心：构建统一的政法外部网络跨网协同交换平台，高速、安全、可靠的网络连接，支持政法系统内部及跨部门的网络互通，确保数据传输的实时性和安全性。
e) 多仓统管数据中心：建设 1 个协同数据总仓、5 个省级政法单位分仓、11 个市级政法分仓，链接 N 个公共数据平台，保障政法机关的案件、人员信息及文书卷宗等数据共享平台目录管理、数据治理、供需对接、数据共享、数据分析等基础能力。

5.2.2 协同平台

协同平台包括协同枢纽，刑事、民事、行刑衔接等内部业务协同，具体业务协同交换要求应符合DB33/T 1420.2的规定：

a) 刑事协同业务：包括法律援助、提请批准逮捕、变更强制措施、数字换押、立案监督、移送起诉、一审公诉、二审上诉、刑罚执行、暂予监外执行、社区矫正、减刑、假释、涉案财物等协同环节；
b) 民事协同业务：包括民事抗诉、民事再审检察建议移送、法律文书及证据材料交互、裁判文书送达、审执案件在线调卷等协同环节；
c) 行刑衔接协同业务：包括行政执法机关向公安机关移送涉嫌犯罪案件、行政执法机关向公安机关移送需行政拘留案件、公安机关向行政执法机关移送案件等协同环节；
d) 协同枢纽：包括协同业务基线管理，管理协同业务依据、流程、数据、数字卷宗、通道等内容，支撑协同业务相关任务管理，基于协同基线的内容，通过任务管理模块实现任务协同处理、跟踪及反馈。

5.2.3 应用场景

应用场景包括关键场景、赋能执法办案、赋能监督制约、赋能社会治理等：

a) 关键场景：包括办案源头数字化、换押和送达业务、音视频证据随案移送、涉案财物在线管理与处置、“检察+”协同共治、刑事案件庭审实质化、刑罚执行一体化和“减假暂”协同业务等；
b) 赋能执法办案：赋能公安执法办案应用、公安监管应用、检察业务应用、全国法院“一张网”（全国法院办案办公平台）、社区矫正办案应用和监狱执法办案应用等；
c) 赋能监督制约：赋能全域数字法治监督、党委政法委执法司法监督、检察机关大数据法律监督等；
d) 赋能社会治理：赋能社会治安综合治理、综合研判分析、矛盾纠纷预防化解协同应用、重大决策社会风险评估等。

5.2.4 用户端

面向各级政法机关用户，为办案人员提供便捷高效的平台统一入口，是各类用户获取所需服务的主要入口和交互界面。根据不同的使用场景和用户群体，分别提供PC端、移动端等主要交互界面：

a) PC 端：提供全面的功能操作、展示和监督；

b) 移动端：注重便捷性和移动性。

6 应用功能

6.1 关键场景

6.1.1 办案源头数字化

应在案件办理各阶段，实现文书笔录数字化、移动办案、互联网远程办案、远程办案、涉案款项在线执收与退还、文书电子送达和数字卷宗等办案源头数字化功能。数字卷宗相关要求应符合DB33/T 1420.3的规定。

6.1.2 换押和送达业务

6.1.2.1 数字换押业务

应在案件移交阶段，实现数字换押协同、线上流程节点羁押期限变更协同、线上开庭排期协同等数字换押业务功能。

6.1.2.2 数字送达业务

应在诉讼过程中，实现向被羁押人员、被害人家属等当事人文书数字送达业务功能，以及政法机关间文书送达及反馈业务功能。

6.1.3 音视频证据随案移送

应在案件移交阶段，实现音视频证据随案移送功能。音视频证据随案移送应符合DB33/T 1420.4的规定。

6.1.4 涉案财物在线管理与处置

应在办案各阶段，实现涉案财物在线管理与处置。涉案财物在线管理与处置应符合DB33/T 1420.5的规定。

6.1.5 “检察+”协同共治

应对接跨部门大数据办案平台、全域数字法治监督等省域应用，实现检察机关与政法机关、行政机关、企事业单位的线上多跨协同。功能包括行刑正向衔接、反向衔接、检察建议等协同场景和重点领域共治场景。

6.1.6 刑事案件庭审实质化

应建设具备远程视频开庭和提审、证人安全作证、庭审录音录像、庭审语音激励、语音识别转文字、庭审智能交互、智能文书、电子签名、捺印等功能的标准化智能化数字法庭。

6.1.7 刑罚执行一体化

应在案件执行阶段，实现社区矫正的调查评估综合评估鉴定、社区矫正对象和重点安置帮教对象公安列管数据推送等刑罚执行一体化功能。

6.1.8 “减假暂”协同业务

应在案件执行阶段，实现减刑假释和暂予监外执行等“减假暂”业务协同功能。

6.2 赋能执法办案

6.2.1 公安执法办案应用系统

平台应赋能公安执法办案应用系统，实现价格认定、司法鉴定、前科数字调取、不动产查控、智能辅助阅读、社区矫正再犯通报协同和行刑衔接等功能。

6.2.2 公安监管系统

平台应赋能公安监管系统，实现同案犯审批协、“减假暂”办理、羁押表现纳入量刑和代办法务等功能。

6.2.3 检察业务应用系统

平台应赋能检察业务应用系统，实现审查逮捕、延长羁押期限、不捕复议复核、审查起诉、量刑建议调整、委托调查评估、法律帮助、法律援助、不诉复议复核、强制措施、检察监督、提起公诉、二审抗诉、审判监督抗诉、法院决定再审、减刑假释暂予监外执行、社区矫正、民事案件在线调卷、民事抗诉、再审检察建议等业务协同功能。

6.2.4 全国法院“一张网”（全国法院办案办公平台）

平台应赋能全国法院“一张网”（全国法院办案办公平台），实现二审上诉、二审抗诉、法院决定再审、再审审查－审判监督抗诉、再审审查－刑事申诉再审抗诉、强制医疗、减刑假释、变更强制措施、法律援助、变更羁押期限、交付执行、社区矫正、解回再审、数字换押、调取罪犯信息及释放证明、自诉转公诉、改变管辖、审判活动监督、限制出境、刑满释放等业务协同功能。

6.2.5 社区矫正办案应用系统

平台应赋能社区矫正办案应用系统，实现治安处罚、收监执行、减刑、调查评估、入矫、解除（终止）矫正、撤销缓刑、撤销假释、逮捕等业务协同功能。

6.2.6 监狱执法办案应用系统

平台应赋能监狱执法办案应用系统，实现减刑、假释、暂予监外执行办理等功能。

6.3 赋能监督制约

6.3.1 赋能全域数字法治监督

平台应赋能全域数字法治监督，实现法治统筹、监督建模、监督协同、监督评估等功能。

6.3.2 赋能党委政法委执法司法监督

平台应赋能党委政法委执法司法监督，支撑执法司法态势分析和执法司法突出问题监督模型，实现专题分析、风险清单和协同处置等功能。

6.3.3 赋能检察机关大数据法律监督

平台应赋能检察大数据法律监督，构建刑事侦查活动、审判活动、刑罚执行、社区矫正等领域智能审查大数据法律监督模型。

6.4 赋能社会治理

6.4.1 综合研判分析

平台应赋能综合研判分析，实现平安建设态势分析、社会稳定风险研判、矛盾纠纷隐患感知、社会治安风险预警，为风险隐患处置提供决策支撑。

6.4.2 社会治安综合治理信息系统

平台应赋能社会治安综合治理，支撑纠纷预防化解、社会治安防控、专项排查整治、网格工作管理等功能。

6.4.3 矛盾纠纷预防化解协同应用

平台应赋能矛盾纠纷预防化解，支撑县、乡两级矛调中心业务统筹、协同联动和运行管理，实现“一站式接收、一揽子调处、全链条化解”。

6.4.4 重大决策社会风险评估系统

平台应赋能重大决策社会风险评估，推动重大决策社会风险防范治理信息化、数字化、智能化。

7 运行要求

7.1 稳定可靠

7.1.1 运行保障

应具备运行维护和保障能力，采用包括但不限于防火、防水、防雷、防电磁干扰等措施加强数据中心、存储和网络安全设备等关键基础设施的物理安全防护，保障硬件设备和平台的安全稳定运行。

7.1.2 故障预警

应具备运行监控和故障预警能力，提前发现潜在隐患。

7.1.3 故障恢复

应按照GB/T 29765建立容灾备份制度，具备故障恢复能力，保障业务连续性和系统安全，具体要求如下：

a) 一般故障恢复时间小于 2 小时；
b) 较大故障恢复时间小于 8 小时；
c) 重大故障恢复时间小于 12 小时。

7.2 日志管理

7.2.1 日志监控应记录系统中硬件、软件和系统问题的异常，监控系统中发生的事件，包括进程日志、数据库日志、系统备份记录等。

7.2.2 资源监控应记录数据运行状态和系统运行状态，平台出现异常时，系统自动提醒通知运维人员。

7.3 便捷操作

应注重用户体验，提供简洁明了的操作界面、便捷的操作方式和常见操作问题解答，提供全面、准确的培训服务，降低用户的学习成本和使用难度。

7.4 功能可拓展

应具备功能可扩展性，能够根据实际需求安装部署新的功能模块和业务流程，保障系统正常运行同时满足不断变化的工作需求。

8 安全要求

8.1 平台中涉及数据采集、传输、交换、存储和使用的系统和过程均应符合 GB/T 22239—2019 中的第三级安全要求并获得相关认证。涉及公共数据的，相关系统安全能力的建设和管理应符合 DB33/T 2487、DB33/T 2488 的规定。涉及音视频数据的，应符合 GB/T 28181—2022 的第 8 章。

8.2 应按照 GB/T 31168、GB/T 35274，根据各政法机关的安全需求建设数据资源交互链路，在安全边界处配备防火墙、入侵检测、安全审计、安全隔离和集中监控报警等安全设备，实现网络边界的安全隔离，防止非法访问。应按照 GM/T 0132 等开展密码应用。

8.3 宜参照 GB/T 43697 对所有涉案数据进行分类分级管理，涉密或其他法律法规另有规定的数据，按照相关法律法规执行。

8.4 应部署数据防泄露、数据脱敏、个人信息去标识化等安全功能组件；建立严格的数据访问权限控制机制，在全流程采用数字签名等方式进行实名制身份管理，只有经过授权的办案人员才能访问相关数据，并对数字签名进行核验：

a) 构建签名有效性核验机制，包括与认证服务机构进行数字签名证书生效状态确认 ；
b) 构建智能核验模块，提供相应数字签名有效性证明、签名主体数字身份证明等核验服务；
c) 实现数据原文、数字签名、数字证书等信息的一体化存证。

8.5 应加强数据监督和审查，对用户进行数据存证与核验的流程进行过程行为数据存证，妥善记录和保存数据的来源、提取和访问等信息，提供全流程追踪查询服务，确保数据的可追溯性：

a) 保存用户数字签名的状态数据；
b) 对用户使用数字签名的各项操作进行归档，包括但不限于操作用户、操作时间、操作内容、操作结果等；
c) 具有用户行为的审计功能，包括但不限于上传数据、查阅数据、使用数据等各项记录；
d) 具有数据状态的审计功能，包括但不限于数据上传、数据查阅、数据修改、数据使用、数据流转的各项记录。

8.6 应对敏感个人信息设置严格的信息安全保护措施：

a) 严格管理敏感个人信息的使用记录，对每条敏感个人信息每次读取和修改的时间、申请人查询和修改范围做详细记录；
b) 将敏感个人信息单独存储，采用国密算法加密与数字加签等技术手段保障数据安全。

8.7 应建立网络安全应急预案和响应机制，对可能发生的网络安全事件进行快速响应和有效处置。定期开展网络安全攻防演练和专项培训，增强办案人员的网络安全意识和应对能力。

附 录 A
（资料性）
政法元数据信息实体

A.1 基本属性

政法元数据信息实体和信息元素进行描述使用表A.1中所示的5个属性。表A.1中：

a） 描述属性：描述信息实体和信息元素的属性；

b） 要求：描述信息实体和信息元素的该属性是必备属性还是可选属性；

c） 定义及说明：对属性的说明。

表 A.1 信息实体和信息元素的描述属性

序号	描述属性	定义及说明
1	中文名称	信息实体和信息元素的中文名称
2	数据类型及格式	详细说明见A.2和A.3
3	约束/条件	详细说明见A.4
4	值域	信息元素所允许的值的集合
5	说明	对信息实体和信息元素含义的解释或进一步补充说明

A.2 数据类型

信息实体的数据类型为复合型，信息元素的数据类型表示方法见表A.2。

表 A.2 数据类型取值

数据类型	数据类型的表示	取值
字符型	C	可包括字母字符、数字字符或汉字等在内的任意字符
数值型	N	用“0”～“9”数字表达的数值
日期时间型	YYYY-MM-DD	格式见GB/T 7408
文本型	Text	长度不确定的文本
二进制流	BY	图像、音频、WAN.RM.AVI.MPEG等二进制流文件格式

A.3 数据格式

使用以下格式来表达信息元素的数据格式：

a） 字符型和数值型后加正整数表示定长格式；

注1：C6表示6位定长的字符。

注2：N16表示16位定长的数值。

b） 字符型和数值型后加“x..y”表示从最小到最大长度的格式；

注3：C1..10表示最短1位、最长10位的字符。

注4：N1..6表示最短1位、最长6位的数值。

c） 字符型后加“.ul”表示长度不确定；

注5：C..ul 表示长度不确定的字符，一般多为大量的文本内容。

注6：数值型（N）后加“x,y”表示小数位。

示例1：N..17,2表示最长17 位、小数点后2位的数值。

d） 二进制流（BY）后加具体的媒体格式。

示例2：BY-JPEG表示“JPEG”格式的文件。

A.4 约束/条件的标识

表示一个信息实体或信息元素是必备的还是可选的，具体表示方法如下：

a） M：必备，表示该信息实体或信息元素是必选的；

b） C：条件必选，表示该信息实体或信息元素在一定条件下必选，当满足约束/条件中所定义的条件时应选择，具体条件在备注中说明；

c） O：可选，表示该信息实体或信息元素根据实际应用是可选的。

A.5 信息扩展

A.5.1 信息扩展要求

当政法数据的信息实体无法满足特殊需要时，根据实际需要，对政法数据的信息实体进行扩展。扩展的信息或数据表述与数据元素、通用数据、应用数据和相关表述保持一致。

A.5.2 信息扩展方法

根据不同实际需要扩展信息实体和信息元素，扩展方法包括：

a） 扩展信息实体：可增加信息实体和扩展信息实体；

b） 扩展信息元素：可在信息实体中增加信息元素，信息元素按附录A.1规定的属性进行描述。

A.5.3 扩展信息属性

信息元素中的属性的扩展取值方法包括：

a） 在扩展信息元素属性时，不改变本标准中规定的信息元素的中文名称、字段、说明、数据类型及格式、约束/条件等属性名称；

b） 对信息元素的约束/条件更严格限制，如原先是可选的信息元素，经扩展后可以是必备的；

c） 建立新的代码表，补充或代替现有值域中的代码表。