珠海市公安局（科信支队）
珠海公安大数据智能化
建设采购项目
用户需求书

2022 年 5 月

目录

目录 2
第 1 章 总体需求 6
1.1 整体架构 6
1.2 门户管理 10
第 2 章 基础设施需求 13
2.1 基础设施需求概述 13
2.2 (IaaS)基础设施层 15
2.2.1 计算资源池需求 15
2.2.2 存储资源池需求 15
2.3 (PaaS)平台服务层 16
2.3.1 资源服务需求 16
2.3.2 大数据资源池需求 16
2.4 IDC 机柜租赁需求 16
2.5 非功能性需求 17
2.5.1 计算和存储架构需求 17
2.5.2 标准规范需求 18
第 3 章 数据资源需求 18
3.1 数据采集汇聚需求 19
3.1.1 新建数据采集管理平台 19
3.1.2 升级改造数据接入平台 25
3.1.3 扩大数据汇聚需求 30
3.2 数据处理组织需求 33
3.2.1 数据处理 33
3.2.2 数据组织 33
3.2.3 大数据处理实施 39
3.2.4 数据运维管理 44
3.3 非功能性需求 46
3.3.1 标准规范需求 46
3.3.2 数据处理非功能性需求 46
第 4 章 服务平台需求 47
4.1 服务开发管理及统一服务目录 48
4.1.1 服务资源目录 48
4.1.2 服务资源管理 49
4.1.3 与上级资源对接 49
4.2 通用数据服务建设 50
4.2.1 查询检索 50
4.2.2 比对订阅 50
4.2.3 模型分析 51
4.2.4 数据推送 51
4.2.5 数据鉴权 51
4.2.6 数据操作 51
4.2.7 数据管理 51

4.3 通用应用服务建设.....51
4.3.1 电子地图服务.....52
4.3.2 专业侦查办案数据融合服务.....54
4.3.3 刑事技术应用服务.....55
4.4 业务应用支撑服务.....55
4.4.1 基础数据服务.....55
4.4.2 建模分析服务.....55
4.5 开发框架需求.....55
4.5.1 开发平台.....56
4.5.2 服务治理平台.....56
4.5.3 API 网关.....56
4.5.4 配置中心.....57
4.5.5 服务注册中心.....57
4.5.6 容器管理平台.....57
4.5.7 统一的代码托管中心.....57
4.5.8 开发要求.....57
4.6 非功能性需求.....58
4.6.1 性能和其他需求.....58
4.6.2 标准规范需求.....58
4.6.3 其他需求.....58
第 5 章 大数据智能应用需求.....59
5.1 通用应用.....59
5.1.1 智慧搜索升级.....59
5.1.2 全息画像升级.....61
5.1.3 智慧关注升级.....62
5.1.4 智能消息升级.....63
5.1.5 短信平台升级.....64
5.1.6 建模平台.....65
5.2 公安一体化政务服务平台.....74
5.2.1 服务门户.....74
5.2.2 工作门户.....74
5.2.3 基础支撑系统.....75
5.2.4 数据可视化.....76
5.2.5 升级公安外部信息资源汇集平台.....76
5.3 可视化大屏平台和定制服务.....77
5.3.1 业务需求.....77
5.3.2 功能需求.....78
5.3.3 定制服务.....80
5.4 非功能性需求.....80
5.4.1 应用软件性能需求.....80
5.4.2 政务服务性能需求.....80
5.4.3 其他需求.....81
5.4.4 标准规范需求.....81
第 6 章 信息安全建设需求.....81

6.1 安全管理中心.....82
6.2 零信任体系.....83
6.2.1 认证服务.....83
6.2.2 权限服务.....84
6.2.3 审批服务.....85
6.2.4 审计服务.....85
6.2.5 环境感知服务.....86
6.3 安全防护体系.....87
6.3.1 网络安全防护.....87
6.3.2 终端安全防护.....88
6.3.3 应用安全防护.....89
6.3.4 数据安全防护.....90
6.3.5 云平台安全防护.....91
6.3.6 边界安全防护.....92
6.4 安全访问.....92
6.4.1 单位内部人员访问需求.....92
6.4.2 合作企业人员访问需求.....93
6.5 安全业务统一门户.....94
6.6 其他安全服务.....95
6.6.1 驻场安全保障服务.....95
6.6.2 漏扫及渗透测试服务.....96
6.6.3 互联网网站云防护服务.....96
6.6.4 利旧设备续保服务.....98
6.6.5 等保测评服务.....98
6.6.6 国密应用安全性评估服务.....98
6.6.7 边界测评服务.....98
6.7 安全要求.....98
6.8 安全性能需求.....99
第7章 运营运维需求.....101
7.1 基础设施运营机制.....102
7.1.1 警务云资源使用管理.....102
7.1.2 警务云基础设施资源使用管理.....102
7.1.3 各业务应用上云指南.....102
7.2 数据资源运营机制.....103
7.2.1 数据治理流程机制、成效评价管理.....103
7.2.2 数据质量评估标准和管理.....103
7.2.3 数据申请和使用管理.....103
7.3 服务应用运营推广及评价管理.....103
7.3.1 服务使用评价及淘汰.....103
7.3.2 应用评价管理.....103
7.4 资源运营服务平台需求.....104
7.4.1 业务需求.....104
7.4.2 架构需求.....105
7.4.3 功能需求.....107

7.4.4 资源分类参考.....112
7.4.5 非功能性需求.....112
7.5 一体化运维服务需求.....112
7.5.1 运维服务技术系统建设.....113
7.5.2 运维制度规范建设.....119
7.5.3 运维服务中心.....120
7.5.4 品高云平台运营服务.....121
7.5.5 非功能性需求.....121
第8章 其他需求.....123
8.1 验收要求、方式和内容.....123
8.1.1 验收要求.....123
8.1.2 验收依据和方式.....126
8.1.3 验收内容.....126
8.2 商务要求.....127
8.2.1 服务期要求.....127
8.2.2 售后服务要求.....128
8.2.3 驻场服务要求.....129
8.2.4 培训要求.....129
8.3 支付及结算要求.....130
8.3.1 支付方式.....130
8.3.2 结算材料要求.....130
8.3.3 其他要求.....131
第9章 附录.....132
9.1 附录1 数据资源附录.....132
9.1.1 数据接入处理能力要求.....132
9.1.1 数据处理需求.....133
9.1.2 前置区数据融合处理.....140
9.2 附录2 运营运维附录.....142
9.2.1 资源分类参考.....142
9.2.2 服务器监控指标.....144
9.2.3 网络设备监控指标.....145
9.2.4 数据库监控指标.....147
9.2.5 中间件监控指标.....148
9.2.6 应用监控指标.....151
9.3 附录3 采购清单附录.....152
9.3.1 硬件清单.....152
9.3.2 软件清单.....176
9.3.3 机房租赁清单.....179

第1章 总体需求

根据上级建设要求，结合市情和采购人业务特色，全面采用成熟先进的大数据技术，优化大数据智能化整体架构，到2023年建成较为完整的大数据运行体系（包括基础设施、数据资源、服务平台、全警全域应用）和支撑体系（包括大数据安全纵深防御、统一运营运维），为采购人各业务部门全面构筑大数据智能应用生态奠定基础。

本项目的所有硬件、基础软件的运维保障时间均要求完成最终验收后五年，项目完成最终验收后运维运营服务均不少于一年时间，▲在项目建设和运维运营服务期内，应遵循大数据上云总体技术要求持续为存量应用的迁移或改造上云、新建应用上云提供技术支撑。

整个大数据平台对稳定性的要求如下：

平台类：基础设施之平台服务层（云平台和大数据套件），数据资源之数据接入、数据处理、数据组织等，服务平台，大数据智能应用之公安一体化政务服务平台，运营运维之资源运营管理平台和统一运维平台等的故障平均间隔时间(MTBF)≥1万小时，平均故障修复时间（MTTR）不超过0.5小时(因为停电等不可预测因素除外)。平台全面贯彻“分层解耦，异构兼容”的设计思想，单个模块的故障不能导致平台整体失效。平台装载或卸载某个功能服务时，不得间断平台运行。

应用类：平台外其他功能应用，需考虑高可用、负载均衡不能因为应用并发造成业务中断、停止等故障，应用故障平均间隔时间(MTBF)≥1500小时，平均故障修复时间（MTTR）不超过4小时(因为停电等不可预测因素除外)。

后续章节对稳定性要求与上述要求有冲突的以上述为准。

1.1 整体架构

为了确保整个系统可持续发展，要求不同层的软件、硬件、数据要实现分层解耦，每层的软件、硬件、数据修改、更换或升级都不会影响其它层软硬件的正常运行。

基础设施：统一基础设施包括在前置区和数据域的IAAS和PAAS层，按照采

购人“一片云”思路，统一管理前置区和数据域的 IAAS 和 PAAS 层，持续支撑各类数据不断汇聚融合，持续推进各业务部门的应用上云。本项目要充分利旧原有基础设施，并确保云计算资源池、存储资源池、云数据库、各种大数据组件等随着各业务部门应用的部署能在安全、稳定、可靠的前提下逐步扩容。

数据资源：统一数据资源主要负责将各类数据资源，按照上级制定的大数据标准和知识库的要求(知识库的内容是由各业务单位根据业务经验生成的数据标签、关联关系规则、常用的搜索和分析规则、算法和模型等），生成原始库、资源库、主题库、业务库。统一数据资源包括数据采集管理平台、数据接入平台、数据处理平台。其中数据采集管理平台是实践大数据采集管理办法，落实年度数据采集任务、专项采集任务和零散数据采集需求，解决数据采集汇聚中“采什么？谁来采？怎么采？采得怎么样？”等关键问题的抓手，从而实现全过程数据采集管理。数据处理平台负责按照上级大数据处理标准，将数据采集管理平台采集的所有数据资源统一接入数据接入平台，然后通过数据处理、数据治理、数据组织，实现数据资源分类建库，存储到原始库、资源库、主题库、知识库、业务库、业务要素索引库，同时对前置区和数据域的数据资源统一编目、统一对外提供服务，为业务单位和政府部门提供数据资源服务支撑。

服务平台：加强与上级单位服务资源的整合，实现上级单位的服务资源、本地化服务资源在服务平台的统一注册、申请、对接和管理，建立三级服务资源目录，实现联动。丰富数据服务方式，强化服务能力，围绕普遍性场景，开发查询检索、比对订阅、消息推送等通用的数据服务，开发电子地图、工作流、专业侦查办案融合、刑事技术查询比对、视频融合等通用应用服务，以各业务单位的业务需求为牵引，围绕重点工作等提供定制化的服务支撑。

全警全域应用体系：一是开展通用应用的建设和推广。基于专业侦查办案数据融合，归并前期已建设同类型应用，整合优化升级智慧搜索(含全息画像)、智慧关注、智能消息三大通用应用；开展平台型应用建设，包括升级改造建模平台、建设新的可视化大屏平台，为用户各业务部门按需自行开展大数据特色展示分析模型建设奠定基础；开展公安一体化政务服务平台建设，打造为民服务的服务门户、后台各服务部门的工作门户，为公安各业务部门构建以民生服务为主要目标的应用奠定基础，实现政务服务的集约式管控和常态化监测的全面感知。二是以

SaaS 化通用应用、云平台和大数据各层的服务为支撑，各业务单位开展各自的特色业务应用建设，遵循上云总体要求及时入驻门户的应用市场，纳入统一的管理，业务应用涉及审批、订阅、预警、消息提醒、待办等也应统一接入门户。

大数据安全纵深防御体系：按照上级提出的大数据安全建设标准和要求，从“云、数据、应用、网、边界、端”六维开展纵深防御体系建设，保障大数据全程可知、可管、可控、可查。一是开展零信任体系建设，通过认证、权限、审计、审批、环境感知等服务能力规范应用安全访问、数据安全使用，严格按照职责任务优化高敏应用数据访问审批流程，建立业务系统角色和业务场景相匹配的细粒度授权模式；二是开展安全防护体系建设，保障终端、网络、应用、数据、云平台、边界实体安全，为发现安全风险提供底层支撑；三是开展安全管理中心建设，做到风险事前监测发现、上网行为事中监督、违规行为事后溯源。利用安全大数据、关联分析和智能分析技术，综合分析各类安全系统安全数据，实时监督发现安全风险并进行告警，隔离安全风险的传播途径，事后溯源到 IP、个人或单位等。通过对接第三方平台派发处置工单，提出安全风险解决建议措施，并及时复查处置结果，实现闭环的安全风险处置，并对引发安全风险的单位或个人进行通报；四是升级完善用户安全访问与数据交换通道，实现各业务单位的动态精细化访问控制和安全防护，满足外部网络的数据安全交换。五是定期开展攻防渗透等实战演练，充分发挥安全服务人员的技术能力，提前发现网络安全薄弱环节和潜在风险；六是开展等级保护三级测评、国密测评和边界测评，并建设配套的国产密码设施基础资源池，全面推进国产密码改造工作。七是建立安全工作考核机制，层层考核、层层落实安全责任。

统一运营运维体系：包括统一运营平台和统一运维平台。

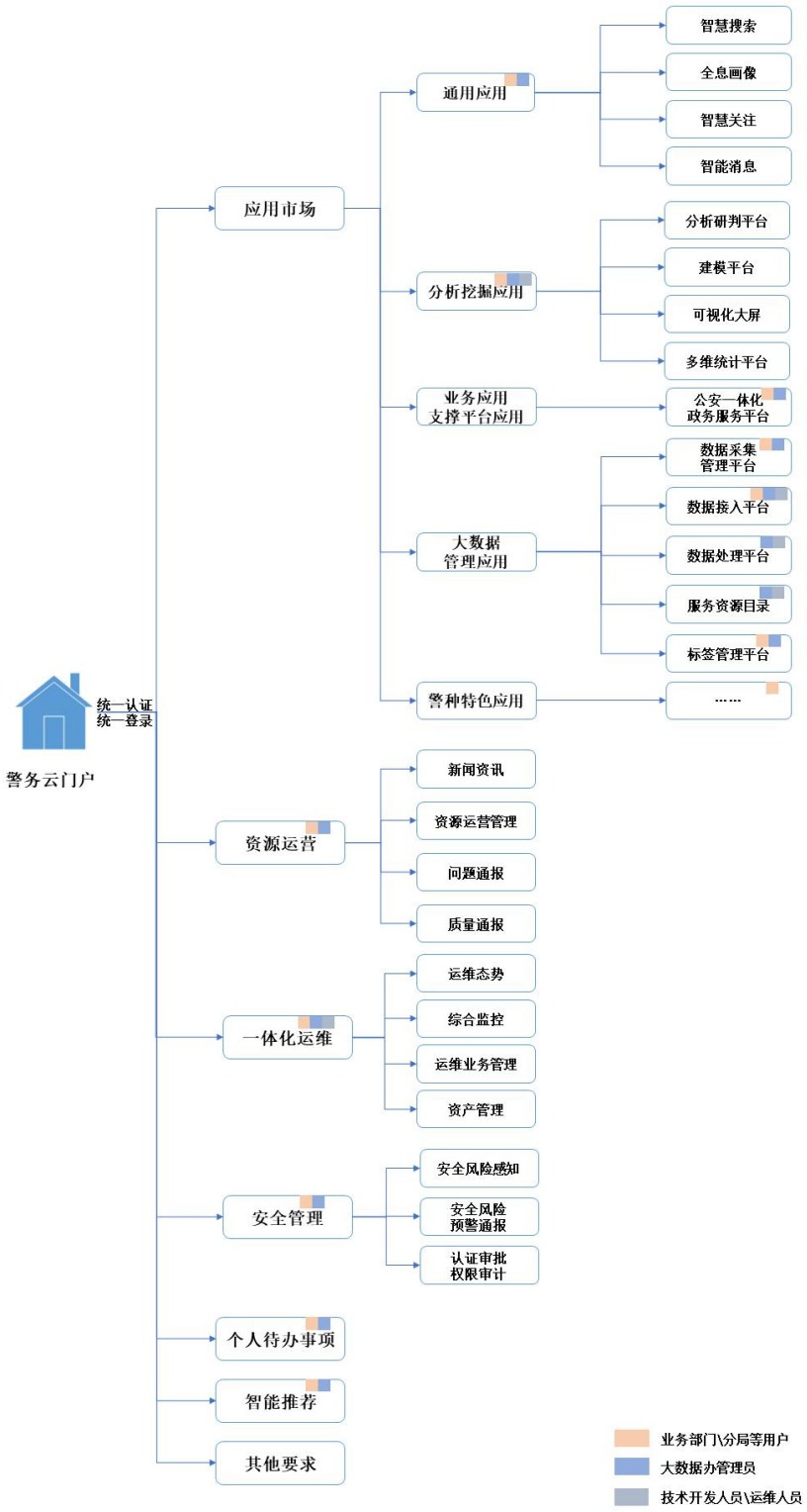
统一运营平台：统一运营平台主要解决六个方面的问题，一是对新一代公安网上基于警务云和大数据建设的所有资源进行统一运营，优化采购人现有的统一运营平台，围绕前置区、数据域 IPDS 各层资源申请、审批、评价考核等资源运营管理需求，升级统一运营平台；二是对接上级单位的统一运营平台，实现省市资源联动；三是对接入新一代公安网的各种前端和终端设备进行申请、审批；四是对采购人各单位的安全管理情况进行评估；五是对采购人各单位的运维管理情况进行评估；六是对采购人各单位引发的应用、安全、运维、数据治理问题进行

通报。

统一运维平台：统一运维平台主要负责整个新一代公安网软硬件的高效运维，它主要解决五个方面的问题。一是发现问题，通过实时监测整个新一代公安网上的所有软硬件运行情况，发现可能存在的软硬件故障或问题；二是故障或问题溯源，即找到故障或问题的源头，确定故障或问题的责任单位或责任小组；三是建立故障受理中心，统一受理采购人各单位的报障信息，提供智能的报障咨询服务；四是故障或问题处置，即由系统派单给责任单位或小组，同时监督整个故障或问题的处置过程；五是资产管理，将新一代公安网上的所有软硬件纳入统一的资产管理，明确资产关联的项目、建设单位、承建单位、运维单位、管理单位等相关基础信息，为明确运维和安全管理责任奠定基础。

新一代公安网：按照公安大数据新一代公安信息网标准规范，采购人已建设新一代公安信息网基础框架，运行网络需求已基本满足。

1.2 门户管理



所有用户（包括公安各业务部门、各层级用户，各个承建企业的开发人员，各个运维企业的运维人员，各个安全企业的安全服务人员）均通过警务云门户登

入，整个门户包括应用市场、资源运营、一体化运维、安全管理和个人待办事项、智能推荐、其它要求七个部分。根据机构用户角色及权限分配各个应用或功能的使用权限（所有应用或系统，以及各业务单位特色应用均需对接零信任体系的认证服务、审批服务、权限服务和审计服务），上图为大数据智能化建设项目主要的应用或平台。

资源运营：

资源运营是指对所有资源进行统一运营管理，采购人新一代公安网上基于警务云和大数据建设的所有资源对用户提供服务的统一窗口，用户通过该平台发现、申请、审批、使用各类资源，包括前端、终端设备以及云平台、数据、服务、模型、标签、IP 地址、应用、安全等 IPDS 资源，并对采购人的资源问题和质量进行管理和效能评估。主要用户为各业务部门、各层级用户和大数据管理职能单位用户。

一体化运维：

一体化运维是对新一代公安网软硬件进行全局的集中资产管理、统一监控、统一运维服务管理，保障采购人资产的高效运维。主要用户为各业务部门各层级用户、大数据管理职能单位用户和运维人员。

应用市场：

提供采购人各类应用使用的统一窗口，主要包括通用应用、分析挖掘类应用、业务应用支撑平台、大数据管理应用和各业务单位的特色应用。

1、通用应用：为各业务部门用户提供的工具类、基础业务类应用，用户可直接使用，包括智慧搜索、智慧关注、智能消息、全息画像等。

2、分析挖掘类应用：为各业务部门用户提供的平台型应用，各用户可以在应用中基于大数据资源进行分析研判、模型构建、可视化统计和展示等，包括分析研判平台、建模平台、可视化大屏平台、多维统计平台等。

3、业务应用支撑平台：为各业务部门提供业务应用构建支撑能力，包括公安一体化政务服务平台等。

4、大数据管理应用：为大数据管理职能单位管理用户、业务部门用户和技术开发人员提供大数据建设管理能力，主要指大数据平台数据资源及服务能力建设所需的管理工具及平台，包括数据采集管理平台、数据接入和处理平台、服务

资源平台、标签管理平台等。

5、各业务单位特色应用：指由业务部门利用大数据能力自行开展的特色大数据智能化应用。

安全管理：

实现新一代公安网各类安全风险的感知、预警、溯源、处置和通报，并提供认证服务、审批服务、权限服务、审计服务，为所有应用及系统提供多维度的身份认证、细粒度的权限管理、动态的审批监管和全面的业务安全审计。

个人待办事项：

个人待办事项包括等待个人查看和需要处理的各类事项，并满足以下要求。

1、统一消息任务

通过统一的消息支撑服务，将各系统的多种消息（包括订阅、通知、预警等）进行统一汇总、融合、分组、过滤等处理，再针对不同用户提供个性化工作界面，提升资源利用效率，实现消息的统一服务。

2、统一流程提醒

流程中心整合各业务系统的工作流，将工作流进度整合展示在门户，提升警务办事效率，减少沟通带来的时间成本。

3、数据个性化展示

通过将各个业务系统的数据整合，根据不同维度进行重组展示，也可根据个人需求定制化展示。

智能推荐：

大数据系统根据个人工作需要和使用偏好，自动推荐各类信息，提高个人工作效率，加强部门和人员之间的协作。大数据系统可以针对搭建业务模型、个人分享、课题学习等主题进行综合讨论，并根据热度推送给其他相关人员，减少重复沟通成本，达成经验分享，做到业务深耕。

其它要求：

▲按照“一门进千户”理念，建设统一门户，门户兼容常规PC、大屏、移动警务等多种前端设备，可根据业务的需要进行配置展示。门户对前期建设成果以及本期项目中的子系统及应用进行统一管理，实现一站式登录认证、一站式信息发布、一站式在线办事和一站式应用等。

第 2 章　基础设施需求

基础设施层为统一数据资源、统一服务平台、全警全域应用体系、大数据安全纵深防御体系、统一运营平台、统一运维平台提供基础存储能力、计算能力和数据交换能力。采购人利用已有的基础设施和视频云项目相关基础设施，构建了前置区警务云。数据域已有的基础设施仅够满足当前数据汇聚和应用需求，难以满足新增数据存储计算、应用上云的需要。本项目将在充分利旧的基础上，对基础设施进行扩容。

2.1　基础设施需求概述

本次规划的大数据平台需要按照公安部大数据智能化建设的要求，构建统一的大数据平台，面向全警提供标准的涵盖 IaaS 和 PaaS 层的云计算服务，建设云支撑架构和大数据组件开发，提升 IaaS、PaaS 层支撑能力，构建分层解耦，异构兼容的技术体系，打造具备珠海特色、开放共享的基础设施。

本项目建设需充分考虑国家关于信息技术创新建设发展的大趋势，站在面向未来国产化演进的角度，支持国产 X86 和 ARM 芯片，支持混合部署能力。即根据行业趋势和市场变化，本次规划平台的某架构服务器，后期能支持扩容选择另外架构类型的服务器。

1、基础设施

本层主要是由各种硬件设备组成，包括服务器（既有用于计算的服务器，也有用于存储的服务器）和网络设备等硬件基础设施。

2、资源池

资源池包括计算资源池、存储资源池、网络资源池。

将各种硬件设备池化后形成资源池，可以按需提供计算、存储和网络能力，提高硬件设备的利用率、容错能力、可扩展性、可靠性和稳定性。

3、资源服务

资源服务层包括自动伸缩、网络服务、存储服务、VPC 服务、弹性主机、负载均衡、资源编排等服务。

资源服务层统一管理多个数据中心云资源层提供的资源池，提供云资源的统

一运营和运维管理，构建统一的融合资源池，实现资源共享。

自动伸缩需能够根据应用负载情况自动扩张和收缩应用环境所使用的计算资源，也可以有计划的根据指定的规则进行自动扩张和收缩应用环境所需要的计算资源，以提高可预测高峰期的运行效率。

▲存储服务必须包含分布式的块存储、对象存储、文件存储，支持对视频、图片、音频等非结构化数据、半结构化数据和结构化数据进行高效的存储和访问，利用率要达到70%以上。

负载均衡需能够同时支持软件和硬件的实现方式，以保证上层服务和应用响应时间的性能要求。

4、计算组件

计算组件必须包括离线计算、流式计算、实时计算和图计算，需保证在海量数据超大规模计算下平台的高性能、高可用、高可靠、高扩展，以及托管管理、快速部署的能力。

5、存储组件

存储组件为云平台中不同的数据应用提供数据存储的能力，采用不同的存储方式以满足不同类型的应用对海量数据的存储和访问需求。涉及到的存储方式包括：对文件数据进行存储的分布式文件存储系统，对结构化数据进行存储的分布式关系型数据库系统，对多种键值类型的数据进行存储的列式数据库，对数据进行高速访问的内存数据库，对文本信息进行存储的海量全文数据库，对多媒体信息进行存储的对象存储系统，对实体以及实体关系信息存储的图数据库系统，对海量数据进行多维分析、快速查询的多维分析数据库。

6、应用支撑

应用支撑包括但不限于分布式消息、分布式缓存、API 网关等。

分布式消息须具备高一致、高可靠、高并发的能力，具备所有应用所需的海量消息堆积、高吞吐、可靠重试等特性。

分布式缓存须具备数据持久化、高性能、高速内存读写等特性。

API 网关能够实现完整API 托管的服务，用于协助开发者轻松完成API 的创建、维护、发布、监控等整个生命周期的管理。

2.2 (IaaS)基础设施层

2.2.1 计算资源池需求

资源池是整个云平台的基础，通过虚拟化软件、云管理平台对底层硬件和软件基础设施进行合理的组织和抽象，对外呈现统一的资源表现形式。云计算资源池包括计算资源池、存储资源池，能够满足采购人各系统对计算资源、存储资源的需求。

为实现资源的弹性伸缩和按需分配，有效降低单位资源成本，需要新购一批高性能服务器、存储设备。

▲根据应用需求，数据域云计算资源池 CPU 物理数量不少于 10 个，物理核数不少于 160 核，物理内存不低于 5120GB，云平台使用的分布式存储可用容量不低于 198TB,计算资源池由标准 X86 服务器设备组成。前置区云计算资源池 CPU 物理数量不少于 40 个，物理核数不少于 640 核，物理内存不低于 20480GB，云平台使用的分布式存储可用容量不低于 48TB，计算资源池由标准 X86 服务器设备组成。

2.2.2 存储资源池需求

分布式云存储系统，是将数据分散存储在多台独立的设备上。分布式存储系统采用可扩展的系统结构，利用多台存储服务器分担存储负荷，利用位置服务器定位存储信息，提高系统的可靠性、可用性和存取效率、扩展性。根据不同的数据类型，分布式存储包括分布式块存储、文件存储、对象存储。

▲需支持新增不低于 198T 分布式块存储,用于云平台建设;新增不低于 120T 对象存储，用于存储音频；新增不低于 240T 文件存储，用于存储图片。

本项目需充分利旧服务器资源全面整合迁移原有大数据平台（前置区）建成的云文件中心。构建高速分布式存储网络上的新文件存储中心，将前置区大量不同类型的存储设备通过应用软件集合起来协同工作,形成一个安全的数据存储和访问的系统，适用于各单位的数据资料存储、备份、归档等一系列需求。实现对所有非结构化数据（包含文件、图片、音频、视频等）进行文件上传、下载等。

需基于利旧服务器资源，建设云文件中心，支撑大数据智能化项目各类服务以及应用对文件的应用需求。

2.3 (PaaS)平台服务层

2.3.1 资源服务需求

支持离线计算、流式计算、实时计算、图计算和内存计算等计算组件，分布式文件存储系统、分布式关系型数据库系统、内存数据库、全文数据库、图数据库、实时多维分析数据库、时序数据库、对象存储等存储组件。

支持分布式消息、分布式缓存、API 网关、服务目录、分布式数据库中间件等应用支撑服务。

2.3.2 大数据资源池需求

本项目在汇聚本地公安业务主数据基础上，扩展汇聚各类新增数据资源，对数据域大数据平台数据融合集群进行扩容规划。

2.4 IDC 机柜租赁需求

- 本项目机柜租赁需求

需租赁满足本项目的不少于 25 个（包括所有新上设备）4400W 标准 47U 机柜，建设期加终验后一年内均需要租用设备，费用以 20A 满负荷计算。

- 市局机房设备搬迁机柜租赁需求

为采购人二楼机房边界等设备实施搬迁到大数据机房租用机柜，需租用 8 个 4400W 标准 47U 机柜 15 个月，共需 120 个柜月，费用以 13A 计算。

- 机房基础设施需求

符合《信息安全技术 信息系统物理安全技术要求》GBT21052-2007 第三级物理安全技术要求，并具备等保 2.0 标准下的机房基础设施平台系统第三级备案证明文件（建设时提供该证明文件）。

机房应满足公安信息网信息安全管理要求及接入标准，并具备接入公安信息

网所需专网万兆链路。机房所在大楼应具备两路独立的一级市电，即两路市电都是从独立的变电站输送，供电线路上配备稳压器和过电压防护设备，保证机房供电电源质量符合相关规定要求。机房内 UPS 不间断供电系统应设置为 N+1 或 2N 架构，为机房内信息设备供应备用电力，保障信息设备在公用电网供电中断情况下，关键业务服务的持续性。机房后备电源应具备三台或以上的发电机，专门用于保障供电，与主要供油单位应具备紧急供油协议或备忘录，以便在恶劣天气时能及时补充燃油，为油机提供稳定的燃料。

2.5 非功能性需求

2.5.1 计算和存储架构需求

2.5.1.1 可靠性

在云计算、云存储、云数据库、大数据中，任一集群都要保证集群中的任意两台服务器故障时，不能导致数据丢失。对于网络设备，任一设备或线路故障，不能影响系统正常运行。

2.5.1.2 稳定性

要采用成熟稳定的基础设施，整个基础设施每年出现问题导致应用中断的次数要少于 2 次，确保业务的连续稳定性。

2.5.1.3 先进性

采用先进合理的基础设施，以满足不断变化的业务需求，支持组件的热升级。

2.5.1.4 扩展性

任何基础设施都可以根据需求不断在线扩展，以满足不断增长的业务需求。

2.5.1.5 开放性

要保证任何硬件设备都有3家以上主流厂商的硬件符合需求，IAAS和PAAS层软件均符合上级单位标准要求，每层的软件均可独立进行升级，且不影响上层应用和服务的正常运行。云数据库要兼容MYSQL、ORACLE语法规则。

2.5.2 标准规范需求

基础设施建设需符合国家、上级单位的规范要求，包括但不限于：

GB/T 37722-2019 信息技术 大数据 存储与处理系统功能要求

GB/T 38675-2020 信息技术 大数据 计算系统通用要求

GB/T 38676-2020 信息技术 大数据 存储与处理系统功能测试要求

GA/DSJ 111 — GA/DSJ 124 《公安大数据规范性技术文件》

第3章 数据资源需求

大数据建设应用的核心是大数据处理，需面对海量的数据，且数据多头多源、规模大、类型多、质量参差不齐。为确保数据处理治理的稳定高效实施，大数据处理工作除遵循公安大数据处理技术标准规范外，还需按照本地资源情况以及业务需求，采用成熟先进的自动化、智能化工具开展数据采集、接入、处理、治理、组织等，以及开展数据摸底、标准化映射梳理、数据关联规则分析、质量监测分析和数据全生命周期运营运维等工作，才能保障数据精细化融合关联、增值增效，贴合业务单位实战业务，让数据好用、易用。本项目要求在合同签订后7个月内完成存量和持续接入数据的大数据处理，避免项目拖延造成资金浪费。

大数据智能化建设将大数据平台划分为前置区和数据域，数据资源的采集汇聚由各业务部门梳理本单位需求后提交大数据管理职能单位，由大数据管理职能单位汇总全局需求后将采集任务分发给责任单位，由各责任单位完成数据采集和向大数据平台汇聚。部分数据汇聚到大数据平台（前置区），在前置区标准化后

形成原始库，并将原始库数据向数据域汇聚；部分数据直接汇聚到数据域，在数据域标准化后与前置区汇聚的数据进行全局的大数据处理。数据域接入的数据资源可分为实时数据和历史数据，实时数据接入数据域后实时进行处理，历史数据以离线文件方式接入数据域，再进行离线处理。大数据处理以知识库的知识数据和规则方法等为支撑，对来源数据进行逐级提炼和分层存储，生成原始库、资源库、主题库和业务库。

3.1 数据采集汇聚需求

数据采集汇聚主要完成两方面任务，一是建立与各数据提供单位的联动平台（即数据采集管理平台），以便全面收集各单位数据采集和购买需求，并向有关单位下发数据采集任务和计划，监督采集任务的执行情况，修改补充错漏数据，将各单位采集的数据汇聚到大数据平台（前置区）；二是数据接入平台负责将各类数据资源在数据域进一步持续汇聚。同时要建立完整的数据采集和接入工具，保障数据质量及接入流程的全过程管理。

3.1.1 新建数据采集管理平台

为提升大数据采集汇聚工作的规范化管理水平、辅助管理监督各单位数据采集任务、进展、质量、成效等工作，建设数据采集管理平台，实现采集需求申请、审核、采集任务分发、签收、采集计划审核、采集进展监督、存疑数据核查补正、数据质量评估的闭环管理。

数据采集管理平台要求包括数据采集工作台、采集管理、数据汇聚管理、共享管理，并提供数据采集移动 APP 应用，满足数据采集、管理、监控、核查、补正的需要，具体功能需求如下：

3.1.1.1 工作台

针对每个用户提供工作作业台，要求可直观查阅采集、汇聚、质量等统计信息和所负责的采集汇聚任务进展。

1、统计分析

平台可自定义配置在工作台首页需展示的统计分析内容，主要包括：采集任务、采集进展、数据共享统计、数据质量统计、采集任务完成情况排名和采集概览等功能。

2、任务统一管理

提供任务统一管理，自动获取展示登录用户所负责的采集任务、整改任务、需求审核等，提供任务快速签收、需求快速审核的入口。

提供待办管理，包含待办签收、待办审核，方便用户操作。

3、采集成效发布管理

通过调用大数据平台（前置区）、数据域大数据平台开放的数据质量报告和服务开放统计接口，联动展示大数据平台（前置区）、数据域大数据平台的数据采集质量报告和服务资源使用情况。

3.1.1.2 采集管理

针对采集工作需要，提供数据采集管理，包括采集需求管理、采集任务管理和采集计划管理。

1、采集需求管理

各单位提出的数据采集需求和数据购买需求，系统自动记录采集需求的操作日志信息，包含各需求的责任人、责任机构、提出时间等信息。大数据管理职能单位汇聚整理合并各单位提出的采集需求。

2、采集任务管理

大数据管理职能单位根据汇聚的采集需求，创建采集任务，下发给责任单位，由责任单位签收，并确定责任人，并对任务进展进行跟踪反馈管理。系统自动记录采集任务操作日志信息，包含责任人、责任机构、签收人、签收时间、反馈时间等信息。

各责任单位可根据实际情况创建子任务，下发给下级单位执行。

3、采集计划管理

各责任单位在接到采集任务后，要制定采集计划，提供给大数据管理职能单位和采集需求提出方审核，采集计划通过审核后，在前置区信息服务资源平台和数据域大数据平台按照采集计划开展数据接入治理工作。采集计划包含任务详

情、任务要求时间限制、数据更新频率、采集计划描述和文件上传功能。

采集计划包含：采集计划描述、审核意见、负责人、负责人电话、联系人、联系人电话、预计开始时间、预计结束时间、任务频率、空间范围、数据提供方式、数据所属网域等内容。

4、采集任务监督

采集任务监督包含采集任务情况、任务进展情况、数据质量评估情况。

3.1.1.3 跨网汇聚管理

在有边界的情况下，跨网数据汇聚，可以选择跨网数据汇聚边界设备，并选择交换方式。各数据采集单位提出跨网汇聚申请，大数据中心审批、分配跨网边界设备。

3.1.1.4 共享管理

其他政府部门需共享公安数据时，由各业务单位审批，审批后方可共享，审批后形成共享任务，再由大数据平台具体执行。针对与政府部门间的数据共享，提供数据共享管理，主要包括共享需求管理、共享任务管理，提供数据共享的统计报表，并支持报表数据项的配置、支持报表导出 excel 文件。

3.1.1.5 监管管理

3.1.1.5.1 对账管理

1、提供方对账单管理

各业务单位数据汇聚方案制定审核通过后，在汇聚实施过程中，按照对账方式对提供方对账单进行维护，提供方对账单包括账单编号、数据条数、数据大小、数据起始编号、数据结尾编号、数据来源存储位置、上次失败账单号（异常重发的需提交上次账单号）、数据提供方管理员及联系电话、数据来源名称、数据来源类型（数据包、文件、数据库）。支持通过 excel 文件导入方式进行维护。

对账单提交后由接入方进行对账，若数据汇聚任务由下级单位负责，下级单

位提交对账单后由业务单位负责对账；业务单位统一负责本单位的对账单管理，由大数据管理职能单位进行对账。

2、接入方对账单管理

接入方在数据入库后，对接入方对账单进行维护，接入方对账单包括账单编号、数据条数、数据大小、数据起始编号、数据结尾编号、数据来源存储位置、上次失败账单号（异常重发的需提交上次账单号）、数据接入方管理员及联系电话、接入时间、数据来源名称、数据来源类型（数据包、文件、数据库）。支持通过 excel 文件导入方式进行维护。

3、对账管理

接入方根据提供方对账单和接入方对账单进行对账，系统支持自动对账和手工对账，对账完成后形成对账报告，并将对账结果反馈给数据提供方。其中自动对账指业务警种向大数据平台汇聚数据后，由大数据平台完成对账。

3.1.1.5.2 质量监控管理

1、质量评估规则管理

大数据管理职能单位收集审核各业务单位的数据采集需求后，形成采集规划，同时对各类数据资源的采集汇聚和接入的质量评估规则进行管理，采集质量规则下发给数据采集权责警种，接入质量评估规则同步到大数据平台，由大数据平台完成接入质量监测。

➢数据采集汇聚质量评估规则

主要包括数据有效性、及时性、完整性，如关键字段非空、字段值不合规、汇聚超时等。

➢数据接入质量评估规则

主要包括资源目录注册内容是否准确、字段是否空值、关联是否失效、更新是否异常、数据元及数据项是否符合部标等。

2、质量报告管理

业务单位根据质量评估规则负责监测数据采集汇聚的质量，并维护质量报告，主要包括是否漏数据、是否更新不及时、是否关键字段空缺等问题。若数据采集汇聚由下级单位负责，可将质量报告下发给具体负责单元，负责对质量结果

进行反馈或数据质量整改。

数据接入大数据平台后，由大数据平台根据质量评估规则自动完成数据质量监测、质量报告生成，质量报告同步到数据采集管理平台，大数据管理职能单位用户可在该模块中查询质量报告，并对质量报告进行核实。质量监管结果不达标的可将接入质量报告发送给权责业务单位，由权责业务单位反馈或质量整改。

3、统计报表管理

系统自动形成数据质量统计报表，主要包括字段空值报表、字段合规报表、数据及时性报表：

➢字段空值报表

主要包括数据来源、来源单位名称、资源总数(类)、核心字段总数(个)、平均空值率（本月空值率、上月同比）、本月排名、上月排名等。支持对报表字段进行配置，系统自动根据配置生成对应报表。支持查看报表明细，包括资源名称、数据项英文名、数据项名称、数据总量(条)、空值数据量(条)、空值率、整表字段平均空值率等。

➢字段合规报表

主要包括数据来源、来源单位名称、资源总数(类)、核心字段总数(个)、平均不合格率（本月不合格率、上月同比）、本月排名、上月排名等。支持对报表字段进行配置，系统自动根据配置生成对应报表。支持查看报表明细，包括资源名称、数据项英文名、数据项名称、数据总量(条)、检验规则、不合规数据量(条)、不合规率、整表字段平均不合规率等。

➢数据及时性报表

主要包括数据来源、来源单位名称、抽样条数、时效（最小差值、最大差值、平均差值、累计超时率）等。支持对报表字段进行配置，系统自动根据配置生成对应报表。

3.1.1.5.3 考核管理

根据采集数据的种类、数量、质量等维度，和业务单位、资源情况等维度，建立科学的考评体系，灵活配置针对每个业务单位设置考核的指标和得分项，并根据管理的需要进行动态更新。

1、考核项目定义

考核项目是能得分的项目，可以包括采集资源的门类、数量、质量分等维度进行定义。通过一定的公式和模型，赋予每个单位周期内的考核得分。

2、考核指标设置

考核指标是指得分的标准，每个单位的指标线是可以根据实际情况进行调整，考核项目得分和考核指标对比得到最后的得分。

3、考评排名

根据得分情况对各级采集单位进行排名。

3.1.1.5.4 通报管理

1、监管结果通报

该模块向大数据管理职能单位用户提供数据对账、质量、考核等监管结果通报管理功能。

用户可查询对账报告、质量报告、质量统计报表、考核结果等监管结果，选择需通报的内容、通报对象、通报方式等，通过二级审核后进行通报。通报方式包括采集管理平台内部通报、资源运营服务平台通报等。支持设置通报反馈时限、整改时限设置等，通报对象需按时进行反馈、整改。

2、问题反馈

通报结果发送到通报对象用户后，用户可对通报的监管结果进行反馈，支持多用户意见反馈、抄送、转发、回复等操作。支持大数据管理职能单位用户根据反馈意见撤销通报结果。

3.1.1.5.5 督导管理

根据监管结果通报，大数据管理职能单位用户可对权责业务单位发起督导，跟踪整改情况。支持关联整改前后的质量报告、考核结果进行对比；支持对权责业务单位进行预警或重复督导。权责业务单位根据采集汇聚任务，对下级单位或具体责任人进行督导。

3.1.1.5.6 资源熔断管理

1、资源使用情况查询

系统通过对接数据资源目录、服务目录等，提供用户目前使用的数据资源情况、服务情况等。业务单位用户只可查询本单位使用资源情况。大数据管理职能单位用户可关联查询各业务单位通报结果、考核结果、督导历史等情况，支持根据情况对各业务单位资源使用进行熔断。

2、熔断管理

大数据管理职能单位用户选择业务单位目前使用的一类或多类资源，进行熔断，经过二级审核后，限制业务单位资源的使用。支持限制使用时限的管理。资源熔断后系统自动提醒业务单位用户。

3.1.1.6 APP 端

提供数据采集管理平台的移动 APP 端，支持如下功能：

支持各单位的数据采集任务负责人及各级领导进行数据采集任务管理与监督，主要包括采集需求管理、任务管理、采集概览、采集统计、存疑数据核查、存疑数据补正等工作台上的功能，可以在移动 APP 端实现。移动 APP 端运行在公安移动信息网。

3.1.1.7 系统对接

数据采集管理平台需要与资源运营服务平台、大数据平台（前置区）、数据接入平台等系统对接。

3.1.2 升级改造数据接入平台

3.1.2.1 业务需求

大数据平台一期已建设了数据接入平台，初步实现数据接入数据域大数据平

台的探查、定义、读取功能，但随着本项目数据采集汇聚源头增多，大数据平台面临着数据接入源增多、数据接入质量不一和接入一致性、完整性、及时性无法保障等问题。为解决以上问题，需对数据接入平台进行功能升级：

一是数据对账，大数据平台从各部门业务系统接入源头数据时，大数据平台与业务系统进行对账，保障数据准确、无误地接入；同时数据接入大数据平台后会根据业务需求分发到资源库、主题库或业务库，对账应能保障数据分发的准确性，各部门利用数据接入平台将数据接入构建本部门业务库时，也可进行对账。

二是数据接入质量检核，能够动态配置接入数据的质量检核规则，实现对数据的质量评估，包括对源头数据的属性、值域或格式等，以及对数据接入后入库的完整性和及时性进行检核。源头数据质量出现问题将在资源运营服务平台进行质量通报，并根据情况暂停接入该源头数据。

3.1.2.2 功能需求

新增数据对账和数据接入质量检测功能，需符合 GA/DSJ 213 和 GA/DSJ 232 等要求。数据接入处理主要能力详见附录“数据接入处理能力要求”部分。

分类	功能项	功能需求描述
数据对账	数据接入对账	提供数据接入过程中的即时对账功能，包括提供方对账单信息和接入方对账单信息，对账单应包括数据接入方数据资源、接入方数据条数、提供方数据资源、提供方数据条数等。
	数据接入后盘点对账	提供数据包和数据库数据接入后盘点对账功能，支持双边盘点对账和单边盘点对账。 1、单边盘点对账，由系统生成一方对账单，由用户根据模板录入对账单数据后导入系统进行对账。 2、双边盘点对账，由系统进行提供方和接入方双边盘点，支持配置不同盘点对账策略，应包括即时全量统计、即时时间段内统计、即时间隔统计、定时全量统计和定时间隔统计等。
	数据分发对账	提供数据分发对账功能，支持 1 对 1 分发数据对账、1 对多分发数据对账和分发盘点对账。
	账单策略配置	提供账单策略配置功能，支持增删改查、导出、启停等，账单策略应包括对账方法、对账调度类型（即时对账和定时对账）、对账角色、开始时间、频率值等，支持接入过程中的即时对账和接入后的盘点对账（包括双边盘点和单边盘点），支持配置 1 个或多个需对账的数据资源。

	对账单	提供数据提供方、数据接入方、数据提供方盘点、数据接入方盘点等对账单查询、销账、导出功能。并对对账结果进行统计分析，包括数据接入方资源信息、接入方数据条数、提供方资源信息、提供方数据条数、数据量差异、对账方法、对账时间、对账结果、状态等信息。支持对账异常告警。
	对账服务	提供根据 GA/DSJ 213 的规范要求制定对账服务。对账服务接口主要包括对账分析服务、异常告警服务、对账单信息查询服务、对账单统计信息查询服务、异常数据查询服务接口，为数据服务提供支持。
	对账报告	通过柱状图、趋势图、饼图等方式可视化展示数据对账结果，包括对账频率统计、对账失败统计、对账时间统计等维度的统计结果。支持查看数据对账报告详情。
数据接入质量检测	质量检核管理	通过作业调度的方式对数据接入质量检核任务进行管理和调度，提供任务下发、启用、停用等功能。支持对探查的资源进行清单式管理，包括查看探查报告、修改、数据导入、删除等；支持对质量规则进行增删改查以及启用/停用；支持配置管理测评方案，配置需进行质量检测的资源指标，支持增删改查以及启用/停用。
	数据探查检核	1、支持属性完整性检核，检核质量情况应包括数据总量、字段编码、字段名、空值数量、空值率等，保障数据的内容完整满足业务要求。 2、支持值域和格式有效性检核，检核质量情况应包括数据总量、字段编码、字段名、异常数量、异常率等，保障数据的精确性和可靠性。 3、支持业务探查，业务探查目的是获取数据来源单位、所属应用系统、业务含义描述、数据删除方式、安全性要求、安全等级、以及主外键名称、表关联关系等内容。 4、支持接入方式探查，通过对来源表的存储位置、提供方式等维度进行探查，为数据定义提供依据。 5、支持数据集探查，主要针对来源数据集表名、引用数据元情况，探查数据集是否是标准数据集。探查数据总量、增量及更新情况，为数据接入、处理和组织提供依据，包括数据集标准探查及数据集规模探查。 6、支持问题数据探查，探查字段中不符合规范的数据，给后续数据清洗规则的制定提供依据。探查问题分类一般包括代码字典表问题、数据类型问题、数据值逻辑问题、归一化原则问题、数据格式问题、必填项为空等。对每次探查结果记录并形成报告。
	数据读取检核	1、支持记录完整性检核，检核质量情况应包括数据

		总量、业务时延、处理时延、读取时延、推送时延等，保障数据的内容完整及满足业务要求。 2、支持及时性检核，检核质量情况应包括源库数据量、接收数据量、差异率等，保障数据的及时录入和更新。 3、支持数据解压，支持对使用常见压缩算法的数据进行解压，支持包括 RAR、ZIP、GZIP、LZ4 等常见的压缩格式。 4、支持生成作用于数据全生命周期、全局唯一的主记录 ID 和附件记录 ID（如果存在附件），并建立主记录和附件记录的关联。不同数据组织中，记录 ID 的生成方法不同。 5、支持字符集转换工作，将读取的数据转换成符合数据处理要求的格式，包括半结构化数据转换及字符集转换。
数据定义	数据接入定义	支持数据接入定义，主要是根据数据源探查结果，定义源数据从源系统中的读取策略。 不同的读取方式（数据库、文件、接口、消息总线等），其读取策略的描述不同。要求至少应包含数据资源描述、数据源访问描述、数据读取策略描述、数据解压策略描述、数据解密策略描述等内容。
	数据治理定义	支持元数据定义，根据数据探查中业务探查和字段探查的结果，建立源数据中原始字段项与标准数据元的映射关系以及原始字典代码集与规范化字典代码集的映射关系。 支持数据目录注册定义，将数据接入后数据经过数据组织标准化后，将数据资源注册到数据资源目录。 支持按照 GA/DSJ 231 和 GA/DSJ 230 等规范的要求，定义数据集、数据项、数据项关系敏感度分类，定义数据记录敏感级别的标注规则。 支持数据血缘定义，要定义来源数据、原始库、资源库、主题库、知识库、业务库等各层数据资源、数据项间的继承关系。 支持数据质量核查定义，能够定义数据资源全生命周期的质量核检、实时质量分析、数据质量报告等相关策略。 支持定义数据接入、处理、组织和服务等各项任务的运维监测、记录、输出等相关策略。
	数据处理定义	支持按照业务需求，定义从来源数据提取所需数据的策略。来源数据包括原始来源数据、原始库、资源库、主题库和业务库。应支持数据提取策略定义的内容包括两个方面，一是结构化/半结构化数据提取策略的定义，二是非结构化数据提取策略的定义。 支持数据清洗策略定义，按照数据格式定义要求及业

		务需求，定义数据的清洗策略，以生成满足标准及质量要求的数据。数据清洗策略定义的内容包括数据格转策略定义、数据过滤策略定义、数据去重策略定义。 支持按照业务需求，定义数据的关联策略，为后续的关联回填、关联提取提供策略支撑。 支持按照业务需求，定义数据的比对策略，明确比对源与比对目标之间的比对条件。 支持按照业务需求，定义数据的标识策略，明确数据标识时所使用的标签规则。 支持根据不同应用场景下的数据分发需求，定义数据的分发策略。
	数据组织定义	支持根据数据产生原始库、资源库、主题库、知识库、业务库的数据敏感度、数据规模（存量、增量）、数据预期使用规划、数据性质等因素，确定数据存储分区管理、数据加密、数据库技术、索引建立、数据备份等策略。

3.1.2.3 非功能性需求

1、性能指标

用户并发访问：≥300。

简单事务处理（如各类信息录入、修改、查询业务、主要页面等）平均响应时间：≤2s。

交互式研判工具平均响应时间：≤5s。

复杂查询或统计平均响应时间：≤10s。

2、可操作性

界面操作简捷、布局合理、提示及时，对于层次结构数据尽量使用树形结构，便于定位选取，展示数据的有效工作区最大化。

3、兼容性（详见附件数据接入处理能力要求）

支持 Oracle、MySQL、KDB、SQL Server、PostgreSQL、Greenplum、Hive、HBASE、Libra、TBase、TDSQL、TBDS、GBASE、MPP、Kafka、Elasticsearch、FTP 等主要数据库读取，支持 WORD、EXCEL、WPS 等文本文件内容和关键字提取。

3.1.3 扩大数据汇聚需求

在大数据平台一期基础上，继续扩展汇聚大数据平台（前置区）的数据资源，加大本地特色数据汇聚，满足日增量37亿条汇聚能力，力争在实战急需数据采集难等问题上实现重大突破。

3.1.3.1 本地专业侦查办案数据汇聚

在大数据平台一期项目基础上，继续开展专业侦查办案数据汇聚，并展开数据融合。

3.1.3.2 新增汇聚视频云数据

目前大数据平台（前置区）已汇聚了部分视频监控数据，此部分数据在大数据平台（前置区）存储90天，标准化后实时汇聚到数据域大数据平台。

大数据平台汇聚视频图像数据，开展聚类归档、精准落地，并与其他数据进行关联融合，组织形成原始库、资源库、主题库，丰富信息维度，通过融合服务为大数据平台上层应用、各业务单位的业务系统、视频平台等提供融合智能化服务支撑。

3.1.3.3 新增汇聚刑事技术类数据

通过本地刑事技术类数据采集汇聚，本项目需要开展采购人已采已汇、已采未汇以及上级下发刑事技术数据汇聚，包含各业务单位以条线采集类似数据等，开展全警数据融合治理，丰富对象信息。

3.1.3.4 新增汇聚出入境管理类数据

通过本地数据域大数据平台与上级大数据平台对接，服务调用方式使用上级单位出入境管理类等数据。

3.1.3.5 上级单位数据资源共享

争取上级单位大数据平台下发本区域数据，利用数据下载接口主动下载所需数据；不能下发的，应充分利用上级平台的数据服务接口，实现为我所用。

3.1.3.6 丰富地图数据资源

大数据平台一期已开展了大数据平台地图数据资源的汇聚工作，主要包括从PGIS系统汇聚存量的地理数据，如基础地理数据、公共地理数据和业务专用地理数据等，以及对接上级资源、数字珠海综合服务平台资源、国土资源、各业务单位采集地理数据、空间标准地址数据等地理数据。

本项目需要在已建的地图数据基础上，负责梳理我局基础数据图层和所有业务业务图层，通过对接我市已建地图资源及采购数据等方式，更新基础地图矢量数据、重点区域建筑物数据、卫星影像数据等。全市范围基础地图矢量数据为1：2000比例尺，重点区域比例尺根据需要调整增大，保证所有道路和建筑物都清晰可见，且需符合2000国家大地坐标系（CGCS2020）规定要求，数据内容包括各类信息点面、全市所有路网、行政区划、绿地、水系、建筑物等，路网数据可用于实现基础导航功能，并提供蓝白等多种配图风格。在更新的过程中需要保证数据的及时性和准确性，在项目建设和运营运维期内保持基础地图数据更新服务，保证合同有效期内做到同步更新，街道、道路(包括城中村、社区里面的道路)、建筑物等数据需做到每三个月内更新，其他类基础数据更新频率需要满足业务方的需要，对于数据需具备运营能力并解决所有地图数据互操作性。基础地图数据包括但不限于下表内容：

大类	图层别名	类型
水系	点状水系	点
	线状水系	线
	面状水系	面
	点状水系附属设施	点
	线状水系附属设施	线
	面状水系附属设施	面
	水系标注	标注
地貌	点状地貌	点
	线状地貌	线

	面状地貌	面
	地貌标注	标注
植被与土质	点状植被	点
	线状植被	线
	面状植被	面
	植被标注	标注
	植被辅助层	线
基础设施	卡口	点
	图像监控资源	点
通信保障	通信基站	点
	通信点	点
	通信线	线
单位信息	党政机关	点、面
	人民团体与民主党派	点、面
	社会福利机构	点、面
	基层群众自治组织	点、面
	公安机关	点、面
	企事业单位	点、面
	教育	点、面
	科研设计	点
	文化团体	点
	医疗卫生	点
	金融证券	点
	新闻广电与出版	点
	邮电通信物流	点
	危险品存放地单位	点
	重点控制单位	点、面
	企业	点
	行政机构（政府）	点、面
	其它单位	点
场所	公共活动场所	点、面
	交通场所	点、面
	娱乐场所	点、面
	商贸场所	点、面
	旅游场所	点、面
	体育场所	点、面
	文化场所	点、面
	居民服务场所	点
	宗教场所	点
	互联网上网服务营业场所	点
	住宿服务场所	点、面

	餐饮服务场所	点
	特殊行业服务场所	点、面
	其它场所（小区、社区）	点、面
交通	公交电汽车站	点
	公路	线
	城市道路	线
	公路控制点	点
	道路交叉口	点
	道路路段	线
	道路网	网

3.1.3.7 扩展汇聚其他数据

新增多种数据资源、进一步扩展汇聚大数据平台（前置区）数据，汇聚到前置区，由大数据平台（前置区）标准化处理治理后汇聚到数据域。数据汇聚情况详见附录“扩展汇聚其他数据”部分。

3.2 数据处理组织需求

数据一旦接入到数据接入平台后，系统将自动对接入的数据进行标准化处理和组织。要求数据处理、数据组织都必须采用标准化、成熟稳定的产品，实现“接入即处理”。

3.2.1 数据处理

数据处理是为数据资源融合建库，进行科学分类形成标准数据资源的必备的重要环节，按照数据接入环节的数据定义，针对规模巨大、类型多样、高速流转、复杂多变、质量参差不齐、价值密度高低不一的大数据特性，以数据应用为导向，通过规范化处理，提升数据价值密度，为数据智能应用实现数据增值、数据准备、数据抽象。数据处理平台需符合 GA/DSJ 220 的基础数据处理引擎以及音频处理提取引擎，详细内容参见附录“数据处理需求”。

3.2.2 数据组织

针对实战需求，围绕五要素等主题对象，融合各类数据资源，建设原始库、

资源库、主题库、业务库等核心库，通过数据的凝练和增值，满足各业务单位利用大数据平台核心库开展建模分析、挖掘，以及利用核心库数据和业务数据进一步融合构建各业务单位的业务库等场景。

针对大数据数据源多源异构的特点，在数据汇聚源头按照来源、类型、格式不同进行分类设计，实现多源异构数据的汇聚。通过各数据库之间逐级抽取，按需汇聚等渠道生成并逐步沉淀，形成对五要素，以及时间、空间、关联的全面刻画，对上层应用形成多维度的支撑。

原始库：从源头获取数据，按照统一的数据元、数据项、代码字典等标准进行标准化，包括格转、校验、去重、标识等。前置区和数据域分别建设原始库。

资源库：综合各类数据资源建立的关键要素（各种标识类属性，如公民身份号码、车牌号等）以及要素之间关联、关系的公共数据集合。

主题库：从资源库和原始库获取数据，按照面向对象的思想、数据仓库的方法进行主题库组织。主题库建设于数据域（视频云项目的主题库建设于前置区），需基于接入的数据源进行构建，新增数据源时应能满足将新增数据源的要素集合到已构建的主题库中；新增主题库时，需基于历史数据和实时数据进行构建。

业务库：从原始库、资源库、主题库获取业务领域数据，也可以是外部导入的数据，并将业务数据返回给数据源，面向一定的场景构建相关业务库。

知识库：一方面从整个数据资源中抽取有规律或可找到规律的数据，另一方面可由业务部门将业务经验总结成知识规则维护到知识库，支撑整个数据处理过程。知识库建设于数据域。

3.2.2.1 原始库

主要用于保留原始数据信息，包括各类数据资源，根据数据接入处理，保留原始数据信息，并在此基础上补充对各种来源数据进行一系列处理加工后产生的标准化数据项、代码项和基础标签、行为标签、业务标签和分级分类属性，能够反映原始业务场景的数据集合。

原始库并非是源头汇聚原始数据，而是同时包括原始数据字段和标准化字段。保留原始数据字段是尽可能还原原始场景，支持数据溯源和特定业务需要；标准化字段通过统一的标准来支撑不同数据的融合，以便将不同要素进行关联、

将实体对象进行抽象和聚拢。

需按照 GA/DSJ 240 要求建设原始库。

3.2.2.2 资源库

资源库是综合各类数据资源，建立关键要素以及要素之间的关联、关系的公共数据集合，要素及要素的行为、内容（言论）的时空分布，要求在数据处理过程，进行逐条记录的解析，并按照预置的规则，分发入库。资源库是公共数据，对各项业务工作都具有支撑作用，可以脱离任何业务而独立存在，也与每一项业务相关。

需按照 GA/DSJ 244、GA/DSJ 241 和其他上级的规范指引建设资源库，汇聚的各类数据资源其中包含的业务关键要素（在业务要素索引库定义）均需要构建资源库，同时需保证要素实体的唯一性，不同格式内容但同一实体数据应能归一到同一要素实体。资源库的建设需基于接入的数据源进行构建，新增数据源时应能满足将新增数据源的要素关联关系补充到已构建的资源库中，另一方面新增资源库时，需基于历史数据和实时数据进行构建。

1、要素关联库

要素关联库是从原始数据资源中进行两两关键要素的提取，如果提取的要素能够归属到同一主体的，则提取到要素关联库中。根据要关联的要素字段，按照设置的规则，与业务库、知识库以及其他相关的数据资源，进行关联。

需构建要素关联库，包含不限于车辆关键要素信息关联、通讯工具关键要素信息关联、身份关联扩展信息。

2、要素关系库

要素关系库从原始数据资源中进行两两关键要素的提取，如果提取的要素能够归属到不同主体，则提取到要素关系库中。需要记录关系的时空分布信息，包括建立关系的最早时间、最近时间、关系发生次数以及关系所发生的区域，区域的粒度至少要到市域行政区划。

3、要素重点行为库

要素重点行为库主要是存储各种要素在不同时空分布下的重点行为信息，并记录行为的类型、行为的最早发生时间、最近发生时间、发生的次数。以支撑已

知对象行为刻画、未知对象发现等业务工作。

4、要素重点内容库

要素重点内容库主要是存储各种要素在不同时空分布下所发布的重点内容，并对内容进行抽象归纳标识，需记录内容的类型、内容最早发布时间、最近发布时间和发布次数。

根据业务开展过程之中需要关注的内容，对不同要素在不同时空分布下所发表的文字、图片、音视频等信息，通过结合业务知识库或者关键样本对内容进行文本匹配或者特征匹配，并对匹配提取的内容和关键字进行标识并记录。

5、要素时空分布库

针对梳理定义的每个关键要素（包括关联要素、关系要素），一一构建要素分布库，记录关键要素最后出现地点、历史出现的区域及在哪个数据资源存在，支撑要素资源位置的快速定位、活动地分析等业务需求。要素时空分布库包括要素最后分布和要素分布变迁时序，要素最后分布主要是解决要素最后出现地的问题，要素分布变迁时序主要是解决要素历史曾经出现的区域问题。通过要素最后分布和要素分布变迁时序，能够用于支撑全国范围基于要素资源位置的快速定位问题以及支撑活动地分析等业务工作。

要素最后分布主要是用于记录各类关键要素最后的分布情况，包括最后出现的时间以及最后出现的区域，区域可以按照每个地方不同的关注粒度进行抽象，抽象粒度至少要到区县或镇街一级。

要素分布变迁时序主要是记录了要素的历史分布明细，是要素最后分布的历史明细表。记录了要素的历史连续活动区域。

⑴要素资源分布库

要素资源分布库记录要素在哪个数据资源中存在，是数据资源的总索引，以支撑要素值的快速定位使用。

⑵要素频次统计库

要素频次统计库是对要素的关联、关系、重点行为、重点内容、分布变迁进行每日出现次数的统计，从而体现要素的近期活跃情况，要素频度统计库包括要素关联频次统计库、要素关系频次统计库、要素重点行为频次统计库、要素重点内容频次统计库、要素分布变迁时序频次统计库和要素行为频次统计库。

要素关联库、要素关系库、要素重点行为库、要素重点内容库、要素分布变迁时序库中记录了首次和末次采集时间、总采集天数和次数，但无法体现要素在一段时间内详细的活跃程度，所以需要同时记录各库每天的统计次数信息，作为各库统计频次的明细表。

3.2.2.3 主题库

主题库是基于原始库、资源库，按对象主题重新组织数据，围绕人、地、案、事件、物、组织等主题工作对象，构建多种维度的公共数据。需按照 GA/DSJ 242 建设各类主题库等。

▲主题库建设需提供对象属性融合算法将对象要素关联关系数据集合到同一个主题对象上（需要有对象的唯一标识等），并保证对象的唯一性，指向同一实体，保证用户基于不同证件号码查询人员信息时，返回同一且唯一的对象信息。主题库的建设需基于接入的数据源进行构建，新增数据源时应能满足将新增数据源的要素集合到已构建的主题库中；另一方面新增主题库时，需基于历史数据和实时数据进行构建。本项目需建设人员主题、车辆主题、手机主题、案件主题、事件主题、场所主题、组织主题、地址主题等不少于 40 个主题库。

3.2.2.4 业务库

业务库是各专业领域业务的数据库，支撑各专业领域业务的数据，记录业务过程，并为各业务活动提供数据的支撑等。业务库的数据来源可以是按需获取原始库、资源库、主题库和知识库的数据，也可以是外部导入的数据。业务库可根据实际情况建设于前置区或数据域。按照数据组织的方式，业务库主要由各业务部门主导建立，可以分为业务生产库、业务资源库、业务专题库和业务知识库等。

1、业务生产库

业务生产库是存储与具体业务流程相关的数据，来源于业务人员使用业务系统的过程中所产生的数据，其中记录了业务人员进行业务开展与流程等业务活动相关的一切数据，包括业务办理过程中涉及的人员、案件、线索、时间、工作流转、审批等业务工作信息。

2、业务资源库

业务资源库是指在业务系统内的数据资源，来源于根据一定的业务规则从原始库、资源库、主题库提取或分发过来的数据，为业务的分析提供数据支持。业务系统也可以有另外的数据来源，比如通过业务系统的入口录入或导入或通过其他的第三方方式。

3、业务知识库

业务知识库是根据日常业务工作总结出的犯罪活动规律、人员行为特征、技战法等经验，通过人、地、物、事、行为、关系等一个或多个要素组合，描述专题业务特点及关系的知识，形成能够预测、掌握趋势的知识，它可以来源于知识库里的共享，也可以是在业务系统内进行分析挖掘所形成的领域内的知识。

4、业务专题库

业务专题库是针对某类特定的业务需求，以多维的、面向主题的方式进行数据组织，构成面向业务支持或决策分析支持的数据集。业务专题库的数据可以来源于原始库、资源库或主题库，根据具体业务场景在专题库中按照数据集市进行构建及呈现。其核心在于要满足特定用户群体或部门在查询、分析、挖掘等方面的特殊需要。

3.2.2.5 知识库

知识库指公共安全领域共享的知识数据和规则方法集合，包括数据接入、处理、治理、组织和服务需要的知识性数据，各种规则、方法、过程集合，以及公共安全领域各种通用模型需要的知识性数据、通用算法。主要包括：

1、基础知识库

针对行政区划、组织机构代码、号码信息、各类数据代码字典、同义词库等公共知识数据构建基础知识库。

2、基础算法库

针对各种基本算法、数值分析、加密算法、排序算法、检索算法、随机化算法、并行算法、分类算法、聚类算法、随机森林算法、图算法等构建基础算法库。

3、智能信息处理

针对文本自然语言处理、OCR、多媒体数据处理等过程所需要的规则、模型、

算法或知识性数据构建处理知识库，如本项目建设的音频库。

4、规则库

针对数据接入、处理、治理和组织、服务各个环节中提炼的规则方法构建规则库；数据运维过程中的监测、告警和处置规则；数据质量监测、告警管理规则；数据探查、读取和对账规则方法；数据处理各环节的规则方法等。

本项目需构建各类知识库。同时数据处理过程中的提取规则、清洗规则、关联关系规则等，以及标签管理平台创建的标签能够自动归集到知识库中，支持对知识库进行新增、删除、编辑、查询等操作。

3.2.3 大数据处理实施

大数据处理实施服务包括业务主数据治理、专业侦查办案数据标准化治理、视频云数据融合处理、地理数据融合实施等。

3.2.3.1 业务主数据治理

业务主数据是具有共享性的业务基础数据，可以在公安机关内部跨越各个业务单位被重复使用，处于相对高价值，高共享，相对稳定的状态。主数据具有以下特性：(1)特征唯一性：在不同的应用和系统中有高度的一致性；(2)识别唯一性：在公安机关内部，不分系统、部门都可以唯一识别出来；(3)长期有效性：长时间都是有效的数据，该业务对象贯穿于整个生命周期甚至更长,需要长期保存；(4)业务稳定性：一旦录入系统中就很少改动，数据质量要求高。公安主数据不归属某一特定的部门而归属整个公安机关，是采购人的核心数据资产。

对应于五要素实体模型，采购人目前存在的主数据主要包括：(1)人员类：户籍人口、居住证人口等；(2)事件类：110 警情、刑事案件等；(3)物品类：机动车、危险品等；(4)地址类：街路巷、门楼牌等；(5)组织类：治安管理单位、行业场所等。

上述业务主数据是资源库、主题库、知识库的重要数据来源，需要进行全量、标准化、高质量的数据处理治理，符合 GA/DSJ 232 的要求。

3.2.3.2 数据标准化治理

数据标准化是数据融合的前提，汇聚到大数据平台的各类数据资源需按照统一的数据标准进行治理，形成高质量、高价值的公安数据资源，本项目统筹和整合前置区、数据域所有数据资源进行标准化工作，主要包括：

1、字典对标

以现有上级制发标准及相关行业标准的数据字典为基础，分析专业侦查办案数据资源的数据字典的实际意义，将相同意义的数据字典进行汇聚和融合，达到字典码和字典值的一一对应。

2、数据项集对标

按照上级数据标准化要求进行数据资源的标准数据项集对标。

3、字段对标

按照上级数据标准化要求对原始数据表的字段进行数据元和限定词对标。

4、字段值标准化

基于字段对标结果，按照 GA/DSJ 220，根据数据元的值域对原始数据表字段值进行标准化，包括重复数据合并或清除、非标数据转换成标准格式、数据完整性和一致性校验等。

5、数据表和字段命名标准化

按照 GA/DSJ 230，对数据资源表名称进行标准化。

6、数据编目

按照 GA/DSJ 230，对数据资源进行梳理，并赋予唯一的目录标识符和编码，完成数据资源信息数据项和数据资源数据信息数据项的编目，并注册到数据资源目录。

7、数据分级分类

按照 GA/DSJ 231，完成数据内容的敏感程度或数据开放范围的分级维护，对数据获取方式、数据资源种类、字段等的分类维护，确保数据的安全使用。

8、数据血缘分析

建立数据产生、加工融合、流转流通到最终消亡等过程中形成的转换关系集合，并对映射关系进行管理，监控数据资源数据流向和变更影响分析。

9、数据质量评估

从数据及时性、有效性、完整性等方面分类制定数据质量评估规则，实时对资源进行多维度的质量探查监测，并定期输出详细的数据质量报告，将报告及时反馈给数据提供方、数据处理和数据使用方的相关部门及人员。

10、标准管理

在公安行业标准基础上维护本地标准，包括元数据、数据元、限定词、字典代码、数据集、同义词等。

11、资源目录管理

对本地数据资源目录进行管理，保证数据资源可读性，包括数据资源的注册、维护以及与省级目录接收及上传等对接工作。

3.2.3.3 前置区数据融合处理

数据融合处理是按照数据接入环节的数据定义，对数据资源开展规范化处理，为数据组织和数据服务提供支撑，主要包括提取、清洗、关联、比对、标识、分发等环节，同时对日志信息、问题库数据进行分析和整理，支撑数据运维及质量控制、评估。

针对各类重点数据资源进行数据融合处理，主要包括数据提取、清洗、关联、比对、标识和分发等实施工作。详细处理过程参见附录“前置区数据融合处理”部分。

3.2.3.4 地理数据融合实施

针对本项目汇聚的地理数据，开展数据融合处理：将接入的本地业务数据与PGIS、政务网地图、互联网地图等地理数据融合匹配，形成专题图层资源，并依托大数据平台，为采购人提供基础地图服务。包括警用业务地理信息融合处理、标准地址空间资源融合处理、警用基础地理信息融合处理、警用公共地理信息融合处理、时空轨迹数据融合处理、二维与三维地理数据融合处理。

3.2.3.5 标签平台

按照“人、地、事、物、组织”等核心要素，规划数据标签体系建设，从基本

属性、行为、关系等多个维度对核心要素进行刻画，设计数据标签的特征计算规则，形成体系化、动态、可扩展的标签体系。标签平台、标签服务升级或者具体标签的变更、下线等行为不影响上层应用的正常使用。

3.2.3.5.1 标签生产

针对不同层级、不同业务单位用户需求，提供多种标签生产模式，实现全方位、多维度的标签生产系统。

分类	功能项	功能描述
标签生产	经验规则打标	提供人工打标服务接口，把业务专家实战经验转换成标签规则，落地业务标签。
	智能建模打标	提供可视化标签建模工具，支持拖拉拽方式建立模型标签，为数据自动打标。
	外部标签融合	提供标签生产 API 接口，支持标签导入、导出和融合，在不触及外部数据基础上，实现外部标签的导入和融合。外部标签在导入和融合的过程中支持对标签增加来源标识，比如行业标签、上级标签等等。
	标签分类	提供基础标签、行为标签、敏感度标签、公共字段标签、业务标签等标签分类，实现全方位、多维度标签体系库构建。

3.2.3.5.2 标签管理

针对不同层级、不同业务单位用户，提供个人用户标签管理，实现各业务单位标签服务全生命周期管理。实现标签的查询、申请、订阅、发布维护、删除、审核和调度管理的全流程配置化支撑，支持用户快速配置标签、更新标签；通过标签归属对应不同的标签审核流程，标签新建并提交发布后开始进行审核，审核通过后标签发布生效。

分类	功能项	功能描述
标签管理	标签查询	提供用户查询标签体系功能，为标签申请、订阅提供基础。
	标签归属	标签生产过程中可以对标签分成个人、部门、共享三类标签归属，个人标签个人可见，部门标签部门可见，共享标签所有人可见。
	标签审核	通过标签归属对应不同的标签审核流程，标签新建并提交发布后开始进行审核，审核通过后标签发布生

分类	功能项	功能描述
		效。
	标签发布管理	提供标签测试、发布、下线等管理功能，支持 Rest Api 等标准服务。
	基础标签管理	提供用户对基础标签信息进行注册、启用、停用等，实现自动获取标签知识库中的标签类型，支持通过列表形式选择所使用的标签。
	行为标签管理	提供用户对行为标签信息进行注册、启用、停用等。
	敏感度标签管理	提供用户对敏感度标签信息进行注册、启用、停用等。
	公共字段标签管理	提供用户对公共字段标签信息进行注册、启用、停用等，标签类型包括区域标签、空间位置标签等。 实现自动获取标签知识库中的公共字段标签类型，支持通过列表形式选择所使用的标签。
	业务标签管理	提供用户对业务标签信息进行注册、启用、停用等； 实现自动获取标签知识库中的业务标签类型，支持通过列表形式选择所使用的标签。

3.2.3.5.3 标签监测

提供标签平台的统计报表、日志审计和标签评估等监测分析功能：

分类	功能项	功能描述
标签监测	标签统计报表	提供各层级、各类别标签被查询、被申请、被订阅、被请求等统计报表，包括日统计量、周统计量、月统计量等。
	标签日志审计	提供标签新增、修改、变更、下线等操作日志的审计。
	标签评估	提供标签质量评估功能，支持标签按数量、人工、请求量、业务应用量等维度进行评价，推动高质量标签进行全警全域推广、低频低质标签及时更新升级。

3.2.3.5.4 标签应用

针对各业务单位的业务应用需求，提供多种类型的标签应用服务能力：

分类	功能项	功能描述
标签应用	标签检索	提供基于业务标签特征的检索功能。
	标签画像	提供五要素等对象进行标签多维度可视化展示功能。
	标签圈人	提供以人员静动态标签特征为检索条件，逐步精确定位目标人员，支持单个或多个标签组合的方式圈人。

3.2.3.5.5 标签服务化

具备以具体对象、标签等为要素的各种查询检索、比对、研判的服务，支持标签导入、导出和融合，在不触及外部敏感数据基础上，实现外部标签的导入和融合。外部标签在导入和融合的过程中支持对标签增加来源标识，比如行业标签、上级标签等。以上服务应接入服务平台统一编目、治理使用。可以通过视频专网共享本项目的标签服务。

3.2.3.5.6 开展数据的标签化治理

▲开展符合统一规范的标签定制服务，不少于1000项标签生产；完成存量和持续接入数据的标签化治理。

3.2.4 数据运维管理

数据运维管理是指通过采集、接入、处理、治理数据流程中各项任务的状态信息，对异常状态进行预警和处理，实现对各任务的实时监控和管理。

3.2.4.1 运维状态监控

1、支持数据采集、接入、处理、治理各个环节的状态采集监测点配置。

2、来源数据通道监控：固定时间周期内发起来源数据通道联通状态检测，在连续时间周期（如3个时间周期）内联通状态检测失败，则认定来源数据通道状态异常。

3、数据接入、处理监控：运行状态是否正常，支持固定时间周期（如每5分钟），检测数据接入及处理服务是否正常。

4、数据入库监控：支持按数据来源、时间等不同查看每个实例的实例ID、开始时间、结束时间、耗时、速率、状态、输入数据条数、输出数据条数、失败数据条数等信息。

3.2.4.2 数据运维报表

1、支持数据资源报表：支持以天、周、月等不同的时间段要求，对数据组织的分类（原始库、资源库、主题库、知识库、业务库）、数据的来源、数据属性、字段分类、资源分类等多维度的统计分析，形成资源总数报表。

2、支持数据对账报表：支持通过关键信息，比如记录 ID、数据来源、数据种类、数据总量等维度，对数据对账环节进行监控记录，形成数据对账环节的完整性报表。

3、支持数据有值率报表：根据数据接入形成接入对账单，数据经由数据处理环节（主要是数据清洗）最终入库形成入库对账单，通过分析对比接入对账单和入库对账单，可按数据分类、时间等维度记录数据有值率，最终以多维度方式展示有值率报表。

3.2.4.3 预警管理

1、支持实时流数据异常监控：支持在不同实时流数据处理环节中，按照时间周期、数据断流等告警阈值规则的配置。比如时间周期设置 5 分钟等，即在最近 5 分钟内，没有数据流量产生则进行告警。

2、支持离线处理数据异常监控：数据质量或者离线处理任务执行失败，则告警。比如每天的数据离线处理任务中，当离线任务执行失败或者离线处理结束后，产出数据的数据质量监测发生异常，则进行告警。

3、支持运行状态异常监控：根据运行监控指标要求，若低于指定配置阈值则告警。比如对外服务接口中断，数据传输通道中断、数据库服务中断等，则告警异常。

4、支持数据质量异常监控：参考数据质量管理规范中的要求进行数据质量的告警展示。比如在身份证字段类型中，字段值明显不是身份证，则告警异常。

5、支持数据告警信息推送：按照预设告警规则，产生告警信息，可以通过即时通信、短消息等通信方式推送给运维系统或运维人员（具体推送方式以用户实际要求为准）。

3.2.4.4 运维日志审计

1、支持运维日志记录：对所有对外服务接口、系统操作、运维操作等所有大数据平台上的操作进行日志记录。支持按照操作者、操作时间、操作模块、操作类型、操作内容，操作来源（如 IP 地址）、来源地域（行政区划）、操作结果（成功、失败）等维度进行日志记录。

2、支持运维日志查询：管理员可通过多个查询条件组合进行查询（操作者、操作时间、操作模块、操作类型、操作内容，操作来源、来源地域、操作结果），并支持日志导出。

3、支持运维日志报表：通过操作用户、操作时间、操作模块、操作类型等几个维度进行不同时间段的操作次数统计生成报表，并支持报表导出。

3.3 非功能性需求

3.3.1 标准规范需求

数据资源建设需符合国家、上级单位的标准规范要求，包括但不限于：

GB/T 36073-2018 数据管理能力成熟度评估模型

GA/DSJ 200- GA/DSJ 290 《公安大数据规范性技术文件》

3.3.2 数据处理非功能性需求

1、性能指标

用户并发访问：≥500；

简单事务处理（如各类信息录入、修改、查询业务、主要页面等）平均响应时间：≤2s；

交互式研判工具平均响应时间：≤5s;

复杂查询或统计平均响应时间：≤10s。

支持结构化与非结构化数据处理，且数据去重的平均准确率≥99%。

支持千万级结构化数据实时比对。

支持万级关键词实时比对。

支持每天处理 1 万条音频特征提取。

2、可操作性

界面操作简捷、布局合理、提示及时，对于层次结构数据尽量使用树形结构，便于定位选取，展示数据的有效工作区最大化。

3、兼容性

流式处理目标端引擎支持 Kafka、HDFS、MongoDB、Hbase、ES、Solor、MySql、Tbase、TDSQL、TBDS、LibrA、PG、Greenplum。

第 4 章 服务平台需求

大数据中心通过融合大数据平台（前置区）和视频云平台的服务、前置区各层级业务系统的服务、数据域大数据平台的数据服务和上级大数据平台共享的服务，建立大数据平台统一的服务资源目录，并通过统一服务资源目录对各业务单位及政府部门提供数据或应用服务支撑。

同时提供丰富数据服务方式和能力，需要同时面向业务人员和开发人员等角色，开发人员侧重系统对接和二次开发，业务人员侧重在系统中对标签、模型等服务的使用。针对不同应用场景提供通用数据服务、通用应用服务和业务应用支撑服务三大类服务：

一是通用数据服务。围绕普遍性实战场景，基于大数据平台汇聚融合的各类资源，按照公安大数据处理标准提供查询检索、比对订阅等全警通用的智能化数据服务。

二是通用应用服务。提供满足基本业务需求的共性工具类应用服务，包括电子地图、专业侦查办案融合、刑事技术查询比对服务，不仅能向用户提供基础的应用功能，还能向通用应用和各业务系统提供能直接集成利用的基础组件服务，业务系统可在前端页面上集成这些应用服务进行展示和交互，无需对接不同的数据服务进行组合和前端展示页面开发。

三是业务应用支撑服务。如果通用数据服务和通用应用服务不能满足业务应

用建设需求时，各部门可向大数据平台申请定制化的服务，本项目将重点围绕但不限于各类系统建设提供定制化服务。

4.1 服务开发管理及统一服务目录

4.1.1 服务资源目录

构建统一的服务资源目录管理平台，针对大数据平台（前置区）和视频大数据平台、前置区各层级业务系统和数据域大数据平台数据服务等各类服务资源，建立服务注册、分类、构建、编排、开放、运维运营的大数据一体化服务能力，实现开放、共享的数据和应用服务生态。

按照 GA/DSJ 250，构建统一的服务资源目录，实现对数据和应用服务资源的管理。

分类	功能项	功能描述
服务资源目录	服务概览	提供服务总数、今日请求数、请求总数等信息的可视化展示，支持柱状图、饼图、列表、曲线图等展示方式;支持针对服务请求、客户端请求等进行统计分析。
	服务目录	提供服务目录查询、服务使用者对服务进行评价和查询详情、服务发布支持对服务进行打标识等功能。
	服务监控	1、访问统计，按照日、周、月、季、年等方式进行统计，支持同比和环比等统计方式，需要统计请求量和平均耗时信息。 2、访问趋势，固定时间段内的所有已发布服务请求量以及平均耗时信息，和访问趋势情况。 3、错误统计，固定时间段内的所有已发布服务错误的请求量以及平均耗时信息。 4、节点监控，支撑服务的服务器、虚拟机或容器的节点、连通状态等信息进行监控，为统一运维平台故障溯源提供支撑。 5、客户端调用统计，按照日、周、月、季、年等方式进行统计，支持同比和环比等统计方式，需要统计请求量和平均耗时信息。 6、服务警告，提供服务告警配置和通知功能。
	服务管控（运维中心统一管控）	1、提供服务请求控制规则配置功能，通过该功能配置具体服务的调用数、频率等控制规则信息，实现服务请求方、客户端账号在指定的调用次数、及频率下请求并调用服务。 2、提供服务并发控制规则配置功能，通过该功能配置具体服务的并发量限制规则，实现服务请求方、客

		户端账号在短时间内(1 秒)请求次数下请求并调用服务。 3、提供服务请求流量规则配置功能，通过该功能配置对应的客户端或针对服务进行请求流量及返回流量控制，面对大流量时，通过控制策略，降低服务提供方的业务系统的负载能力，防止非预期的大流量请求而压垮业务系统。 4、提供服务中断规则配置功能，通过该功能配置指定数据服务的中断策略，当请求后返回的是指定代码时，将中断查询并返回指定消息。
	服务安全防护	提供 IP 黑白名单控制功能，管理员用户可以通过该功能实现对服务请求多维度的白名单、黑名单控制，包括 IP 及客户端账号的配置，保证系统中服务请求的安全性。与服务申请审核功能进行联动。
	服务参数配置	服务分类管理、服务标识管理（由大数据中心根据实际情况来定义，各应用承建单位新增需要联系大数据中心统一定义）

4.1.2 服务资源管理

1、服务注册发布

支持各单位或大数据中心进行服务的注册和发布，发布前支持接口调试功能。

2、服务订阅

支持各单位或大数据中心进行服务的订阅管理，支持对已订阅的服务进行查看和使用，同时订阅方可以在系统中进行模拟调用。

3、服务文档

大数据中心提供服务注册规范文档和服务调用规范模板，服务发布方提供服务调用说明，便于用户了解平台及相关开发技术。大数据中心需要对文档进行统一管理和监控，包括统计文档编写错误率、使用率等指标。

4.1.3 与上级资源对接

推进上级大数据平台的数据共享，争取上级大数据平台下发本区域数据，利用数据下载接口主动下载所需数据；不能下发的，利用上级平台的数据服务接口，进行联查。数据下发来源包括前置区下发和数据域下发两种渠道。

▲通过省市两级运营平台申请上级服务，审批通过后纳入服务平台统一管理，需完成在建设和运维周期内所有需要对接的上级服务（不少于150项）数据查询、推送等数据服务以及电子地图、OCR、音频识别、图片识别等PaaS层服务的对接，同时该部分服务数据亦可以作为建模平台的数据源补充供模型运算灵活调用。

4.2 通用数据服务建设

通用数据服务即由大数据中心统一建设，通过大数据平台的数据生成的通用服务。

▲围绕本地业务特色数据，将大数据平台原始库、资源库、主题库等核心库数据作为一种服务，针对通用业务场景，完成在建设和运维周期内所有需要的查询检索、比对订阅等通用数据服务接口（不少于150项），向上层应用、各业务单位业务系统提供种类丰富、类型多样的服务接口与服务能力。

4.2.1 查询检索

查询检索服务包括数据资源情况的查询检索接口、以及各类结构化和非结构化数据的查询检索接口，支持精确/模糊、分类、组合、批量等多种查询方式，支持返回数据统计汇总信息、判定查询关键词（实体）是否命中（存在）的信息，以及数据摘要或明细信息。

需按照GA/DSJ 251.1建设查询检索服务。

4.2.2 比对订阅

比对订阅服务是针对一种或多种动态活动开展的信息订阅业务。根据输入的比对条件或预先设定好的规则，与结构化或非结构化数据进行比对，在比对过程中支持完全匹配、关键词匹配、正则匹配、多条件逻辑组合匹配，同时比对后实时返回比对结果信息。

需按照GA/DSJ 251.2建设比对订阅服务。

4.2.3 模型分析

模型分析服务须根据业务需要，基于相应知识库的算法对数据进行统计、分析、规律性探索、预测，并返回结果，以支撑应用层业务场景复杂、多变的需求。

4.2.4 数据推送

数据推送服务是大数据平台各级节点间、公安网内部与外部其他部门间进行数据交换和信息推送的基础核心能力，主要包括数据汇聚、数据下发。

需按照 GA/DSJ 251.3 建设数据推送服务。

4.2.5 数据鉴权

数据鉴权服务是基于数据的访问控制规则，实现数据的访问权限鉴别的过程。访问控制规则从内容分级、数据来源、数据种类、字段分类、红名单管理等维度进行资源权限的控制，资源鉴权通过用户的数据资源权限，使用数据鉴权服务实现对数据资源的访问控制。

4.2.6 数据操作

数据操作服务提供数据的增加、修改、删除操作接口服务。

需按照 GA/DSJ 251.4 建设数据操作服务。

4.2.7 数据管理

数据管理服务须按需将数据治理和数据服务的能力进行接口封装，为其他应用系统、平台内其他子系统提供服务。

4.3 通用应用服务建设

通用应用服务即由大数据中心统一建设，各业务系统统一会使用到的应用或服务，比如电子地图服务、标签服务等，同时支持第三方微服务以容器的形式入

驻。

4.3.1 电子地图服务

需完成以下服务定制内容，且在项目建设和运维运营服务期内负责为各业务单位改造和新建涉及电子地图的应用系统提供技术指导和服务支撑。

4.3.1.1 电子地图白板组件服务

支持在地图实现标绘、添加文本、图标、线、面要素的功能，可自定义的标绘场景。

4.3.1.2 空间分析组件服务

提供多种风格的空间数据分析模板，支持业务数据按热力分布、聚合分析、区域统计、多色分析等多种空间分析，实现业务数据快速上图分析。

4.3.1.3 三维地图服务

1、基础三维地图服务：包括三维地图数据接入服务、地图控件服务、图层渲染服务、二次开发服务等。服务将接入三维倾斜摄影建模数据，通过三维地图服务对外发布。接入的过程中保证接入数据的同步及时性和数据的准确性。使用与二维相同的地图属性数据，并在此基础上支持二、三维的叠加展示。

2、建筑信息模型服务：支持 BIM 模型数据加载，包含主流 BIM 软件 Bently 的 dng 格式、Revit 的 rvt 格式。支持室外浏览、室内第一人称浏览、浏览路线设定等。能够通过资源树控制 BIM 中各楼层、各对象的高亮、显示、隐藏，并且支持设备传感器数据接入，在 BIM 场景中监控、管理设备的状态。

3、数字高程服务：支持 tif 格式 DEM 数字高程数据加载，可支持 30-60m 分辨率高程数据。数字高程数据描述的是地面高程信息，可为作战部署提供精确的地形研判依据。

4、三维拓展服务-三维模型服务：支持通用三维模型数据加载，数据格式包

含 obj、fbx、dae、3ds、stl、vrml、shp（3d studio）、dwg、dxf 等。数据内容包含基础设施、交通工具、人、环境等各类模型。

5、空间分析服务：提供淹没分析功能，能够设定淹没起始高程、预警高程、淹没速度，来模拟淹没过程，同时支持淹没水体的颜色、透明度设置，协助观察淹没过程中水位对地形和建筑的影响程度。同时提供视域分析功能，可通过设定观察点位置、观察水平方向角范围、垂直俯仰角范围，来设定具体的视域范围扇形体，通过场景内三维对象的空间计算、判定，返回给用户可见区域范围与不可见区域范围。

6、可视化服务：支持多种三维特效场景渲染，包括：三维热力、三维航线、动态航班等，能实现业务数据的快速上图展示。

7、标准服务：支持 OGC 标准服务，包括 WMS、WMTS 服务；地图服务聚合后，支持发布为地图 REST 服务、WMS 服务、WMTS 服务等。

4.3.1.4 定制化制图服务

提供地图定制化制图服务，标准参考自然资源局印刷版要求。采购人用户能将浏览到的地图生成并输出大图文件，用于打印、展示、汇报、宣传等用途。需要一个能将地图瓦片快速拼接生成大图的服务组件，可以通过在地图标绘任意范围、选择不同地图级别、叠加不同属性图层来生成图片，同时可以叠加辖区范围边界（需要渲染、配色），在生成大图时一并标绘在图片中。生成图片的底图类型能兼容目前常用的底图类型，包括：PGIS、百度、高德、市政地图等。该功能既可以通用工具的方式提供给采购人各用户直接使用，也可作为组件在各地图应用中使用，方便用户在各种场景中都能使用到地图制图功能。

4.3.1.5 其他地图服务

1、轨迹纠正服务：提供轨迹纠正服务，通过传入轨迹信息结合路网数据计算，将原始巡逻轨迹数据纠偏后返回。

2、最佳路径服务：提供公安网内的最佳路径计算服务，通过起止点坐标，依托现有路网数据计算得出最短路径，并以线对象的 WKT 格式返回。

3、融合定位服务：提供融合定位服务，对定位数据进行标准化处理，实现多星源、多设备数据的融合接收，并提供标准的定位数据对接服务。

4、历史轨迹搜索服务：依托采购人大数据平台能力，提供历史轨迹搜索服务，可根据时间、人员、设备等信息检索。

5、在建设和维保期提供现势性不晚于3个月且符合GA/T628-2006《城市警用地理信息空间数据质量》，具备导航功能1:2000基础矢量（包含但不限于路网、信息点、土地、绿地、水系、建筑物等），影像数据等。

6、POI数据准确性要求：1.地图满足标准GB/T 28441－2012《车载导航电子地图数据质量规范》、GB/T 19711-2021《导航地理数据模型与交换格式》的基本要求； 2. POI分类包含：餐饮、住/宿、批发/零售、汽车销售及服务、金融/保险、教育/文化、卫生/社保、运动/休闲、公共设施、商业设施/商务服务、居民服务、公司企业、交通运输/仓储、科研及技术服务、农林牧渔业、自然地物/地名； 3.可行车路网（双向道路按单程计，立交桥、盘桥等不计入里程），其中含5大类信息，属性值超过200个； 4. 各等级道路数据100%经过车辆与人工结合方式实地验证； 5.全市1：2000（最大比例尺可达1：500）； 6.路网（9级路网：高速、城市高速、国道、省道、县道、乡镇村道、其它道路、渡口联络线等）精度10~15米；7.详细道路数据（城市内道路）准确度>=99.5%。

7、地址聚合治理与地址标准化服务：将全市一标多实、空间标准化地址、警情案件地址等所有可共享地址信息进行大数据聚合，按照公安行业标准规范统一地址结构，对现有地址数据进行标准化处理、治理，形成地址主题库。地址结构至少需包括省市区县、乡镇街道、社区居村委、街路巷、门楼牌、小区、建筑物、房屋等。在地图上，通过算法提供支持地址的语义搜索，支持标准地址的转换、匹配、解析，以及地址和经纬度的互相转换。通过对接相应服务实现业务系统地址录入标准化、警情地址地图定位、警务资源实时上图和事件关联分析等。

4.3.2专业侦查办案数据融合服务

大数据中心负责统一建设，结合资源库、主题库等数据，通过数据算法模型及模型编排能力，将专业侦查办案数据融合分析能力封装成服务，通过统一服务

资源目录支撑各单位使用。包含但不限于：关系亲密度、时空信息、场景化关系、关联同行、首末次出现、多区域碰撞、区域分析、活动规律和对象规律等分析。

4.3.3刑事技术应用服务

4.3.3.1 音频注册服务

经过预处理后，提取出特征数据，再结合其他结构化信息，注册到库中。

4.3.3.2 音频查询服务

针对特定目标信息，搜索获取其关联的信息。

查询比对服务，提供 1:1 和 1:N 的比对功能。

4.4 业务应用支撑服务

4.4.1基础数据服务

满足业务应用对数据资源基础的查询、订阅需求，提供查询检索、比对订阅类、数据推送和上级服务对接共 250 项定制化数据服务接口的开发。

4.4.2建模分析服务

▲针对业务应用的大规模数据挖掘、分析研判场景需求，提供数据挖掘建模分析服务，通过对象特征规律，并一一分析对象特征所涉及的海量数据资源关键要素之间的关系，提炼成技战法，构建数据挖掘模型。建模分析结果以服务的方式为业务应用提供支撑，需完成 60 个数据挖掘模型的开发。

4.5 开发框架需求

大数据开发框架为所有进行大数据软件开发、测试、部署、维护提供开发、

测试、部署、运维环境，开发框架需采用与广泛使用的 SPRING CLOUD 新版本兼容的商业开发框架，要在公安网建立统一的开发框架，包括但不限于开发平台、服务治理平台、API 网关、配置中心、服务注册中心、容器管理平台、代码托管中心，并且要构建起开发、测试、部署、运维全流程自动化流水线能力。其他软件开发单位须使用此统一的开发框架进行开发，不能够使用各自相互独立的开发框架。

4.5.1 开发平台

一是开发平台要确保所有开发人员的源代码在统一的代码托管中心保存，并且可以清晰便利地访问所有源代码，每个开发单位的人员只能访问自己开发的源代码，从而既保障各自开发源代码的私密性，又保障所有开发的服务可以持续进行升级；二是开发人员在开发平台中可以找到所有已在注册服务中心中注册的服务，为服务的共享提供有效支撑；三是开发人员对已注册的所有资源进行访问必须先通过运营平台提出申请，审批通过后才能有效访问；四是为数据资源访问提供完善的读写分离机制、访问控制管理和开发调试级的日志审计；五是对每个注册的服务，系统要明确地记载开发单位、开发人员、开发时间、主要功能和参数描述，并为服务打上服务分类标签，以方便开发人员查找；开发人员对自己建立的未注册的资源可以随意访问。

4.5.2 服务治理平台

所有 DAAS、SAAS 和应用层的软件都必须基于统一的服务治理平台进行服务治理，不允许不同开发商采用不同的服务治理平台进行服务治理。服务治理平台主要包括服务注册与发现、服务调用拓扑的监测、服务版本的平滑更迭管理、服务的安全管理、服务治理策略的分发。

4.5.3 API 网关

所有的服务开发商，都必须使用大数据统一的 API 网关，形成所有对外服务的统一访问入口，确保对服务的访问可以做到以下几点：一是基于统一的安全策略开放不同服务的访问权限；二是统一限制对某些微服务访问的流量；三是对所有服务的访问请求和返回结果进行统一记录，便于日后的日志分析，并对各种服务的响应性能进行实时监控；四是在发现一些服务出现问题时，可统一进行服务

降级，以确保不影响其他服务的正常运行；五是基于统一的策略，对发生异常的请求进行重试。

4.5.4 配置中心

为所有开发的应用、中台、平台软件的配置文件建立统一的配置中心。配置中心支持配置文件的实时刷新、版本管理、配置回滚，支持 JSON、YAML、Properties 等多种格式，支持高并发、高可用，支持多环境、多集群部署。当配置信息发生变化时，配置中心支持动态推送，实时生效，无需重启服务。当配置变更不符合预期时，可根据配置的发布版本进行回滚。配置中心要支持将开发测试环境和生产环境分开，或根据不同的业务线存在多个生产环境。对稳定性要求比较高的应用、中台或平台，其配置文件不允许各个环境相互影响时，要支持多个环境之间的安全隔离。

4.5.5 服务注册中心

建立统一的服务注册中心，所有开发的服务必须在统一的服务注册中心中注册，确保开发平台安全、便利地访问所有已注册的服务资源。

4.5.6 容器管理平台

建立统一的容器管理平台，所有微服务的运行只能在统一的容器管理平台下获取容器资源。

4.5.7 统一的代码托管中心

建立统一的代码托管中心，确保所有开发的源代码均保存在统一的代码托管中心。

4.5.8 开发要求

制定相应开发规范，确保整个大数据系统的开发满足以下需求：

1、前端和后端开发的软件要与终端解耦，即开发的前后端软件要可支持多种终端（电脑、平板、手机），所有应用均支持统一的浏览器。

2、各软件开发单位开发的软件要完全解耦，各自都可以独立地进行软件升级，不受其他开发单位的束缚。

3、支持逐步扩大对升级服务版本的应用范围，以减少升级版本错误导致的问题。

4、要确保每个可共享的服务具有通用性，避免类似的服务资源重复建设。

4.6 非功能性需求

4.6.1性能和其他需求

本项目建设的服务平台是服务应用系统、各业务单位的支撑平台，性能和稳定性要求较高，在性能上应满足如下需求：

1、用户访问

用户并发访问：≥2000。

2、服务访问

服务调用返回最大延迟：≤5s。

服务平均响应时间：≤1s。

3、响应性

简单服务（如简单的各查询检索、简单的比对订阅、数据推送、数据操作等）平均响应时间：≤2s。

复杂服务（如复杂的各查询检索、复杂的比对订阅、模型战法等）平均响应时间：≤5s。

4、可用性

服务接口简捷、合理、提示和文档信息全面。

4.6.2标准规范需求

服务平台建设需符合国家、上级的规范要求，包括但不限于：

GA/DSJ 250- GA/DSJ 254 《公安大数据规范性技术文件》

4.6.3其他需求

兼容信创终端浏览器。

第5章 大数据智能应用需求

基于大数据平台汇聚的各类数据，建设搜索类应用、全息画像类应用、关注类应用、消息分发信息订阅类应用、模型算法类应用和大数据看板类应用等各类通用应用。

建设面向民生服务的公安政务一体化平台，打造统一的公众服务门户、统一的警务人员工作门户以及基础支撑系统，实现业务部门的数据开放和资源共享，以民生服务为主要需求驱动，实现政务服务的集约式管控和全面感知，最终逐步实现“一个账号、一个入口、全业务办理”。服务门户主要部署在互联网，主要使用人员为珠海市民，向市民提供面向互联网的统一警务民生服务；工作门户主要部署在公安网，主要使用人员为警务人员，实现对业务系统和业务信息的整合和管理，通过跨网数据接口，将数据推送给其它业务部门；基于统一身份认证、统一电子证照、统一标准地址、统一电子印章服务等业务支撑服务内容，提供统一的数据应用共享服务，支撑建设各业务单位便民服务事项。

5.1 通用应用

5.1.1 智慧搜索升级

5.1.1.1 业务需求

智慧搜索应用为大数据平台一期建设的通用应用，目前已经实现了针对汇聚融合到大数据平台的数据资源的组合检索、关键词检索、批量检索和专题检索功能。

随着大数据平台数据资源的丰富，以及与上级资源的联动、本地各业务单位应用的逐渐上云，数据搜索范围大大增加，但目前智慧搜索的搜索范围、搜索对象要素的全面性及检索能力不足以支撑各业务单位整体应用需求。为避免各业务单位应用重复建设搜索类功能，减小重复开发，需对大数据平台一期建设的智慧搜索应用进行升级改造，主要改造需求包括：

1、扩大智慧搜索范围。实现统一的搜索入口，支持多平台数据资源搜索。提供统一的智慧搜索服务，各业务系统能够集成进行搜索，支持包括多媒体、地

图、移动端、前置区等多种搜索入口：1）移动端和前置区搜索通过零信任中的权限服务控制返回非高敏数据。2）地图搜索，通过集成电子地图搜索服务，支持根据场所名称、地址、空间范围等方式进行搜索，并在地图上标记位置；同时能够根据经纬度检索相关数据。3）多媒体检索，通过集成视频云平台服务，支持图片抓拍等检索能力。

2、实现搜索对象要素多样化、智能化。基于大数据平台汇聚的各类数据，增加包括地理范围、图片、音频等对象要素的识别检索能力。

3、提升多关键词组合搜索能力。实现对海量非结构化和结构化文本索引内容、原始资源的结构化文本索引内容执行一键全文搜索。

4、提升批量检索能力。支持通过上传导入或拖拽表格文档的方式，批量执行搜索。

5、实现搜索结果的聚合展示及分析，可以对查询结果按照数据价值、数据质量、业务相关度等进行排序，并综合推荐出匹配价值高的若干条查询结果，用户可以根据习惯个性化配置搜索展示结果。通过对不同搜索来源的数据进行聚合，按照人、地、事、物、组织等维度展示对象全维度信息，整合扩展全息画像功能，支持基于搜索结果查看对象全息档案；通过对搜索对象要素的智能分析，实现关键要素的交叉分析。

6、实现对搜索对象的一键关注功能，并实现与智慧关注功能的联动。

7、实现自然语言语义搜索能力，用户可以通过键入自然语言文本或者通过语音（普通话、粤语）输入搜索条件，系统自动展示用户期望的结果集。

8、可选择某一个或多个资源，根据该资源的属性配置，生成查询条件输入项（文本输入框、字典清单等），用户输入检索条件，对选择资源执行检索。

5.1.1.2 功能需求

5.1.1.2.1 搜索资源

基于对接的数据和应用系统，依托 DaaS 层的数据融合支撑体系，实现多数据源、多业务系统的数据资源整合搜索，通过提供统一的搜索入口，实现大数据平台数据、标签、模型、数据服务等各类资源的搜索。

5.1.1.2.2 一站式搜索

构建一站式综合搜索体系，实现“业务数据一站式”“全国数据一站式”“信息输入一站式”“结果反馈一站式”，即业务数据融合搜索、全国数据互联查询、统一搜索入口、统一查询结果。同时可记录查询搜索历史信息。

在PC端和移动端上提供统一搜索功能，兼容传统的全文搜索方式，提供分类、分表、分字段、要素搜索、精确搜索、模糊搜索、多源关联检索、二次检索、自然语言搜索、综合搜索、高级搜索等搜索功能，支持自动适配扩展搜索，提供从视频图像到对象等多种搜索方式，围绕各类对象要素，实现对象智能检索、精准检索，以对象维度聚合、卡片形式、查询命中词高亮显示等展示搜索结果，并实现与智慧关注、全息画像等应用联动。

5.1.1.2.3 系统管理

提供水印管理、同义词\反义词等应用基础管理功能。

分类	功能项	功能需求描述
系统管理	水印管理	根据用户的检索结果，在检索结果界面同步展示用户水印。涉及水印配置信息维护，支持对水印信息进行修改、删除。
	同义词\反义词管理	建立同义词/反义词库，可进行添加、删除和修改。
	系统对接	支持对接零信任体系的认证服务、权限服务、审计服务、审批服务。

5.1.2 全息画像升级

5.1.2.1 业务需求

随着警务模式向智能化阶段迈进，智慧警务是警务智能化的一种重要形态，智慧警务以提升公安机关核心战斗力为主要目标，打造丰富的全息画像是智能化的重要基础服务。目前的画像服务与业务贴合度不够、支撑能力不足，针对用户业务需求，依托大数据平台已整合的各类数据，为用户各业务提供多维度全息刻画支撑，提升用户业务实战的全面性、精确性和效率。

5.1.2.2 功能需求

基于大数据平台融合的数据，根据公安业务需求，针对各种业务要素提供画

像功能。需基于新增数据源扩展对象刻画维度，同时与智慧搜索、智慧关注功能实现全面融合联动，实现统一的入口、统一对象画像刻画展示与分析。

▲本项目需升级建设人员画像、车辆画像、手机画像、案件画像、场所画像、关注对象画像等不少于20个主题的画像功能，其中人员画像需同时支持个人和群体画像功能。

5.1.3 智慧关注升级

5.1.3.1 业务需求

在现阶段已建设的基础上，打造新一代智慧关注通用应用，具体需求如下：

1、建立关注对象档案的需求，不同用户需要针对不同关注对象进行建档。一方面结合大数据平台数据对对象信息进行自动补全、智能推荐；另一方面在关注对象档案中增加备注信息；支持根据标签形成对象档案，用户可通过标签平台创建标签后，将标签对象转换成对象档案；当用户通过智慧搜索应用无法检索到目标对象时，可以将该对象添加到关注对象档案，当该对象出现符合用户自定义的行为时可提醒用户。

2、满足提升关注对象动态管理的需求，提供动态模型的管理。根据用户业务需求，提供各类动态模型，用户可基于系统提供的模型模板配置动态模型，根据智能研判分析成果，向用户实时精准推送动态信息。也可以通过建模平台构建提醒模型后，在智慧关注中基于构建的模型对对象进行动态关注，或者选择将关注的规则推送给视频云使用。

3、实现趋势分析的需求，能够通过柱状图、折线图、饼图、热力图等多样化的可视化形式，直观的呈现关注对象的时空动态、趋势分析等内容，辅助决策。

4、实现推送关注对象的动态信息日志可查询可回溯的需求。

5.1.3.2 功能需求

5.1.3.2.1 关注对象档案

关注对象档案可通过人工录入、业务系统导入、基于标签或系统自动分析研判形成，如用户通过智慧搜索应用检索出车辆对象，可将该车辆添加到关注对象档案，并可进一步对车辆进行关注提醒；如根据分析挖掘出其他人员后，可批量

添加到关注档案里。根据关注对象构建实体库，支持对实体库进行管理；提供关注对象的创建、修改、删除、查阅、审批等功能（其中“审批”需实现可配置，开启时配置相应的审批表单和流程，关闭时则无需审批）；支持对关注对象进行智能化分析；支持移除功能。

分类	功能项	功能需求描述
关注对象档案	对象实体库	根据各种关注对象构建实体库,支持对实体库进行管理。
	对象转入服务	提供关注对象转入服务接口,实现外部应用关注对象导入系统功能。
	关注对象管理	提供关注对象的创建、修改、删除、查阅、审批等功能。
	关注对象分析研判	支持对关注对象的关系、轨迹进行分析。
	其他对象转关注对象	支持将智慧搜索检索到的对象一键添加到关注对象档案，支持根据标签形成对象档案；支持移除功能。

5.1.3.2.2 关注对象动态管理

根据公安业务需求，通过大数据查询、模型配置、感知发现等手段对关注对象及相关要素动态管理,并支持根据用户提交的备注记录结合大数据分析进行综合分析，可进一步根据公安业务需求细化动态管理的功能。

5.1.3.2.3 关注对象综合分析

根据公安实际业务需求提供关注对象态势分析、趋势分析、行为分析、区域分布、活跃度分析、流动统计，以及自定义区域聚集趋势分析和标签命中结果分析等功能。例如关注对象态势分析，可以按照不同关注对象，基于地图展示关注对象分布情况；基于时间维度进行统计；基于流入、流出、首次进入维度统计；支持按照区域层级进行下钻统计；支持关注对象统计的时空热图展示。

5.1.4 智能消息升级

打造统一的消息收发服务、信息订阅、关注分发等能力集成化平台。实现统一的消息管理能力，满足于不同业务系统、不同平台网络对消息的建设需求，以及不同区域对消息统一运维和共享的需求,为用户业务需求提供统一的消息服务平台。

1、梳理各种消息交互渠道、通过格式化、规范化等手段对各种交互渠道（短

信、邮箱、OA、移动警务、智慧关注）等进行集成接入。

2、提供标准化消息服务接口，为各业务系统提供统一消息接收、发送、推送、转发的消息集成服务平台，满足于不同业务系统、不同平台网络对消息的建设需求，为警务业务需求提供统一的消息服务平台。

3、实现统一的消息运营、运维管理，将消息内容集中管理、对消息内容进行监控分析。

4、能支持跨网的消息发送和接收，由高到低进行跨网消息发送的，需根据网络安全管理的要求进行审批；同时所有消息发送都需要进行日志记录便于审计。

5、用户可通过移动端 APP 开展消息查看、管理、签收、审批等功能。

5.1.5 短信平台升级

短信平台在现有功能、性能、稳定性的基础上新增但不限于以下内容：一是支持通过接口形式或直接发送全国号码短信（包含中国移动、中国电信、中国联通）；二是支持自动识别号码归属运营商、自动识别是否可接收短信（如物流卡无法接收）、自动识别号码是否有效等，并分流至对应网关发送；三是支持 A 运营商可通过运营商之间网关发送 B 运营商号码短信的功能；四是支持三大运营商（中国移动、中国电信、中国联通）一个端口对应多个签名模版（如 106******* 支持 XX 局、XXX 办公室等多个签名）；五是支持短信报文发送速率不低于 50 万条/小时，平台发送 50 万短信号码的提交后响应时间不高于 15 秒；六是支持通过时间、单位、系统、端口号等条件统计平台发送短信总量并导出短信发送内容；七是支持自动监测平台运行情况并输出互联网及公安网端故障告警日志（运营商端口故障可通过其他运营商端口发送告警短信）；八是支持系统安全设计符合等保 2.0 国家标准要求。

5.1.6 建模平台

5.1.6.1 业务需求

近年来，通过实施信息化、大数据应用整合提升工程，从技术层面初步解开了信息孤岛和信息碎片化的死结，为实现更大范围、更高层次的共享应用奠定了基础，但在提升业务部门的自主分析和展示能力，适应不断变化的业务需求方面仍然面临诸多问题。建设统一的大数据可视化建模平台，便于业务部门自主建设各种分析模型，以适应不断变化的业务需求成为大数据建设成功的关键，主要业务需求如下：

1、可视化建模。用户能够通过拖拉拽的便捷操作方式，全程可视化进行模型构建，同时应支持流式建模，即对实时数据进行建模，如卡口车流数据、图片比对数据、日志数据等，降低用户的数据分析门槛。模型计算结果不仅能直接展示，也能通过服务的方式集成到可视化大屏上，对计算结果进行可视化展示页面设计。

2、建模数据管理。用户能够充分利用大数据平台、视频云平台各类数据资源以及个人数据进行模型构建，同时能将模型计算结果作为一类新的数据资源或者发布成数据服务给业务系统使用。

3、模型便捷共享。不同用户创建的模型或算子能够进行分享、复用和组合，促进经验共享和知识沉淀。

5.1.6.2 功能需求

为满足用户业务实战需要，需要可视化建模工具将用户的实战经验和技战法转换为模型，用户可通过拖拽的方式进行在线分析建模，满足分析研判需要；在侦查破案等用户业务工作中，用户可通过建模工具利用已知条件，通过模型推演、预测，发现未知或实现场景还原。

建模平台以大数据平台丰富的数据资源为支撑，集成丰富的模型组件、规则引擎和典型案例，提供托拉拽方式的在线可视化分析建模功能，支撑用户通过建模深挖大数据价值，沉淀、共享实战经验知识。

5.1.6.2.1 综合展示

建模平台首页功能帮助用户快速了解平台能力、个人建模能力、系统运行性能情况、模型任务运行统计情况。

支持展示数据资源总数量、模型总数量、应用数量、模型任务统计概览等，并结合个人应用建设数量、技战法分享数量、模型发布数量、算子发布数量、模型建设数量等因素综合评估个人能力指数。

5.1.6.2.2 数据集市

数据集市为用户提供丰富的建模原始数据以及灵活的数据接入能力。包括但不限于数据资源目录申请对接，多种格式个人数据导入、追加导入以及数据库数据快速注册接入。

分类	功能项	功能需求描述
数据集市	全局搜索	支持全局数据按表名、按字段进行快速搜索定位。
	数据资源目录	提供数据资源目录数据接入功能；支持 MySQL、SQLServer、Oracle、DB2 等其他业务系统数据对接；支持 API 导入。
	个人数据	提供个人数据导入功能，支持个人数据展示和搜索；支持上传 EXCEL、CSV、TXT，MySQL、Oracle 等数据库文件数据，支持多文件单表合并、多表拆分，以及文件编码识别功能。
	模型结果数据	提供模型结果数据按列表资源展示;支持将模型结果数据注册至数据资源目录,支持将模型结果封装成服务并发布至数据服务目录。

5.1.6.2.3 模型管理

模型管理实现模型全生命周期管理功能，支持对模型的状态监测、运行、分享、发布等操作，并同时提供创建模型入口和模型导入功能。

分类	功能项	功能需求描述
模型管理	模型分类	默认模型分类包括默认文件夹、他人分享文件夹、分享给他人文件夹、近期修改文件夹、第三方模型文件夹，提供新建分类功能。
	模型列表	提供缩略图和列表展示方式，支持模型详情查看、模型运行、重新运行、删除、导出、分享、发布。

5.1.6.2.4 模型创建

提供拖拉拽方式的模型创建、运行、分享、发布等全程可视化模型搭建功能，并集成算子资源、资源库和丰富的画布功能。支持模型保存、运行、模型日志等功能。

分类	功能项	功能需求描述
模型创建	建模资源库	提供模型创建过程当中所需的数据集，支持自定义添加将所需数据资源，支持数据源以拖拉拽的方式导入画布。
	可视化拖拽	支持以拖拽方式将集合导入画布，提供一键排版、曲线连接、折线连接等画布排版功能，画布支持信息展示、放大、缩小、连线配置等功能。
	模型分步调试	提供模型每一步骤的运算调试功能，支持对分步调试运行数据结果查看，同时在画布上以图标实时显示算子状态。
	模型设置	1、提供模型入参配置功能，支持整数类型、浮点型、长整型、字符串、布尔型、浮点型、时间戳、时间等参数； 2、提供模型运行调度配置功能，支持按次、天、周、月、自定义方式进行运行规则配置。
	模型封装	支持将现有模型所使用的算子、模型逻辑、算子参数配置进行统一封装转换为新的模型算子。
	模型复用	支持对现有模型进行复制。

5.1.6.2.5 流式建模

▲满足数据实时计算的应用需求，如过车数据分析、实时布控等业务场景领域，通过流计算作为一类针对流数据的实时计算模型，有效缩短全链路数据流时延、实时化计算逻辑。需基于流数据进行数据分析，支持车流数据、图片数据等流数据进行建模。

5.1.6.2.6 算子管理

建模平台提供丰富的算子资源供用户使用，包括基本算子、数据处理算子、AI 算子、ML 算子、模型算子，不同类型的算子可满足各类建模使用者在任何阶

段对数据处理、数据分析、数据挖掘的需求。

分类	功能项	功能需求描述
算子管理	基本算子	提供过滤、聚合、交集、并集、差集、连接、自连接、去重、自定义 SQL、添加字段、表结构处理、输出算子。
	数据处理算子	提供列计算、类型转换、列转行、行转列、字段值替换、缺失值处理、值映射、时间处理、数据校验、数据归一化、数据清洗算子。
	AI 算子	提供文本提取和文本分类算子。
	ML 算子	提供分类、聚类、异常、关联规则、时间序列等算子。
	模型算子	支持将已构建的模型封装成算子，进行复用。

5.1.6.2.7 模型超市

模型超市为各类已发布的模型、算子提供展示平台，支持模型评价、经验交流、模型共享、技能培训等，满足对模型的分发、收集、整合、应用、管理等功能，实现数据运营、经验共享和知识沉淀，构建可闭环的众创建模生态圈。

分类	功能项	功能需求描述
模型超市	精品超市	支持按模型综合评分、使用率、查阅率、收藏率等综合因素所评价的精品模型和算子进行展示。
	应用中心	支持按照模型、算子、技战法的方式进行分类展示。
	模型评价	提供模型和算子评价功能，支持星级评价和文字评价。

5.1.6.2.8 监控中心

提供对全部任务、正在运行、运行异常、运行成功任务数量监控统计功能。

5.1.6.3 上云迁移改造需求

依托大数据平台组件、大数据平台治理后的全量数据，将情报等部门已建模型进行上云迁移和前后端分离改造。包括上云迁移及改造、数据服务对接、前后端分离改造、模型服务输出等。

5.1.6.3.1 上云迁移及改造

当前建模平台是基于 10 台物理服务器单独搭建的 Hadoop 集群，对接大数

据平台后需要进行集群切换，由独立的集群环境切换到云平台集群环境。需要进行虚拟服务器和大数据组件申请。上云后的平台统一使用大数据平台提供HDFS、hive 进行数据的存储和查询，使用 spark 进行数据任务的计算。

5.1.6.3.2 数据对接

按照大数据平台建设规划，数据统一采集和治理后流入离线计算进行统一开放应用，建模平台作为 SaaS 应用，不再直接对接业务数据库，需支持通过离线计算实现数据对接。数据接入需支持关系型数据库接入、大数据平台接入、流式数据对接、文件接入以及接口接入。

1、关系型数据库接入

支持连接指定的关系型数据库，包括但不限于 Oracle、MySql、SqlServer、DB2 等，通过可视化的配置方式配置 IP 地址、数据库用户信息即可进行数据库连接，并支持数据的增量、全量、定时更新。

2、大数据计算框架接入

支持主流大数据计算框架的数据接入。支持通过数据表映射的方式进行数据的接入，并支持数据的增量、全量、定时更新。

3、流式数据接入

支持通过消息总线对接视频、图片等流式数据。

4、文件接入

- 文件批量接入

支持 Excel、CSV、TXT 等外部文件单文件导入和批量导入，提供每次操作的操作记录，以便于进行操作日志查询。

- 文件接入回滚

同一个文件会有多个版本的导入，支持指定任意一个版本的回滚操作。

- 文件导入数据字段选择

导入数据解析完毕后，支持勾选选择字段;支持数据异常检测，并进行异常数据提示；对字段可以进行新字段的生成、分列、以及衍生字段生成等操作。支持数据直接查询，提供过滤器;支持显示接入统计信息。

5、接口接入

接口适配按照配置，支持定时调用指定接口，获取数据资源。接口适配支持各种接口格式，包括但不限于 REST、WebService 等。

6、接入管理

➢ 增量策略配置

数据接入可以通过多种方式获取增量数据。主要包括基于时间戳、触发器、业务变更标识、全表比对方式、逻辑增量、数据库日志分析等。

➢ 任务配置

对调度任务进行配置，主要是配置数据接入的处理流程，包括模板编排定义、执行计划配置等内容，同时任务配置也需要确定数据的接入策略。

➢ 任务调度

任务调度是在任务配置的基础上，对具体接入任务的执行进行调度。提供多种任务调度周期方式，如按日、按周、按月、时间间隔以及立即执行等，另外还支持任务之间的依赖调度以及跨周期依赖调度。

5.1.6.3.3 模型服务输出

建模平台为用户提供海量数据计算和分析能力，模型数据结果及可视化结果需提供服务化输出接口，实现对模型结果和可视化结果的业务系统调用。

1、Web 端图表内嵌接口

Web 端需支持通过 URL 链接的方式将图表内嵌至第三方系统。

2、移动端图表内嵌接口

移动端需支持通过 H5 的方式进行图表内嵌。

3、可视化分析内嵌接口

需提供可视化分析仪表盘内嵌至第三方系统的接口。

4、模型结果输出接口

需提供模型结果服务化输出接口，支持快速发布至 API 网关，供有需要的用户进行模型结果的调用。

数据输出需集成丰富的数据输出组件，支持注册到资源目录、输出到文件、输出到主流数据库。

注册资源目录:模型结果可以作为数据资源重新注册到资源目录。

输出到文件：支持 Excel 和 CSV 文件格式导出。同时需要充分考虑数据管理安全和平台资源占用管理，根据用户权限设置下载权限和下载速度。

输出到数据库:通过在模型中的输出数据库组件，可以把模型结果数据导出到其他的数据库，包括：Mongodb、Mysql、Hbase、ES 等。

5.1.6.4 分析研判平台

建设集关系分析、时空分析等通用分析研判组件于一体的一站式可视化分析平台，满足公安大数据研判侦查、线索挖掘等多场景研判分析实战需求，提供关联拓线、关系分析、思维引导、时空分析、统计分析等通用可视化分析组件，支持多人协作、成果共享，以及研判工作的图谱式记录及研判引导。

5.1.6.4.1 业务需求

随着大数据环境下，现有手段对复杂多源数据的研判分析存在困难，传统研判工作模式也存在一定瓶颈，缺少一种将大量、未知质量、低关联性、低价值信息转化为少量、易于理解、高关联性、高价值可操作情报的方法和工具，主要体现在三个方面：一是信息难理解，海量多源异构数据难以被用户理解，导致深层次、多层关系网络的推导难，海量数据价值无法充分体现。二是研判无协作，用户对情报数据的挖掘往往需要结合不同的线上或线下的工具，导致研判过程、结果无法统一，以往研判过程积累的结果也无法复现更无法与其他用户进行分享和协作。三是工作无条理，研判分析被分散在各业务单位的业务，无法进行统一管理，各业务单位的研判成果无法进行沉淀和梳理。

为破解以上问题需构建一站式的可视化分析平台，满足以下业务需求：

1、提供高可用的可视化研判平台，提供便捷的研判分析环境（工作环境、分析环境、协作环境），和丰富的可视化研判分析能力，包括常用的关系分析和轨迹分析组件，用户可在平台直接使用满足用户复杂的实战需求，降低用户理解与学习成本。

2、创新研判工作模式和手段，利用一站式分析平台，打破原有传统、封闭的研判工作环境，实现对研判工作的规范管理，辅助研判工作向多人协同模式进

行转变，促进研判经验与方法的有效积累和快速分享。

3、作为大数据快速赋能的有效载体，利用大数据治理成果和计算能力，高效赋能用户研判分析工作，体现大数据价值，用户通过大数据服务平台申请数据服务、应用服务等服务能力，并能在可视化分析平台上进行组合研判。

5.1.6.4.2 功能需求

5.1.6.4.2.1 研判任务管理

提供用户分析研判工作任务管理功能，实现研判全过程管理和溯源，支持建立多个分析小组、多人共同分析、分析工作合并、协作交流评价和成果共享等。

5.1.6.4.2.2 可视化研判分析

根据用户实际业务需求，通过图挖掘、图分析技术实现关系分析功能，支撑用户挖掘各种实体对象、时间、事件序列以及关联关系和线索，支持新的实体和关系的发现、拓展。支持基础研判、图表分析、路径分析、时序分析、统计分析、智能分群等分析功能。

5.1.6.4.2.3 空间轨迹分析

基于地图服务，实现思维导图、可视化研判分析功能的联动，支持基于地图的轨迹分析、热度分析、联动分析等功能。

5.1.6.4.2.4 思维引导图谱

集成各类数据服务和关系分析、地图分析等研判能力，通过思维导图方式引导用户开展研判工作，同时支持记录沉淀研判结果形成知识，引导往后研判思路。

分类	功能项	功能需求描述
思维引导图谱	推演编排	通过思维导图方式提供事件过程和研判思路的推导模型编排功能，支持数据实时比对和对象的二次编辑；提供流程图、鱼骨图、树状图等风格布局；支持引导图形编排、节点编辑、连接编辑、图标编辑等编排和编辑功能；支持大纲视图，导入导出操作。
	联动分析	支持推演编排模型与分析组件的联动，包括查询检索、比对分析，以及分析组件。

5.1.6.4.2.5 可视化组件及服务

分析平台的思维导图、关系分析、可视化等组件支持以服务的方式提供其他系统集成调用，分析平台也支持调用服务资源目录中的各类服务。

5.1.6.5 多维统计平台

5.1.6.5.1 自助分析

根据业务需求，可选择数据并自主编排，根据用户不同业务部门需求定制数据报表，自助分析功能包括：图表支持、仪表盘设计、数据填报录入、异常数据预警推送、报告水印、报表管理、数据校验等。

5.1.6.5.2 多维分析

需具备全面的数据分析功能，至少包括数据集切换、维度\度量\参数选择、过滤、排序、特性分析，并内置图形化组件和分析算法，展示分析结果，功能包括可视化分析、联动分析。时间维度支持按照天、周、月、季、年不同周期统计。度量支持切换不同的聚合方式去展示数据，聚合方式包括总和、平均、最大值、最小值、计数、精确不同值计数、协方差等。地址维度支持按照市局、分局、派出所、警务区（社区）不同地域统计，其他维度按照标准字典项进行统计，维度可以依据需求定制添加。需要建立多维数据模型，支持模型的上卷、下钻、切片、切块等功能。

5.1.6.5.3 PC 端展示

支持 PC 端可视化展示，在 PC 上通过数据建模和维度指标设计，以丰富的图表展现形式，自由拖拽布局设计，快速构建出多个主题的可视化展现界面。维度指标可以自由拖拽，图表形式可以自由切换。同时可以关联大屏显示。

5.2 公安一体化政务服务平台

建设具备高效管理、高效运作、便民利民的公安一体化政务服务平台，打造“两个门户”以及基础支撑系统，两门户即“服务门户”和“工作门户”，升级公安外部信息资源汇集平台，实现与各委办局以及业务部门的数据开放和资源共享，以民生服务为主要需求驱动，实现政务服务的集约式管控和全面感知，最终逐步实现“一个帐号、一个入口、全业务办理”。

建设公安一体化政务服务平台实现与市政数局电子证照、电子印章、身份认证对接，实现业务在局内统筹，作为平台核心基础能力，供各业务单位共享互用。同时与市政数局公共数据资源登记管理平台、共享资源目录管理平台对接，将各业务单位的开放、共享、归集数据统一收集，实现数据统一集中出口。

5.2.1 服务门户

服务门户向市民和委办局等社会面提供面向互联网的统一入口，主要部署在互联网，主要使用人员为社会面各单位。通过公安一体化政务服务平台的建设，对服务的能力进行标准化的梳理和服务指标的监控，实现互联网便民服务的线上、线下的支撑，实现公安对外服务的统一。功能需求如下：

1、用户中心，提供身份认证、用户注册、电子证照查询等功能；

2、查询中心，提供同名查询、实时路况查询等便民服务；

3、标准地址，在小程序上实现标准地址服务，即展示标准地址信息，地图定位、地址曾用名、地址纠错等地址应用服务；

4、消息中心，与统一消息推送服务对接，通过短信或小程序向实名认证用户推送各类消息提醒；

5、在小程序平台提供实名认证、电子证照查看、同名查询、实时路况查询、标准地址查询纠错等民生服务。

5.2.2 工作门户

工作门户主要部署在公安网，主要使用人员为警务人员，工作门户主要对民生服务以及基础数据进行管理，通过与警务云通用审批系统对接等方式实现服务

申请的办理，同时可以查看服务门户的申请信息、咨询信息、结果信息等动态信息。同时，工作门户提供服务管理、权限管理和业务联动管理等功能。功能需求如下：

1、服务管理，提供服务申请、查询、流程调度、审批情况、启用与禁用等功能；

2、权限管理，依托已建的统一用户中心的组织架构和用户信息，对接零信任体系的权限服务，建立工作门户的用户权限功能；

3、业务联动管理，支持事项办理业务、内外网业务的联动；

4、日志管理，记录各业务系统的处理日志，从而实现对业务的审计和跟踪管理；

5、系统对接，与统一机构用户对接，实现统一身份登录。与审批对接，可利用已有的警务云通用审批系统申请审批流程。

5.2.3 基础支撑系统

功能需求如下：

1、身份认证中心，对接广东省统一身份认证系统，提供身份鉴权服务等功能；

3、消息推送，对接智能消息平台，提供消息收集、管理、推送和应用配置功能；

3、电子证照，对接珠海市政数局电子证照系统和广东省政数局电子证照系统，提供电子证照管理中心、证照共享管理、推送管理、查验、查看等功能，其中电子证照查验提供服务应答总时长不大于 4 秒；

4、电子印章，对接珠海市政数局电子印章系统，提供用章管理、印章管理等功能，对业务系统提供用章、日志、服务等接口，在业务使用和系统主动抓取中形成电子证照留存库；

5、基础数据，在前置区汇聚公安政务服务数据和需要共享给其他委办局的数据。基于基础数据形成数据服务并服务于其他委办局，把需要共享的数据共享到珠海市政数局政务信息资源共享平台，支撑一体化政务服务平台数据可视化展示。数据包括办件数据、好差评数据、监管数据、标准地址数据、信用信息数据、

资源目录数据等；

6、配合政数局的要求保障平台的安全、可控。

5.2.4 数据可视化

为了更直观、通俗易懂地呈现服务门户和工作门户统计分析的各指标业务内容，需要良好的数据可视化界面。通过对政务服务数据的分析和统计，从数据维度、应用维度、服务角度以及内部运维四个方面来实现数据结果的展示，为整个公安政务服务提供数据决策支撑，同时展示公安向数字政府建设过程所归集、开放和共享的数据资源，全面体现公安对数字政府建设的贡献。

5.2.5 升级公安外部信息资源汇集平台

公安外部信息资源汇集平台是沟通公安信息网与外部信息网，用于信息交互、信息汇集与共享平台。该平台目前尚有许多待完善的地方，主要有：同步能力不足;数据解析能力不足;并发访问性能不足，容易阻塞，导致数据延迟、丢失；不支持移动信息网和公安信息网之间服务按需合规互通；数据汇集与对接功能不够完善；监管与审计功能薄弱。因此需要具备以下能力，可在原有平台基础改造，也可重新建设，主要功能需求如下：

1、可随时侦测源端的状态，并形成报告和预警；对接边界平台，实现跨网域的数据接入、同步以及共享服务；

2、支持通过配置的方式注册资源提供方以及服务方的相关信息以及资源信息，尽量减少因软件配置支撑能力不足导致需大量进行个性化的代码级处理和开发工作；

3、支持不同形式的资源接入以及服务方式（主要包括库对库、文件服务、尤其是服务接口等三种方式）；

4、构建符合公安业务移动化规律和特点，实现移动信息网和公安信息网之间服务按需合规互通，满足移动应用对数据资源、服务接口等的跨网访问需求，应与上级级联实现联动；

5、提供跨网域访问代理能力，提供跨网域服务访问支撑，实现服务接口和数据资源的合规跨网调用、数据安全跨域共享，可应用于各类移动应用场景，实

现公安信息网和移动信息网之间跨网域的服务相互调用；提供跨网服务使用情况的监督、审计和运维管理。

6、主要性能：通过测试上传下载 1KB 文件，测试极限性能指标。具体指标要求如下：系统每笔交易的成功率需大于 99.94%；系统正常运行情况下，CPU 及内存资源利用率需小于 70%；在 HTTP 协议下，支持每秒处理交易量 5000 以上；跨网响应时间延迟<10ms; 跨网数据接口服务支持 100 万行单表有索引的数据请求响应时间不大于 5 秒；对外共享服务能够满足 200 用户的并发请求需求，基于跨网精确条件查询≤5 秒。

5.3 可视化大屏平台和定制服务

5.3.1 业务需求

为满足各业务单位轻量级应用建设、大数据智能化成果展示、态势分析及应急指挥演练等可视化搭建需求，通过提供统一的、灵活的、可快速构建的可视化工具，以便用户通过简单的拖拉拽等方式，利用大数据平台的数据服务、应用服务等，快速灵活支撑个性化应用构建和可视化大屏动态演示。

1、“零代码”开发，各部门或应用开发单位可以以线上可视化构建过程取代编码过程，零代码地形成部分前端页面，包括大屏展示页面等，如利用表格、平铺列表、图表、输入项等各种组件的组合构建常规的 SAAS 层应用页面。

2、“泛应用”构建，配合服务资源目录，以数据资源和服务知识促进应用组织，形成动态的应用能力。用户可通过服务资源目录申请查询检索、比对订阅等数据服务，以及电子地图、轨迹分析、关系分析等应用服务，或者通过建模平台构建模型后将模型计算结果进行集成展示，快速构建轻量级的应用。

3、“挖价值”分析，以丰富组件支撑对目标数据的交互钻取、统计分析、算法挖掘展示过程。

4、“可视化”展示，通过定制服务，展示大数据智能化不同业务单位主题的建设内容。

5、可视化展示页面需自适应大屏分辨率。

5.3.2 功能需求

能够基于海量多源数据和组件，通过拖拉拽方式提供应用页面、建模结果数据展示、大屏可视化构建等可视化页面建设功能，实现前端页面快捷构建和成果共享，避免传统前端大量的编码工作，提高开发效率，实现应用页面快速落地，最大程度地满足各业务单位和基层用户对大数据智能应用页面动态化、个性化、标准化的需求。

5.3.2.1 工作台

工作台是集构建、展示、分享的载体，需要拥有对外提供拖拽、配置形成目标页面(组件)的能力，能够支持将构建页面所需的组件、容器、布局拖拽至画布页面进行布局，根据页面显示内容和业务关注维度，选配适宜数据源或数据集，最终形成目标页面(组件)。根据业务需求、构建需要、场景分析等需求不同，包括页面工坊、组件工坊、菜单页构建等模块。

分类	功能项	功能需求描述
工作台	页面工坊	需提供一系列的基础的布局、组件、容器工具，根据业务需求，在图形化的画布界面上进行组合衔接；预览、查看其组件和各数据源之间的血缘关系，或导出页面源码。
	组件工坊	需提供普通组件、业务组件、混合组件构建功能，支持通过基本的元素组合、堆砌衍生出任何复杂组件。
	菜单页构建	需提供菜单页默认布局,支持自定义选择所需的页面布局，构建成新的布局方式，形成新的菜单页布局。
	可视化构建	需提供拖拽方式把所需的组件、布局、容器拖至画布当中，根据页面构建需求，自定义进行页面排版，支持基础信息录入展示；提供画布放大、缩小、资源拖拽、组件、布局、容器的拖拽和配置功能。
		需提供拖拽方式进行页面设计或布局编排，支持预览、导出源码、发布、保存等功能。
		需提供可视化展示和源代码展示切换,支持通过代码编辑同步更新展示页。
		需支持与建模平台、服务资源目录、数据资源目录对接，实现组件和数据源关联、数据传入参数配置、数据项配置。

5.3.2.2 页面中心

页面中心包含多种类型页面，满足应用页面构建、大屏可视化和建模平台模型结果展示等各种场景需求，主要包含用户本身历史构建的页面、平台用户放在共享池内的页面，用户可以对现存的页面进行修改或新建页面。支持页面分类查找、预览、编辑、收藏、删除、分享等功能。

5.3.2.3 素材中心

素材中心是对组件工坊、组件注册等多种渠道知识沉淀，并对素材中心进行统一管理，包含组件、布局、容器、数据源等素材，构建过程无感知沉淀海量素材。

分类	功能项	功能需求描述
素材中心	组件注册	需支持组件自定义设计，将一个以上的组件进行混合构建，形成新的组件，通过将新构建的组件注册到组件库后，对外提供服务。提供开源组件框架组件等第三方组件注册功能。
素材中心-素材库	组件	需提供卡片类、表格类、智慧搜类、图表类、地图类、媒体类、文本类、交互类等组件。
	布局	需提供通栏、单列、双边侧栏、三列、侧边栏等布局工具。
	容器	需提供 tab 容器和卡片容器，支持容器新增、导入、导出功能。
	临时组件	需包括封装后的业务组件和用户在构建页面时系统自动存储的临时组件。
	数据源	需支持浏览展示现有的数据源，支持导出/导入。

5.3.2.4 个人中心

作为个人资源管理，里面包含与个人有关的页面、素材、收藏和回收站，支持资源快速定位、搜索查找，快速应用于业务建设中，进一步提升工作效率，包括我的工作台、素材中心模块。

5.3.2.5 后台配置

后台配置主要是对容器、组件、布局工具等资源的统一管理、初始化设置以及权限的分配和平台操作查看。主要包括初始化库、权限配置、日志查看等功能。

5.3.3 定制服务

根据用户需求提供定制化大屏服务，包括整体策划、脚本、解说词，实地开发制作大数据智能化综合建设成效展示、警务云数字孪生、大数据全景看板、智能应用聚合展示以及一段不少于5分钟的宣传片。

5.4 非功能性需求

5.4.1 应用软件性能需求

本项目建设的各应用系统之间联系紧密，需要进行数据或功能的相互调用，所以应用系统的性能要求较高，在性能上应满足如下需求：

1、用户访问（内外网访问）

用户并发访问：>=1000。

2、响应性（内外网访问）

简单事务处理（如各类信息录入、修改、查询业务、主要页面等）平均响应时间：<=2s。

交互式研判工具平均响应时间：<=5s。

复杂事务或统计平均响应时间：<=10s。

3、可操作性

界面操作简捷、布局合理、提示及时，对于层次结构数据尽量使用树形结构，便于定位选取，展示数据的有效工作区最大化。

5.4.2 政务服务性能需求

为实现公安与其他政府部门高效协同能力，本项目建设的公安一体化政务服

务平台性能需求如下：

用户并发访问：>=10000。

响应时间：确定条件的简单信息查询响应时间≤1 秒。

跨多网的每笔业务的响应时间在≤3 秒，提供给企事业单位和个人的在线服务，要求响应时间在≤5 秒。

一般查询统计应控制在 10—60 秒；大型复杂的查询统计应≤10 分钟。

5.4.3 其他需求

兼容信创终端浏览器。

5.4.4 标准规范需求

全警全域应用体系建设需符合国家、公安部、省公安厅标准规范要求，包括：

GB/T 37721-2019 信息技术 大数据 分析系统功能要求

GB/T 38643-2020 信息技术 大数据 分析系统功能测试要求

GB/T 38672-2020 信息技术 大数据 接口基本要求

GB/T 38673-2020 信息技术 大数据 大数据系统基本要求

GA/DSJ 350-351 《公安大数据规范性技术文件》

第 6 章 信息安全建设需求

根据上级有关大数据安全体系规划和相关工作要求，建设大数据安全框架和“安全、可信、合规”的防御体系。

1、以提升风险发现能力、审计溯源能力、协同防护能力、闭环处置能力为重点，打造大数据安全管理中心。提供统一的安全门户，集中展示各类安全能力，对接运维、运营两体系相关安全资源，做到风险事前监测发现、上网行为事中监督、违规行为事后溯源。

2、构建市级零信任体系，打破旧式的“网络边界防护”思维，实现对内外部所有事物都不信任机制，重点解决认证不统一、权限分散且颗粒度大、日志采集

不全面且违规行为难发现、缺乏规范化的审批机制难追责等问题。主要搭建零信任体系认证、权限、审批、审计、环境感知五项服务，其中权限服务复用上级能力，实现多维度的身份认证、细粒度的权限管理、动态的审批监管、全面的业务安全审计和实时度量的环境感知。

3、以公安网现有的安全能力为基础，解决传统安全设备能力不足、性能不足等问题，加强终端安全、网络安全、数据安全、应用安全、边界安全、云平台安全等六维实体安全防护措施，实现安全能力换档升级。在充分利旧的情况下升级安全防护体系，结合云、网、端、数据、应用、边界等不同实体的安全特性，提出针对性强实用性高的安全技术措施，提升安全识别、安全防护、安全检测、安全响应等能力。

4、根据新一代公安信息网特点，搭建市级用户域与数据域之间的安全访问通道，支撑本地公安网用户安全可信地访问大数据智能化应用，为大数据安全提供新型的安全保障能力。整个访问的过程应用零信任的思想，实时检控应用访问请求，实现访问用户的身份可信，确保业务仅对合法用户提供服务；持续监测评估终端等环境的安全状态，实时分析网络流量及时发现网络攻击行为。

5、依托第三方专业团队技术力量，开展公安相关工作网络和应用系统漏洞扫描、渗透测试、安全驻场等安全服务工作，切实提升各类安全隐患的发现能力，加快处置响应效率。

6、▲确保本项目达到等级保护测评、国密测评以及边界测评要求，满足项目验收的硬性指标，且通过第三方检测挖掘现有体系存在的安全风险，及时夯实完善，提升网络安全防护水准。

7、坚持安全是为应用保驾护航的理念，在做好安全的同时，要确保安全所占用的资源不会影响应用的正常运行，所有安全设备在高并发、大数据量请求的情况下均可正常、稳定运行。

8、建立相关的安全管理机制。

6.1 安全管理中心

安全管理中心旨在形成新一代公安信息网安全业务的信息汇聚中心、安全分析中心、决策指挥中心，运用大数据技术汇聚各类安全数据，通过采集治理、综

合分析等手段，提升内外部风险感知能力、协同安全防护能力、攻击检测分析能力、违规行为发现能力、应急事件响应能力和态势感知预警能力。安全管理中心应满足以下需求：

1、需具备安全大数据全过程的处理能力，包括安全数据接入、安全数据预处理、安全数据组织、安全数据治理、安全数据服务、安全数据分析等，采集接入公安大数据安全应用所需的数据，形成统一的安全基础数据资源，为各类溯源安全应用的开发和运行提供数据支撑。

2、需具备安全事件溯源能力，通过采集分析各类安全数据，对公安信息网发生的病毒木马感染传播、设备违规外联、用户异常访问应用、数据库高危操作、网络攻击等安全场景进行溯源，追溯至安全事件源头设备 IP 地址等信息，关联出具体单位信息、人员信息，便于通报处置。

3、需全面提升安全协同能力，形成安全闭环处置。一是需与运维管理体系对接，将安全事件下发给相应的责任人，同时记录反馈、整改等情况；二是需与运营评价体系对接，完成安全类业务流程的前置审批，规范安全业务执行；三是需与本地零信任和安全防护体系相关资源对接，提升联动阻断的能力。

6.2 零信任体系

完整的零信任体系所依赖的身份认证与访问控制能力由认证服务、权限服务、业务审批服务、业务审计服务、可信环境感知服务及安全管理中心业务安全策略控制组成，整体上采用动态的访问控制技术实现。本项目建设具体包括认证服务、审批服务、审计服务、可信环境感知服务，权限服务复用上级资源。另外考虑到后期需根据上级相关工作要求，向上级上报相关数据，本期预留接口，以备满足上级考核要求。

6.2.1 认证服务

认证服务负责在全面身份化的背景下解决“你是不是你”的问题，即为大数据智能化应用提供统一的人员身份管理和身份认证，包括令牌管理、认证功能、用户管理、组织机构管理、日志管理、认证代理、上下级联动、外部服务联动等功

能。认证服务重点需要满足如下要求：

1、本级认证服务的用户信息、组织机构信息需与上级统一用户平台数据保持一致，定期更新，确保数据鲜活。

2、具备令牌的全生命周期管理，包括应用令牌和用户令牌的生成、撤销、更新、验证等。

3、认证因子需包括但不限于用户名密码认证、短信验证码认证、警务即时消息认证、数字证书认证等方式。

4、提供6000个指纹证书，支持国密算法，无缝兼容现有的PKI系统，并适配信创终端。

5、支持跨域部署，认证代理和认证服务分别部署在前置区和数据域，分别为不同区域应用提供认证支撑。

6、支持对组织机构、用户内容的管理，包括但不限于增、删、改、查、排序、批量导入。

6.2.2 权限服务

权限服务负责对权限进行维护，作为第三方独立于应用系统之外，提供统一精细化的权限管理，即解决“能不能看见和使用”的问题。考虑到权限服务复杂度和成熟度，本项目采用复用上级服务的方式实现应用级的权限管控。权限服务重点需要满足如下要求：

1、具备授权管理功能，核心支持在授权主体与授权客体之间建立映射关系，形成授权策略，实现应用级授权。其中，在授权主体的管理上，授权主体即将权限授予给谁，主体包含用户、岗位、机构、应用等。授权客体是指需要授予的具体权限资源，授权客体包含应用资源、功能资源、数据资源等。授权管理通过角色将授权主体与授权客体建立绑定关系，可将授权主体通过属性、机构、群组、组合等方式和角色建立映射关系，当属性、机构、群组、组合发生变化时，授权主体权限自动变更，实现授权主体到客体之间的动态对应策略。

2、提供鉴权服务功能，核心支持通过鉴权请求获取鉴权条件，依据鉴权条件动态返回鉴权结果。即用户访问时，无感知地向鉴权服务传递令牌信息，鉴权服务对令牌的内容、有效性、完整性进行校验，对于验签不通过或未按要求携带

签名信息的鉴权请求不予鉴权。验签通过、令牌合法的情况下，返回鉴权结果，就可以访问相应的资源。

6.2.3 审批服务

审批服务解决“发起高敏数据访问行为的原因是什么”的问题，主要负责用户在侦查办案、警情处置过程中需查询高敏数据访问时，要求前置审批，只有通过审批后，才能访问相应高敏数据资源。审批服务重点需要满足如下要求：

1、支持自定义审批机制（原则上为两级审批机制，可响应用户特殊情况下自定义审批层级的需求），针对已立案的实行一案一审批，针对未立案的实行一线索一审批的工作要求。

2、根据数据资源和实际情况，支持自定义审批表单配置，且审批服务可根据业务单位需求随时开启或关闭，以满足业务单位差异化需求。

3、用户可通过公安网 PC 终端和移动警务终端 APP 进行审批操作，提升审批效率。

4、支持创建与管理代理审批人，用于代理审批工作开展，形成快速响应机制。

6.2.4 审计服务

审计服务负责接收零信任体系各服务的日志、大数据智能化应用日志和其他日志，重点解决违规使用发现的问题。并对用户访问敏感数据、执行关键操作行为等各类业务日志进行真实、全面的记录，实现多方面日志数据的采集、汇聚，提供基础的异常行为分析、发现、告警和处置的能力，尤其是审计分析敏感数据查询、异常访问等操作。包括但不限于：

1、提供零信任认证、权限、审批、审计、环境感知日志采集标准，确保各服务日志统一性和完整性。

2、提供策略配置规则，通过数据分析并构建分析模型，对用户异常行为进行分析研判。

3、具备对审计日志以及预警信息进行人工和自动处置的能力，包括告警、通报、核查、反馈等。

4、日志审计，支持向审计人员提供日志查询、检索以及统计分析等功能，为异常行为的预警处置提供决策依据。

5、应用日志的字段、信息等需满足公安机关应用日志采集相关规范要求。

6、支持前端动态审计及管控、外部服务联动。

6.2.5 环境感知服务

环境感知服务负责对终端身份进行不可仿冒标识，对终端环境进行感知和度量，即解决“环境怎么样”的问题。环境感知服务应具备生成终端身份标识、系统环境感知与度量、物理环境感知与度量、安全配置风险感知与度量、安全环境感知报告等功能。

1、环境感知客户端支持物理 PC 机和桌面云部署，支持 32 位和 64 位操作系统安装，通常情况占用的 CPU 和内存资源不得过高，运行过程中不得影响其它应用和系统软件的正常运行。

2、允许管理员自定义感知策略、感知内容、风险等级、评分规则、执行频率等。支持对可信环境感知客户端上报的环境感知结果进行综合分析和风险判定，并对终端环境状态和风险报告进行统一展示和呈现。

3、环境感知系统需具备各类监测能力，包括服务监测、注册表监测、弱密码监测、共享资源监测、高危端口监测、程序运行监测、漏洞补丁监测、杀毒软件监测、FTP 行为监测等。

4、支持多种环境的风险评估，包括硬件配置变化风险、网络环境及变化风险、系统账户风险、安全配置风险、恶意代码风险、系统关键对象风险、浏览器风险、系统环境风险、物理环境风险等，尤其需支持通过配合摄像头来评估授权人离席、屏幕拍照等环境风险。

5、能够对终端风险进行评估和分析，并能综合计算出终端可信状态，支持对接可信检控点和安全管理中心业务安全策略控制服务。

6、本项目需提供至少 1000 个终端可信环境感知许可。

6.3 安全防护体系

安全防护体系包含安全识别、安全防护、安全检测、安全响应等四种服务能力。本项目通过部署各种软硬件安全产品，分别作用于网络、终端、应用、数据、云平台、边界等六维实体，初步形成安全防护体系基础安全能力，实现对各实体的基础安全防护，确保其能有效应对大数据架构下的新型突出网络安全威胁。随着安全形势的变化，不断完善安全防护体系的服务种类。

6.3.1 网络安全防护

网络安全防护核心是强化网络基础安全措施，应对标上级考核要求，建立安全监测手段，及时发现安全风险，主要包括如下：

1、提升新一代公安信息网用户域网络入侵检测能力。通过部署专业的入侵检测系统，检测专网内核心流量，整体监控流量不低于10G，针对其中的蠕虫病毒、木马控制、高级威胁及感知设备的重放攻击、漏洞利用等网络攻击行为，进行检测并予以告警。

2、提升新一代公安信息网用户域网络流量分析能力。通过部署专业的流量分析系统，实时监控网络性能，并自动定位、告警相关故障，填补现网流量分析、数据挖掘和回溯分析能力不足的问题，检测端口扫描、异常访问、网络攻击等情况，及时通过流量分析发现安全事件线索，预警并通报流量安全威胁。整体分析流量不低于40G。

3、提升新一代公安信息网用户域网络违规外联监测能力。通过部署专业的网络违规外联监测设备，基于网络嗅探和网络报文综合分析，对公安信息网网内私搭WIFI/MiNiWIFI、便携式网卡透传、办公终端同时连接互联网和专网等行为，进行监控并予以告警和阻断。支持15万个IP资产的违规外联发现。

4、提升新一代公安信息网用户汇聚节点和数据汇聚节点网络访问控制能力。以双冗余、异构方式部署下一代防火墙，实现用户域与数据域的网络访问控制，且开通网络访问策略，需严格落实审批程序，确保先审批后开通。

5、提升互联网上网行为管控能力，在互联网出口处部署安全设备，引入多元化的认证方式，理清互联网资产台账，做到规范化、实名化的上网管理。

6、提升新一代公安信息网用户域网络准入能力，实现对入网终端设备的准入控制，可通过证书、IP/MAC 地址绑定等一系列技术手段，确保非授权终端不能入网使用。

7、提供攻击诱捕能力，实现对用户接入网络的攻击行为进行诱捕，并支持将相关情况传递至安全管理中心，实现对攻击行为的进一步分析。

8、提供网络漏洞扫描能力，针对网络、主机、数据库、中间件、WEB 扫描等，根据漏洞扫描结果提供人工分析，给出分析结果和修复方案或建议，并通过对接运维平台进行派单。

6.3.2 终端安全防护

终端安全主要从可信环境感知、违规外联、病毒防护、外设管控等方面开展：

1、提升公安信息网终端安全状态环境感知能力，实时采集分析终端的各类数据，综合形成终端安全状态评分，且安装环境感知客户端后不能影响终端使用。

2、支持内网终端违规行为监测，重点针对计算机设备的“一机两用”“两网互通”行为进行实时监控和阻断。

3、支持对内网终端病毒、木马、恶意软件等进行扫描查杀，及时清除终端安全隐患。

4、具备终端外设管控能力，限制终端外接 U 盘、移动硬盘等行为，严禁违规接入和使用外设。

为了确保在实现终端安全防护的情况下，应用仍能正常使用，对终端安全防护的实现突出以下要求：

- 终端客户端性能要求。终端客户端应充分考虑终端现状，系统资源应尽可能少占用，内存占用应小于 500MB，非执行特定检查要求时 CPU 占用率小于 5%。注：以上要求包含客户端程序及客户端程序的运行环境的总和。
- 终端客户端兼容性要求。终端客户端应充分考虑终端操作系统种类繁多，从 WinXP 到 Win10 全系列操作系统版本。客户端需全面支持以上操作系统，包含但不限于 32 位、64 位的大的分类，并且针对单个版本的 Windows 版本内的家庭版、专业版、企业版、核心版等等版本全部支持。由于此平台还涉及应用准入，所以客户端不仅需要支持以上终端操作系统同时还需要支

持 Windows2003 以上的服务器操作系统（版本要求同终端操作系统版本），还需要支持信创操作系统。

6.3.3 应用安全防护

应用安全方面需求如下：

1、应用日志采集。建设应用日志采集系统，满足日志采集上报要求，支持对网络流量数据进行解析和提取，实现对本地应用系统的日志采集分析和处置管理，满足日志数据实时上报或准时上报至上级安审平台，保障应用的安全访问。主要具备以下功能：数据采集、数据过滤、数据解析、日志数据提取、形成操作日志等。

2、应用身份认证。针对新上线的应用系统，统一对接本项目中零信任体系认证服务，根据应用的种类和重要程度配置不同的认证因子，解决多场景人员身份问题。

3、应用访问控制。根据用户所属组织（岗位）、角色等身份属性，并且结合案事件审批机制，进行权限分配，实现业务应用细颗粒度的访问控制。

4、应用攻击防护。针对应用攻击行为的安全防护，主要包括 WEB 攻击防护、防网页爬虫和应用层 DDoS 攻击防护等内容，支持不少于 300 个应用站点防护。

5、应用国密改造。提供符合国密要求的密码机、云密码管理平台等密码设备，提供 SM1、SM2、SM3、SM4 等标准国密算法，支撑核心应用开展国密改造工作，满足国密测评的相关要求。

6、应用日志审计。应用系统自身需做好日志审计，包括详细用户访问审计和管理员操作审计，并按照上级规范要求的标准格式输出，统一报送至零信任体系业务审计服务。

7、应用水印功能。针对存在较为敏感数据的应用系统需提供水印功能，为截屏、截图等操作泄露重要数据的行为提供溯源支撑。

8、应用终验前检测。结合实际情况，增加安全审核和检测流程，提升应用系统自身的安全性和稳定性。

6.3.4 数据安全防护

1、数据库审计。针对新一代公安信息网前置区和数据域两侧重要数据库（如原始库、资源库、主题库、业务库、知识库、索引库）、移动警务相关网络的数据库，开展数据库细粒度操作行为的审计，通过深度识别和立体分析，识别异常登录、爬库删库等危险行为。数据库审计具备以下功能：

（1）支持多种类型数据库

同时支持但不限于 Oracle、MS-SQL、DB2、MySQL、HBase、MongoDB 等。

（2）深度探测

支持嵌套、函数、绑定变量、长语句、返回结果、脚本等复杂操作和隐秘操作审计，精确防范各种危险操作行为。

（3）识别 SQL 注入攻击

内置丰富的 SQL 注入规则库和高效解析算法，可通过对 HTTP、SQL 语句两个层面解析，准确检测各种 SQL 注入攻击行为，弥补 WEB 应用防火墙的不足。

（4）审计记录检索

利用全文检索技术，通过任意关键字实现少量审计记录快速高效检索。

（5）多维度报表

内置特权操作、异常分析、访问源等多种报表类型，同时支持多条件组合自定义报表生成。通过多维度报表的统计分析，可快速准确发现潜在安全威胁。

2、数据全生命周期的安全。针对数据采集、数据接入、数据处理、数据治理、数据组织、数据服务各个阶段，提供差异化的策略和措施保障数据安全。

（1）数据采集：支持对大数据平台数据采集设备进行认证和识别，并能够对重要数据进行加密，以此保证数据采集过程的安全性；

（2）数据接入：存在对账机制，可以对数据提供方和数据接入方的完整性、一致性、正确性进行核对和检验；

（3）数据处理：数据处理的整个过程中，强化数据资源库账号的安全管理，防止账号被泄露，保障数据的安全；

（4）数据治理：对数据库和数据文件系统的操作过程，进行细粒度记录和管理。另外支持对运维和测试数据进行脱敏操作，最大程度保障高敏数据不外流；

（5）数据组织：按照业务需求建立各类原始库、业务库、主题库等，针对

需共享的数据资源建立共享库，并按照最小化原则开放数据权限。针对关键敏感的数据开展加密操作，保障数据存储安全；

（6）数据服务：需支持通过数据层接口提供数据服务，根据用户属性、数据属性、数据操作行为配置数据访问权限策略。在应用服务调用数据服务之前，需验证应用服务身份，确保合法性。

6.3.5 云平台安全防护

云安全是大数据智能化安全体系重要组成部分，主要承担云平台自身安全能力，以及对云上各用户及应用的安全提供保障和支撑。

云平台包括两个部分，分别部署在新一代公安网前置区和数据域，两侧云平台安全具体需求如下：

1、需实现云主机安全，应通过对云主机进行安全加固，定期对主机系统配置进行安全审查，包括弱口令检测、配置检测；全面监测异常登录、文件异常、系统后门、进程异常等。支持入侵监测、主动防御。

2、需实现云网络安全，对云平台南北向流量和东西向流量进行安全访问控制，确保云内网络运行的安全性。重点利用防火墙、VDC、VPC、Vlan 划分等技术，使云平台物理服务器和云上虚拟主机按照最小原则开放网络访问行为，收缩访问路径，并通过防火墙对访问流量进行过滤及安全防护。

3、需实现云应用安全，应利用 WEB 安全访问控制、WEB 安全防护、恶意代码防范、网页防篡改等，防止 WEB 攻击、网页爬虫等，为应用访问提供安全环境。

4、需实现云存储安全，应利用多副本冗余、数据加密等机制，保障云存储安全可靠；对重要业务系统或数据，采用加密方式，防止数据泄露。

5、▲需提供云密码服务，即需在数据域、前置区的云平台分别部署国密密码机、云密码管理平台等密码设备，为本项目提供统一的密码服务。

6、云内安全的组件主要为云服务的方式部署，需做到合理消耗计算资源控制。

6.3.6 边界安全防护

边界接入平台需求主要包括两部分，一是新建新一代公安信息网前置区与数据域边界平台，二是升级扩容外部网络至新一代公安信息网前置区边界接入平台，包含党政军接入链路、企事业接入链路、互联网接入链路，本项目提供的各类隔离设备需支持纳入统一安全管理。具体需求如下：

1、建设新一代公安信息网前置区至数据域专用数据安全交换通道，支持格式化文件摆渡，最大支撑带宽不低于4Gbps，满足前置区与数据域之间的数据交换需求。

2、升级扩容党政军接入链路，将原有的千兆链路升级为万兆链路，支持格式化文件摆渡，最大支撑带宽不低于4Gbps，满足新一代公安信息网前置区党政军业务接入需求。

3、升级扩容企事业接入链路，将原有的千兆链路升级为万兆链路，支持格式化文件摆渡，最大支撑带宽不低于4Gbps，满足新一代公安信息网前置区企事业业务接入需求。

4、升级扩容互联网接入链路，将原有的千兆链路升级为万兆链路，支持格式化文件摆渡，最大支撑带宽不低于6Gbps。同时支持多套单向隔离通道资源的动态调度和统一管理，满足新一代公安信息网前置区互联网业务接入需求。

5、实现集中监控与审计、统一调度、统一边界管理。

6.4 安全访问

6.4.1 单位内部人员访问需求

根据新一代公安信息网架构特点和要求，需在用户域和数据域之间搭建一条用户安全访问通道，用于支撑用户安全可信访问数据域应用业务，适用于本地用户访问本地应用、异地用户访问本地应用、本地用户异地访问本地应用场景。其中，针对异地用户访问本地应用时，前置区应用均对外开放，而数据域应用不对外开放，特殊情况需向相关部门申请单独开通；针对本地用户异地访问本地应用时，前置区应用可正常访问，数据域应用访问应向相关部门申请安全资源，根据

其使用时间长短的不同需求开通不同的资源，如虚拟桌面、环境感知服务等。整个用户访问通道应用零信任的思想，具体需满足的安全能力如下：

1、具备用户接入安全能力。用户访问应用前首先通过零信任体系中的认证服务进行身份认证，访问过程中应对用户身份合法性进行持续校验，确保用户身份可信。同时针对 PC 终端利用零信任体系的环境感知服务感知实现接入终端的安全状态评估，确保终端安全可信，实现安全接入。

2、具备虚拟桌面能力。用户访问数据域高敏应用时，必须采用虚拟桌面技术访问桌面云，提升敏感数据防护能力，确保敏感数据不出数据域。虚拟桌面需对接本地零信任认证服务，支持通过可信接入检控登录使用，包括虚拟桌面令牌的颁发和校验。

3、具备访问控制能力。在网络访问控制层面，需利用用户汇聚节点和数据汇聚节点部署的下一代防火墙，实现安全访问相关的网络访问控制，使各组件只能访问授权的网络资源。在应用访问控制层面，需通过零信任体系对用户身份、应用身份进行统一验证，并引入可信接入检控点和可信应用检控点。在功能访问控制层面，由各个应用系统自身根据用户角色实现功能级控制。在服务访问控制层面，需通过服务实际挂接的系统实现服务级的权限控制。

4、具备应用攻击防护能力。利用安全防护体系云平台设计的 WEB 防护系统提供应用安全防护服务，检测并阻止攻击行为。

5、具备网络安全检测能力。在用户访问通道内建立专项安全检测区，部署网络入侵检测系统和网络流量分析系统，实时采集、分析用户访问网络流量，及时发现网络攻击行为。

6、具备日志采集能力。通过部署专门的日志采集系统，采集应用访问过程中设备的安全日志、告警等数据，并统一发送至安全管理中心。

6.4.2 合作企业人员访问需求

针对运维用户安全访问，包含第三方合作企业、运维人员、开发人员、测试人员等，应满足以下需求：

1、需构建专门的运维人员访问通道，实现移动信息网、新一代公安信息网的安全运维。即利用堡垒机建立基于唯一身份标识的全局实名制管理，实现统一

账号管理策略，对运维人员基于最小权限原则进行精准授权，实现集中精细化运维操作管控与审计。

2、针对开发测试人员使用数据的要求，提供数据脱敏能力，将敏感数据通过脱敏规则进行数据变形后，从生产数据库同步到开发测试的数据库，确保开发测试人员无法泄露真实业务数据。

3、提供第三方合作企业人员特权账号管控能力，及时发现未纳管账号、后门账号、僵尸账号和违规提权账号；需持续对特权账号的活动进行监控，全面了解特权账号活动相关的时间、操作者、事件内容。

4、实现对所有运维用户的操作监管和安全审计，全面监测并阻断窃取数据、篡改资料、非法查询、破坏系统等安全风险，防止相关安全事件发生。

6.5 安全业务统一门户

安全业务统一门户向安全决策者、安全管理员（警员）、安全服务人员（企业人员）提供安全态势展示服务、安全业务管理服务，根据不同角色对应不同的功能界面，支撑不同类型用户开展安全工作。

1、为安全决策者提供安全态势展示界面，全面展现新一代公安信息网的安全态势及安全风险预判，包括资产态势、威胁态势、脆弱性态势、安全事件态势等。可视化呈现网络安全事件发生情况，使安全决策者可直观感受整体安全能力现状与安全风险趋势，为安全管理决策提供支持。

2、为安全管理员提供安全业务管理界面，包括安全资产管理、安全模型分析管理、风险告警信息管理、系统权限配置管理、日常系统运维管理等，帮助安全管理员理清全网安全资产，及时发现各种攻击威胁、行为异常、安全风险等，可以对攻击路径、手段进行快速判别与溯源，并进行有效的安全决策和响应。

3、为安全服务人员提供特定的安全业务管理界面，包含安全数据管理、安全风险人工研判等，便于安全服务人员根据业务需要，集中对数据进行统计、分析、规律性探索、预测、人工研判，协助安全管理员进行安全决策与响应，使安全决策更加有效。

6.6 其他安全服务

6.6.1 驻场安全保障服务

提供4人驻场安全保障服务，服务期不少于1年，主要包括工作现场技术支持、设备基础运维、运维值守、建立新一代公安信息网安全管理体系、网络安全检查及网络安全事件排查与处置、推进等级保护工作、协助开展保密检查、提供重大安保服务等，具体要求如下。

1、现场技术支持：故障诊断及故障点定位、故障处理；

2、设备基础运维：针对新建基础设备的运维保障工作，包括但不限于设备巡检、监控检查、问题故障解决等。

3、运维值守：提供专业的现场值守服务，保证各个系统的正常运转。重要时刻现场值守期间，每日按巡检记录表对相关部位进行巡查登记，保证重要时刻设备稳定运行。如出现预警、故障情况，及时向相关主管人员报告，启动预警或故障处理流程。

4、配合建立新一代公安信息网安全管理机制：成立安全通报与响应工作小组，落实安全问题发现、通报、处置全流程管理，协助编制网络安全管理制度、编制安全运维规范、开展网络安全培训等。形成全局安全整体把控机制，对提交的安全建设方案，进行综合性评估并给出修改意见。并根据实际需求，对安全厂商进行安全考核。

5、网络安全检查及网络安全事件排查与处置：协助完成上级要求的网络安全工作，包含年度网络安全检查、重要系统安全漏洞排查等。同时，完成安全事件的排查与处置工作。

6、协助推进等级保护工作：协助落实等级保护工作，编制工作方案、方法和流程等。同时，全面排查梳理，详实掌握各类公安业务信息系统建设应用底数，完成等级保护定级备案工作。

7、协助开展保密检查等工作：协助开展内部保密教育、保密检查等工作；制定检查方案，严格、细致地开展检查工作；对保密制度建设、非密计算机保密管理等情况进行自查等。

8、驻场人员进行阶段性技术服务情况汇报，并提交汇报材料，包括该阶段

所发生全部服务内容的执行情况、下一阶段的维护服务计划等。

9、配合开展应急演练，具体开展次数、开展时间和内容可根据用户实际需求进行调整，如针对网络中断、黑客攻击、大规模病毒攻击、数据库系统故障、设备硬件故障、应用系统相关故障开展应急处理。

10、提供重大安保服务，包括重大节假日、大型活动、公安等级勤务期间的安全服务保障。主要从以下方面开展重大安保服务：

（1）编制重大安保安全保障方案；

（2）落实重大安保期间安全措施，包括重要设备安全检查、核心网络流量分析、入侵检测、7×24 小时的现场值守以及 7×24 小时的应急响应；

（3）输出重保总结报告，不限于相关保障方案、应急预案、问题处置跟踪记录、责任人分配表等。

6.6.2 漏扫及渗透测试服务

提供专业性渗透测试服务，针对相关工作网络、应用系统进行漏扫及渗透测试，并形成测试报告，提供不少于 1 年服务，其中漏扫服务不限制次数，渗透测试服务不少于 4 次/年。

类别	内容
服务方式	漏扫工具、渗透工具和人工方式
服务周期	不少于 1 年服务周期，其中漏扫服务不限制次数，渗透测试服务不少于 4 次/年
服务范围	新一代公安信息网核心主机操作系统、数据库系统、WEB 应用系统、边界等
服务成果	《XXX 漏洞扫描报告》《XXX 渗透测试报告》
预期效果	及时查找出专网中可能存在的薄弱点，及时修复
评价指标	全年开展服务次数及服务质量

6.6.3 互联网网站云防护服务

对 10 个互联网网站提供以下服务，服务期不少于 1 年。包括远程网站漏洞扫描服务、远程网页挂马实时监测服务、远程网页敏感内容监测服务、网站可用

性监测服务、网站域名解析监测服务、钓鱼网站监测服务、远程网页篡改监测服务、安全通告、安全预警等，具体要求见下。

1、远程网站漏洞扫描服务：对互联网网站定期进行安全检查，能够识别WEB应用漏洞，并且定位WEB应用漏洞所在的位置，提供合理的解决建议。

2、远程网页挂马实时监测服务：对互联网网站进行检测，判别网站页面是否存在挂马，准确定位网页挂马所在的位置。发现网站被挂马后及时告警并处理。

3、远程网页敏感内容监测服务：对网页中出现的敏感内容进行监测，判断页面是否存在敏感内容，如内网IP地址信息、数据库信息、网站调试信息、网站目录浏览、WEB服务器路径泄露、电子邮件地址信息、不安全的Flash参数配置，若发现敏感内容及时告警并处理。

4、网站可用性监测服务：对服务站点进行可用性监视，跟踪重点对象的访问情况，判断网站是否被拒绝服务攻击，并根据严重程度及时告警并处理。

5、网站域名解析监测服务：对被监控域名在各省主要运营商DNS服务器及授权域名服务器的域名解析情况进行监控，如发现异常及时告警并处理。

6、钓鱼网站监测服务：对钓鱼网站进行监测，发现钓鱼网站后及时告警并处理。

7、远程网页篡改监测服务：对检测目标站点的页面情况进行监测，当网页篡改发生时及时告警并处理。

8、安全通告：定期搜集主流操作系统、产品、应用软件等厂家发布的漏洞补丁信息和安全资讯，帮助了解当前网络安全状况，及时采取应对措施。

9、安全预警：对应用程序、开发框架等相关的高危漏洞以及安全事件进行监控，当发生安全威胁时及时告警并处理。

类别	内容
服务方式	引入第三方平台远程防护
服务周期	不少于1年
服务范围	远程网站漏洞扫描服务、远程网页挂马实时监测服务、远程网页敏感内容监测服务、网站可用性监测服务、网站域名解析监测服务、钓鱼网站监测服务、远程网页篡改监测服务、安全通告、安全预警等
服务成果	《XXX服务报告》
预期效果	及时查找出互联网网站中可能存在的薄弱点，及时修复
评价指标	全年开展服务次数及服务质量

6.6.4 利旧设备续保服务

对现有在用边界平台已过保设备进行例行巡检和预防性维护，及时发现设备运行中出现的隐患，并进行相应的处理，以减少设备发生故障的概率，保证设备的稳定运行。设备续保服务，包括设备维修、系统维护产生的费用。维保服务周期不少于1年，详细维保设备如下。

序号	设备名称	数量	设备用途
1	单向传输系统	1套	互联网边界单向传输系统（外到内）
2	数据交换系统	1套	企事业边界数据传输系统
3	单向传输系统	1套	互联网边界单向传输系统（内到外）
4	数据交换系统	1套	党政军边界数据传输系统
5	数据交换系统	1套	企事业边界数据传输系统

6.6.5 等保测评服务

本项目需达到等级保护测评要求，具体见《信息安全技术网络安全等级保护基本要求》。本项目建设期内，每年需完成前期建设的大数据平台三级等级保护测评服务；项目完成后配合第三方测评机构开展等级保护测评工作，包括定级、备案、测评、安全建设、监督检查等。

6.6.6 国密应用安全性评估服务

本项目关键业务系统需达到国密测评要求，具体见《信息系统密码应用基本要求（GB/T 39786—2021）》。项目完成后配合采购人聘请的第三方国密测评机构开展国产密码应用安全性评估工作。

6.6.7 边界测评服务

本项目实施的边界平台部分需满足公安部边界测评要求。项目完成后，需聘请第三方测评机构对公安信息网边界链路进行测评，并出具测评报告，通过测评后方可交付使用。

6.7 安全要求

1、通报响应要求：须在安全通报要求的时限内，响应并完成安全事件、系统漏洞等情况处置。发生紧急突发重大安全漏洞或安全事件的，须在24小时内提供有效处置方式。

2、网络安全预警要求：发生任何网络攻击、病毒、木马、蠕虫、漏洞、暗链以及各种违规操作等，系统须立即发现并在24小时内溯源。

3、安全通报要求：如有网络安全问题，安全服务提供方须第一时间发现相应问题并报告采购人。

4、安全事故处置要求：发生任何网络安全问题（非本项目提供的安全设备和服务导致的安全事故除外），皆不得导致应用系统无法正常工作1个小时以上。如整个虚拟化平台（大数据）出现安全问题，不得导致与虚拟化平台（大数据）相关的3个以上（包括3个）的应用系统无法正常运行。重要活动或敏感日期，不得因安全服务不到位导致发生重大安全事件或严重安全事件。

5、安全检测要求：对管理方组织的安全检测对抗，须在24小时内发现并溯源。

6.8 安全性能需求

序号	板块名称	细项名称	性能指标
1	整体要求	风险发现指标	支持发现已知和未知终端的木马蠕虫、恶意软件、勒索病毒等。
2			支持发现安全漏洞（包括最新的0DAY安全漏洞），包含但不限于终端漏洞、数据库漏洞、系统漏洞、WEB漏洞，如DBMS漏洞、权限提升漏洞、SMB远程执行漏洞、3389远程漏洞执行漏洞、redis未授权访问、MSRPC漏洞、MySQL系统漏洞、Apache Tomcat 安全漏洞等。
3			支持发现应用攻击行为，如WEB攻击、应用层DoS攻击等
4			支持发现网站恶意行为，如SQL注入、执行恶意代码、异常上传文件、XSS与Cookie篡改、网页挂马等。

序号	板块名称	细项名称	性能指标
6			支持发现用户异常登录行为，如非法时间登录、非常用登陆地登录等。
7			支持发现用户异常访问行为，如超越权限访问、绕过安全防范手段对应用和数据访问、非法时间访问、违规访问等。
9			支持发现数据库异常操作行为，如拖库、爬库、删库、越权访问等。
10			支持发现数据库攻击与入侵行为，包含MS-SQL、Oracle、MYSQL 等常用数据库。
11			支持发现违规外联行为，如私自搭建的连接互联网等外部不受控网络的网络边界和通道；私自搭建网中网（NAT 网络）、网闸、私网代理服务器等；便携式热点、WIFI/MiNiWIFI、便携式网卡透传等。
14			支持通过流量回溯，发现 TCP SYN 风暴、TCP 拒绝连接、TCP 端口扫描、ARP 广播风暴、DDOS 攻击等。
16			支持发现黑客攻击行为，如定向探测、暴力破解、口令猜测、主机扫描、恶意扫描、端口试探、敏感端口扫描、漏洞利用等行为。
18		安全溯源指标	支持内网病毒木马感染传播、设备违规外联、用户异常访问应用、数据库和中间件高危操作、网络攻击等多类安全场景的溯源。
19			平均溯源通常应在 20 分钟内完成，特殊情况（如分析体量庞大、完全未知新型威胁等）除外。
20	安全管理中心	访问性能	支持 100 用户并发访问，页面响应时间低于 1.5 秒。
21		对接要求	支持对接运维平台、运营平台、零信任体系和安全防护体系相关安全资源。
22	零信任体系需求	认证服务	支持无上限用户规模
23			支持 3000 并发用户使用
24			支持的认证方式不低于 4 种，包括用户名密码、短信、警务即时消息认证、数字证书。
25			6000 个指纹数字证书
26		审批服务	最大支持用户在线 300 个
27		审计服务	审计存储不低于 97TB
28		环境感知服务	支持至少 1000 个终端授权
29	安全防护体系需求	网络安全需求-网络入侵检测	监控流量不低于 10G
30		网络安全需求-网络流量分析	用户安全访问分析流量不低于 40G
31			用户域分析流量不低于 20G

序号	板块名称	细项名称	性能指标
32		网络安全需求-网络违规外联	支持 15 万个 IP 资产的违规外联发现
33		网络安全需求-网络访问控制	最大吞吐量不低于 20Gbps
34		终端安全需求-可信环境感知	支持至少 1000 个终端授权
35		应用安全需求-应用攻击防护	支持不少于 300 个应用站点
36		数据安全需求-数据库审计	支持通用数据库、大数据库审计
37		云平台安全需求-主机安全加固	支持对所有虚拟主机和物理主机的安全加固（不少于 1000 个 license）
38		边界安全需求-新一代公安信息网前置区至数据中心专用链路	最大支撑带宽不低于 4Gbps
39		边界安全需求-党政军接入链路	最大支撑带宽不低于 4Gbps
40		边界安全需求-企事业接入链路	最大支撑带宽不低于 4Gbps
41		边界安全需求-互联网接入链路	最大支撑带宽不低于 6Gbps
42	安全访问通道需求	使用用户访问需求	最大支撑带宽不低于 1Gbps
43		运维用户访问需求	设备管理授权不低于 1000 个
44	安全管理需求	安全通报管理需求	用户并发数不低于 100
45			业务响应小于 1 秒
46	安全服务需求	驻场安全保障服务需求	驻场人员 4 人，周期不少于 1 年
47		漏扫及渗透测试服务需求	每年提供无限次漏洞扫描和溯源服务，渗透测试服务不少于 4 次/年
48		互联网网站云防护服务需求	对采购人 10 个互联网网站提供服务，服务周期不少于 1 年
49		利旧设备维保服务需求	服务周期不少于 1 年

第 7 章 运营运维需求

建立统一、标准的运维服务规范制度，规范提供服务内容，明确相关服务组织或人员的责任范围、服务内容、操作规程及协作方式，统一服务受理、监控巡

检、机房管理、资源管理、例行服务、响应式服务、故障处置、通信保障等工作标准，并结合实际在工作中不断改进和优化，提高运维质量和服务水平。

建立统一、集中的服务运行、监控和受理中心（服务台），通过统一服务号码和服务门户，将分散的服务受理渠道和值守人员集中起来，统一受理所有的服务和故障申请，并提供工单派发、任务处置、流程跟踪、信息反馈及数据分析等服务支持工作。梳理组织机构及职责划分，规范一体化运维管理中各个参与要素（人员、流程、工具）的管理制度与工作流程，确保服务效率和质量满足服务级别协议。

建设一体化运营运维服务技术系统，实现信息系统运营运维服务统一监控、统一申请、统一受理、集中办理、统一反馈、全流程监督和智能运维、数据可视等。

7.1 基础设施运营机制

配合制定整个基础设施的运营机制。

7.1.1警务云资源使用管理

针对警务云 IPDS 四层资源依法依规使用管理要求，明确资源的统一调配、逐级管理、分级审批、服务实战、安全保密等使用管理原则。

7.1.2警务云基础设施资源使用管理

在警务云资源使用管理规定机制下，细化明确警务云基础设施资源使用要求，达到最大效率的使用资源，避免资源浪费。

7.1.3各业务应用上云指南

为促进用户各业务单位的业务应用按照分层解耦的云化架构新建或迁移上云，支撑用户各业务单位集约化建设和融合式发展，制定上云指南，明确分层解耦架构、方式、要求等。

7.2　数据资源运营机制

7.2.1数据治理流程机制、成效评价管理

为明确大数据管理职能单位、各业务单位、相关治理厂商，以及前置区和大数据平台的工作职责和合作机制，从数据治理流程和数据治理需求、处理与反馈等方面进行全流程管理，需制定数据治理共建工作机制。

7.2.2数据质量评估标准和管理

从完整性、一致性、准确性、及时性、唯一性等评估维度，对数据采集汇聚、接入、处理的全流程质量评估管理，实现事前、事中、事后数据质量监测、处理、反馈的统一管理，按照采集和治理工作职责，推进数据质量提升工作。

7.2.3数据申请和使用管理

明确数据资源分级分类及大数据管理职能单位、各业务单位管理职责，从数据资源申请、审批、使用流程等方面进行规范化管理，确保大数据平台各类数据资源使用的合法、合规。

7.3　服务应用运营推广及评价管理

7.3.1服务使用评价及淘汰

从数据应用服务的热度、稳定性、用户使用评价等维度，对服务评价标准及淘汰进行管理，通过对每类数据开展数字化、可量化、动态化的评价，实现对每类数据应用服务的评分，及时淘汰、删减不稳定、不可用的数据应用服务。

7.3.2应用评价管理

为保障大数据应用建设有序健康发展，搭建公平、公正、竞争的良好生态环境，引入更多优质合格厂商共同参与大数据应用建设，构建“百花齐放”式业务应

用，从技术架构、应用性能、安全机制、战果成效、用户体验等对应用进行评价管理。

7.4 资源运营服务平台需求

按照公安大数据“一切资源化、资源目录化、目录全局化、全局标准化”的要求，建设资源运营服务平台，将大数据智能化各类资源进行统一运营管理，服务各层级用户，作为公安云计算、大数据、安全等平台的服务中心及服务流程管理平台，通过运营服务中心汇聚各平台服务能力，包括资源服务、数据服务、应用服务、安全服务，并面向服务使用方提供服务，同时借助运营服务流程规范各平台的服务过程，提升全局运营服务全生命周期的管理能力，服务使用方通过服务目录申请服务，服务提供方审批服务申请工单，将服务指令传递至云平台、大数据平台、安全服务平台进行服务开通，资源运营服务平台将服务开通结果通知至服务使用方，服务使用方在使用过程中针对效能进行评估分析，最终提升业务系统的建设、运行及管理水平。

7.4.1 业务需求

运营平台对所有资源进行统一运营管理，是新一代公安网上基于警务云和大数据建设的所有资源对用户提供服务的统一窗口，也是各部门应用系统登录的入口。用户通过该平台发现、申请、审批、使用各类资源，包括前端、终端设备以及云平台、数据、服务、应用、安全等 IPDS 资源。运营平台需满足以下业务需求：

1、提供统一标准的线上服务运营流程管理能力，用户对各类资源的申请、变更、维护不再需要通过邮件或线下纸质方式开展，资源不仅包括本地提供的也应包括上级提供的，本地用户若需申请上级资源也通过本地的运营平台进行申请。业务部门或分局申请本地资源采用两级审批，一级审批由各分局、支队、处领导审批，二级审批由大数据管理职能单位审批，审批通过后发放资源；申请上级资源采用三级审批，上级审批后将数据、服务等资源挂载到本地运营平台，后续其他单位或其他申请事由须再次申请上级资源的，须重新申请，采用三级审批。用户通过资源运营服务平台对各应用和各业务系统发起的申请，都要能通过零信

任体系的审批服务进行审批。例如用户想申请移动警务终端接入，可以通过运营平台发起申请，审核审批后进行接入；部门业务应用系统建设可在平台申请前置区或数据域云平台资源、数据服务资源或应用服务资源，并在平台上注册应用，系统建成后通过平台进行登录。同时，需支持移动 APP 端资源审批操作，支持各环节审核人及各级领导在移动 APP 端上对待办审批申请信息进行批准、拒绝等。

2、服务质量的管理，服务质量不仅包括运营平台中服务资源提供方所提供的服务，还包括各业务单位所负责的安全、运维、应用系统等服务，运营平台需具备服务评测体系，通过对评价、指标项、权重、分值等定义，同时配合服务绩效报告、运营情况报告等报表视图，帮助服务提供方和服务运营管理者对服务质量进行评估。

3、问题通报，运营平台需能与运维平台进行联动，将运维平台所发现的各业务单位或厂商引发的数据采集、数据治理、数据服务、应用、安全、运维等问题进行通报及反馈。

4、资源审批即发放，用户通过平台申请 IPDS 资源时，需实现审批后即能实现资源的使用，无需再通过工单流转以及手工处理，同时要建立统一的审批入口，确保审批人进入统一的审批入口即可实现对所有申请事项的审批。大数据智能化建设所涉及的数据采集管理平台、接入平台、服务资源目录、智慧搜索、智慧关注等应用系统，以及各业务单位的业务系统都需对接零信任体系的认证服务、审批服务、权限服务等，用户申请数据、服务、应用资源时，审批通过后即能使用资源，但对于电话业务申请、机房出入申请、移动警务用户申请、公安网设备入网注册申请、计算机接入互联网、数字证书申请和边界链路申请等特殊业务申请仍需进行工单处理。

7.4.2 架构需求

平台按照前后置分离进行部署，通过统一的资源服务目录，汇聚前置区和数据域 IPDS 四层的基础设施服务、数据资源、数据服务、应用服务等，通过运营资源服务平台服务目录申请及标准化的流程审批后，提供给各应用系统使用。

1、资源运营服务平台涵盖统一展示门户、服务质量管理、资源运营管理、用户中心、监控中心、帮助中心等模块内容，主要包括:

（1）统一展示门户，汇聚资源服务、数据服务、应用服务等各平台系统服

务能力，面向服务使用者提供统一服务的窗口、资源管理和质量通报的入口。提供门户资源审批移动 APP 端。

（2）服务质量管理，从指标管理、资源评价、服务成效等维度进行质量管理，提升各类资源的服务能力，保障用户体验。

（3）资源运营管理，提供统一的标准化、规范化资源服务生命周期管理，将新一代公安网各类前端、终端设备以及前置区和数据域 IaaS、PaaS、DaaS 和 SaaS 资源以服务的形式提供给用户，提供目录管理和资源申请、审批、授权、回收等资源服务全生命周期管理功能。

（4）用户中心，对接认证服务，实现平台统一机构用户管理、统一认证，支持省市两级工单的联动管理。

（5）监控中心，通过统计不同的运营监控指标，从资源、用户、审计等维度对报表进行分类，实现运营情况分析诊断的专业化、智能化，为运营决策提供支持。

（6）帮助中心，提供门户使用过程中关于资源流程、资源使用等常见问题的查看、反馈和知识库管理等功能。

2、资源运营服务平台与云平台、大数据平台、大数据平台（前置区）、安全体系资源和上级的对接需求包括：

（1）云平台，前置区、数据域云平台的 IaaS、PaaS 层的资源、服务通过资源运营服务平台进行注册、开通等对接，服务使用方申请资源后，由云平台进行资源分配和开通；资源运营服务平台采集获取云平台资源总量、已分配量等运营数据。

（2）数据域大数据平台，资源运营服务平台对接大数据平台数据资源目录和服务资源目录，获取数据资源、数据服务、应用服务等资源信息以及运营运维数据（包括数据接入、处理、组织、服务等），服务使用方申请资源后，由大数据平台进行资源的开放。

（3）大数据平台（前置区），大数据平台（前置区）数据资源、服务资源统一注册到数据域数据资源目录、服务资源目录，资源运营服务平台对接需求同大数据平台。

（4）安全体系，资源运营服务平台通过调用认证服务实现与 IPDS 各层的

统一认证授权、用户管理；安全体系资源与资源运营服务平台的服务目录、管理流程进行对接，统一对外提供服务。

（5）上级，对接上级资源运营服务平台，实现省市两级资源申请审批联动，服务目录同步，珠海本地用户可以查看并申请上级单位资源。

7.4.3 功能需求

7.4.3.1 统一展示门户

汇聚资源服务、数据服务、应用服务等各平台系统服务能力，面向服务使用者提供统一资源管理、服务的窗口和质量通报的入口。

同时为满足警务实战业务发展对数据资源需求的快速变化，支持业务单位深度参与数据治理工作，推进数据治理向精细化转变。提供数据治理需求管理和治理质量成效管理功能，支持各业务单位结合业务需要提出数据关联关系、比对等治理需求，如提出建设新的主题库或增加原有主题的刻画维度，大数据管理职能单位可动态将需求进行分发和成效考核，提高各业务单位对数据资源的认可度。支持对数据资源采集和质量统计分析和督导通报功能。

分类	功能项	功能需求描述
统一展示门户	文档资料	提供大数据文档的发布与管理，将大数据相关的标准规范、开发文件、使用手册等各类文档，大数据相关的各类工具进行统一管理，统一发布，供使用者下载使用。支持文档上传、发布，支持文档上线、下线的的自定义审核流程，支持文档多级自定义分类维护。
	应用市场	将应用进行分类，如上级推广、通用应用、业务应用等。支持统计应用总数、应用访问/评论总次数、评论数/访问数/点赞数最高的前 10 个应用。
	质量通报	根据服务质量评估结果，对服务质量进行通报，包括运营平台中服务资源提供方所提供的云平台、数据、服务、应用、安全等各类资源的服务质量，以及各业务单位所负责的安全、运维、应用系统等服务质量。
	问题通报	与运维平台进行联动，将运维平台所发现的由各业务单位或厂商引发的数据采集、数据治理、数据服务、应用、安全、运维等问题进行通报及反馈。
	数据汇聚治理成效管理	1、治理需求管理：用户可进行治理需求的提出，通过本单位审批后提交大数据管理职能单位。 2、治理任务下发及处理：大数据管理职能单位用户根据治理需求，将治理任务下发给厂商，由任务接收方进行数据治理。 3、治理结果反馈及评价：数据治理任务完成后，系

		统自动通知数据治理需求提出方，由需求提出方对治理结果进行反馈及评价。 4、治理成效通报：按照数据治理质量、服务效果、服务能力等不同维度，对数据共享率、需求满足率、同步更新率、共享使用率、数据合规率、业务应用率、好评率等核心治理成效指标进行统计分析。 5、对接数据采集管理平台，实现数据采集汇聚进展、成效的统计以及考核通报展示，包括采集进展统计、汇聚进展统计、对账情况统计、考核排名、监管结果通报等。
	工作台	为每个用户提供处理资源服务个人事项的工作平台，可按照待办事项、处理中事项、已办事项和申请单来分类查看个人需要处理和已经完成的事项工单。
	新闻资讯	已有功能、复用
	IPDS 资源展示	已有功能、复用

7.4.3.2 服务质量管理

服务质量主要从指标管理、资源评价、服务成效等维度进行管理，提升各类资源的服务能力，保障用户体验。支持根据资源的访问量、稳定性、用户使用评价等自定义维度，对资源进行淘汰，通过服务绩效运营角度，不断向用户提供高质量的资源服务。

分类	功能项	功能需求描述
服务质量管理	指标管理	通过设计定义的评价指标以及系统化的评估机制，对存在的服务质量问题做出科学判断并给出有效的干预措施建议。支持设计考核分值、权重、考核指标项、考核指标项说明，一级评价指标包括服务的可用性、安全性、可靠性、效率和可维护性指标。支持基于模型进行评估。
	资源使用评价	提供对资源综合评价反馈，综合评价反馈包括用户评价反馈和系统评价反馈。评价因素包括用户对资源使用点赞、评分、评论等因素，以及资源的使用次数、分享次数等因素。提供资源评论、资源排名、自定义指标配置、自定义指标墙功能。
	服务成效	提供服务运营和质量的总体分析、API 类服务对上云应用的支撑情况、服务使用方对服务的评价，通过图表的方式进行汇总、统计、分析并集中展现。
	资源淘汰管理	管理员用户可对各类资源进行淘汰管理，通过设定条件，系统自动统计需淘汰的资源，用户核对确认后，经过审核审批进行资源淘汰，系统自动通知资源所属业务单位或厂商。

7.4.3.3 资源运营管理

资源运营管理提供统一的标准化、规范化资源服务生命周期管理，将新一代公安网各类前端、终端设备以及前置区和数据域 IaaS、PaaS、DaaS 和 SaaS 资源以服务的形式提供给用户，用户可以从服务目录上申请，对于已经申请的服务，用户可以使用、变更、退订、评价。

提供目录管理和资源申请、审批、授权、回收等资源服务全生命周期管理功能。提供门户资源审批的移动 APP 端。

分类	功能项	功能需求描述
资源运营管理	资源申请管理	根据平台中所配置的资源，展示不同的资源目录申请的创建、变更、终止等申请内容，包括基本申请信息、申请理由、所需资源信息、使用时长等。用户根据需求提交申请内容形成申请单，并进入资源申请流程。
	资源审批管理	用户提交申请后，申请单根据配置好的申请流程，自动流转到审批人，审批人可以查看需要审批的申请单，以及对待办审批申请信息批准，拒绝等。
	资源授权管理	审批通过后，平台将会按照服务申请单配置，根据资源申请单中的申请内容，自动或者手动开通所申请的资源权限。
	资源回收管理	用户不再使用平台资源或服务（未到期的资源）的情况下，可由服务使用方发起资源退回申请。服务回收是指将非 API 类资源进行销毁并将资源回归资源池，或特殊资源进行回收站暂存。
	资源实例管理	资源开通完成后生成资源实例，资源实例是对资源使用的一种展现方式。提供对资源实例进行变更、终止、启动、停止等功能。
	资源目录管理	整合服务注册、应用注册等已有功能，提供统一的资源目录管理功能，包括资源注册、变更、回收\下架、查询等。
	资源审批移动 APP 端	提供门户资源审批的移动 APP 端，支持如下功能：支持各环节审核人及各级领导在移动 APP 端对待办审批申请信息进行批准、拒绝等，移动 APP 端运行在公安移动信息网。

7.4.3.4 用户中心

对接认证服务，实现平台统一机构用户管理、统一认证。提供资源运营工单管理功能，支持服务发布、应用注册以及服务申请流程所需的业务表单信息、流程定义等，支持对接上级单位，实现省市两级工单的联动管理。

分类	功能项	功能需求描述

分类	功能项	功能需求描述
用户中心	我的申请	对接认证服务，实现用户管理。提供用户资源申请管理功能。
	我的订阅	提供资源订阅管理功能。
	线上审批及工单管理	工单管理包含服务发布、应用注册以及服务申请流程所需的业务表单信息、流程定义，并提供工单的待办、已办、发起，以及工单处理的流程轨迹信息查询、工单的处理和归档，所有流程都要通过工单为用户提供单点联系，解答用户的相关问题和需求，或为用户寻求相应的支持人员。数据采集管理平台、接入平台、服务资源目录、智慧搜索、智慧关注等应用系统，以及各业务单位的业务系统都需对接零信任体系的认证服务、审批服务、权限服务等，用户申请数据、服务、应用资源时，审批通过后即能使用资源。资源审批或处理应符合管理办法，对于特殊业务和云平台资源等申请仍需进行工单处理。上级单位资源申请审批需按照上级单位的要求，通过接口对接的方式实现省市之间资源运营服务平台的联动。

7.4.3.5 监控中心

通过统计不同的运营监控指标，从资源、用户、审计等维度对报表进行分类，实现运营情况分析诊断的专业化、智能化，为运营决策提供支持。支持通过图表的方式对运营数据进行汇总、统计、分析并集中展现。提供访问统计、访问趋势、错误统计、节点监控、客户端调用统计、资源报表、日志审计等统计分析报表。

7.4.3.6 数据治理需求及成效管理

通过对数据治理需求、处理、反馈、成效进行统一管理，明确大数据管理职能单位、各业务单位、相关治理厂商工作职责、治理成效。

7.4.3.6.1 治理需求管理

用户可进行数据治理需求的提出，通过本单位审批后提交大数据管理职能单位。

7.4.3.6.2 治理任务下发及处理

大数据管理职能单位用户根据数据治理需求，按照权责业务单位、厂商将治理任务进行下发，由任务接收方进行数据治理。

7.4.3.6.3 治理结果反馈及评价

数据治理任务完成后，系统自动通知数据治理需求提出方，由需求提出方对治理结果进行反馈及评价。

7.4.3.6.4 治理成效通报

按照数据治理质量、服务效果、服务能力等不同维度，对数据共享率、需求满足率、同步更新率、共享使用率、数据合规率、业务应用率、好评率等核心治理成效指标进行统计分析，对各业务单位、相关治理厂商的数据治理成效进行通报。

7.4.3.7 帮助中心

提供门户使用过程中关于资源流程、资源使用等常见问题，支持用户进行线上反馈，支持运营服务平台问题知识库的维护管理。

分类	功能项	功能需求描述
帮助中心	常见问题	支持用户查看常见问题;支持管理员对常见问题的创建、修改、删除等管理功能。
	用户反馈	支持线上的问题反馈及回复。
	问题知识库	通过发现、定位、跟踪处理问题，持续维护问题案例库，支持问题发现、问题诊断、问题处理、知识库等功能。

7.4.3.8 前置区资源运营对接需求

对接前置区云平台以及大数据平台（前置区），实现前置区服务器、云资源、数据等统一运营，应包括：

1、物理设备资源，包括计算服务器（实例、实例主机、实例备份、主机设备）、存储服务器（存储设备、共享存储服务器）等；

2、服务实例资源，云主机、镜像、弹性 IP、弹性负载均衡（负载均衡、负载均衡应用容器）；

3、大数据集群资源，包括集群数量、组件数量、服务器数量、存储总量等；云平台资源，包括 vcpu、gpu、内存、磁盘的总量、剩余量、使用率和分配率等情况；

4、数据平台（前置区）的数据和服务等资源情况。

7.4.3.9 资源联动需求

对接上级单位资源运营服务平台，实现省市资源联动，需对接包括获取 IaaS、PaaS、DaaS、SaaS 目录等接口。

7.4.4 资源分类参考

结合资源定义分类规则，所有资源在平台目录中展示，供用户查看及申请使用，详见附录“资源分类参考”部分。

7.4.5 非功能性需求

1、性能指标

注册用户数：≥10000。

并发用户数：≥3000。

简单事务处理（如各类信息录入、修改、查询业务、主要页面等）平均响应时间：≤2 秒。

交互式研判工具平均响应时间：≤5 秒。

复杂事务或统计平均响应时间：≤10 秒。

2、可操作性

界面操作简捷、布局合理、提示及时，对于层次结构数据尽量使用树形结构，便于定位选取，展示数据的有效工作区最大化。

7.5 一体化运维服务需求

项目需建设包括一体化运维服务技术系统、统一的运维服务规范制度以及统

一的运维服务运行和受理中心，实现公安网的一体化运维。

1、建设一体化运维服务技术系统，实现信息系统运维服务统一监控、统一申请、统一受理、集中办理、统一反馈、全流程监督和智能运维、数据可视的目标。通过统一的告警中心将其他业务的监控告警数据接入告警中心，实现告警的统一管理。一体化运维系统通过根因和关联分析及时、精准地定位故障或问题根因，故障或问题的溯源率达到90%以上。告警故障的溯源需实现故障或问题关联到运维公司负责小组，故障关联到应用组件、故障关联到硬件等方式实现对故障的溯源分析。通过告警自动化转工单的能力，将故障推送给到对应的负责小组。

2、要配合建立统一、标准的运维服务规范制度明确相关服务组织或人员的责任范围、服务内容、操作规程及协作方式，统一服务受理、监控巡检、机房管理、资产管理、例行服务、响应式服务、故障处置、通信保障等工作标准，并结合实际在工作中不断改进和优化，提高运维质量和服务水平。

3、建立统一、集中的运维服务运行、监控和受理中心（服务台），通过统一服务号码和服务门户，将分散的运维服务受理渠道和值守人员集中起来，统一受理所有的运维服务和故障申请，并提供工单派发、任务处置、流程跟踪、信息反馈及数据分析等运维服务支持工作，确保运维服务效率和质量满足要求。

7.5.1 运维服务技术系统建设

信息系统运维服务需实现统一监控、统一申请、统一受理、集中办理、统一反馈、全流程监督和智能运维、数据可视的目标。

7.5.1.1 综合监控管理

综合监控需实现对机房动环监控管理、服务器监控管理、网络设备监控管理、数据库监控管理、应用服务监控管理等。其中机房动环监控管理通过对接现有的机房动环系统以及大数据机房动环系统。

1、机房动环监控对接，管理机房各种智能设备：UPS、配电系统、精密空调、漏水检测、温湿度传感器、消防信号、新风系统、门禁系统、视频、网络设备等，便于随时随地了解系统运行状态。

2、服务器监控，对主流服务器操作系统实现实时监控管理。管理主机性能数据包括 CPU 利用率、磁盘容量、系统内存（物理使用内存及缓存）使用情况、磁盘利用率、文件系统、日志、关键进程、软硬件资源、告警信息等，针对服务器相关的性能指标能够按照实际情况设定不同级别的性能阈值，对于超过性能阈值的性能指标系统能够进行故障告警或预警并通知相应的管理人员。监控指标项要求参见附录“服务器监控指标”。

3、网络设备监控，对路由器、交换机、安全设备、负载均衡等设备的性能指标采集和预警，支持主流厂家型号及其对应监控指标，包括 CPU 利用率、内存利用率、Ping 延时和丢包、端口状态、端口出入流量、告警信息等指标。监控指标项要求参见附录“网络设备监控指标”。

4、数据库监控，对数据库进行管理，保证数据库的安全，优化数据库的性能。能够对运行在主机设备上的各种数据库的运行状态、性能数据和告警信息进行统一有效的管理。系统支持但不限定 TDSQL、Tbase、TBDS、SQLServer、Oracle、DB2、MySQL 等数据库的监控管理。监控指标项要求参见附录“数据库监控指标”。

5 中间件监控，支持市场上各类主流应用服务中间件的信息监测，包括有 Apache、Nginx、Tomcat、Weblogic、IIS 及国产的各类主流中间件等。监控指标项要求参见附录“中间件监控指标”。

6、应用监控，对基础软件、应用软件的运行数据进行监控，当出现指标异常时则报警提示，信息推送到对应的群组或者个人，并按照设定的处置流程进行告警处理。可支持 URL 拨测、端口连接性、进程存活等能力。监控指标项要求参见附录“应用监控指标”。

7、告警管理，将其他业务的监控告警数据接入统一告警中心，实现告警的统一管理,包括机房、IPDS、各业务单位独立建设的业务系统等各类告警。通过根因和关联分析及时、精准地定位故障根因，故障的溯源率达到 90%以上。告警故障的溯源需实现故障关联到负责小组，故障关联到应用组件、故障关联到硬件等方式实现对故障的溯源分析。提供告警自动化转工单功能，对接现有工单系统。将故障推送给到对应的负责人员。

8、其他监控能力，支持告警自愈：需要自动化运维工具实现常规故障的故

障自愈，常规类故障如磁盘空间不足、CPU 或内存负载过高、进程服务终止。

9、运维日志监控：实现各类运维日志的集中采集、集中管理，实现海量日志的快捷查询与统计分析。

7.5.1.2 运维数据分析

为了尽早发现系统存在的故障隐患，需要对网络数据联通状况、机房动环情况、应用服务运行情况等进行展示。以便运维中心服务人员尽早分析出系统存在的故障隐患。通过将传统的各类应用逻辑架构图与鲜活的运维数据整合，全景式地展现各类应用系统的真实运行情况，帮助运维服务人员提高监控故障发现、复杂故障处理、系统变更恢复等工作的效率。展示需支持但不限于以下能力：

1、至少支持柱状图、饼图、折线图、百分比图等图表类型；

2、具备数据源管理功能，能够对数据源进行维护，包括增删改查；

3、数据源的类型至少支持 API、数据库、CSV，不同类型数据源对应不同的填写表单，且支持对数据进行二次加工；

4、具备视图模板管理功能，能够提供内置的模版样例，支持查看、删除已有模版，且支持以模版为基础创建视图，无需从零开始设计；

5、具备可视化设计功能，支持在线设计，能够通过对组件的添加、排版、样式设置以及数据源绑定来设计出满足需求的视图；

6、支持使用大屏方式展示用户定义的运维视图。

（1）资源使用情况分析

功能	功能描述
综合管理视图	综合管理视图从整体层面综合显示一体化运维管理的全局情况，可以显示信息系统各类型数据，如机房资源数据、集中监控数据、应用全景数据、服务受理数据、网络拓扑数据、运维安全数据、警务云数据、运维团队数据、服务考评数据等。
运维资源管理视图	资源管理视图，主要管理及展示信息系统资源分类、资源状态、资源分布、资源数量等情况，能够基于机房、不同的区域位置，显示所关心的运维数据。展示已有资源的类型、资源的状态、资源的使用情况、资源的增长趋势和资源的使用部门等，掌握资源的实际情况。
服务受理管理视图	服务受理视图，主要管理及展示一体化运维服务受理分析汇聚统计的场景，帮助用户可以实时地掌握业务受理情况。显示运维服务业务受理情况的统计数据，如服务工单的类型、工单的数量、工单的

	分布和处理状态等。
网络拓扑管理视图	网络拓扑管理视图,主要管理及展示相关工作网络进行拓扑展示及管理，并在拓扑图可以显示网络流量、网络性能、链路告警等运维数据。
运维安全管理视图	运维安全管理视图,主要管理及展示制度规范:各类运维安全制度、流程、规范、安全监督、安全宣贯、检查、运维安全事件等展示。
警务云管理视图	警务云管理视图,主要是对警务云基础数据的展示,包括物理设备:服务器、网络设备、存储设备等；服务实例：弹性云、裸金属、桌面云、云硬盘等数量；大数据集群：集群数、组件数、服务器数量、存储总量等。
数据资源管理视图	对 DaaS 层的数据接入处理过程的监控，包括数据传输、接入、处理、组织等环节的时效性、堆积情况、数据量，并形成数据报表。包括数据时效监控、数据处理监控、数据对账监控、关键资源监控、数据运维报表。

（2）应用运维情况分析

功能	功能描述
全景应用透视	全景应用墙透视需提供业务全局视角,运维管理者的关注重点在于 IT 应用的全貌以及 IT 应用对业务的整体影响，通过业务全景应用墙综合展示，管理者能够通过全局视角了解整个 IT 应用的现状，对业务系统的运行状况一览无余。
配置关系透视	配置关系透视需与各类第三方平台的数据对接,包括各类日常运维管理当中的资源基本信息、资源状态监控信息、资源性能容量信息、资源日志信息等,同时围绕业务运维需求对接各类业务运行的监控数据及运行状态数据。
性能透视指标	为了辅助到运维工作的各种场景,系统除了能够对对象的配置数据进行展示外，也需支持在视图中查看对象当前性能指标值，与第三方平台的数据对接，可查看对象的服务量、响应时间、响应率等指标值，同时在视图里面也可展示相关告警信息。
告警数据透视	通过运维监控视图管理,能够在业务架构图上展示业务应用的性能数据和业务数据，可以通过性能面板查看业务应用实时性能指标数据，支持对业务应用的历史性能数据的查看,同时也能够提供设备告警状态展示和告警查看，通过运维监控视图管理，可以快速的对故障源呈现，做到对故障源的快速分析查看。

（3）运维数据集中分析

运维数据规范范围包括服务事项工单数据、资产信息数据、硬件监控指标、基础软件监控指标和告警数据五项指标。

运维数据仓库的建设包括前期的数仓规划设计和对应的建模分析。数仓的建设包括服务事项工单数据、资产信息数据、硬件监控指标数据、基础软件监控指

标数据及告警指标数据共五大类。运维数据服务系统主要承担运维数据的接入、脱敏、管理、分发共享、权限管理、审计、授权及数据的建模分析等工作。

7.5.1.3 运维流程管理

运维流程管理需以服务管理为核心，以流程支持服务的执行，实现一体化运维服务过程的流程工单管理。提供包括请求管理、变更管理、问题管理、服务级别和 SLA 管理等。

1、请求管理。请求管理是指在运维工作开展的过程中，使用系统的用户对负责运维管理的部门提出的各种不同类型要求的一般描述。其中很多实际上是小量的变更或者日常服务，具有低风险、高频需求、低成本等特征。例如开通权限，资源申请，数据支持，安装软件，咨询服务等将此类与其他标准化的服务类型区分开，可以得到更高效的处理。

2、变更管理。变更是对 IT 生产环境中的软硬件及相关文档所作的增加、修改或移除。变更管理的目的在于管理和控制好变更（如变更的分类、审批、实施、回顾等），最小化变更所带来的风险。

3、问题管理。问题管理是为了分析所有可用信息，包括事件数据库，来确定引起事件发生的真正的潜在原因以及提供的服务中可能存在的故障。问题管理的目标是消除引起事件的深层次根源以防止事件再次发生。

4、服务级别及 SLA 管理。为了项目的需要，需为不同服务类型设置服务级别及相应 SLA 配置，确保服务的及时响应。

7.5.1.4 门户管理模块

门户管理模块能实现外部服务与内部管理的整合，通过服务注册上线、服务申请办理、服务数据集中展示，建立运维工作的相互协同、统筹管理机制。包括通知公告、运维动态、服务台专线、业务服务、工作台、考核工作、运维工作、规范标准、用户指南、知识库等。各类服务数据根据采购人实际情况，协调各运维服务商及用户根据相关模板要求进行收集填写，并由专职人员进行录入。

7.5.1.5 3D 机房管理

3D 机房管理是通过 3D 技术实现对信息中心机房的真实展现，能够实现基于三维环境对信息中心机房、机柜和各类设备的管理功能，构建信息中心机房环境、设备和管理信息的可视化，可视化管理能让 IT 的资产配置信息和运行状况更加直观，使复杂的 IT 信息变得易于表达、理解和传播，从而消除 IT 运营过程中不同角色之间的认知偏差和监管盲区，实现管理的透明化，更进而有效提升资产管理与监控管理的效率，真正实现一个立体式、可视化的新一代信息中心机房运行维护管理。各类资产配置、机房、环境数据，通过协调各运维服务商及用户及专职人员调研提供，由专职人员进行建模、绘制、维护及管理。3D 机房管理模块通过一体化运维服务技术系统各个模块、与第三方系统对接、静态数据收集等方式进行各类资产数据的采集录入。

7.5.1.6 运维资产管理

运维资产管理需支持对资产的批量导入和导出、信息更新等，每周核对 1 次数据校验，提供统一的对外集成标准规范接口与第三方系统进行对接，不涉及第三方系统的对接改造。详细功能要求如下：

系统	系统描述	功能项	功能描述
资产管理	资产管理展示了设备各维度信息，包括设备基本信息和与其他设备的关联关系	资产模型定义	支持信息自定义配置，包括资产类型、资产数量、型号。
		资产信息采集	支持多种资产模型，在配置完资产模型后，可实现该类资产的灵活采集。
		资产批量处理	支持批量导入模板，包含的资产类型，按照平台提供的模板标准填写资产信息即可轻松实现资产批量录入。
		资产关系可视	支持对运维管理系统中相关资产的集中展示。
		资产周期生命管理	支持对资产已入库、上架中、使用中、下架等状态资产管理。

7.5.1.7 项目文档管理

根据实际情况，做好系统技术文档的收集、整理及保管，明确文档的使用范围并严格控制。做好各类运维工作过程的记录。制定运维操作规程，规范各项运维服务工作。提供项目文档管理入口，实现对项目合同、项目标准规范、运维使用手册等项目文档的管理。支持对文档的上传、发布等维护操作，支持对项目文档进行分类维护。

7.5.1.8 运维 APP

基于 VPN,每个运维人员自己的手机提供统一运维 APP,支持安装在 Android 或鸿蒙系统移动终端设备，通过移动 APP 实现任务自动派单和结果反馈功能，清晰记录维护信息和过程，可推送故障位置和故障时间等信息，功能包括系统登录、告警管理、工单管理、系统管理。详细功能要求如下：

大类	功能	功能描述
移动 APP	系统登录	提供登录功能，只有合法的用户才能访问系统的数据，保证系统安全性。
	告警管理	支持用户可查看告警状况，及时了解设备的故障。
	工单管理	支持用户及时查看工单的情况,并随时随地进行工单处理，包括查看、创建、审批。
	资产管理	支持用户查看资产的统计信息及资产详情。
	系统管理	支持用户权限管理，限制相应功能的访问。

7.5.2 运维制度规范建设

建立统一、标准的运维服务体系，明确相关服务组织或人员的责任范围、服务内容、操作规程及协作方式，统一运维服务机制规范、服务过程管理、服务组织、服务评价等工作标准，并结合实际在工作中不断改进和优化，提高运维质量和服务水平。配合制定运维管理规范，制定的规范内容包括不限于：机房管理规范、监控巡检规范、服务受理规范、资产管理规范、故障处置规范。

7.5.3 运维服务中心

建立运维服务中心，配备一定数量的运维服务人员，提供7x24小时的运维服务响应。按照相关管理要求，制定重大活动保障规程。运维服务中心需按照不同的工作内容配备不同专业的技术和管理人员，根据服务对象类别及服务内容建立专业服务组，实现运维服务的统一调度和管理，满足项目的运维管理要求。

服务团队岗位职责：

岗位名称	岗位职责
运维经理	1、 对整个运维服务中心服务过程要全程管理，保证安全、高效，包括变更、升级、扩容等。 2、 负责运维机制规范建设。 3、 重大活动及应急事件保障的组织。 4、 召开例行运维会议以及业务汇报。
服务热线岗	1、归属运维经理管理。 2、接收来自服务请求方的一线通信，及时响应受理来自一线故障，记录问题单，按照工单流程转对应技术岗位。 3、升级请求单，按照响应及处理周期实际要求，升级请求单处理级别。对于重大事件、周期超过正常响应时限的通知运维经理。 4、日志和分类请求单，根据受理问题进行分类派发技术支持组对应技术岗位进行处理。 5、通知客户更新和中断，涉及服务中断以及业务中断的及时报备运维经理、客户。得到授权后，才能允许现场进一步操作。
监控巡检岗	1、日常巡检，每日对传输链路、网络设备、云平台、应用软件、机房环境等监控对象进行巡检，分析巡检结果，建立问题巡检单交由技术支持组对应处理，整理详细《系统巡检报告》汇报用户。 2、重大活动及应急事件保障，针对全市重大活动和应急突发建件负责全面协调。 3、月度、季度、年度巡检分析，复盘分析复发故障，避险突发事件经验总结等。
云平台运维岗	1、云平台、大数据的告警处理、巡检、保障。 2、维护云平台的正常运行，升级、补丁实施操作。 3、配合平台侧故障的协助排查。 4、负责云平台的运维案例总结。 5、负责传输系统的资源管理和运行报告。
应用运维岗	1、应用系统的告警处理、巡检、保障。 2、维护应用的运行，升级、补丁实施操作。 3、应用平台侧故障的排查和处理。 4、负责应用的运维案例总结。 5、负责应用系统的资源管理和运行报告。

岗位名称	岗位职责
资料分析岗位	1、负责所有资产的生命周期管理，全面和准确地记录涉及项目相关资产整个生命周期的相关信息。包括不限于资产信息、配置参数，确保资料数据完整、准确。 2、负责数据分析、知识库体系建设，发现潜在故障隐患，保证系统平稳运行。 3、参与监控巡检组月度、季度、年度组织的巡检分析会议，汇报数据分析成果。

7.5.4 品高云平台运营服务

为原品高6.0云平台提供1年运维和迁移服务，支撑前置区云平台的整体建设。

7.5.5 非功能性需求

7.5.5.1 性能指标

1、注册用户数：≥1000。

2、并发用户数：≥200。

3、简单事务处理（如各类信息录入、修改、查询业务、主要页面等）平均响应时间：≤2秒。

4、交互式研判工具平均响应时间：≤5秒。

5、复杂事务或统计平均响应时间：≤10 秒。

6、系统有效工作时间要求：≥99%。

7、监控告警实时性满足需求，告警生成到告警入库、告警发送时延不超过5秒。

8、本系统需保证7×24小时不间断运行，出现故障应能及时告警。系统的最长故障修复时间不超过4小时。

7.5.5.2 实时性

一体化运维服务技术系统要确保实时发现所有故障和隐患，对90%以上的故障或隐患要保证30分钟内准确溯源。

7.5.5.3 共享性

本项目建设的一体化运维服务技术系统可开放共享给其它部门使用，减少重复建设，实现一体化运维。

7.5.5.4 演进性

今后随着新的应用的建设，运维系统要将新建的应用全部纳入统一的运维管理。

7.5.5.5 可靠性

一体化运维服务技术系统能长期稳定运行。相关组件服务对外提供服务能力时，应具备应用服务升级或两台服务器宕机时不影响系统正常运行。

第8章 其他需求

8.1 验收要求、方式和内容

8.1.1 验收要求

8.1.1.1 硬件验收要求

1、所有设备到达指定地点，安装、调试至正常运行并能投入使用；

2、提供全部产品及完整的技术资料；

3、设备符合技术规格书的要求，性能满足要求；

4、设备符合国家相关产品质量标准。

8.1.1.2 软件验收要求

本项目采购的基础软件和软件开发等应用系统软件验收需符合以下要求：

1、功能指标测评。包括本项目所有建设系统功能内容、功能结果、相关接口等内容，系统功能需符合本项目建设所要求的功能需求；

2、性能指标测评。需对用户访问、系统稳定性、系统响应时间等性能指标进行测评，具体指标如下：

性能指标测评表

序号	类型	内容	指标
1	用户访问	并发访问	>=1000
2	系统稳定性	基础设施之平台服务层（云平台和大数据套件），数据资源之数据接入、数据处理、数据组织等，服务平台，大数据智能应用之公安一体化政务服务平台，运营运维之资源运营管理平台和统一运维平台	故障平均间隔时间(MTBF)≥1万小时，平均故障修复时间（MTTR）不超过30分钟(因为停电等不可预测因素除外)。

3		其他应用功能	需考虑高可用、负载均衡不能因为应用并发造成业务中断、停止等故障，应用故障平均间隔时间(MTBF)≥1500 小时，平均故障修复时间（MTTR）不超过 4 小时(因为停电等不可预测因素除外)。
4	系统响应性	简单事务处理（如各类信息录入、修改、查询业务）	<=2 秒
		交互式研判工具	<=5 秒
		复杂事务或统计	<=10 秒

8.1.1.3 测评验收要求

边界测评、等保测评、验收测评、国密应用安全性评估验收标准以第三方机构出具的相关测评报告为准。

8.1.1.4 运营运维验收要求

序号	服务名称	验收标准
1	驻场保障服务	1、开展服务工作的人员数量：中标人须在所承诺的服务期内提供驻场人员 4 人（2 名中级工程师，2 名初级工程师）。在开展应急演练和重大安保服务期间需提供 1 名高级工程师。 2、完成服务工作的工作形式：现场技术支持。 3、完成服务人员的季度考核：用户对技术支持人员进行季度考核，以此作为人员服务的评价。 4、完成用户需求书该部分所有服务工作内容。 5、完成服务工作的服务质量：提供开展服务成果报告，如《安全事件处置记录》《等级保护系统推进记录表》《应急演练预演方案》《应急演练安全问题总结》《重大安保期间安全保障方案》等。
2	利旧设备续保服务	1、完成服务工作的工作形式：中标人须提供现场技术支持。 2、完成用户需求书该部分所有服务工作内容。 3、完成服务工作的服务质量：提供开展服务成果报告，如《例行巡检报告》《系统健康状况记录》《设备问题处置记录》等。

序号	服务名称	验收标准
3	漏扫及渗透测试服务	1、开展服务工作的人员数量：中标人须在所承诺的服务期内提供专业技术人员 3 人（1 名高级工程师、2 名中级工程师）。 2、完成用户需求书该部分所有服务工作内容。 3、完成服务工作的服务质量：提供开展服务成果报告，如《漏洞扫描报告》《渗透测试报告》等。
4	互联网网站云防护服务	1、完成服务工作的工作形式：中标人须在所承诺的服务期内对第三方平台远程进行安全监测。 2、完成用户需求书该部分所有服务工作内容。 3、完成监测网站的数量：监测范围是 10 个互联网站系统。 4、完成服务工作的服务质量：提供开展服务成果报告，如《互联网站安全通告》《互联网信息系统安全监测报告》等。
5	运维服务中心	1、开展服务工作的人员数量：中标人须在所承诺的服务期内提供驻场人员 10 人，其中 4 人（1 名高级工程师，3 名中级工程师）5×8 小时的驻场；6 名（初级工程师）提供 7×24 小时驻场服务（白班 3 人晚班 3 人）。 2、完成服务工作的工作形式：现场技术支持。 3、完成服务人员的季度考核：用户对技术支持人员进行季度考核，以此作为人员服务的评价。 4、完成用户需求书该部分所有服务工作内容。 5、完成服务工作的服务质量：是否提供开展服务成果报告，如《巡检报告》《服务质量报告》《季度和年度分析报告》《服务质量考核评价记录》等。
6	大数据组件开发支持服务	1、开展服务工作的人员数量：合同签订之日起提供 19 个月的驻场人员 3 人（初级工程师 1 人，中级工程师 1 人，原厂高级工程师 1 人）。 2、完成服务工作的工作形式：现场技术支持。 3、完成服务人员的季度考核：用户对技术支持人员进行季度考核，以此作为人员服务的评价。 4、完成用户需求书该部分所有服务工作内容。 5、完成服务工作的服务质量：提供开展服务成果报告，如《运营周报/月报》《例行检查报告》等。

8.1.1.5 项目整体验收要求

1、合同完成情况：包括系统建设内容完成情况、变更完成情况；

2、项目资料文档完整情况：本项目验收文档可根据实际情况调整，主要包括：《深化设计方案》《项目实施方案》《需求规格说明书》《概要设计说明书》《详细设计说明书》《数据库设计说明书》《安装部署手册》《测试报告》等。

3、中标人在项目系统试运行不少于3个月并配合第三方检测机构完成验收测评。测评合格后，由采购人根据合同建设内容，包括功能建设情况、系统运行情况、项目资料文档等进行验收，形成正式竣工验收报告。验收合格后，由采购人报送珠海市政务服务数据管理局申请最终验收。

8.1.2 验收依据和方式

8.1.2.1 验收依据

根据采购人的项目管理要求、签订的项目合同以及建设过程中经采购人和中标人同意增加的约定文件（如补充协议、会议纪要）等，以及国家相关规定进行验收。

8.1.2.2 验收方式

1、验收应在采购人、中标人和采购人委托的监理单位共同参与下进行，并按国家有关规定、规范进行；

2、采购人组织项目验收小组按国家有关规定、规范进行验收，邀请相关等保测评机构、第三方验收测评机构参与验收；

3、合同签订后16个月内完成初步验收；上线试运行不少于3个月，试运行通过后，并通过验收测评后进行项目最终验收。

8.1.3 验收内容

本项目验收主要分为初步验收和最终验收。

8.1.3.1 初步验收

中标人根据建设合同内容，完成所有硬件设备安装、软件系统开发和测试，经自检合格后，提交初步验收申请。采购人及采购人委托的监理单位根据验收依据开展初步验收。中标人需按照要求配合第三方开展功能性及性能要求等验收测评事项，对验收测评提出的缺陷、问题进行整改。初步验收完成后，采购人、中

标人和采购人委托的监理单位签署初步验收报告。通过初步验收后，中标人方可提交试运行申请。

8.1.3.2 最终验收

系统上线试运行不少于3个月，且试运行期间未发现系统严重缺陷，并且完成等保测评、国密应用安全性评估等实施服务，否则采购人有权延长试运行或重新进行系统上线试运行。试运行期满后，中标人可向采购人提出正式竣工验收申请，由采购人组织专家组对本项目所有建设内容实施结果进行竣工验收，合格后由采购人报送珠海市政务服务数据管理局申请最终验收。

8.2 商务要求

8.2.1 服务期要求

1、自合同签订之日起19个月内完成项目建设及最终验收。

2、本项目质量保证期为5年（含基础软件、所有硬件），质量保证期和技术支持服务自通过珠海市政务服务数据管理局组织的最终验收之日起开始计算。（若国家和/或生产制造商对本项目所涉物的质量保证期的规定高于本项目的要求，应按国家和/或生产制造商的规定执行；若中标人承诺质量保证期比上述要求长的，按照其承诺执行）

3、自通过珠海市政务服务数据管理局组织的最终验收之日起计算，中标人需承诺为采购人提供不少于1年的运营运维服务（该运营运维期内产生的运营费、维护费等相关费用均包含在投标总价中，采购人不再另行支付费用）。中标人承诺的运营运维期结束后，中标人承诺有偿延续提供运营运维服务。

4、自项目开展建设之日起至项目最终验收结束后一年，由中标人承担机柜租赁的全部费用。

5、自通过珠海市政务服务数据管理局组织的最终验收之日起，中标人需为采购人提供不少于1年的软件产品及开发系统升级和维护服务（维保期内产生的升级和维护费用均包含在投标总价内，采购人不再另行支付费用）。

8.2.2 售后服务要求

8.2.2.1 技术支持服务要求

中标人应在中标后在珠海设立专门机构（分公司、子公司、售后服务点），对平台运行、维护提供7×24×365的全年实时技术支持服务，成立技术支持服务中心，提供免费7×24小时电话热线技术支持服务。

8.2.2.2 技术服务响应时限要求

1、时限要求：响应时限为立即响应，现场响应时限为30分钟内，特大故障3小时内修复，重大故障2小时内修复，一般故障1小时内修复。保证在8小时内排除设备故障，恢复正常。

2、故障定级标准：

（1）一般故障：指一般性技术故障，设备所服务的系统的操作性能受损或性能下降，但设备或应用系统仍可保持正常运行或最终用户大部分业务运作仍可正常工作。

（2）重大故障：指部分设备故障或应用系统故障，现有设备或应用系统运行性能严重下降,或由于性能明显下降,影响和限制了部分业务运营；设备或应用系统在运行中出现的故障具有潜在的业务中断的危险，并可能导致设备或应用系统的基本功能不能实现或全面退化。

（3）特大故障：指严重的设备故障或应用系统故障，引起设备或系统瘫痪，导致业务中断或对业务运作造成灾难性影响，造成业务中断1个小时以上或导致关键业务数据丢失的故障。

（4）所有因发生故障而对最终结果造成严重影响的，都定为重大故障或特大故障。故障定级标准以采购人评定为准。

8.2.2.3 维保期内提供技术支持与服务要求

1、日常巡检服务。定期对系统的软硬件和接口进行检测，发现故障，排除隐患，提出改进意见。中标人应高度重视巡检过程中发现的异常情况，及时通知

维护人员，查找原因，排除故障隐患，并不断完善重要监测点的实时监控机制。

2、系统性能优化服务。应对系统运维中出现的性能下降、故障频繁等异常现象高度敏感，积极主动进行原因分析，提出合理解决方案和建议，并配合进行实施;对应用软件的运行情况进行监控;系统分析员对应用软件的性能进行分析，指出可能引起性能问题的应用软件及其原因；结合业务发展情况，分析业务变化对应用软件的影响，提出合理的优化建议；根据长期维护经验，指出应用软件可以改善、提高性能的地方，提出合理的优化建议。

3、维护期后，在平台的建设、升级、维护和日常运行管理方面继续给予技术协作和咨询，提供有偿维护。

8.2.3 驻场服务要求

1、中标人在项目启动后5天内完成项目办公场地的建设和配套办公设备安装，采购人提供15个办公位，剩余办公位由中标人在项目办公场地安排，项目办公场地至采购人办公地点距离不超过2公里，驻点办公人员接采购人通知后，须15分钟内到达现场。在采购人提供的办公场地办公的，中标人须负责主要管理责任，严格落实防疫规定，并服从采购人各项管理制度及考勤制度。在中标人项目办公场地办公的，采购人须通过企业微信、钉钉等方式对驻点办公人员进行考勤考核。项目启动后，采购人如在定期检查中发现驻点办公人员存在违规问题的，在下一次付款时扣除合同金额的1‰，如出现违规问题被通报批评的，在下一次付款时扣除合同金额的2‰。

2、合同维护期内，中标人须根据业务需要对平台进行相应的调整优化。合同维护期后，由于需求发生变化所引起的服务需求变动，中标人应以优惠价格提供给采购人。

8.2.4 培训要求

中标人至少必须满足本章要求的培训服务，所提供的培训课程表随投标文件一起提交。培训授课人必须是经过厂家认证的工程师、技术员等。中标人必须制定培训计划、培训方案，为所有被培训人员提供免费培训所需的文字资料和讲义等相关培训文档、用品，提交采购人和监理人员审查，所有的资料必须是中文书

写，培训费用所有费用由中标人承担。培训内容与课程要求：中标人需对建设内容提供总课时不少于20课时的培训；提供本项目所有设备和软件的安装和使用和维护培训。培训完成后，提交培训记录表和培训反馈表。

中标人须对本项目提供至少5个宣传视频，视频内容须包含建设内容对应的建设成效。

8.3 支付及结算要求

8.3.1 支付方式

双方签订合同后，按照项目完成进度分阶段多次支付。第一期支付前，须满足①中标人委派的综合人员到位并满足采购人要求；②攻坚方案通过采购人审核。其他具体要求合同另行约定。

一期：合同签订后采购人支付合同总价的25%作为预付款，同时中标人须提供预付款同等金额的预付款保函；

二期：完成超过硬件设备和基础软件总价的90%供货安装调试，并通过货物验收和系统安装运行报告后，支付合同总价的20%；

三期：采购人出具初步验收报告后，支付合同总价的15%；

四期：珠海市政务服务数据管理局出具最终验收报告后，支付合同总价的15% ；

五期：最终验收之日起满一年，采购人支付合同总价的5%；

六期：最终验收之日起满两年，采购人支付合同总价的6%；

七期：最终验收之日起满三年，采购人支付合同总价的6%；

八期：最终验收之日起满五年，采购人支付合同总价的8%。

8.3.2 结算材料要求

1、合同；

2、中标人开具的正式发票；

3、中标通知书；

4、监理档案资料；

5、项目结算文档。

8.3.3 其他要求

1、上述支付方式中的实际支付金额=合同总价×本期支付比例-本期考核扣款金额（考核方案详见招标文件附件3）。

2、因采购人使用的是财政资金，采购人向政府采购支付部门提出办理财政支付申请的视为采购人已经按期支付，中标人不得以款项未到账为由延迟、取消或更改交付服务计划。在汇款过程中，因中标人账户的原因（包括但不限于账号被注销、被冻结等）导致其无法收取款项的，由中标人自行承担相应后果。

第9章 附录

9.1 附录1 数据资源附录

9.1.1 数据接入处理能力要求

本项目建设的数据接入平台、处理平台及其处理引擎应支持结构化和非结构化数据接入和处理，对于非结构化数据进行结构化处理后，应能支持数据提取、清洗、关联、比对、标识和分发6大标准处理环节。如针对电子笔录、简要案情和情报文档等大文本处理时，能够提取关键线索，支持在智慧搜索应用中基于已知信息等进行检索和查看，支持用户在全息画像等应用中关联查看原始文本信息。

数据接入处理主要能力应包括：

序号	类型	文件或数据库类型	读取	写入	处理
1	结构化	Oracle	√	√	结构化数据提取、清洗、关联、比对、标识、分发等
2		MySQL	√	√	
3		SQL Server	√	√	
4		PostgreSQL	√	√	
5		Greenplum	√	√	
6		TIDB	√	√	
7		Hive	√	√	
8		Libra	√	√	
9		TBase、TBDS、TDSQL	√	√	
10		MongoDB	√	√	
11		KDB	√	√	
12		Hbase	√	√	
13		GBASE	√	√	
14		Elasticsearch	√	√	
15		Solr	√	√	
16		Kafk	√	√	
17		HDFS	√	√	
18		S3	√	√	
19	非结构化	txt	√	√	文件文本数据结构化，姓名、身份证号、手机号、车牌号等关键要素提取，关键词和摘要提取。
20		csv	√	√	
21		bcp	√	√	
22		xls/xlsx	√	√	

23		xml	√	√	
24		json	√	√	
25		doc/docx	√	√	
26		网址	√	√	
27		邮箱	√	√	
28		域名	√	√	
29		情报、文章、案情、笔录	√	√	文件文本数据结构化，姓名、身份证号、手机号、车牌号等关键要素提取，关键词和摘要提取。文本智能分类、实体关系抽取需要文本语义分析引擎支撑。
30		视频	√	√	需要多媒体处理组件支撑，如视频结构化等
31		图片	√	√	需要多媒体处理组件支撑，如图片分类引擎等
32		音频	√	√	通过音频引擎，提取、比对特征

9.1.1 数据处理需求

9.1.1.1 业务需求

数据处理应满足可视化动态编排、策略/规则配置及过程监控需求，支撑基于知识库中经过业务沉淀形成的处理策略规则，逐步对数据进行萃取，提炼数据价值，实现对上层提供数据服务的能力。

数据处理提供数据提取、数据清洗、数据关联、数据比对、数据标识、数据分发的规则配置管理功能，允许用户根据各种引擎构建任务，如处理引擎或第三方引擎。建立数据处理数据流和控制流的统一协同机制，根据不同数据结构、数据类型和业务需求采用不同的智能处理引擎，实现数据处理的可视化和自动化。对处理过程中每个节点的处理结果进行可视化展示，如去重条数，根据某个过滤规则过滤的条数，根据某个关联规则关联的数据条数等。提供对运行中的处理任务和已停止的任务的监控，如处理任务中每个节点的输入输出量、处理耗时、是否异常、运行状态等。

数据处理的核心需求是能根据业务经验对数据提取、清洗、关联、比对、标识、分发等过程的规则进行动态配置，业务经验可提前维护在知识库中，在配置过程中进行选用，也可以是在配置处理过程中根据需求进行维护，并沉淀归拢到

知识库中，便于往后进行复用。

1、数据提取：提取的关键是根据不同需求从不同数据中提取关键要素。

2、数据清洗：清洗的关键是保留有用数据、去除无用或冗余的数据，同时对必要的数据进行格式转换。

3、数据关联：关联的关键是将多张表进行关联，并丰富表的字段信息。

4、数据比对：可以对关注对象进行布控预警。

5、数据标识：标识可以对数据打上基础标签、行为标签或业务标签等，一方面可以根据用户在标签管理平台创建的标签进行打标；另一方面可以根据知识库对数据进行打标。

6、数据分发：即将处理后的数据按照种类分发到原始库、资源库、主题库或各部门建设的业务库中。

9.1.1.2 架构需求

数据处理整体架构包括数据处理平台、基础数据处理引擎和音频数据处理提取引擎。数据处理平台基于动态、可编排、可扩展的架构，向用户提供拖拉拽可视化方式，基于知识库中处理规则和标签，对不同数据结构、数据类型和业务需求的数据处理过程进行策略/规则配置及过程监控；基础数据处理引擎是按照部标准提供提取、清洗、关联、比对、标识、分发 6 个标准处理环节引擎；音频数据处理提取引擎能够对原始音频文件进行加工处理形成特征。

9.1.1.3 数据处理平台功能需求

9.1.1.3.1 处理过程可视化

数据处理过程可视化实现对各种数据资源类型的提取、清洗、关联、比对、标识、分发过程的多种维度的可视化展现，便于数据治理人员监控数据处理过程、统计分析等。支持数据提取、清洗、关联、比对、标识、分发等全流程的可视化展示与管理。

分类	功能项	功能需求描述
数据处理过程	处理任务总览	可视化展现每个任务执行历史的各个处理环节（包括

分类	功能项	功能需求描述
可视化		提取、清洗、关联、比对、标识、分发等环节）总共收到多少数据量、处理多少数据量、发出多少数据量，可按各个维度统计每个处理环节数据量。
	资源任务监控	支持查看各个处理任务的详情，包括引擎类型，接受数据量、处理数据量、发出数据量以及各个统计值平台最新更新获取时间等。

9.1.1.3.2 引擎中心

大数据处理包括提取、清洗、关联、比对、标识、分发6个处理环节，每个环节根据不同的数据类型和业务需求需要不同处理引擎（工具或插件）完成不同的数据处理任务。数据处理平台支持所有的处理引擎动态可编排，即根据业务需求编排、配置不同的处理环节及引擎，同时各个处理引擎是松耦合的、采用插件方式、支持按照一定的标准自定义开发和二次开发。

引擎中心实现对处理引擎的全生命周期的管理，包括注册、启用、停用等，所有的处理引擎需在引擎中心完成注册并启用后才能由用户进行编排完成流程化的数据处理任务，处理引擎包括本项目开发的处理引擎、第三方开发、开源处理引擎等，通过引擎中心实现统一的注册管理。根据提取、清洗、关联、比对、标识、分发不同的标准化处理环节和自定义处理环节，提供不同环节的引擎管理功能。

分类	功能项	功能需求描述
引擎中心	引擎管理	提供流式处理方式的可视化管理，支持包括源端引擎、处理过程引擎（提取、清洗、关联、比对、标识、分发等过程）、目标端引擎管理。支持新增、删除和修改引擎，支持集成第三方引擎，支持Kafka、HDFS、MongoDB、Hbase、ES、Solor、MySql、TBase、TDSQL、TBDS、LibrA、PG、Greenplum等目标端引擎。
	UDF函数管理	提供Table-SQL流式处理方式的可视化管理，支持配置处理环节中可调用的函数方法，支持上传、新增、批量删除、修改UDF函数。提供校验时间、中文转拼音、校验必填字段、解析IP信息，以及身份证、MAC地址、固定电话、手机号码、硬件特征串、电子邮件、IMEI、URL、日期、时间、虚拟身份、IP地址、证件号码、经度纬度坐标等归一化等常用UDF函数。

	JAR 包管理	提供对处理引擎所使用的 UDF 函数管理，维护类型、版本号、存储路径等 JAR 包信息，支持对 UDF 函数 JAR 包进行上传、审批、删除和查询。

9.1.1.3.3 配置中心

配置中心，实现与数据接入平台数据定义模块的对接，提供针对每一类数据资源处理策略的查询及更新，处理策略包括数据提取策略、数据清洗策略、数据关联策略、数据比对策略、数据标识策略、数据分发策略。

分类	功能项	功能需求描述
配置中心	数据提取	1、提供数据提取规则管理功能，维护规则类型、优先权值、提取回填字段、字段校验方法、规则内容等配置信息；支持新增、编辑、删除、启动、停止等。 2、提供文件类型管理功能，对数据内容中需提取的文件格式进行维护，支持新增、编辑、删除、启动、停止等。 3、提供资源提取规则管理功能，维护数据资源中需进行提取的字段，支持编辑、删除、启动、停止等。
	数据清洗	提供数据过滤、数据去重、数据格转、数据校验的规则配置功能。 1、支持维护过滤规则，包括过滤模式、规则描述、应用资源、字段编码等，支持新增、删除、停用、启用、审批等。 2、支持维护去重规则，包括去重策略、去重方式、是否统计、去重数据项等，支持规则编辑、审批、查询等，去重策略支持全量去重或时间窗口去重。 3、支持维护格转规则，包括内部标识符、中文名称、格转类型等，支持规则编辑、审批。 4、支持根据校验知识库对数据进行检验。
	数据关联	提供数据关联规则配置功能，维护包括关联模式、关联表、过滤规则、关联规则、回填字段等，支持编辑、删除、修改、启用/停用等。
	数据比对	支持按照比对规则对结构化和非结构化数据进行相同比较或相似比较，将比中的数据返回。
	数据标识	提供数据资源与标签关联配置功能。
	数据分发	支持根据不同数据的使用场景，按照分发策略将结果数据对应分发到原始库、资源库、主题库、业务库、知识库；支持统计资源名称、分发表总数、最后更新时间等信息；支持新增分发。

9.1.1.3.4 执行中心

对某类数据资源配置数据处理流后，可通过执行中心选择执行模式并启动该数据处理流的执行任务。系统自动从引擎中心获取所有的已配置数据处理流、执行状态、执行模式等，未启动的数据处理流，用户可以选择执行模式并启动。

提供处理任务执行管理，支持单机执行、集群执行和分布式执行。

分类	功能项	功能需求描述
执行中心	执行资源管理	1、提供对处理任务新增、删除、启用、停用等。支持分组管理，支持新增、修改、删除资源分组。 2、提供可视化执行画布功能，支持通过可视化拖拉拽的方式，从数据拉取到数据处理环节到分发的流程配置；支持配置参数，包括算子并行度、算子链模式、部署标签等；支持配置处理集群和版本；支持对各个节点进行启停。
	处理集群管理	提供数据处理使用的集群以及对应版本的管理功能。支持新增、编辑、删除等集群维护功能，支持在线测试数据库、集群连接；支持修改、删除、上传文件等版本管理。
	敏捷开发管理	提供敏捷开发方式，通过编写 SQL 的方式快速响应数据治理过程。支持 SQL 处理任务分组管理，以及新增、修改、删除资源分组；支持配置数据源、目标端、udf 函数。

9.1.1.3.5 监控中心

开发面向工具自身及所开发配置数据传输任务的监测器，监控调度节点运行状态及任务调度情况，监控执行节点运行状态及传输任务执行情况，及时采集各类监控对象的运行状态和重要性能数据，实现专用工具自身运行状态及相关数据传输任务的实时监控，实现异常情况的自动报警提醒。

监控每个任务执行状态，监控处理环节之间的处理速度是否相匹配、上下游数据处理速度是否不匹配。可通过监控的数据流的实际情况，及时调整处理环节并发度等，方便进行动态调优参数。

分类	功能项	功能需求描述
监控中心	运行中任务监控	实时监控运行中的任务，包括当前任务总的子任务数目以及正在运行中的子任务数、任务运行的持续时间等。支持查询任务详情，包括任务名称、任务开始时间、每个处理环节运行状态、接收数据字节数、数据

		条数、持续时间、平均速率、处理速度等。
	已停止任务监控	监控已停止的任务，包括当前任务总的子任务数目以及已停止运行的子任务数、任务运行的时间等。支持查看任务具体信息，包括任务名称、任务开始时间、每个处理环节运行状态、接收数据字节数、数据条数、持续时间、平均速率、任务停止时间等。

9.1.1.4 基础数据处理引擎功能需求

按照《GA/DSJ 220-2019 公安大数据处理 数据处理技术要求》，大数据处理包括提取、清洗、关联、比对、标识、分发6个处理环节，每个环节根据结构化、非结构化等数据类型和业务需求，需要不同智能处理引擎（工具或插件），实现数据处理自动化。处理引擎需要在数据处理平台的引擎中心进行注册，数据处理人员通过数据处理平台配置中心和执行中心根据已经注册的引擎对各类数据资源进行处理流编排和执行。

本项目需针对各个处理环节提供6大类基础数据处理引擎，针对数据域数据资源，实现关键要素的提取、清洗，结合数据资源，经标准化处理、治理后数据汇聚，实现人员身份、活动场所、时空、车辆物品、账号等关联。

9.1.1.4.1 数据提取引擎

数据提取是根据数据定义，从源格式数据中提取出目的格式数据。通过提取策略、规则和数据解析得到从来源数据集/字段到目的数据集/字段的映射关系、运算规则、转换及整合等，获得按照目的数据形式组织的数据支持提取姓名、地址、身份证号、手机号等要素信息。

9.1.1.4.2 数据清洗引擎

数据清洗是指根据数据定义结果进行数据过滤、去重、格转、校验等操作，生成满足标准及质量要求的数据。

支持数据过滤，包括基于样本数据的垃圾过滤、基于规则的垃圾过滤、POST垃圾过滤。

支持数据去重，包括结构化和非结构化数据去重。

支持数据格转，包括代码转换、数据截断、数据内容格式统一等。

支持数据校验，包括完整性校验、空值校验、取值范围校验、数值校验、长度校验、精度校验、多字段条件校验、一致性校验等。

9.1.1.4.3 数据关联引擎

数据关联是指根据数据定义中的关联规则或算法，将数据和其它知识数据、业务数据等进行关联，并输出关联信息，支持关联回填、关联提取。

9.1.1.4.4 数据比对引擎

数据比对是指在数据处理过程中，按照规则对结构化和非结构化数据进行相同比较或相似度计算需要，对于命中规则的数据，支持按照输出描述进行输出，常用于信息布控和信息订阅。

支持结构化比对，包括完全匹配、模糊匹配、范围匹配、正则匹配等。

支持非结构化比对，包括关键词比对、文本相似度比对、二进制比对等。

9.1.1.4.5 数据标识引擎

数据标识是指基于标签知识库、标签资源目录，对数据进行比对分析、模型计算，并对其打上标签，为上层应用提供支撑，支持规则解析、规则编译、规则路由和规则执行。支持根据用户在标签管理平台创建维护的标签规则对数据进行标识。

9.1.1.4.6 数据分发引擎

数据分发是指完成数据提取、清洗、关联、比对和标识之后，根据不同应用场景，按照数据定义的分发策略，将处理过程产生的关联、关系、标签等信息，以及数据本身信息，按照数据定义的要求，进行同步或异步的相关处理，并将结果数据对应分发到原始库、资源库、主题库、知识库、业务库。支持任务调度服务、分发任务管理、数据分发、分发统计、数据核销及任务监控。

9.1.1.5 音频数据处理提取引擎功能需求

开发建设音频数据提取引擎，满足对音频数据处理需求。通过音频处理引擎对原始音频文件进行加工处理最后形成高质量的特征，形成的特征结合其他信息注册到数据库中形成音频数据资源，对外提供注册、查询、比对应用服务。

9.1.1.5.1 音频预处理

音频预处理引擎满足对语音预处理需要，对原始音频文件进行音频解码处理、检测有效、去除噪声等，提高特征提取的效率和质量。满足音频库对上传的检材进行格式校验转换、有效检测提取等预处理操作。支持能量四门限算法、基于规则的噪声判断算法及基于模型分类器判决等，分别针对不同的场景类型进行检出，最终实现不同的场景分割并检测出其中的有效音频片段。

9.1.1.5.2 音频特征提取

提供音频特征提取引擎，满足基于新的多系统融合引擎，实现特征提取。

引擎的融合策略包括多特征、多系统融合，可支持提取多套特征，提升特征提取引擎的效果和效率。

9.1.2 前置区数据融合处理

9.1.2.1 数据提取实施

根据数据定义，开展从源格式数据中提取出目的格式数据实施工作。根据数据提取策略，梳理分析业务需要及数据项内容，针对全警各类数据配置所需的数据提取引擎，管理数据提取执行过程，主要提供结构化数据提取、非结构化数据提取。

9.1.2.2 数据清洗实施

本项目针对前置区数据包括视图数据开展数据清洗工作，数据清洗的目标是去除视图数据中错误、无效的数据，避免这些数据在后续的分析中形成噪声干扰。并完成数据格式的转换，主要包括过滤、去重、格转、校验、数据标准化操作，生成满足标准及质量要求的视图数据。

9.1.2.3 数据关联实施

根据数据定义，开展关联信息实施工作。根据数据关联策略，配置对应的数据关联引擎，管理数据关联执行过程，实现将数据和其他知识数据、业务数据等的关联，包括关联回填和关联提取。

9.1.2.4 数据比对实施

根据数据定义过程中的数据比对策略、规则，梳理分析业务需要及信息布控、订阅等实战需求，针对结构化数据和非结构化数据配置所需的数据比对引擎，管理数据比对执行过程。并按照规则对视图数据进行相同比较或相似度计算，对于命中规则的数据，按照输出描述进行输出，便于进行信息布控和信息订阅。

9.1.2.5 数据标识实施

根据数据定义中数据标识策略，为数据打标配置合适的标签引擎，同时根据打标类型、数据分布等业务场景，配置执行平台的规则路由，完成对数据的比对分析、模型计算、打标工作。对图片及其结构化描述信息等进行标签化处理，以描述性的词语或者短语，对无语义的数据属性进行知识化概括或对有语义的数据属性进行知识化的深加工。同时定时校验数据打标的准确性，如有误需分析、整理原因，并重新调整标识引擎配置。根据业务需求、比对分析、模型计算等需求的变更，实时调整标识策略及引擎配置。

为支撑数据标识执行过程，需建立并维护标签知识库。

9.1.2.6 数据分发实施

根据数据定义中的数据分发策略，根据不同的应用场景和分析数据本身信息、关联、关系、标签等信息，针对视频数据还需包括图像及其描述信息，配置对应的分发引擎，将提取、清洗、关联、比对和标识后的数据对应分发到原始库、资源库、主题库、知识库、业务库。

9.2 附录 2 运营运维附录

9.2.1 资源分类参考

结合资源定义分类规则，所有资源在平台目录中展示，供用户查看及申请使用，资源分类参考如下：

资源类型	一级分类	二级分类	资源名称	备注
IAAS	计算资源	前置区/数据域	裸金属	
			虚拟机	
			容器	
			云桌面	
			弹性云服务	
	存储资源	前置区/数据域	云硬盘	
			文件存储	
			对象存储	
			块存储	
PAAS	计算组件	前置区/数据域	流式计算	
			离线计算	
			图计算	
			内存计算	
			交互式计算	实时计算
	存储组件	前置区/数据域	分布式文件系统	
			分布式列式数据库	
			分布式关系数据库	
			内存数据库	
			全文数据库	
			图数据库	
			时序数据库	
			多维分析数据库	
	应用支撑	前置区/	分布式消息	

		数据域	分布式缓存	
			API 网关	
			工作流	
			负载均衡	
			微服务	
			容器服务	
			服务目录	
			服务编排	
			服务开发平台	
DAAS	数据处理	前置区/数据域	数据元标准	
			元数据	
			数据血缘	
	数据组织	前置区/数据域	原始库	
			资源库	
			主题库	
			知识库	
			业务库	
			视图库	仅对接前置区
	数据服务	前置区/数据域	查询检索	
			比对订阅	
			模型分析	
			数据推送	
			数据鉴权	
			数据操作	
			数据管理	
			与上级对接	
			视频图像	仅对接前置区
SAAS	安全服务	前置区/数据域	认证服务	
			权限服务	
			审批服务	
			审计服务	
			加密服务	
			解密服务	
	应用服务	前置区/数据域	电子地图	
			标签平台	
			音频应用	
			专业侦查办案	
			智慧消息	
	通用应用	前置区/数据域	智慧搜索	
			智慧关注	
			全息画像	
			全网追逃	
			建模平台	

			可视化大屏	
	业务应用	前置区	一体化政务服务平台	
			分析研判平台	
			多维统计平台	
			统一运营平台	
			一体化运维平台	

9.2.2 服务器监控指标

对象	指标描述	类型	单位
服务器	cpu 总使用率	CPU	%
	cpu 单核使用率	CPU	%
	接收字节流量	网络	KB/s
	发送字节流量	网络	KB/s
	发送包速率	网络	个/s
	接收包速率	网络	个/s
	established 连接数	网络	个
	time_wait 连接数	网络	个
	listen 连接数	网络	个
	last_ack 连接数	网络	个
	syn_recv 连接数	网络	个
	syn_sent 连接数	网络	个
	fin_wait1 连接数	网络	个
	fin_wait2 连接数	网络	个
	closing 连接数	网络	个
	closed 状态连接数	网络	个
	UDP 接收包量	网络	个
	UDP 发送包量	网络	个
	可用物理内存	内存	MB
	交换分区已用量	内存	MB
	物理内存使用率	内存	%
	物理内存使用量	内存	MB
	应用内存使用量	内存	MB
	应用内存使用率	内存	%
	磁盘使用率	磁盘	%
	读速率	磁盘	次/s
	写速率	磁盘	次/s
	磁盘 IO 使用率	磁盘	%
	系统进程数	进程	个
	Agent 心跳丢失-GSE	事件	
	磁盘只读-GSE	事件	
	磁盘写满-GSE	事件	
	Corefile 产生-GSE	事件	
	PING 不可达告警-GSE	事件	

对象	指标描述	类型	单位
	进程端口	事件	
	自定义字符型	事件	
	系统启动时间异常	事件	

9.2.3 网络设备监控指标

对象	指标描述	类型	单位
网络设备	网络设备 MAC 地址	信息指标	
	网络设备名称	信息指标	
	可用性	可用性指标	
	响应时间	性能指标	毫秒
	系统 OID	信息指标	
	连续运行时间	信息指标	秒
	网络设备说明	信息指标	
	所有 IP 地址	信息指标	
	网络接口个数	信息指标	
	吞吐量	性能指标	bps
	接收丢包率	性能指标	%
	发送丢包率	性能指标	%
	丢包率	性能指标	%
	接收 ICMP 包率	信息指标	包/秒
	发送 ICMP 包率	信息指标	包/秒
	TCP 端口连接数	信息指标	
	接收广播包率	性能指标	包/秒
	发送广播包率	性能指标	包/秒
	广播包率	性能指标	包/秒
	接收广播包数	信息指标	包
	发送广播包数	信息指标	包
	内存总容量	信息指标	字节
	CPU 平均利用率	性能指标	%
	内存利用率	性能指标	%
	内存已使用容量	信息指标	字节
	内存可用容量	信息指标	字节
	SNMP 可用性	可用性指标	
	接口名称	信息指标	
	接口别名	信息指标	
	接口描述	信息指标	
	索引	信息指标	
	接口类型	信息指标	
	接口带宽	信息指标	bps
	MAC 地址	信息指标	
	管理状态	信息指标	
	接口开关状态	可用性指标	

对象	指标描述	类型	单位
	操作状态	信息指标	
	带宽利用率	性能指标	%
	接收速率	性能指标	bps
	发送速率	性能指标	bps
	接收带宽利用率	性能指标	%
	发送带宽利用率	性能指标	%
	接收丢包率	性能指标	%
	发送丢包率	性能指标	%
	丢包率	性能指标	%
	接收丢包速率	信息指标	包/秒
	发送丢包速率	信息指标	包/秒
	丢包速率	信息指标	包/秒
	接收丢包数	信息指标	包
	发送丢包数	信息指标	包
	接收的错包数	信息指标	包
	发送的错包数	信息指标	包
	接收单播包率	信息指标	包/秒
	发送单播包率	信息指标	包/秒
	单播包率	信息指标	包/秒
	接收单播包数	信息指标	包
	发送单播包数	信息指标	包
	接收广播包率	性能指标	包/秒
	发送广播包率	性能指标	包/秒
	广播包率	性能指标	包/秒
	接收广播包数	信息指标	包
	发送广播包数	信息指标	包
	接收组播包率	性能指标	包/秒
	发送组播包率	性能指标	包/秒
	组播包率	性能指标	包/秒
	接收组播包数	信息指标	包
	发送组播包数	信息指标	包
	接口子网非单播包累计接收的包数	信息指标	包
	接口子网非单播包累计发送的包数	信息指标	包
	接收错误包率	性能指标	%
	发送错误包率	性能指标	%
	接口总流量	性能指标	bps
	风扇索引	信息指标	
	风扇名称	信息指标	
	风扇可用性状态	可用性指标	
	风扇运行状态	信息指标	
	电源索引	信息指标	
	电源名称	信息指标	
	电源可用性状态	可用性指标	
	电源当前状态	信息指标	

对象	指标描述	类型	单位
	温度索引	信息指标	
	温度名称	信息指标	
	温度当前值	性能指标	℃
	温度当前状态	信息指标	
	索引 id	信息指标	
	索引	信息指标	
	名称	信息指标	
	类型	信息指标	
	软件版本	信息指标	
	序列号	信息指标	
	厂商	信息指标	
	生产日期	信息指标	
	实体型号	信息指标	
	温度	信息指标	

9.2.4 数据库监控指标

对象	指标描述	单位
数据库	花费在 行锁上的时间	毫秒
	行锁每秒要等待的次数	次/秒
	连接到服务器的速率	连接数/秒
	服务器启动同时使用的最大数目连接数	连接数
	删除语句的速率（次数/s）	次/秒
	删除多语句的速率（次数/s）	次/秒
	插入语句的速率（次数/s）	次/秒
	插入 SELECT 语句的速率（次数/s）	次/秒
	代替 SELECT 语句的速度（次数/s）	次/秒
	SELECT 语句的速度（次数/s）	次/秒
	更新语句的速度（次数/s）	次/秒
	更新多语句的速度（次数/s）	次/秒
	执行语句时每秒创建的服务器内部磁盘上的临时表的数量 （表数量/s）	个/秒
	每秒创建临时文件的数量 (文件数/s)	个/秒
	每秒执行语句时创建的服务器内部临时表的数量（表数量/s）	个/秒
	在内核空间中花费的 CPU 时间占比	百分比
	键缓存利用率 (百分比)	百分比
	打开的文件数	个
	打开的表数量	个
	查询缓存命中率	次/秒

对象	指标描述	单位
	查询的速率 (次数/s)	次/秒
	服务器执行的语句的速率（次数/s）	次/秒
	慢查询的速率（次数/s）	次/秒
	由于表锁定请求无法处理需要等待的总次数	次
	当前打开的连接的数量	连接数
	正在运行的线程数	线程数

9.2.5 中间件监控指标

对象	指标描述	单位
Apache	总计传输的字节数	字节数
	每秒传输字节数	字节数/秒
	总的请求数	请求数
	每秒请求数	请求数/秒
	活动线程数	线程数
	CPU 负载	百分比
	空闲线程数	线程数
	Apache 运行时间	秒
Nginx	接受的客户端连接的总数	连接数
	当前客户端连接数	连接数
	删除的客户端连接的总数	连接数
	当前空闲客户端连接数	连接数
	配置(configuration)重新加载的总数	个
	上次重新加载配置（configuration）的时间（自 Epoch 以来的时间）	毫秒
	连接丢失率	连接数/秒
	打开连接的速率	连接数/秒
	活动连接的总数	连接数
	读取客户端请求的连接数	连接数
	请求的处理速率	请求/秒
	等待工作的 keep-alive 连接的数量	连接数
	等待上行（upstream）响应 和/或 将响应写回客户端的连接数	连接数
	处理状态请求的工作进程的 ID	无
	异常终止并重新生成的子进程的总数	个
	当前客户端请求数	请求数
	客户端请求的总数	请求数
	未发送响应而完成的请求总数	请求数
	当前正在处理的客户端请求数	请求数

对象	指标描述	单位
	从客户端接收的数据总量	字节
	从客户端接收的客户端请求的总数	请求数
	具有 1xx 状态码的响应数	响应数
	具有 2xx 状态码的响应数	响应数
	具有 3xx 状态码的响应数	响应数
	具有 4xx 状态码的响应数	响应数
	具有 5xx 状态码的响应数	响应数
	发送到客户端的响应总数	响应数
	发送到客户端的数据总量	字节
	成功的 SSL 握手总数	次
	失败的 SSL 握手总数	次
	SSL 握手期间的会话重用总数	次
	自 Epoch 以来的时间	毫秒
	当前空闲的 keepalive 连接数	连接数
	当前活动连接数	连接数
	指示服务器是否为备份服务器的布尔值	是/否
	服务器变成 “unavail” 或 “unhealthy” 的时间（自 Epoch 开始）	毫秒
	服务器处于 “unavail” 或 “unhealthy” 状态的总时间	毫秒
	与服务器通信失败的总次数	次
	health check 请求总数	次
	health check 的失败数	次
	布尔值，指示上次运行状况检查请求是否成功并通过了测试	是/否
	服务器变得不健康 (state “unhealthy”) 的次数	次
	服务器的 ID	无
	从此服务器接收的总数据量	字节
	转发到此服务器的客户端请求总数	请求数
	具有 1xx 状态码的响应数	响应数
	具有 2xx 状态码的响应数	响应数
	具有 3xx 状态码的响应数	响应数
	具有 4xx 状态码的响应数	响应数
	具有 5xx 状态码的响应数	响应数
	从此服务器获取的响应总数	响应数
	上次选择服务器以处理请求（1.7.5）的时间（自 Epoch 开始）	毫秒
	发送到此服务器的数据总量	字节
	由于失败尝试次数达到 max_fails 阈值，服务器对客户端请求不可用 (state “unavail”) 的次数	次
	Weight of the server	无

对象	指标描述	单位
	nginx 的版本	无
Tomcat	每秒接收的字节数	字节/秒
	每秒发送的字节数	字节/秒
	每秒访问缓存的次数	次/秒
	每秒缓冲命中的次数	次/秒
	发生错误的请求数	错误数/秒
	web 模块中加载的 JSP 数量	页/秒
	web 模块中重新加载的 JSP 数量	页/秒
	最长的请求处理时间 (milliseconds)	毫秒
	每秒所有请求的处理时间之和	次
	每秒总请求数	请求数/秒
	servlet 接收的错误请求数 /s	错误数/秒
	每秒经过 servlet 的所有请求的处理时间之和	秒
	每秒经过 servlet 的总请求数	请求数/秒
	正在使用的线程数	线程数
	当前线程池的线程数	线程数
	线程池最大可以产生的线程数	线程数
Weblogic	部署状态，当前应用的部署状态，如正在部署、部署失败、部署成功等	无
	检查 JSP 文件是否发生更改并需要重新编译的频率	无
	应用程序当前会话数	无
	应用程序最高会话数	无
	检查 servlet 是否已被修改的频率	无
	会话缓存保留时长	秒
	会话 id 长度（数字位数）	无
	将超时和无效会话释放前等待的时间	秒
	会话超时设置	秒
	应用程序会话打开数/周期，周期指设置的数据采集周期	无
	执行各个 servlet 调用的平均时长	秒
	执行最长 servlet 调用的时长	秒
	执行最短 servlet 调用的时长	秒
	执行完所有 servlet 调用的时长	秒
	servlet 调用总次数/周期，周期指设置的数据采集周期	无
	servlet 池的线程最大容量	无
	servlet 重载的次数/周期，周期指设置的数据采集周期	无
	已处理的守护请求数/周期，周期指设置的数据采集周期	无
	已处理的请求数/周期，周期指设置的数据采集周期	无

对象	指标描述	单位
	挂起的守护请求数/周期，周期指设置的数据采集周期	无
	挂起的请求数/周期，周期指设置的数据采集周期	无
	假死的线程数	无
	堆内存空闲量	MB
	堆内存使用百分比	%
	堆内存使用量	MB
	堆内存最大允许值	MB
	jvm 的 cpu 负载	%
	jvm 运行时长	秒
IIS	options 方法请求数	请求数
	head 方法请求数	请求数
	del 方法请求数	请求数
	cgi 请求执行数	执行数
	isapi 请求执行数	执行数
	文档未找到导致错误的次数	次
	每秒接收的文件数	个/秒
	put 方法请求数	请求数
	trace 方法请求数	请求数
	每秒尝试连接数	个/秒
	每秒非匿名用户的请求数	请求数/秒
	每秒传输的字节总数	字节/秒
	每秒接收的字节数	字节/秒
	每秒发送的字节数	字节/秒
	活跃连接数	个
	文档锁定导致的错误数	个
	每秒匿名用户的请求数	个/秒
	每秒发送的文件数	个/秒
	post 方法请求数	个
	get 方法请求数	个
	iis 服务器运行时间	无

9.2.6 应用监控指标

对象	指标描述	单位
应用监控	url 响应时间	秒
	返回状态码	无
	url 连通状态	无
	端口连通状态	无
	进程连接状态	无

9.3 附录 3 采购清单附录

9.3.1 硬件清单

说明：以下设备不限定品牌、型号、CPU 和主机架构。①设备的性能，功能，内存、硬盘等存储规格和裸容量，网络、硬盘等 IO 的规格和数量以及服务不得低于当前配置。②主机 MTBF 不低于 10 万小时。③可以根据实际情况上调设备配置，在提高性能、不低于上述功能性、稳定性和可用存储容量基础上，增加设备数量，但不得低于当前要求。

类别	序号	硬件名称	配置参数	数量
服务器及配件	1	云管理节点	CPU：2×14 core 2.2GHz X86 架构； 内存：14×32GB DDR4； RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容； 硬盘：7×600GB SAS、5×4TB SATA、1×1.6TNVMe SSD； 网络：2×GE+4×10GE；4×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	1
	2	数据域计算节点	CPU：2×16 core 2.3GHz X86 架构； 内存：不少于 1024GB DDR4，每个内存通道平均分配； RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容； 硬盘：2×600GB SAS； 网络：2×GE+6×10GE；6×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	5

	3	前置区计算节点	CPU：2×16 Core 2.3GHz X86 架构； 内存：不少于 1024GB DDR4，每个内存通道平均分配; RAID 卡：LSI G2 掉电保护模块(含超级电容)(2U 标卡 RAID),12Gb 2 端口 SAS RAID 卡(带 1GB 缓存,支持 8 个 SAS 口）；支持 RAID0,1,5,6,10,50,60； 硬盘：2×1200GB SAS； 网络：4×GE+4×10GE；4×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	20
	4	分布式存储（云平台）	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：160GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：12×8TB SATA、2×600GB SAS、2×1.6TB NVMe SSD; 网络：4×GE+4×10GE；4×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	3
	5	对象存储	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：160GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：12×8TB SATA、2×600GB SAS、3×1.6TB NVMe SSD; 网络：4×GE+4×10GE；4×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	3
	6	文件存储	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：160GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：11×8TB SATA、2×600GB SAS、1×1.92TB SSD; 网络：4×GE+4×10GE；4×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	3
	7	多用途 A	CPU：2×16 core 2.3GHz X86 架构； 内存：512GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容;	23

			硬盘：2×600GB SAS 15K； 网络：2×GE+6×10GE；6×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	
	8	多用途B	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：12×4T SATA、2×600GB 10K SAS； 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	5
	9	深加工	CPU：2×32 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：4×1.2TB SAS、2×600GB SAS； 网卡：2GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	2
	10	高级运算	CPU：2×32 Cores 2.6GHz ARM 架构； 内存：512GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、2×3.84T SSD； 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	17
	11	HBase组件计算存储节点1（存储节点）	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、36×6TB SATA、1×1.6TB PCIE-SSD； 网络：2×GE+4×10GE;4×SFP+ 万兆模块； 分布式大数据存储软件和授权 提供最终验收合格后五年原厂维保及硬盘不返还服务。	7

	12	HBase 组件计算存储节点 2（计算节点）	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、2×6TB SATA; 网络：2×GE+2×10GE;2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	13
	13	ES 服务器	CPU：2×32 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、24×1.8TB SAS; 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	28
	14	图数据库组件	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：512GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、24×1.8TB SAS; 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	2
	15	Hive 组件集群	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：12×4T SATA、2×600GB 10K SAS; 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	4
	16	Redis 组件集群	CPU：2×32 Cores 2.6GHz ARM 架构； 内存：512GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、24×1.8TB SAS; 网络：2×GE+2×10GE；2×SFP+ 万兆模块；	3

			提供最终验收合格后五年原厂维保及硬盘不返还服务。	
	17	Spark 组件集群	CPU：2×48 Cores 2.6GHz ARM 架构； 内存：512GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：12×4T SATA、2×600GB 10K SAS； 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	3
	18	大数据控制节点	CPU：2×32 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、8×600GB SAS； 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	2
	19	MPPDB 组件集群	CPU：2×32 Cores 2.6GHz ARM 架构； 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：2×600GB SAS、24×1.8TB SAS； 网络：2×GE+2×10GE；2×SFP+ 万兆模块； 提供最终验收合格后五年原厂维保及硬盘不返还服务。	4
	20	图情处理服务器 1	CPU：2 颗 10 核(主频 2.5GHz）X86 架构; 内存：256GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：4×1.8T 10K SAS； 网卡：2×10GE 光口和模块 GPU 卡：5 块 GPU 卡 提供最终验收合格后五年原厂维保及硬盘不返还服务。	1

	21	图情处理服务器 2	CPU：2 颗 12 核(主频 2.6GHz） X86 架构; 内存：512GB DDR4; RAID 卡：支持 RAID0,1,5,6,10,50,60，2G 缓存，超级电容; 硬盘：4×1.8T 10K SAS; 网卡：2×10GE 光口和模块 GPU 卡：4 块 GPU 卡 提供最终验收合格后五年原厂维保及硬盘不返还服务。	1
	22	内存条	原厂 DDR4 32GB 内存条（匹配升级已部署的服务器设备） 提供最终验收合格后五年维保。	208

类别	序号	硬件名称	配置参数	数量
网络设备	23	接入交换机	一、硬件参数： ≥24×10GE SFP+端口，配置≥14 个万兆多模模块，配置包转发率≥720Mbps、交换容量≥2.56Tbps，冗余电源。 二、功能参数： 1、支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 2、支持 VxLAN 功能，支持 BGP EVPN； 三、其它参数： 提供最终验收合格后五年维保。	2
	24	TAP 交换机 1	一、硬件参数： ≥24 个 SFP+端口，配置≥8 个万兆多模模块。 二、功能参数： 1、流量复制/汇聚/分流一体化： 2、支持报文切片； 3、支持时戳和标记源端口； 4、支持 Hash 动态均衡负载，从而保证流量输出的会话完整性；支持五元组、IP 碎片分析、报文内容标识等过滤； 5、具备流量数据管控策略业务定义能力及数据来源、去向、状态展示能力。 三、性能参数： 处理性能≥480Gbps。 四、其它参数： 提供最终验收合格后五年维保。	1
	25	TAP 交换机 2	一、硬件参数： ≥12 个 SFP+端口，配置≥6 个万兆多模模块。 二、功能参数：	1

			1、流量复制/汇聚/分流一体化： 2、支持报文切片； 3、支持时戳和标记源端口； 4、支持 Hash 动态均衡负载，从而保证流量输出的会话完整性；支持五元组、IP 碎片分析、报文内容标识等过滤； 5、支持将设备接收到的所有网络流量合并后，传输至 1 个或多个不同的流量监控系统。 三、性能参数： 处理性能≥240Gbps。 四、其它参数： 提供最终验收合格后五年维保。	
	26	交换机 1	一、硬件参数： ≥12 个 10/100/1000Base-TX 口，≥6 个万兆 SFP+口，配置≥6 个万兆多模模块，冗余电源。 二、功能参数： 1、支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 2、支持 VxLAN 功能，支持 BGP EVPN； 三、其它参数： 提供最终验收合格后五年维保。	2
	27	交换机 2	一、硬件参数： ≥24 个 10/100/1000Base-TX 口，≥8 个万兆 SFP+口，配置≥8 个万兆多模模块，冗余电源。 二、功能参数： 1、支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 2、支持 VxLAN 功能，支持 BGP EVPN； 三、其它参数： 提供最终验收合格后五年维保。	2
	28	交换机 3	一、硬件参数： ≥48 个 10/100/1000Base-TX 口，≥20 个万兆 SFP+口，配置≥20 个万兆多模模块，冗余电源。 二、功能参数： 1、支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 2、支持 VxLAN 功能，支持 BGP EVPN； 三、其它参数： 提供最终验收合格后五年维保。	1

	29	万兆接入交换机 1	一、硬件参数： 1、交换容量≥4.8Tbps，包转发率≥1600Mpps，冗余电源； 2、≥48 个万兆光口、≥6 个 40GE 光口，配置≥30 个万兆模块，≥2 个 40GE 模块； 二、功能参数： 1、支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 2、支持 VxLAN 功能，支持 BGP EVPN； 三、其它参数： 提供最终验收合格后五年维保。	8
	30	千兆接入交换机	一、硬件参数： 1、交换容量≥1.6Tbps，包转发率≥406Mpps，冗余电源； 2、≥48 个千兆电口、≥4 个万兆光口，配置≥4 个万兆模块； 二、功能参数： 1、支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 2、支持 VxLAN 功能，支持 BGP EVPN； 三、其它参数： 提供最终验收合格后五年维保。	9
	31	万兆接入交换机 2	一、硬件参数： 1、交换容量≥4.8Tbps，包转发率≥1600Mpps，冗余电源； 2、≥48 个万兆光口、≥6 个 40GE 光口，配置≥48 个万兆模块，≥2 个 40GE 模块； 二、功能参数： 1、支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 2、支持 VxLAN 功能，支持 BGP EVPN； 三、其它参数： 提供最终验收合格后五年维保。	2
网络与系统安全设备	32	可信接入检控	一、硬件参数： 标准机架式设备，配置≥2 个千兆电口，≥2 个万兆 SFP+光口。 二、功能参数： 1、具备协议格式检查与控制功能：提供请求和响应报文头、报文格式检查能力，支持 HTTP、WebSocket 及虚拟桌面等的通信协议，根据检查结果阻断或放行； 2、具备令牌检查与控制功能：提供用户令牌、应用令牌检查能力，支持令牌格式、签名、内容、有效期的安全检查，根据检查结果阻断或放行； 3、具备终端身份检查与控制功能：配合环境感知系统提供接入终端的身份核验能力，支持终端身份进行安全检查，根据检查结果阻断或放行； 4、具备日志记录与报送功能：提供用户访问日志、检控告警记录及上报能力； 5、具备流量管控功能：支持对应用请求信息进行流量控制，	1

			支持基于请求内容大小、请求速度、请求连接数和访问时段等参数进行流量控制； 6、具备熔断机制功能：支持访问超时熔断和并发熔断； 7、具备通道安全功能：支持国密 SSL 协议，对业务流量进行加密。 三、性能参数： 1、吞吐率：≥1.2Gbps； 2、并发连接数：≥6000 条/秒； 3、延迟：＜200ms。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	33	下一代防火墙 1	一、硬件参数： 1、标准机架式设备； 2、≥6 个 10/100/1000M Base-TX，≥配置 6 个 SFP+口，配置≥6 个万兆多模模块。 3、含防病毒模块、入侵防御模块； 二、功能参数： 1、实现网络访问控制、病毒防护、入侵防御等； 2、支持透明、路由、混合、旁路 4 种工作模式； 3、支持网络地址转换，所投产品支持源 NAT 和目的 NAT； 4、支持访问控制，能够基于源、目的、应用协议做会话数限制； 5、支持未知威胁检测能力； 6、具备 IPSec VPN 智能选路功能，根据线路质量实现自动链路切换。 三、性能参数： 1、整机吞吐量：≥20Gbps； 2、并发连接数：≥600 万。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务（含特征库升级）。	4
	34	堡垒机 1	一、硬件参数： 标准机架式设备，配置≥4 个网口、≥2 个 SFP+口（含≥2 个多模模块）。 二、功能参数： 1、实现集中账号管理、集中访问控制、集中安全审计； 2、支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权； 3、支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功。 4、支持国密算法下的身份鉴别功能，数据传输机密性功能，数据传输完整性功能、数据原发抗抵赖和数据接收抗抵赖功能； 5、支持同时对数据库会话记录审计及命令提取审计，支持对	1

			数据库上行和下行命令进行审计,具备数据库操作命令执行管控能力。 三、性能参数： 1、管理授权≥3000; 2、最大字符并发≥2500 个; 3、最大图像并发≥500 个。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	35	日志采集设备	一、硬件参数： 标准机架式设备，配置≥2 个网口。 二、功能参数： 1、采集安全访问与数据交换中网络设备、安全设备、应用系统等安全相关日志信息,并进行预处理; 2、具备主动采集和被动采集两种方式，其中主动采集主要包括 SFTP、SNMP Get、WMI 等协议的日志采集，被动采集主要包括 SYSLOG、HTTPS、SNMP Trap 等协议的日志采集； 3、支持与安全管理中心对接，通过 kafaka、消息队列、SFTP、FTP 等协议将数据上报到安全管理中心等外部日志分析处理平台。 三、性能参数： 1、日志采集速率≥10000 条/秒。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1
	36	网络流量分析 1	一、硬件参数： 标准机架式设备，配置≥2 个 SFP+。 二、功能参数： 1、利用网络流量数据，通过网络流量实时检测或网络日志离线检测，识别网络异常行为，发现网络威胁； 2、威胁分析检测的能力应包含但不限于：DNS 异常分析、流量分析、HTTP/HTTPS 日志分析、主机日志分析等安全分析能力;发现恶意 DNS 请求、恶意攻击的 HTTP 请求、恶意 URL 访问、Webshell 访问行为等； 3、利用网络流量数据，通过网络流量实时检测，全量存储所有网络会话数据，识别网络异常行为，发现网络威胁，对并威胁进行原始数据包取证； 4、威胁分析检测的能力应包含但不限于：DNS 异常分析、流量分析、HTTP/HTTPS 日志分析等安全分析能力；发现恶意 DNS 请求、恶意攻击的 HTTP 请求、恶意 URL 访问、SQL 注入、钓鱼网站、木马病毒、僵尸网络及其他异常访问行为等; 5、支持以源 IP、目的 IP 和目的端口三元组的形式聚合网络全流量会话记录，记录分析字段需要包括但不限于协议、请求传输总时间、会话持续时间等等； 6、具备丰富标准的数据接口，实时按需输出网络全量会话、应用日志记录，支持与安全管理中心大数据平台进行数据对	1

			接。 三、性能参数： 1、整机吞吐量≥40Gbps。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	37	万兆入侵检测	一、硬件参数： 标准机架式设备，配置≥6 个 10/100/1000M Base-TX，≥2 个 10G SFP+（含≥2 个万兆多模模块）。 二、功能参数： 1、支持 HTTP Get、Head、Put、Post 等多种协议方法检查； 2、支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等多种协议和应用的攻击检测； 3、支持对数据包进行协议异常检测； 4、支持 IP 地址、通信端口扫描异常检测。 三、性能参数： 1、整机吞吐量：≥40Gbps； 2、并发 TCP 会话数：≥5000 万。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1
	38	应用日志采集设备	一、硬件参数： 1、标准机架式设备，配置≥128GB DDR4 内存，≥240GB SSD 硬盘、≥7TB SAS 热插拔硬盘，支持 Raid； 2、配置≥1×千兆网卡（电口），≥1×双口万兆光纤网卡（含≥2 个万兆多模模块），≥1×RJ45 接口的管理网口。 二、功能参数： 1、具备数据镜像功能，所有通过该路由器或交换机的网络数据通过数据镜像方式从镜像口输出到对应采集探针； 2、具备数据过滤功能，根据预先设置的审计要素，筛选需要的网络数据流量，对于无用数据流量直接舍弃； 3、具备日志数据提取功能，根据日志数据提取规则，按照业务操作模型，提取相应操作内容。 三、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1
	39	数据库审计	一、硬件参数： 配置≥2 个 SFP+口。 二、功能参数： 1、针对大数据平台重要数据库（如原始库、资源库、主题库、业务库、知识库、索引库）实现各类操作行为的审计； 2、审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置； 3、系统无需在数据库服务器上安装任何插件，旁路部署，对系统零影响； 4、支持主动监控 MySQL、Oracle、sqlserver、mongodb、redis 等数据库的状态，可以对数据库服务器运行状态进行实时的监	2

			控与记录，主动发现数据库异常； 5、支持 Hadoop 架构下的大数据库 HBase 的审计，包括其通用的 SQL 及 NoSQL 工具及对外开放的软件接口的监控与审计，如 HIVE 等； 6、支持除去支持对各种数据库访问审计外，还支持 TELNET、FTP、HTTP、NFS、等各种字符型协议对数据库服务器的访问，并可对其设置告警条件； 7、支持通过对组合关联行为审计，能够检测语句系列或重复语句的 APT 攻击行为； 8、支持嵌套、函数、绑定变量、长语句、返回结果、脚本等复杂和隐秘统方等操作的审计，深度识别和立体分析，不漏审、不误审； 9、系统内置敏感数据类型，支持敏感数据自定义，支持同步敏感数据扫描结果中的敏感数据，支持自定义敏感规则，可根据配置字段进行敏感字段的操作行为监控与审计。 10、支持操作语句系列的组合规则，支持重复操作的统计审计规则。 三、性能参数： 1、峰值事件处理能力≥20000 条语句/秒； 2、日志存储≥32 亿条。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	40	云防火墙服务	一、硬件参数： 1、配置≥4 个 SFP+口； 2、提供 2 台防火墙分别部署于前置区云平台、数据域云平台，为云上提供虚拟化网络隔离与访问控制服务。 二、功能参数： 1、支持透明、路由、混合、旁路 4 种工作模式； 2、支持网络地址转换，所投产品支持源 NAT 和目的 NAT； 3、支持访问控制，能够基于源、目的、应用协议做会话数限制； 4、具备未知威胁检能力； 5、具备 CC 攻击防护功能； 三、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务（含特征库升级）。	1
	41	安全雷达系统	一、硬件参数： 标准机架式设备。 二、功能参数： 1、具备资产安全监控功能：系统对网中接入的资产自动获取厂商品牌、设备类型、操作系统类型、协议、智能平台等，并建立设备指纹库，同时对资产非法接入、非法占用、非法替换等网络异常行为进行监控告警；	1

			2、具备边界安全监控功能：采用非侵入式的监控模式，无需部署客户端、改造网络和应用，不间断对全网私自搭建的不受控网络边界进行监控，及时发现数据泄露、外部入侵、僵木蠕病毒入网等重大安全威胁的不受控入网通道。 3、具备网络攻击监控功能：基于 UEBA 安全分析框架对专网内网络通信行为进行大数据建模分析，对网络攻击行为进行监控； 4、具备违规行为监控功能：对网内出现的各类违规行为进行监控发现并告警，如违规访问、违规站点、设备违规入网、移动设备入网等。系统对此类行为建立违规分析模型，通过正则方式匹配网络行为，发现并定位违规主机； 5、具备安全隐患监控功能：对全网设备节点进行全端口扫描监听，针对开放的端口进行识别，实时分析端口、服务开放详情，及时发现网内自身存在脆弱性的资产设备，易被内外威胁利用或被当做攻击载体的设备，对全网造成破坏，引发各类安全事件，包括有：异常端口开放、违规服务搭建、可匿名登陆 FTP 等； 6、具备两网互通监控功能：包括支持违规外联监测，发现终端两网互通的行为，一旦发现，定位其终端地址； 7、具备网络空间测绘功能，能够排查网内存在的非合规或不受控链路节点； 8、具备数据取证功能：支持对发现各种的监测告警行为提供数据取证功能，支持对行为进行取证留存。 三、性能参数： 1、支持≥150000IP； 2、支持软件探针≥300 个； 3、支持 JS 探针≥3 个； 4、支持数据处理性能≥120 万并发会话。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	42	入侵检测系统	一、硬件参数： 配置≥2 个 10/100/1000M Base-TX，≥2 个 SFP，含≥2 个万兆多模模块，冗余电源。 二、功能参数： 1、支持 HTTP Get、Head、Put、Post 等多种协议方法检查； 2、支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等多种协议和应用的攻击检测； 3、支持对数据包进行协议异常检测； 4、支持 IP 地址、通信端口扫描异常检测。 三、性能参数： 整机吞吐量：≥10Gbps。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1
	43	网络流量分	一、硬件参数：	1

		析 2	配置≥2 个 SFP+口。 二、功能参数： 1、支持利用网络流量数据，通过网络流量实时检测或网络日志离线检测，识别网络异常行为，发现网络威胁； 2、支持威胁分析检测的能力应包含但不限于：DNS 异常分析、流量分析、HTTP/HTTPS 日志分析、主机日志分析等安全分析能力；支持发现恶意 DNS 请求、恶意攻击的 HTTP 请求、恶意 URL 访问、Webshell 访问行为等； 3、利用网络流量数据，通过网络流量实时检测，全量存储所有网络会话数据，识别网络异常行为，发现网络威胁，对并威胁进行原始数据包取证； 4、威胁分析检测的能力应包含但不限于：DNS 异常分析、流量分析、HTTP/HTTPS 日志分析等安全分析能力；发现恶意 DNS 请求、恶意攻击的 HTTP 请求、恶意 URL 访问、SQL 注入、钓鱼网站、木马病毒、僵尸网络及其他异常访问行为等； 5、支持以源 IP、目的 IP 和目的端口三元组的形式聚合网络全流量会话记录，记录分析字段需要包括但不限于协议、请求传输总时间、会话持续时间等等； 6、具备丰富标准的数据接口，实时按需输出网络全量会话、应用日志记录，支持与安全管理中心大数据平台进行数据对接。 三、性能参数： 整机吞吐量≥20Gbps。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	44	数据安全交换设备	一、硬件参数： 1、设备由内交换服务器和外交换服务器 2 台物理设备组成； 2、每台服务器硬件为标准机架式，网口配置为≥2 个千兆电口，≥2 个万兆光口。 二、功能参数： 1、具备文件交换功能：支持主动访问、身份鉴别等多种安全模式；支持多种文件传输协议；支持内容过滤、优先级策略设置； 2、具备数据库交换功能：支持多种常用主流数据库之间的交换；支持从文件到数据库的双向交换模式； 3、具备审计和管理功能：基于 B/S 架构，支持细粒度日志审计；支持图形化操作； 4、支持多种类型交换方式，包括但不限于 FTP 文件交换、基于 1400 协议的视图交换、数据库同构同库交换等； 5、提供全面的交换业务的操作日志，记录的信息包括但不限于每一个交换业务的源信息、目标信息、报错信息、交换历史、当前状态等。 三、性能参数：	4

			1、数据库数据增量同步传输速率：≥10000 条/秒； 2、FTP 文件（文件大小为 1MB）同步传输平均传输速率：≥4Gbps； 3、支持数据库数据映射最大字段数：≥256 个； 4、单个最大数据文件：≥100GB； 5、支持文件传输任务数：≥64 个。 四、其它参数： 1、产品生产厂商需入围《通过公安部组织测试的接入平台厂商名单》，提供证明材料（供货时提供）； 2、提供最终验收合格后五年维保及硬盘不返还服务。	
	45	网闸 1	一、硬件参数： 1、标准机架式设备； 2、配置≥8 个千兆电口（含管理口、HA 口）、≥4 个万兆 SFP+插槽（含 4 个多模模块）、≥4 个 USB 接口。 二、功能参数： 1、支持 IPv4、IPv6 双协议栈接入； 2、支持 oracle、Sql Server 、DB2、Sybase 等主流数据库间的同种或异种数据库同步，支持单向和双向同步； 3、支持管理方式采用 B/S 架构的 WEB 方式管理； 4、支持内外网分别采用独立管理口管理； 5、支持内外网主机系统分别支持双系统引导，并可在 WEB 界面上直接配置启动顺序，在 A 系统发生故障时，可以随时切换到 B 系统；且支持系统(包括配置文件)备份； 6、具备抗攻击功能，能够识别和防御 SYN Flood、ICMP Flood 等攻击，提供公安部检测报告（供货时提供）。 三、性能参数： 系统吞吐量≥8000Mbps。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	2

	46	网闸 2	一、硬件参数： 1、标准机架式设备； 2、内网配置≥6 个 10/100/1000Base-T 端口，≥4 个 SFP 接口，≥2 个 SFP+接口（含 1 个万兆多多模块），≥1 个 Console 口，≥2 个 USB 口； 3、外网内置≥6 个 10/100/1000Base-T 端口，≥4 个 SFP 接口，≥2 个 SFP+接口（含 1 个万兆多多模块），≥1 个 Console 口，≥2 个 USB 口。 二、功能参数； 1、支持 IPv4、IPv6 双协议栈接入； 2、支持支持 oracle、Sql Server、DB2、Sybase 等主流数据库间的同种或异种数据库同步，支持单向和双向同步； 3、支持管理方式采用 B/S 架构的 WEB 方式管理； 4、支持内外网分别采用独立管理口管理； 5、支持内外网主机系统分别支持双系统引导，并可在 WEB 界面上直接配置启动顺序，在 A 系统发生故障时，可以随时切换到 B 系统；且支持系统(包括配置文件)备份； 6、具备抗攻击功能，能够识别和防御 SYN Flood、ICMP Flood 等攻击，提供公安部检测报告（供货时提供）。 三、性能参数： 吞吐量：≥4Gbps。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	2
	47	下一代防火墙 2	一、硬件参数： 1、标准机架式设备，≥16 个 10/100/1000M Base-TX，配置≥4 个 SFP+口，含≥4 个万兆多模模块； 2、含防病毒模块，入侵防御模块； 二、功能参数： 1、支持透明、路由、混合、旁路 4 种工作模式； 2、支持网络地址转换，所投产品支持源 NAT 和目的 NAT； 3、支持访问控制，能够基于源、目的、应用协议做会话数限制； 4、具备未知威胁检测能力； 5、具备 IPSec VPN 智能选路功能，根据线路质量实现自动链路切换。 三、性能参数： 1、网络处理能力≥16G； 2、并发连接数≥400 万。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务（含特征库升级）。	6

	48	入侵防御	一、硬件参数： 标准机架式设备，≥4 个 10/100/1000BASE-T 电口，≥1 个扩展槽位，≥4 万兆光口（含 4 个万兆多模块）。 二、功能参数： 1、支持准确检测并防御针对操作系统、应用、服务器等漏洞的攻击； 2、具备防护 WEB 攻击，包括 SQL 注入攻击和跨站脚本攻击等； 3、具备 DDoS 攻击防护，可防范 SYN flood、UDP flood 等种常见网络层 DDoS 攻击及 HTTP、HTTPS、SIP、DNS 等应用层 DDoS 攻击。 三、性能参数： 1、IPS 吞吐量≥10Gbps； 2、并发连接数≥300 万。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务（含特征库升级）。	1
	49	探针	一、硬件参数： 标准机架式设备，≥6 个千兆网络接口。 二、功能参数： 1、支持采集多种设备的运行状态信息； 2、支持对多种设备的流量信息采集； 3、支持 SYSLOG 协议；支持 SNMP v2/SNMP v3 协议； 4、支持与“集中监控与审计设备”对接，转发数据。 三、其它参数： 1、本设备为公安行业边界级联监管专用设备，为保证其审计监管信息的有效性和完整性，设备需符合公安部公安警用装备产品信息库对级联监管系统的基本要求，需提供入围公安警用装备产品信息的证明材料（供货时提供）； 2、提供最终验收合格后五年维保及硬盘不返还服务。	3
	50	入侵检测	一、硬件参数： 标准机架式设备，≥2 个 10/100/1000M 自适应电口；≥2 个万兆 SFP+模块口扩展卡（含≥2 个万兆多模模块）。 二、功能参数： 1、支持 HTTP Get、Head、Put、Post 等多种协议方法检查； 2、支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等多种协议和应用的攻击检测； 3、支持对数据包进行协议异常检测； 4、支持 IP 地址、通信端口扫描异常检测。 三、性能参数： 1、吞吐量≥15Gbps； 2、并发连接≥200 万； 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务（含特征库升	2

			级）。	
	51	边界安全访问控制网关	一、硬件参数： 1、标准机架式设备； 2、配置≥2 个千兆电口、≥6 个万兆光口，含≥2 个多模模块。 二、功能参数： 1、基于国密 SSL 协议创建安全传输通道，保证数据的安全传输； 2、支持对含国密算法 SM1/SM2/SM3/SM4 硬件数字证书的身份认证； 3、基于终端特征的设备认证； 4、多服务器的集中授权管理； 5、基于链路服务的策略管理和下发； 6、基于个人证书及证书 DN 项的访问控制； 7、基于资源的访问控制； 8、基于 URL 的细粒度授权管理； 9、具有黑名单动态下载功能； 10、实现单点登录功能； 11、实现客户端自动安装； 12、支持双机热备； 13、实现系统配置备份/恢复、日志审计等系统管理功能； 14、具备的访问限制能力需提供访问用户限制、访问内容限制功能； 15、具备日志数据生成、日志跟踪管理、可理解的格式、限制日志访问等功能。 三、性能参数： 1、网络吞吐量： （1）SM4 算法≥2.8Gbps； （2）AES 算法≥8Gbps 2、最大在线\并发用户数（客户端双向认证）： （1）SM2 算法在线用户数≥4500； （2）SM2 算法并发用户数≥4500。 四、其它参数： 1、产品应入选“通过公安部组织测试的接入平台安全产品名单”，或是入选产品的升级版，需提供通过公安部组织测试的接入平台安全产品名单的证明材料（供货时提供）； 2、提供最终验收合格后五年维保及硬盘不返还服务。	1
	52	抗 DDOS	一、硬件参数： 标准机架式设备，≥4 个 10/100/1000BASE-T 口，≥4 个万兆光口（含≥4 个多模模块） 二、功能参数： 1、支持各种传输层的拒绝服务攻击，如 SYN Flood，SYN-ACK Flood，ACK Flood，FIN/RST Flood ，UDP Flood，ICMP Flood，IP Fragment Flood、Stream flood 等； 2、支持对不同种类的 DDoS 攻击采用不同的算法识别，从而	1

			准确地区分出恶意 DDoS 报文。 三、性能参数： 1、清洗性能≥15Gbps； 2、小包防御能力（64 字节/pps）≥2500 万 pps。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	53	WEB 防火墙	一、硬件参数： 标准机架式设备，提供≥4 个 10/100/1000M 电口、≥4 个 SFP+万兆插槽（含≥4 个多模模块）。 二、功能参数： 1、支持透明串接、反向代理、旁路引流部署、旁路镜像审计部署； 2、支持主流特征库，对文件上传内容进行检查； 3、支持根据 URL、请求头字段、目标 IP、请求方法等多种组合条件对 CC 攻击进行检测； 4、支持对文件上传内容进行检查，防止恶意 Webshell 上传，对已经上传的 Webshell 发起请求的行为进行拦截阻断。 三、性能参数： 1、网络层吞吐率≥ 16Gbps ； 2、应用层吞吐率≥ 3Gbps ； 3、最大并发连接数≥ 280 万。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务(含特征库升级）。	1
	54	单向安全传输设备	一、硬件参数： 1、由导入前置机、导入服务器和安全传输系统组成； 2、导入前置机和导入服务器，每台服务器配置为标准机架式机箱，网口配置为≥2 个千兆电口，≥2 个万兆光口； 3、安全传输系统由内端机和外端机两部分组成，每端配置为标准机架式机箱，网口配置为≥2 个千兆电口，≥2 个万兆光口。 二、功能参数： 1、支持 FTP 协议，可通过推、拉与混合方式进行文件传输； 2、支持 SAMBA 协议，可通过推、拉与混合方式进行文件传输； 3、支持 NFS 文件服务端至服务端（SS）传输模式； 4、支持设备唯一性认证，导入前置机和导入服务器的认证均能够支持 IP 地址方式校验； 5、支持对应用数据的内容进行审查、过滤，只有符合安全数据才能传输； 6、支持与统一边界平台进行对接，完成交换通道的按需调度和资源资源分配； 7、满足信息流控制策略、基本的信息流控制功能、单向传输保证、残余信息保护、数据完整性保证等单向导入产品要求；	3

			8、支持多种文件格式的深度检查：包含但不限于 txt，exe，pdf，tar，doc，ppt，excel，zip，rar，bmp，jpg，tif，tga，gif，png，文件格式可定制扩展； 9、支持日志上报监管系统，日志可按照预先设定好的格式和策略自动定期上报到集中监控与审计系统。 三、性能参数： 1、产品支持最大传输任务数：≥40 个； 2、产品支持单个文件最大传输大小：≥10GB； 3、产品在 FTP-CS 模式时，小文件（1-5KB）平均传输速率：≥3000 个/秒； 4、产品在 FTP-CS 模式时，大文件（1MB）单向传输最大吞吐量：≥2048Mbps。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	
	55	集中监控与审计设备	一、硬件参数： 标准机架式设备，配置≥2 个千兆网口。 二、功能参数： 1、支持不同接入对象的信息注册和管理； 2、支持对多种设备进行监控，并提供统计分析报表； 3、动态、实时展示平台链路和设备情况； 4、支持 SNMPV2.0/3.0（被管设备需支持 SNMP 协议）、SYSLOG 协议； 5、对边界接入平台进行集中监控与审计； 6、支持按照上级的级联要求及统一标准，实时报送边界平台数据； 7、支持与本项目采购的探针联动。 三、性能参数： 1、日志存储量≥500GB； 2、存储记录数≥5 亿条； 3、每秒可接收日志条数≥200 条。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1

	56	准入网关	一、硬件参数： 标准机架式设备，≥6 个千兆电口，配置≥2 个 SFP+口，含≥2 个万兆多模模块。 二、功能参数： 1、具备多种准入技术，杜绝非法终端接入； 2、支持终端安全基线配置，提升终端安全防护能力； 3、快速进行设备定位、审计溯源和台账管理； 4、可以配置策略禁止使用外部 HTTP 代理、外部 Sock4/5 代理、HTTP,SSL 一些的标准端口上使用其他协议等； 5、可对 SSH、RDP 协议连接开始时间，连接结束时间，传输的流量大小进行审计,可对 SecureCRT、Xshell 等运维类应用的外发附件审计。 三、性能参数： 1、网络吞吐量≥2Gb； 2、支持用户数≥6000； 3、每秒新建数≥12000； 4、最大并发数≥600000。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	2
	57	统一调度系统	一、硬件参数： 1、CPU：≥8 核心 16 线程×2，≥2.4GHz 主频； 2、内存：≥64GB； 3、硬盘：≥1TB； 4、操作系统：CentOS 7.5 64bit； 5、网口：≥2 个千兆电口，≥2 个万兆光口。 二、功能参数： 1、根据业务注册信息特点及业务模式，结合设备状态，为业务提供交换通道资源的动态调度； 2、支持与配置管理中心、各服务系统和交换通道设备以及统一边界安全管理平台进行数据联动； 3、具备对接入业务自动路由功能，根据业务接入类型及节点设备状态，自动分配业务数据传输路径，解决因某个节点设备故障而导致的业务中断问题； 4、具备节点设备状态感知能力，接收各节点设备实时上报的运行状态信息、业务运行状况信息，动态感知各节点状态； 5、支持与本项目采购的单向安全传输系统、请求服务系统、统一边界安全管理平台等边界设备联动。 三、其它参数： 提供最终验收合格后五年维保硬盘不返还服务。	1

	58	统一边界安全管理平台	一、硬件参数： 1、CPU：≥8 核心 16 线程×2，≥2.4GHz 主频； 2、内存：≥64GB； 3、硬盘：≥2TB； 4、操作系统：CentOS 7.5 64bit； 5、网口：≥2 个千兆电口，≥2 个万兆光口。 二、功能参数： 1、集 IT 运维，业务运维和日常管理运维于一体； 2、收集并提供平台各资源资产情况、健康状况及运行状态的展示和查询； 3、收集并提供平台各业务运行情况的展示和查询； 4、具备业务接入全流程监控能力，包括各个节点状态，通道运行状况、阻塞程度等； 5、收集并提供平台各故障或异常告警信息的展示和查询，并定位故障资产所属环境区域，通过工单形式进行故障处理任务下发； 6、支持与本项目采购的请求服务系统、单向安全传输系统、统一调度系统等边界设备联动。 三、其它参数： 提供最终验收合格后五年维保硬盘不返还服务。	1
	59	请求服务系统	一、硬件参数： 1、系统含共 2 台设备 2、每台配置 CPU：≥32 核，≥2.3GHz 主频； 3、每台配置内存：≥128GB； 4、每台配置硬盘：≥1TB； 5、每台配置操作系统：CentOS 7.5 64bit； 6、每台配置网口：≥2 个千兆电口，≥2 个万兆光口 二、功能参数： 1、交换管理： 1）支持 Restful、Webservice 接口方式，并提供统一入口； 2）支持对请求方基于 IP 地址的身份认证及访问权限进行验证； 3）支持基于时间段、请求频次、IP 地址白名单的访问控制； 4）支持对请求和响应报文入参和出参检查。 2、节点管理： 对各节点进行注册绑定和服务分配等管理； 3、支持对接传输系统，实现请求服务类业务的请求、请求结果安全传输与交换； 4、支持与本项目采购的单向安全传输系统、统一调度系统、统一边界安全管理平台等边界设备联动。 三、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1

	60	安全感知平台	一、硬件参数： 标准机架式，配置≥6 千兆电口，≥2 千兆光口 SFP。 二、功能参数： 1、支持全流量威胁分析系统，支持 APT 防护，让安全威胁可视、可控； 2、提供深度流量检测，定位异常网络行为，及时检测和响应； 3、构建威胁统一分析能力、智能协同处置能力、抵御未知威胁能力和安全统一管理能力，提供完整有效的安全保护； 4、支持安全设备、网络设备、DHCP 服务器、蜜罐、中间件等设备日志接入，支持 syslog、winlogbeat、jdbc、wmi、webservice、ftp、snmp trap 等接入方式； 5、支持综合安全风险、主机安全风险、脆弱性感知、外部感知、工单、摘要、处置报告多种呈现方式，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等。 三、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1
	61	公安指纹数字证书	1、集成指纹运算芯片和密码运算芯片的新一代安全设备，支持国密算法，应用无需改造，且可平滑过渡到信创终端。 2、支持证书存储、签名、加解密； 3、支持包含但不限于 RSA 1024，RSA2048，SM1，SM2，SM3 算法； 4、支持公安数字证书驱动客户端（审计版），公安数字证书可准确被识别，实现使用数字证书过程中的行为审计； 5、支持与在用的 PKI 系统和证书管理系统无缝对接。	6000
其他	62	网络准入系统	一、硬件参数： 1、标准机架式设备； 2、标准配置≥6 个 1000MBASE-T 接口。 二、功能参数： 1、支持策略路由、端口镜像、透明网桥、802.1X、ARP、DHCP、VLAN 隔离、Portal 等准入技术，支持准入技术自由组合使用； 2、支持安全客户端（Agent）、安全控件、无客户端等多种模式； 3、支持用户名密码、Ukey、指纹等认证方式； 三、性能参数： 1、吞吐量：≥3.6Gbps； 2、并发连接数：≥14000（条）； 3、支持授权≥6000 个。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1

	63	蜜罐	一、硬件参数： 标准机架式设备，配置≥2 个万兆 SFP+端口； 二、功能参数： 1、支持模拟场景，可基于攻击者在虚拟环境中的行为发现攻击者恶意入侵，包括零日漏洞（0day）攻击及 APT 攻击； 2、支持运行包括但不限于真实的 Mysql、MongoDB、HBase、Hive 等服务的蜜罐； 3、支持运行 Struts2、Tomcat、SQL 注入、文件上传、WEB 页面克隆的蜜罐； 4、支持运行存在真实漏洞服务的蜜罐。 三、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1
	64	数据库审计系统	一、硬件参数： 标准机架式设备，配置≥4 个网口、≥2 个 SFP+接口。 二、功能参数： 1、具备 Oracle、SQL Server、Informix、Sybase、MySQL、MariaDB 等主流数据库审计； 2、具备 MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Canssandra、greenplum、LibrA、graphbase、cache 等数据库审计； 3、具备主流业务协议 HTTP、HTTPS、Telnet、FTP 的审计； 三、性能参数： 1、峰值 SQL 处理能力≥40,000 条/秒。 四、其它参数： 提供最终验收合格后五年维保及硬盘不返还服务。	1
	65	堡垒机 2	一、硬件参数： 标准机架式设备，≥2 个网口、≥2 个 SFP 口。 二、功能参数： 1、支持对核心业务系统、主机、数据库、网络设备等各种 IT 资源的帐号、认证、授权和审计的集中管理和控制； 2、支持国密算法下的身份鉴别功能，数据传输机密性功能，数据传输完整性功能、数据原发抗抵赖和数据接收抗抵赖功能。 三、性能参数： 1、最大字符并发≥800 个； 2、最大图像并发≥200 个； 3、管理资产≥1000 个。 四、其它参数： 提供最终验收合格后五年维保硬盘不返还服务。	1
	66	辅材	所有设备安装、调试用的跳线、网络线材、标签等	1

9.3.2 软件清单

类别	序号	软件名称	具体功能描述	数量
基础软件	1	数据域云软件	云套件标准版许可-每 CPU。	10
	2	前置区云软件	云套件标准版许可-每 CPU。	40
	3	商用大数据软件(按物理 CPU 核数计算授权）	大数据商业版本，具备：分布式文件系统、分布式作业执行调度系统、分布式计算框架、分布式数据库、集群分布式协调工具、分布式搜索和分析引擎、分布式消息、分布式缓存、API 网关、分布式事务型数据库、分布式图数据库、数据仓库工具、分布式缓存、内存计算框架等。每 CPU。	4128
	4	MPPDB 软件(按存储容量授权）	企业级的大规模并行处理关系型数据库，支持行存储和列存储，提供 PB 级别数据量的处理能力。	216
	5	网管软件	200 台服务器、5 台存储、20 台网络设备管理授权。	1
	6	云桌面	1、提供 800 个云桌面许可。 2、需支持与本项目的认证服务开展对接。	1
	7	主机安全加固服务	1、提供 2 套主机安全加固设备，分别部署于前置区云平台、数据域云平台。 2、定期对主机系统配置进行安全审查，包括弱口令检测、配置检测等； 3、支持对主机进行安全加固； 4、支持全面的监测，包括异常登录监测、文件异常监测、系统后门监测、进程异常监测等； 5、支持提供补丁的详细信息，包括补丁的修复建议、修复命令、修复影响； 6、2 套设备总共支持至少 1000 个虚拟机。	1

8	WEB应用防火墙服务	提供2套WEB应用防火墙，分别部署于前置区云平台、数据域云平台，主要是针对WEB应用系统的SQL注入、跨站脚本攻击等行为进行防御阻断，2套设备总共支持至少300个站点。	1
9	认证中心	1、本级认证服务的用户信息、组织机构信息需与上级统一用户平台数据保持一致，定期更新确保数据鲜活。 2、具备令牌的全生命周期管理，包括应用令牌和用户令牌的生成、撤销、更新、验证等。 3、认证因子需包括但不限于用户名密码认证、短信验证码认证、警务即时消息认证、数字证书认证等方式。 4、提供指纹证书，支持国密算法，无缝兼容现有的PKI系统，支持与珠海市公安局信创终端进行适配。 5、支持跨域部署，认证代理和认证服务分别部署在前置区和数据中心，分别为不同区域应用提供认证支撑。 6、支持对组织机构内容、用户的管理，包括但不限于增、删、改、查、排序、批量导入。 7、支持多维度日志记录，包括但不限于注册、配置、认证、维护等操作日志；支持日志的标准化输出。 8、与审批服务、审计服务、应用之间联动，完成数据交互，并按照零信任体系接口设计要求实现对应的接口。 9、支持无上限用户规模。 10、支持并发用户使用≥3000。	1
10	审计中心	1、提供零信任认证、权限、审批、审计、环境感知、各类业务系统、安全访问、数据交换、设备运行和应用系统报送日志的采集； 2、提供日志采集的适配和标准化； 3、提供基于国密密码技术完整性、机密性处理； 4、提供策略配置规则，通过数据分析并构建分析模型，可对用户异常行为进行分析研判； 5、支持对审计日志以及预警信息进行人工和自动处置的能力，包括告警、通报、核查、反馈等形式； 6、支持审计策略配置，提供策略配置规则的前台展示功能。 7、提供数据分析并可构建分析模型，分析模型能够自定义，用以发现用户异常行为； 8、支持向审计人员提供的日志查询、检索以及统计分析等功能，为审计人员异常行为后的预警处置提供决策依据； 9、应用日志的字段、信息等需满足公安机关应用日志采集相关规范要求； 10、与认证服务、审批服务、应用之间联动，完成数据交互，并按照零信任体系接口设计要求实现对应的接口； 11、支持与上级审计中心对接； 12、日志存储周期不小于6个月。	1

11	可信环境感知	1、终端 Agent 采集用户终端设备属性、可信环境信息，通过感知代理传递给零信任体系的环境感知服务，实现对终端可信环境的状态和变化的实时感知。 2、环境感知客户端支持物理 PC 机和桌面云部署，支持 32 位和 64 位操作系统安装，通常情况占用的 CPU 和内存资源不得过高，运行过程中不得影响其它应用和系统软件的正常运行。 3、允许管理员自定义感知策略、感知内容、风险等级、评分规则、执行频率等。支持对可信环境感知客户端上报的环境感知结果进行综合分析和风险判定，并对终端环境状态和风险报告进行统一展示和呈现。 4、环境感知系统需具备各类监测能力，包括服务监测、注册表监测、弱密码监测、共享资源监测、高危端口监测、程序运行监测、漏洞补丁监测、杀毒软件监测、FTP 行为监测等。 5、支持多种环境的风险评估，包括硬件配置变化风险、网络环境及变化风险、系统账户风险、安全配置风险、恶意代码风险、系统关键对象风险、浏览器风险、系统环境风险、物理环境风险等，尤其需支持通过配合摄像头来评估授权人离席、屏幕拍照等环境风险。 6、能够对终端风险进行评估和分析，并能综合计算出终端可信状态，支持对接可信检控点和安全管理中心业务安全策略控制服务。 7、提供至少 1000 个终端的可信环境感知许可授权。	1
12	通报管理平台	1、支持利用本期项目建设的安全设备（如 WEB 应用防火墙、入侵检测、数据库审计、网络流量分析、云安全管理平台等），采集设备的安全数据并进行分析，发现网络环境中可能存在的安全问题。 2、支持根据发现到的安全事件和漏洞情况，如网络异常行为、数据库异常操作、应用攻击行为、云平台业务系统虚拟机漏洞、主机病毒感染情况，结合人工力量展开对下级单位和使用部门的安全通报工作。 3、支持针对发生的网络安全事件进行应急处置工作，总结网络安全事件成因，提供解决方案，及时处置安全事件。 4、支持与上级通报管理平台对接。	1
13	基础数据处理引擎	根据公安部大数据处理规范：数据提取、清洗、关联、比对、标识、分发 6 个标准处理环节，部署基础数据处理引擎,实现数据处理自动化。每个引擎支持处理 5 亿条/天实时数据，本项目日增数据量不小于 37 亿条。	8

	14	语音预处理引擎	对原始语音文件进行语音解码处理、检测有效音、去除干扰噪声等；每套引擎支持每天处理 1 万条语音。	1
	15	声纹特征提取引擎	基于新的多系统融合引擎，实现声纹特征提取；每套支持每天 1 万条语音进行声纹特征提取。	1
	16	分布式存储（云平台）软件	详见 9.3.1.4 提供相应的分布式块存储软件和授权。	1
	17	对象存储软件	详见 9.3.1.5 提供相应的分布式块存储软件、对象存储软件和授权。	1
	18	文件存储软件	详见 9.3.1.6 提供相应的分布式块存储软件、文件存储和授权。	1

9.3.3 机房租赁清单

类别	序号	硬件名称	配置参数	数量
机柜租赁	1	本项目机柜租赁	需租赁满足本项目的不少于 25 个 4400W 标准 47U 机柜，建设期加最终验收合格后一年内均需要租用设备，费用以 20A 满负荷计算。 机房符合《信息安全技术信息系统物理安全技术要求》GBT21052-2007 第三级物理安全技术要求，并具备等保 2.0 标准下的机房基础设施平台系统第三级备案证明文件。 机房应满足公安信息网信息安全管理要求及接入标准，并具备接入公安信息网所需专网万兆链路。	1
	2	市局机房设备搬迁机柜租赁	为市公安局二楼机房边界等设备实施搬迁到大数据机房租用机柜，需租用 8 个 4400W 标准 47U 机柜 15 个月，共需 120 个柜月，费用以 13A 计算。 机房符合《信息安全技术信息系统物理安全技术要求》GBT21052-2007 第三级物理安全技术要求,并具备等保 2.0 标准下的机房基础设施平台系统第三级备案证明文件。	1

			机房应满足公安信息网信息安全管理要求及接入标准，并具备接入公安信息网所需专网万兆链路。	