1、项目概述

深入实施公安大数据战略，按照公安部和省委、省政府部署要求，紧紧围绕“数字警务、智慧公安”，聚焦“实战实效、民警减负、群众满意”，遵循“六统一”原则和 “四化”要求，坚持分层解耦、异构兼容、充分利现、安全可控原则，充分利用物联网、云计算、大数据、人工智能等先进技术，加快推进新一代公安信息网、大数据平台、大数据纵深防御体系和大数据智能应用等重点任务建设。建设由数据域网络和用户域网络组成的新一代公安信息网；构建由“安全管理中心、零信任体系、安全防护体系”组成的大数据安全体系，为公安大数据智能化建设应用提供安全保障；建设大数据平台，建成全警最全最大的数据“大水库”，提高数据关联度和业务紧密度，提升数据质量和精准支撑能力，形成统一调度、精准服务、安全可控的资源服务体系；通过灵活调用、按需搭配基础设施服务、平台服务、数据服务的方式，重塑应用系统开发模式，快速部署开发大数据智能应用，形成强大计算能力、海量数据资源、高度信息共享、智能应用服务、警务运行支撑、严密安全保障的“六大体系”框架，建成大数据智能应用新生态，助推公安工作质量变革、效率变革、动力变革。

2、服务明细

（1）服务一览表

序号	服务名称	数量	单位
2.1	大数据中心（数据域部分）	1	套
2.2	新一代移动警务部分（一期）	1	套
2.3	山东省公安信息网大数据智能化安全体系（一期）	1	套
2.4	山东社会治安动态全息感知网安全防护体系	1	套
2.5	山东省公安厅“一门四通”项目（一期）	1	套
2.6	图像信息综合应用平台人像聚类归档模块	1	套

（2）服务明细表

序号	服务名称	指标需求	重要程度
2.1	大数据中心（数据域部分）	数据接入-公安业务数据分析： 建设内部数据汇聚系统，主要是指对公安民警在执勤、执法和社会秩序管理、业务办理等过程中产生的数据，来源于各类公安建设系统数据的接入汇聚分析。 （1）对 16 个地市数据情况开展调研，包括数据资源名称、数据资源编码、数据种类、来源系统、来源用户、来源方式、来源单位、来源负责人、联系方式、来源警种、数据范围、数据总量、日均增量、更新频率等维	一般

		度，录入调研系统生成数据调研结果。（2）实现 16 地市公安局向省厅大数据平台的资源数据汇聚，各地市建设汇聚中间库，实现数据汇聚任务管理、多种类数据源接入到原始库。（3）通过对各警种业务数据开展数据调研分析，包括来源、数据种类等维度，生成业务数据调研情况结果。（4）通过数据汇聚系统汇聚各业务警种数据到原始库。（5）实现数据汇聚系统任务监控功能，实现针对数据汇聚的任务监控和异常告警，并实现可视化数据汇聚任务的维护工作。（6）实现汇聚任务管理功能，定义维护数据汇聚的规则，包括交换的数据资源、数据项、增量规则，基于已配置的数据资源汇聚规则，管理和执行数据汇聚任务。（7）实现数据下发任务管理，监控下发各地市数据任务的运行状况、下发数据种类情况，提供下发对账和数据下发等工作情况的统计分析。（8）实现记录公安业务数据分析的所有操作日志信息，日志信息可查询。	
		数据接入-公安外部数据分析：建设外部数据汇聚系统，主要是指针对各级政府部门和企事业单位共享服务的各类数据进行接入汇聚分析。（1）针对公安外部数据来源，开展社会数据和政务数据种类调研，包括数据种类、总数据量、日增量等维度，生成数据调研结果。（2）利用多种方式包括人工导入、工具抽取等，实现社会数据、政务数据汇聚接入至原始库。（3）实现新接入的社会、政务数据与已汇聚的社会和政务数据的合并。（4）实现外部数据汇聚任务管理和外部数据资源情况的统计，生成统计图表。（5）实现外部数据汇聚系统任务监控，实现针对外部数据汇聚的任务监控和异常告警，并实现可视化数据汇聚任务的维护工作。（6）实现记录外部数据分析日志，日志信息可查询。	一般
		数据接入-数据探查：建设数据接入系统，通过对来源数据存储位置、提供方式、总量及更新情况、业务含义、数据结构、数据质量等进行多维度分析，数据接入系统性能要求：1000 万基础数据表中每新增、更新、删除百万数据，在现有网络环境下，耗时不大于 5 分钟；	一般

		10 亿条数据 100GB 大小的 CSV 等格式数据文件导入，耗时不大于 15 分钟。 （1）实现人工方式和智能化工具方式进行探查，通过人工探查数据情况、智能技术对数据进行分析、智能推荐、人工分析确认等手段进行探查。（2）实现来源数据的接入方式探查功能，包括环境探查、来源系统、存储位置、访问要求、提供方式，探查结果提供给数据定义功能使用。 （3）实现针对业务探查功能，包括数据来源单位、所属应用系统、业务含义描述、安全性要求、主外键名称、表关联关系等方面的探查。 （4）实现针对字段探查功能，包括空值率、值域及分布、数据元、类型及格式、命名实体等方面的探查。 （5）实现数据项集探查功能，对来源数据集表、引用数据元情况，探查数据集是否是标准数据集、数据集规模、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。 （6）针对省厅和 16 地市汇聚的数据开展数据集探查，掌握各地汇聚数据的质量情况，更新情况等，为数据汇聚和数据模型开发提供依据，指导各地向省厅汇聚数据工作。 （7）实现省厅用户和共建地市用户统一登录省厅平台，开展省厅和共建地市数据探查工作，并分别生成各用户探查结果报告。 （8）实现地市数据探查的结果汇总和管理，省厅可查看各地市数据探查结果报告，并以接口方式对外提供服务。（9）记录数据探查日志，并实现日志信息可查询。	
		数据接入-数据定义：通过对统一接入数据的数据格式、资源目录、数据分级分类、读取策略、清洗策略、关联策略、比对策略、表示策略、分发策略及质量检验规则进行明确定义。数据定义结果应随数据探查结果和业务需求的变更而动态维护，应以元数据的形式描述和输出。（1）开展数据格式定义，从原始字段项与标准数据元映射关系的定义、原始字典代码集与规范化字典代码集映射关系的定义等方面开展数据对标工作。 （2）根据数据格式定义的结果，按照规范要求，实现数据资源注册到数据资源目录。 （3）实现数据分级分类定义，定义数据项的字段性质分类和字段敏感度	一般

		分类，制定数据分级分类工作流程，并输出工作流程审批单。 （4）实现数据读取策略定义，从数据资源描述、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、数据转换策略描述、源数据备份策略描述等方面定义源数据从源系统中的读取策略，作为后续数据读取的依据。 （5）实现数据提取策略定义，按照业务需求，定义从来源数据提取所需数据的策略。实现从结构化/半结构化数据提取策略的定义、非结构化数据提取策略的定义方面提取映射关系、数据项的提取映射关系，根据业务需要和数据项内容，描述要素提取、特征提取等相关提取策略。（6）按照数据格式定义要求和业务需求，定义数据的清洗策略，生成满足标准及质量要求的数据，实现数据清洗策略定义，从数据过滤策略定义、数据去重策略定义、数据格转策略定义等方面的定义。 （7）实现定义数据的关联策略，从关联回填数据描述、关联依赖数据描述、数据关联规则描述明确，为后续的关联回填、关联提取提供策略支撑。 （8）按照业务需求,实现定义数据的比对策略，包括数据资源描述、比对源描述、比对策略描述等。（9）按照业务需求，实现定义数据的标识策略，明确数据标识时所使用的标签规则。（10）根据不同应用场景下的数据分发需求，实现定义数据的分发策略。 （11）实现数据质量核检规则定义，从核检对象描述、质量核检策略描述、质量核检指标描述等方面开展数据质量监测，提升数据质量提供监测依据。（12）建设数据定义系统，省厅和共建地市用户登录到本系统，实现数据相关定义工作。（13）实现各地市数据定义的结果查看，省厅可查看各地市数据定义情况，并以接口方式提供对外服务。	
		数据接入-数据读取： 1、建设数据读取系统，根据不同来源数据，建立跨层级、跨网络、跨安全域、跨平台的数据安全接入通道的能力，为公安内部各警种或政府其他部门数据抽取汇聚提供接口通道，确保数据在传输过程中的保密性、可用性和完整性。要求数据读取	一般

		系统在完成数据探查及数据定义后，从源系统抽取数据或接收读取源系统推送的数据并检查数据是否与数据定义一致，不一致的要求停止接入，并重新进行数据的探查和定义，如一致的执行进一步接入、处理。实现对各种异构数据进行必要的解密、解压操作功能。生成作用于数据全生命周期的记录 ID。实现对数据进行字符集转换、半结构化数据转换等其他转换，使数据符合数据处理要求的格式，供下一步处理。应按照标准化模块管理的方式，建立可适配的多源异构数据资源接入模式。 （1）数据在传输过程中的保密性、可用性和完整性，保障数据传输通道的可靠性。防止数据传输时，被第三方截获等安全风险所带来的数据泄露和篡改风险，避免数据传输过程中的身份抵赖。明确相关类型、级别数据的传输安全管理要求，利用加密、签名、鉴别、认证等机制对传输中的数据进行安全授权、安全防护。针对数据整体交换流程的审批、授权等过程文件进行备案管理，防止传输过程中可能引发的敏感数据泄漏、数据破坏等。 （2）通过数据推送方式的适配，实现结构化数据和非结构化数据的推送分发至地市。 （3）实现实时流式读取各类业务系统采集的数据信息，读取智能感知设备采集并由感知网汇聚后的各类动态信息和结构化数据。 （4）接入各种结构化数据以及常见格式的半结构化和非结构化数据。实现实时、离线和全量、增量等多种接入模式。实现被动接收和主动拉取两种数据获取方式。 （5）实现读取方式管理，根据数据探查和数据定义的结果，从业务系统读取数据或将业务系统推送过来的数据进行读取。应具备读取多种方式存储或推送源数据内容的能力。实现文件读取、数据库、消息总线、服务接口等方式读取。 （6）实现读取规则管理，建立完善的数据接入标准化模块管理体系，包含各类标准化模块生成、策略管理、任务配置、任务调度、状态监控、日志规则管理等。 （7）针对压缩、打包的数据做解压操作，实现数据解压，包括 RAR、ZIP、GZIP、LZ4、TAR 等常见的压缩格式。 （8）实现数据解密，按照公安	

		部标准实现对数据的解密操作。（9）实现用于数据全生命周期、全局唯一的主记录 ID 和附件记录 ID，并建立主记录和附件记录的关联。不同数据组织(数据库、数据表)中,记录 ID 的生成方法不同。（10）生成数据账单，供数据接入对账环节对数据提供方和数据接收方进行数据完整性检验、实时性检验、正确性检验。生成数据接入读取的主记录账单和附件记录账单，供数据分发环节核账。（11）实现读取的数据转换成符合数据处理要求的格式。（12）利用云平台备份机制，实现读取数据备份以供数据核查、回溯等使用，存储周期可配置，生成数据备份审核单。（13）数据读取系统实现省厅和共建地市租户可使用数据读取功能。收集记录省厅、地市数据读取日志，并实现日志信息可查询。 2、提供数据迁移工具，实现数据迁移系统建设。（1）要具备不少于 10 万张表、数万亿条数据的迁移工作及性能保障，完成数据迁移表配置、迁移数据源管理、迁移任务管理等功能。（2）实现迁移后数据的接口开发服务，提供迁移数据及后续新增数据对外接口服务和相关运维运营管理服务。（3）数据接口服务要具备全量及增量数据与公安大数据平台数据接口服务能力保持一致，满足各业务部门数据服务接口需求响应。	
		数据接入-数据对账：实现数据对账系统，完成数据提供方和数据接入方在数据交换过程中，针对数据条数、数据大小、数据指纹进行核对和检验的过程。实现对账完销账，对账异常记录日志。（1）实现数据接入对账，根据接入对账的条件及数据接入对账的要求不同，数据接入对账可采取接入时对账和接入后盘点对账等多种方式，并生成数据对账单。（2）实现数据分发对账，根据分发对账的条件及数据分发对账的要求不同，数据分发对账分数据分发时对账和分发后盘点对账等多种方式，并生成数据对账单。（3）实现三种对账方法（包括但不限于这三种）：即时对账方法（数据接入方在数据入库后，可以立即按对账单验证数据完成对账）、定时对账方法（接入方在	一般

		数据入库后，可以依据提前制定好的对账策略和对账单，完成数据对账。）、盘点对账（包括内部盘点对账、外部数据包对账、外部数据库盘点对账）方法。（4）基于数据资源目录，实现数据对账单和对账结果清单，数据对账结果清单具体内容包括但不限于：对账资源名称、对账单编号、异常次数、异常日志、重发次数、重发日志、销账次数、销账日志详情等信息。（5）实现对账结果使用功能，包括对账结果的统计和查询。实现对账可视化展示，包括对账各个环节的对账情况的图形化、数字化展示。（6）实现发送数据的暂存，数据接入方根据数据对账的异常情况，要求数据提供方重发指定对账单的数据。（7）实现对账服务，包括异常告警服务、对账单信息查询服务、对账单统计信息查询服务、异常对账环节查询服务，实现以接口方式提供服务。（8）实现数据指纹功能，数据内容对账过程中生成数据指纹、根据数据指纹对账，实现数据指纹的加密编码格式。实现指纹编码接口，方便数据接入方根据数据内容编码后，验证内容的一致性。（9）实现全省各地市数据对账工作汇总和可视化查看，各地市开展各自的数据对账工作，省厅实现对各地对账情况的查看和统计。（10）实现对账协议功能，数据提供方和数据接入方在对账过程中的对账单交换需满足主流协议，如 RPC、HTTP 等协议。（11）实现对账单存储与交换，满足但不限于库形式存储对账单、文件等形式存储对账单；满足对账单的数据交换格式。（12）记录数据对账日志，并实现日志信息可查询。	
		数据治理-数据提取：建设数据处理系统，在现有网络环境下，支持并发数据处理任务数不少于 500，数据处理单任务最大执行任务时间不大于 10 秒。实现数据提取系统，根据数据定义从源格式数据中提取出目的格式数据。数据提取实现组件化，可扩展，可配置。（1）实现结构化数据提取，提取的来源和目的数据格式均为结构化，主要是根据数据组织或业务需要进行数据的转换及整合，获得按照目的数据形式组织的数据。（2）完成非结构化数据	一般

		提取，提供文本数据内容提取、音频数据内容信息提取、视频数据内容信息提取、图像数据内容信息提取、网页数据内容信息提取等。实现文本数据提取，通过自然语言处理技术，从文本数据中提取文本要素及其相互关系、事件等信息,以及相关特征信息。与警种相关系统对接实现音频数据提取，通过音频处理技术,从各类音频信息中提取出所需的特征信息。对接并利用视频智能化应用系统实现视频、图像数据提取，从视频、图像数据中提取车牌、文字、图标、人员身份等实体信息，以及相关特征信息。 （3）记录数据提取日志，并实现日志信息可查询。	
		数据治理-数据清洗： 实现数据清洗功能，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。 （1）实现数据过滤，通过对数据进行辨别和分离，实现冗余数据及垃圾数据的滤除。包括样本数据的垃圾过滤和基于规则的垃圾过滤。 （2）实现数据去重，实现各类场景下设定相应的数据重复判别规则以及合并、清除策略,对数据进行重复性辨别，并对重复数据进行合并或清除处理，包括结构化数据去重和非结构化数据去重。 （3）完成数据格式转换，根据数据元标准将非标数据转换成统一的标准格式进行输出，将不同来源的同类数据按照统一规则进行转换，包括代码转换、数据截断、数据内容格式统一。 （4）完成数据检验，符合标准的数据直接入库，不符合标准的数据可进入问题数据库以便进一步分析处理。包括但不限于：空值校验、取值范围校验、公民身份号码/手机号/车牌号/IMEI/MAC/IP 地址等校验、数值校验、长度校验、精度校验等。 （5）实现数据清洗功能，省厅和共建地市租户可使用统一数据清洗工具自行开展数据清洗工作。 （6）记录数据清洗日志，并实现日志信息可查询。	一般
		数据治理-数据关联： 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。 （1）实现关联回填，将不完备的接入数据与知识数据等	一般

		根据场景进行关联，并将关联的要素等信息进行回填。 （2）实现关联提取，根据提取规则，对各类数据资源中关键要素关系或关联进行提取。 （3）实现数据关联功能，实现省厅和共建地市租户使用数据关联工具自行开展数据关联工作。 （4）记录数据关联操作日志，并实现日志信息可查询。	
		数据治理-数据比对： 实现数据比对功能，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，针对命中规则的数据，按照输出描述进行输出，包括结构化数据比对、非结构化数据比对以及结构化与非结构化融合比对等。 （1）实现结构化比对，将目标与比对源指定字段的取值进行比对，实时发现比中信息，包括完全匹配、模糊匹配、范围匹配、正则匹配等功能。 （2）实现非结构化比对，将比对目标与非结构化数据比对，在非结构化数据中实时发现比对目标相关信息。包括关键词比对、文本相似度比对、二进制比对、多媒体信息比对、图像比对、生物特征比对等功能。 （3）根据数据比对策略定义，配置数据比对规则，包括左连接、交集、并集、合集等比对规则，并实现数据比对规则的可视化管理，实现拖拽式操作和多源数据的接入等功能。 （4）实现数据比对结果形成比对结果存储或者比对结果及时自定义目标推送及提醒。 （5）实现数据比对功能工具开发，数据比对工具具有配置数据比对数据规模、比对计算时限、比对结果输出等功能。 （6）记录数据比对日志，并实现日志信息可查询。	一般
		数据治理-数据标识： 基于标签知识库，利用标签引擎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。 （1）实现标签引擎，包括：规则解析、规则路由、规则编译和规则执行。 （2）实现实时数据标识，基于标签知识库，对数据进行实时标签规则计算，为数据实时打标。 （3）实现离线数据标识，基于标签知识库，对数据进行离线标签规则计算，为数据离线打标。 （4）实现数据分级标识、分类标识、区域标识、空间位置标识、信息方向标识等。	一般

		数据治理-数据分发： 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、专题库。 （1）实现任务调度服务：通过统一接收接口接收数据分发任务，并将任务放到分发任务队列。实现分发任务配置，包括数据分发任务注册、报文模板配置和下端模块注册。 （2）实现数据分发：根据任务注册信息获取数据，根据模版组装数据，并向指定下端模块发送组装后的数据报文。 （3）实现数据分发统计：统计数据分发及处理情况。 （4）核账、销账：根据接入环节生成的账单，逐记录核账，以及完整账单的销账。 （5）可视化任务监控：提供分发任务的状态信息可视化监控。 （6）实现数据处理后从原始库到资源库、主题库、知识库、业务库和专题库的分发任务。 （7）实现数据分发操作日志信息记录，并实现日志信息可查询。	一般
		数据组织-公安数据原始库： 应建设数据组织系统，应提供详细设计方案。根据公安部大数据处理相关规范要求，建设原始库。公安数据原始库接入各警种业务数据资源，对各种来源数据进行处理后实现标准化数据、关联要素信息、标签信息和数据分级分类，建设公安数据原始库。为各类应用提供基本的数据支撑，为数据融合、数据抽象和进一步增值完成数据准备，并实现信息溯源、原始场景回溯等业务需要。 （1）实现标准化数据项，通过对公安原始数据项进行格式转换、归一化、截断等标准化处理，得到的符合标准格式要求的数据项，利用数据治理相关功能实现数据标准库。 （2）实现关联回填数据项，通过数据处理的关联回填操作获取关联回填项，并回填到原始数据中用以提升原始数据的关联及价值。 （3）实现标签数据项，通过数据处理的标识等操作对原始数据标识标签数据项，提升数据的价值密度。 （4）实现回溯数据项，记录原始库中的单条数据的获取来源。 （5）实现公	一般

		共数据项，原始库中的每个数据资源都应按照公共数据项的要求进行记录。 （6）公安原始库数据组织过程和结果可查看、可监控、可统计生成相关统计报表。 （7）根据原始库到标准库的数据处理过程，对于非标准或者清洗过的数据，生成公安数据处理问题写入问题库。所有处理过程均留有日志，存入日志库，日志信息可查询。	
		数据组织-政务数据原始库： 根据数据探查结果，建设政务数据原始库。 （1）实现标准化数据项，通过对政务原始数据项进行格式转换、归一化、截断等标准化处理，得到的符合标准格式要求的数据项，利用数据治理相关功能实现数据标准库。 （2）实现关联回填数据项，通过数据处理的关联回填操作获取关联回填项，并回填到原始数据中用以提升原始数据的关联及价值。 （3）实现标签数据项，通过数据处理的标识等操作对原始数据标识标签数据项，提升数据的价值密度。 （4）实现回溯数据项，记录原始库中的单条数据的获取来源。 （5）实现公共数据项，原始库中的每个数据资源都应按照公共数据项的要求进行记录。 （6）政务原始库数据组织过程和结果可查看、可监控、可统计生成相关统计报表。 （7）根据原始库到标准库的数据处理过程，对于非标准或者清洗过的数据，生成政务数据处理问题写入问题库。所有处理过程均留有日志，存入日志库，日志信息可查询。	一般
		数据组织-互联网数据原始库： 根据数据探查结果，构建互联网数据原始库。 （1）实现标准化数据项，通过对互联网原始数据项进行格式转换、归一化、截断等标准化处理，得到的符合标准格式要求的数据项，利用数据治理相关功能实现数据标准库。 （2）实现关联回填数据项，通过数据处理的关联回填操作获取关联回填项，并回填到原始数据中用以提升原始数据的关联及价值。 （3）实现标签数据项，通过数据处理的标识等操作对原始数据标识标签数据项，提升数据的价值密度。 （4）实现回溯数据项，记录原始库中的单条数据的获取来源。 （5）实现公共数据项，原始库中的每	一般

		个数据资源都应按照公共数据项的要求进行记录。 （6）互联网原始库数据组织过程和结果可查看、可监控、可统计生成相关统计报表。 （7）根据原始库到标准库的数据处理过程，对于非标准或者清洗过的数据，生成互联网数据处理问题写入问题库。所有处理过程均留有日志，存入日志库，日志信息可查询。	
		数据组织-社会数据原始库： 通过建设社会数据原始库，来实现对社会资源数据资源接入平台后进行统一分析处理。 （1）实现标准化数据项，通过对社会原始数据项进行格式转换、归一化、截断等标准化处理，得到的符合标准格式要求的数据项，利用数据治理相关功能实现数据标准库。 （2）实现关联回填数据项，通过数据处理的关联回填操作获取关联回填项，并回填到原始数据中用以提升原始数据的关联及价值。 （3）实现标签数据项，通过数据处理的标识等操作对原始数据标识标签数据项，提升数据的价值密度。 （4）实现回溯数据项，记录原始库中的单条数据的获取来源。 （5）实现公共数据项，原始库中的每个数据资源都应按照公共数据项的要求进行记录。 （6）社会原始库数据组织过程和结果可查看、可监控、可统计生成相关统计报表。 （7）根据原始库到标准库的数据处理过程，对于非标准或者清洗过的数据，生成社会数据处理问题写入问题库。所有处理过程均留有日志，存入日志库，日志信息可查询。	一般
		数据组织-感知网数据原始库： 根据数据探查结果，构建感知网数据汇聚库，包括所有前端感知设备获取的结构化数据。 （1）实现标准化数据项，通过对感知原始数据项进行格式转换、归一化、截断等标准化处理，得到的符合标准格式要求的数据项，利用数据治理相关功能实现数据标准库，实现感知视频数据与传统结构化数据的融合。 （2）实现关联回填数据项，通过数据处理的关联回填操作获取关联回填项，并回填到原始数据中用以提升原始数据的关联及价值。 （3）实现标签数据项，通过数据处理的标识等操作对原始数据标识标签数据项，提升数据的价值密度。 （4）实现回溯	一般

		数据项，记录原始库中的单条数据的获取来源。 （5）实现公共数据项，原始库中的每个数据资源都应按照公共数据项的要求进行记录。 （6）社会原始库数据组织过程和结果可查看、可监控、可统计生成相关统计报表。 （7）根据原始库到标准库的数据处理过程，对于非标准或者清洗过的数据，生成感知网问题写入问题库。所有处理过程均留有日志，存入日志库，日志信息可查询。	
		数据组织-要素关联库： 根据公安部大数据处理相关规范要求，建设资源库。建设要素关联库，实现对于关系的深层次、历史性规律进行要素梳理，实现要素关联的准确、全面。要素关联库主要功能是实现存储同一主体不同要素之间关联的时空分布，并记录关联建立的最早时间、最后时间、关联次数等信息。 （1）根据公安部大数据处理规范要求，实现公安要素标识。 （2）实现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。 （3）实现从已汇聚的原始数据资源中，通过数据提取、关联等处理方式记录要素与要素的关联信息。 （4）实现从已汇聚的原始数据资源中，记录关联的时空分布信息，包括最早关联发生时间、最近关联发生时间以及关联所发生的区域，区域的粒度应到区县行政区划一级。 （5）按照公安部大数据处理相关规范要求，实现要素关联的归并统计，记录首末次关联时间，以及关联总发生天数与总发生次数。	一般
		数据组织-要素关系库： 根据公安部大数据处理相关规范要求建设要素关系库，主要是实现存储不同主体间要素关系的时空分布，以支撑落地研判等业务工作。要素关系库全面刻画关系网络内容，形成要素组合展现关系图网的新型体系。 （1）实现从已汇聚的原始数据资源中，通过数据提取、关联等处理方式记录要素与要素的关系信息。 （2）记录关系的时空分布信息，包括建立关系的最早时间、最近时间以及关系所发生的区域，区域的粒度应到区县行政区划一级。 （3）按照公安部大数据处理相关规范要求，实现要素关联的归并统计，记	一般

		录首末次关系时间，以及总发生天数与总发生次数。 （4）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的，则提取到要素关系库中。 （5）根据公安部大数据处理相关规范要求，建设重点行为库，主要是从原始数据资源中，通过数据提取、关联、标识等处理方式记录要素的重点行为信息。（6）实现重点行为的时空分布信息建设，包括行为的最早发生时间、最近发生时间以及行为所发生的区域，区域的粒度不少于要到市行政区划一级。 （7）实现要素频次统计库构建，记录要素关联、关系、重点行为、重点内容每日出现次数的统计值，要素频次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。	
		数据组织-要素分布库： 根据公安部大数据处理相关规范要求建设要素资源分布库，主要功能是用来记录要素在数据资源中存在位置，是数据资源的总索引，以支撑要素值的快速定位使用。要素分布库主要包括要素时空分布库和要素资源分布库等。 （1）实现从已汇聚的原始数据资源中，通过数据提取等处理方式记录的要素时空分布信息。 （2）建设要素资源分布库，实现记录要素在不同数据资源的分布情况，用于基于要素资源位置的快速定位使用。（3）实现要素资源分布数据提取归并，提取要素在具体数据资源的存储位置并进行管理，是数据资源的总索引，以支撑要素值的快速定位使用。 （4）构建要素最后分布库，实现记录要素最后分布的时空信息，包括要素最近出现的区域，在该区域内最近出现的时间，可根据数据资源的条件获取并记录要素最近出现的经度、纬度、海拔等信息。 （5）构建要素变迁时序库，实现记录要素时空分布的历史变迁明细，包括要素连续活动的区域以及在该区域出现的最早时间和最后时间。 （6）按照公安部大数据处理相关规范要求，实现对要素出现区域以及要素出现时间进行实时更新。	一般
		数据组织-要素重点内容库： 根据公安部大数据处理相关规范要求建设要素重点内容库，实	一般

		现存储各种要素在不同的时空分布下所发布的重点内容。主要功能是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，以支撑预警发现、舆情分析等业务工作。（1）实现从已汇聚的原始数据资源中，通过数据提取、关联、标识等处理方式记录的要素重点内容信息。（2）记录重点内容的时空分布信息，包括内容的最早发生时间、最近发生时间以及内容所发生的区域，区域的粒度应到区县行政区划一级。（3）按照公安部大数据处理相关规范要求建设要素重点内容库，实现要素关联的归并统计，记录首末次内容发生时间，以及总发生天数与总发生次数。	
		数据组织-信息主题库： 根据公安部大数据处理相关规范要求和业务需求，建设主题库包括但不限于信息主题库、网上场所主题库、网下场所主题库、案件主题库、人员主题库、组织主题库、群体主题库、业务要素索引库、事件主题库、政务服务主题库等。根据公安机关业务需求，针对其关注信息内容进行梳理分析，并进行多维刻画展示，融合各类原始数据、资源数据，围绕能标识信息为主题对象，长期积累形成的多种维度的公共数据集合，建设信息主题库。（1）梳理与信息主题相关的信息，并形成信息主题库相关资源列表。（2）实现信息主题库建设，信息主题包括信息基本属性、信息传播过程、信息处置结果、涉案事件特征等。（3）利用数据组织系统的数据组织管理工具完成信息主题库的构建实施、管理和服务。	一般
		数据组织-网上场所主题库： 建设网上场所主题库，融合各类原始数据、资源数据，围绕能标识网上场所为主题对象，长期积累形成的多种维度的公共数据集合，形成网上场所主题库。（1）梳理与网上场所主题相关的信息，并形成网上场所主题库相关资源列表。（2）实现网上场所对象主题库构建，所描述的一级维度信息按照公安部大数据处理相关规范要求建设。（3）利用数据组织系统的数据组织管理工具完成网上场所主题库的构建实施、管理	一般

		和服务。	
		数据组织-网下场所主题库： 建设网下场所主题库，融合各类原始数据、资源数据，围绕能标识网下场所为主题对象，长期积累形成的多种维度的公共数据集合，形成包括网下场所主题库。 （1）梳理与网下场所主题相关的信息，并形成网下场所主题库相关资源列表。 （2）实现网下场所对象主题库构建，所描述的一级维度信息按照公安部大数据处理相关规范要求建设。 （3）利用数据组织系统的数据组织管理工具完成网下场所主题库的构建实施、管理和服务。	一般
		数据组织-案件主题库： 建设案件主题库，以各类案件内容为主体，融合各类原始数据、资源数据，围绕能标识案件为主题对象，长期积累形成的多种维度的公共数据集合，形成案件主题库。 （1）梳理与案件主题相关的信息，并形成案件主题库相关资源列表。 （2）构建刑事案件主题库，刑事案件主题包括刑事案件基本信息、嫌疑人员特征、犯罪组织特征、关联警情信息等。 （3）构建行政案件主题库，行政案件主题包括行政案件基本信息、违法人员特征、违法组织特征、关联警情信息等。 （4）构建警情主题库，警情主题包括警情基本信息、关联人员及组织、关联物品特征、关联案事件等。 （5）利用数据组织系统的数据组织管理工具完成案件主题库的构建实施及管理服务。	一般
		数据组织-人员主题库： 建设人员主题库，对人员对象建立的多维刻画，以能够标识人员身份的属性为唯一标识，聚合人员对象各个维度属性描述的信息集合，可通过数据定义实现与其他主题库的关联映射。融合各类原始数据、资源数据，围绕能标识人员为主题对象，长期积累形成的多种维度的公共数据集合，形成包括人员主题库。 （1）梳理与人员主题有关的信息，并形成人员主题库相关资源列表。 （2）按照公安部大数据处理相关规范要求建设人员主题库，人员主题包括人员基本信息、关联身份信息等人员相关的信息。 （3）利用数据组织系统的数据组织管理工具完成人员主	一般

		题库的构建实施、管理和服务。	
		数据组织-组织主题库： 建设组织主题库，融合各类原始数据、资源数据，围绕能标识组织为主题对象，长期积累形成的多种维度的公共数据集合，形成组织主题库。（1）梳理与社会单位有关的信息表，并形成社会单位主题库相关资源列表。（2）建设社会单位主题库，社会单位主题包括社会单位基本信息、社会单位经济情况、社会单位人员情况、单位行为特征、单位轨迹特征、涉案事件特征、单位业务特征等。（3）梳理与自然组织有关的信息，并形成自然组织主题库相关资源列表。（4）建设自然组织主题库，自然组织主题包括自然组织基本信息、自然组织成员特征、自然组织行为特征、自然组织轨迹特征、涉案事件特征、自然组织业务特征等。（5）利用数据组织系统的数据组织管理工具完成组织主题库的构建实施、管理和服务。	一般
		数据组织-群体主题库： 建设群体主题库，融合各类原始数据、资源数据，围绕能标识群体为主题对象，长期积累形成的多种维度的公共数据集合，形成群体主题库。（1）梳理与群体有关的信息，并形成群体主题库相关资源列表。（2）实现群体主题库构建，群体主题包括群体基本信息、群体组成情况、群体行为特征、群体轨迹特征、涉案事件特征、群体业务特征等。（3）利用数据组织系统的数据组织管理工具完成群体主题库的构建实施、管理和服务。	一般
		数据组织-业务要素索引库： 建设业务要素索引库，对业务库的关键要素建立的全局索引。（1）完成要素索引库建设，描述内容包括建立索引公安机构代码、要素索引 ID、建立索引时间；完成业务系统描述、联系人描述。（2）实现自动或手动方式在本地进行注册业务系统要素，实现注册成功后按照公安部要求向上汇聚。（3）利用数据组织系统的数据组织管理工具完成业务要素索引库的构建实施、管理和服务。	一般
		数据组织-事件主题库： 通过对事件相关的各	一般

		类数据进行提炼和重组，建立事件主题库，并以接口形式对外提供服务。 （1）梳理与事件有关的信息，并形成事件主题库相关资源列表。 （2）构建事件主题库，事件主题包括事件基本信息、涉事人员特征、涉及组织特征、事件过程、涉案事件特征等。 （3）利用数据组织系统的数据组织管理工具完成事件主题库的构建实施、管理和服务。	
		数据组织-物品主题库： 建设物品主题库，主要对业务关注类型的物品的多维刻画，融合各类原始数据、资源数据，围绕能标识物品为主题对象，长期积累形成的多种维度的公共数据集合。 （1）按照业务需求，梳理与车辆等物品相关信息，并形成物品相关的资源列表。 （2）完成车辆等物品主题库构建，物品主题包括车辆等基本信息、轨迹特征、涉案事件特征、业务特征等。 （3）按照业务需求，梳理与各类设备业务相关信息，并形成各类设备相关的资源列表。 （4）构建终端设备主题库，终端主题库信息，按照公安部大数据处理相关规范要求开展建设。 （5）梳理与前端采集设备相关信息，并形成前端采集设备相关的资源列表。 （6）构建前端采集设备主题库，前端采集设备主题包括前端采集设备基本信息、采集信息情况等。 （7）利用数据组织系统的数据组织配置工具完成物品主题库的构建实施、管理和服务。	一般
		数据组织-政务服务主题库： 结合公安业务数据以及获取的政务相关各类资源数据，建设政务服务主题库。（1）梳理与政务服务有关的信息，明确与政务服务有关的数据资源列表。（2）按照业务需求，通过将社会数据，整合各类数据资源进行融合处理构建政务服务主题库。 （3）利用数据组织系统的数据组织配置工具完成政务服务主题库的构建实施、管理和服务。	一般
		数据组织-业务生产库： 按照公安部大数据处理相关规范要求建设业务生产库，业务数据是业务人员使用业务系统过程中所产生的数据，其中记录和存储了活动相关的数据。 （1）调研业务警种数据库使用需求，并根据需求辅助	一般

		构建业务生产库。（2）利用数据要素配置工具辅助完成业务生产库的构建实施、管理和服务。（3）为省级管理员和各租户开展运行监控，提供业务生产库运行监控接口，为数据资产全生命周期管理提供日志数据。	
		数据组织-情指勤专项业务专题库：全面整合分析研判数据，案事件数据，PGIS 地图实战数据以及警力、警车、警情等数据和多种实时数据，建设情指勤专项业务专题库。（1）调研情指勤舆业务应用对数据使用需求，并结合情指勤舆业务模型使用经验总结，分析数据需求，明确构建情指勤专项业务库的主要用途和涉及的数据内容。（2）完成情指业务相关数据内容收集，包括原始业务数据表、字典表、资源库表、主题库表、知识库等库表的数据资源列表。（3）根据数据需求，通过情指勤舆专项模型构建和数据开发，为情指勤专项业务专题库提供数据服务。（4）利用数据要素配置工具，完成情指勤专项业务库的构建实施、管理和服务。	一般
		数据组织-平安社区业务专题库：以平安社区的智慧安防小区属性的多种标签方式进行数据的组织，建设平安社区业务专题库。（1）调研智慧安防小区应用对数据使用需求，并结合智慧安防小区业务模型使用经验总结，分析对数据的需求明确构建智慧安防小区专项业务库的主要用途和涉及的数据内容。（2）完成智慧安防小区业务相关数据表收集，包括原始业务数据表、字典表、资源库表、主题库表、知识库等库表的数据资源列表。（3）根据数据需求，通过智慧安防小区模型构建和数据开发，为智慧安防小区业务专题库提供数据服务。（4）利用数据要素配置工具，完成智慧安防小区专项业务库的构建实施、管理和服务。	一般
		数据组织-全息感知业务专题库：实时汇聚上传各地全息感知结构化后的动态数据至省级平台，实现感知视频数据与传统结构化数据的融合应用。（1）完成全息感知数据使用需求调研，并结合感知业务模型使用经验总结分析数据需求，明确全息感知业务专题库的主要用途	一般

		和涉及的数据内容。 （2）完成全息感知业务相关数据表收集，包括原始业务数据表、字典表、资源库表、主题库表、知识库等库表的数据。 （3）根据数据需求，通过全息感知模型构建或数据开发，为全息感知业务专题库提供数据服务。 （4）利用数据要素配置工具，完成全息感知专项业务库的构建实施、管理和服务。	
		数据组织-便民服务业务专题库： 通过便民服务数据建立便民服务业务专题库。 （1）调研便民服务业务应用对数据使用需求，结合便民服务业务模型经验对数据需求进行分析，明确便民服务业务专题库的主要用途和涉及的数据内容。 （2）完成便民服务业务相关数据表收集，包括原始业务数据表、字典表、资源库表、主题库表、知识库等库表的数据内容。 （3）根据数据需求，通过便民服务模型构建或数据开发，为便民服务业务专题库提供数据服务。 （4）利用数据要素配置工具，完成便民服务专项业务库的构建实施、管理和服务。	一般
		数据组织-**分析业务专题库： 建立分析业务专题库。 （1）调研分析业务应用对数据使用需求，结合分析业务模型经验对数据需求进行分析，明确分析业务专题库的主要用途和涉及的数据内容。 （2）完成业务相关数据表收集，包括原始业务数据表、字典表、资源库表、主题库表、知识库等库表的数据局内容。 （3）根据数据需求，通过分析模型构建或数据开发，为分析业务专题库提供数据服务。 （4）利用数据要素配置工具，完成分析专项业务库的构建实施、管理和服务。	一般
		数据组织-涉**对象业务资源库： 建设**对象业务资源库，通用**对象及相关的案件线索、审批流转等数据，以及业务标签等数据构建业务资源库和专题库。 （1）调研**对象管理业务应用对数据使用需求，结合涉**对象业务模型经验对数据需求进行分析，明确涉**对象业务专题库的主要用途和涉及的数据内容。 （2）完成**对象业务相关数据表收集，包括原始业务数据表、字典表、资源库表、主题库表、知识库等数据内容。 （3）根据数据需	一般

		求，通过涉**对象模型构建或数据开发，为涉**对象业务专题库提供数据服务。 （4）利用数据要素配置工具完成涉**对象专项业务库的构建实施、管理和服务。	
		数据组织-实时搜索业务专题库： 建设实时搜索业务专题库、全文搜索业务专题库、图片搜索业务专题库、语义搜索业务专题库等搜索业务专题库，赋能智能搜索应用。 （1）调研实时搜索业务所涉及的数据类型和列表，包括原始业务数据表、字典表、资源库表、主题库表、知识库等数据内容。 （2）根据数据需求，通过搜索相关模型构建或数据开发，为实时搜索业务专题库提供数据服务。 （3）利用数据要素配置工具完成实时搜索业务库的构建实施、管理和服务。	一般
		数据组织-规则库： 建设知识库管理系统，实现省市两级大数据平台知识信息管理，完成公安业务知识的汇集、分析统计、管理和服务。包括数据接入、处理、治理、组织和服务各个环节中提炼的规则方法，形成规则知识库，如通用标签信息、标签分类信息和通用标签规则，知识库检索响应时间不大于 5 秒。 （1）构建知识库，管理公安业务知识和规则方法，主要包括基础知识库、基础算法库、智能信息处理知识库、规则库等。 （2）建设知识库管理系统，实现对知识来源管理、知识新增、修改、删除和知识搜索等功能，知识搜索提供分类授权查询。 （3）实现知识获取接口和用户查询接口。	一般
		数据组织-标签知识库： 通过业务警种定义的规则对数据进行匹配和打标签，实现数据的标签化。 （1）完成标签分类的定义，实现对身份标签、关系标签、行为标签、条线标签、区域标签和专题标签等多种标签分类。 （2）完成标签知识库定义，实现按照标签的对象及来源数据开展标签定义，能够定义名称、描述、标签值类型定义等。 （3）完成标签配置功能，实现业务标签可视化界面配置及模型化配置，提供数据表名称、数据表字段和字典项等多种标签配置依据。 （4）提供标签库可视化自定义标签管理和维护。	一般

		数据组织-算子管理： 建设算子管理系统，实现包括但不限于创建算子、算子规则配置、枚举值配置、虚拟表配置、算子分类、算子检索、算子发布、算子状态、算子权限和常用算子等功能。（1）通过可视化方式实现算子构建和管理。（2）实现算子规则配置、算子规则配置、枚举值配置、虚拟表配置等相关配置管理功能。（3）实现算子分类、算子检索、算子发布、算子权限、算子状态和常用算子查看等功能。（4）算子管理，包括实现对省厅和地市算子资源库的管理。	一般
		数据组织-静态关系算子库： 实现静态关系算子库的构建。（1）实现静态算子的分类管理。（2）实现通过可视化方式构建静态关系算子。（3）在服务期限内实现静态关系算子库的按需开发、持续优化和更新。	一般
		数据组织-虚拟关系算子库： 实现虚拟关系等算子库的构建。（1）实现虚拟关系算子库多种虚拟关系的库表结构创建。（2）实现通过可视化方式构建虚拟关系算子。（3）在服务期内实现虚拟关系算子库的按需开发、持续优化和更新。	一般
		数据组织-基础自运算算子库： 实现包括但不限于数据表字段修改、字段添加、数据聚合、数据过滤、身份证标准化处理、字典映射、选择列、表结构处理、数据去重、机器学习等功能。（1）实现包括但不限于字段修改、字段添加、数据聚合、数据过滤等自运算算子的配置功能。数据过滤包括条件过滤和表达式过滤，可实现多字段的过滤配置，针对不同字段类型，实现多种规则匹配。（2）实现通过可视化方式构建基础自运算算子。（3）在服务期内实现基础自运算算子库的按需开发、持续优化和更新。	一般
		数据组织-碰撞运算算子： 实现包括但不限于交集算子、左连接算子、差集算子、全部合并算子和全关联算子等功能。（1）实现算子等配置管理功能，可管理的算子包括但不限于交集算子、左连接算子、差集算子、全部合并算子和全关联算子、机器学习算子等。（2）实	一般

		现通过可视化方式构建碰撞运算算子，并实现机器学习算子功能，可调用机器学习模型，输出机器学习结果。 （3）在服务期内实现碰撞运算算子库的按需开发、持续优化和更新。	
		数据组织-轨迹方式行为算子： 实现轨迹类行为方式算子构建。（1）实现轨迹频率、频次等行为配置管理功能。（2）实现通过可视化方式构建轨迹方式行为算子。 （3）在服务期内实现轨迹方式行为算子的按需开发、持续优化和更新。	一般
		数据组织-基础知识库： 对文本、多媒体数据处理等过程所需要的规则、模型或知识性数据。 （1）实现包括但不限于行政区划、组织机构代码、手机号码段信息、各类数据字典、同义词库等公共安全领域共享的知识数据内容的构建。 （2）实现基础知识库内容的查询功能，能够检索基础知识库中的内容。 （3）在服务期内实现基础知识库的按需开发、持续优化和更新。	一般
		数据组织-基础算法库： 实现但不限于包括各种基本算法、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、随机森林算法、图算法等各种基本算法的构建和存储。 （1）实现包括但不限于以上算法可视化调用。 （2）实现基础算法库查看功能，能够查看每个算法的定义和参数内容。（3）在服务期内实现基础算法库的按需开发、持续优化和更新。	一般
		数据组织-智能信息处理知识库： 实现对文本、多媒体数据处理等过程所需要的规则、模型或知识性数据的存储。 （1）实现对文本处理规则、模型和方法进行存储。 （2）实现对多媒体处理方法、规则存储。 （3）在服务期内实现智能信息处理知识库的按需开发、持续优化和更新。	一般
		数据组织-人员业务知识库： 实现人员业务知识库建设。 （1）按照人员的主要要素，包括但不限于身份证、姓名、民族、户口等信息构建人员业务知识库。 （2）在服务期内实现人员业务知识库的按需开发、持续优化和更新。	一般

		数据组织-物品标签库： 实现物品标签库建设。 （1）梳理与物品有关的库表信息，形成构建物品标签库有关的数据资源列表。（2）针对梳理的物品数据资源列表信息，实现构建物品标签打标工作。 （3）实现物品标签库可视化配置和物品标签管理。	一般
		数据组织-基础身份标签库： 实现基础身份标签库建设。 （1）梳理与身份标签库有关的库表信息，形成构建基础身份标签库有关的数据资源列表。（2）针对梳理的数据资源列表信息，实现基础身份标签的打标工作。 （3）实现基础身份标签库可视化配置和标签管理。	一般
		数据组织-物感类标签库： 实现智能感知类标签库建设。 （1）梳理与智能感知类标签有关的库表信息，形成构建智能感知类标签库有关的数据资源列表。 （2）实现智能感知类标签的打标工作。 （3）实现智能感知类标签库可视化配置和标签管理。	一般
		数据组织-物流行为标签库： 实现物流行为标签库建设。 （1）梳理与物流行为标签有关的库表信息，形成构建物流行为标签库有关的数据资源列表。 （2）实现物流行为主要是寄件和收件等多种信息标签打标。 （3）实现物流类标签库可视化配置和标签管理。	一般
		数据组织-政务类标签库： 实现政务类标签库建设。 （1）梳理与政务类标签有关的库表信息，形成构建政务类标签库有关的数据资源列表。 （2）实现政务类标签的打标工作。 （3）实现政务类标签库可视化配置和标签管理。	一般
		数据组织-治安行为标签库： 实现治安等业务警种行为标签库建设。 （1）梳理与业务警种行为标签有关的库表信息，形成构建业务警种行为标签库有关的数据资源列表。 （2）实现业务警种行为标签的打标工作。 （3）实现业务警种行为类标签库可视化配置和标签管理。	一般
		数据组织-数据安全保障： 1、应建设大数据平台数据安全保障系统，应提供详细的设计方案，主要提供省级平台的数据安全保障和数据安全管理工作包括数据传输安全、数据访问控	一般

		制、数据库审计服务和管理等工作，要求实现数据安全可视化态势感知管理，达到大数据平台数据安全保障事前预防预警、事中控制监管、事后审计处理等要求，相关预警、监控和审计信息实时推送平台运维运营系统。 2、依照法律、法规的规定，建立全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。本项目必须符合等保三级标准要求实施建设，并配合大数据智能化建设密评工作；按照公安部 GA/DSJ 300-2019 系列标准开展数据安全保障工作；数据安全能力成熟度模型技术部分需达到四级要求，参考国标 GB/T 37988-2019。 3、实现数据接入安全，通过数据对账服务访问控制及数据读取访问控制，保障数据接入安全。 （1）数据对账服务访问控制。需通过安全基础设施，实现按照最小权限原则进行权限分配功能；通过安全基础设施，实现身份认证，确保设备身份的合法性；通过安全基础设施，实现鉴别访问权限，确保没有超出授权使用范围。 （2）数据读取访问控制。通过安全基础设施，实现根据最小权限原则为设备分配数据访问权限；数据的读取访问应基于安全基础设施进行身份认证后的设备，确保读取访问设备身份的合法性；通过安全基础设施，鉴别设备的访问权限，确保没有超出授权使用范围。 4、数据处理安全，通过账号管理服务、数据分析安全、数据正当使用、数据处理环境安全、数据导入导出安全等，保障数据处理安全。（1）通过安全基础设施安全管理服务，对原始库、资源库、主题库、知识库、业务库、业务要素索引库进行安全加固管理、版本补丁升级等工作，防止数据泄露、账号篡改等安全隐患发生。 （2）数据分析安全要求：制定据分析安全审核流程,数据分析的数据源、数据分析需求、分析逻辑按照审核流程进行审核,以确保数据分析目的、分析操作等当面的正当性。针对个人信息、重要数据等数据有恢复需求时，可利用公安云计算平台数据备	

		份系统实现数据恢复功能。 （3）数据正当使用：制定数据使用正当性的制度，保证数据使用在合法合规目的和范围内；实现预防数据使用风险和数据防泄露功能，针对违约责任、缔约过失责任、侵权责任等数据使用风险和数据泄露风险具有预防、预警、分析和处理能力。（4）数据处理环境安全：数据处理环境的系统设计、开发和运维阶段应制定相应的安全控制措施，实现对安全风险的管理，针对用户在数据处理系统上对数据的操作开展定期审计，确定用户对数据的加工处理未超出合法合规的要求。技术工具要求：建立数据处理日志管理工具，记录用户在数据处理系统上的加工操作；对数据完整性和一致性进行定期检测。（5）数据导入导出安全：应采取多因素鉴别技术对数据导入导出操作人员进行身份鉴别。技术工具要求：应记录并定期审计内部的数据导入导出行为，并对操作人员进行身份鉴别，确保未超出数据授权使用范围。 5、数据治理安全，通过数据授权保障数据治理安全。（1）数据授权：基于用户级别和数据级别，配置数据访问权限策略，策略应包括业务范围界定、数据分级分类、数据访问频度、时间范围界定等；数据访问权限应细化到记录和字段；实现静态授权和动态授权。 （2）数据鉴权：支持对用户身份、服务请求和资源访问权限进行鉴别；鉴权能力应覆盖本地的全部数据访问行为。 6、数据服务安全，实现与安全平台对接，通过数据服务化、数据服务访问控制、数据授权、数据鉴权，保障数据服务安全。 （1）数据服务化：通过数据层接口提供的数据服务，降低数据泄露的风险。 （2）数据服务访问控制：通过安全基础设施，根据最小权限原则分配数据服务访问权限；通过安全基础设施提供的认证管理服务，对大数据平台的应用服务进行身份认证，确保应用服务身份的合法性；通过安全管理中心提供的权限管理服务，鉴别应用服务访问权限，确保没有超出授权使用范围。 （3）数据授权：通过安全基础设施，基于用户级别、数据级别配置数据访问权限策略，数据访问权限策略应包含业务范	

		围界定、数据分级分类、时间范围界定等，支持静态授权和动态授权；实现对分级分类的数据按照用户、角色、标签或类别进行授权。（4）数据鉴权：根据数据访问控制规则，实现数据访问权限鉴别。根据请求用户归属地、身份、角色等，对其进行身份鉴别、权限验证，并对其服务请求和资源访问权限进行鉴别。　（5）数据共享安全：流程要求：明确数据共享流程和按照审计要求记录日志,为数据共享安全事件的处置、应急响应和事后调查提供帮助；数据使用申请时，数据申请单应有包括数据安全防护能力的承诺条款。　（6）数据接口安全：通过数据接口安全监控措施，以对接口调用情况进行必要的自动监控和处理； 7、数据存储安全，应通过物理或者逻辑备份，保障数据存储安全。　（1）利用云计算平台备份机制，实现数据定期备份，对定期备份进行检查，确保备份成功。　（2）实现数据定期恢复测试，确保备份数据能应急恢复。　8、应用安全，本项目所有应用和系统要实现与零信任体系权限服务联动，实现统一授权、鉴权和角色管理。并要通过应用展示脱敏、应用数字水印、网页防篡改等功能，实现应用内容保护安全。　（1）应用展示脱敏：为防止敏感数据泄露，通过安全基础设施的数据脱敏服务，对页面展示的人员姓名、照片、户籍、轨迹等敏感数据进行动态脱敏处理。　（2）通过明水印或暗水印的方式，对违规将大数据平台系统应用界面显示的信息进行截图、拍照等行为进行响应处理，包括溯源及阻断等技术措施。（3）对于含有敏感内容的界面，应在终端屏幕自动生成明水印或暗水印，水印包含登录账户、登录 IP、登陆时间等信息。　（4）大数据平台系统开发应按照相关代码安全编写规范和标准，需具备网页防篡改、防 SQL 注入、web 跨站点请求伪造等安全能力。	
		数据管理-数据资源目录管理：　应建设数据资产管理系统，应提供详细的设计方案，按照公安部大数据处理规范中技术要求，整合和建设包括数据标准管理系统、数据资源目录管理系统、数据血缘管理系统、数据模型管理系统、	一般

		元数据管理系统、主数据管理系统、数据质量管理系统、数据安全保障系统、数据分级分类管理系统、标签管理系统、数据授权管理系统和数据共享管理系统等功能。实现数据资源目录管理系统建设，主要包括数据资源目录的提交、审核、注册、停用、启用、注销等功能。按照统一的公安数据资源目录标准规范，对公安数据资源进行统一管理，实现数据资源科学、有序、安全使用，数据资源目录系统性能要求：在现有网络环境下，检索并发不少于300个；检索响应时间不大于3秒。 （1）建设数据资源目录管理功能，实现包括数据元管理、资源分类与编目、目录注册与注销、目录更新、目录同步、目录服务和可视化展现，实现数据资源注册、数据资源查询、数据元对标、数据元申报、字典代码上报等功能。（2）实现数据资源目录可视化管理流程，实现数据资源使用申请相关功能，完成数据目录数据的申请、审批功能，形成数据资源申请单，并实现审批单的上传。数据资源申请包括数据下发申请和数据使用申请两种，均需要进行审批签字。 （3）构建数据资源目录，并实现基于新增数据的实时数据目录更新工作；实现公安部、地市数据资源目录系统对接，形成全省统一数据资源目录管理；与部级大数据平台数据资源目录管理系统对接并实现数据目录上报功能。 （4）实现数据资源目录总览功能，通过数据资源目录总览可查看数据资源的总数、类型、数据量、分类等总体全局的信息。 （5）实现数据资源查询功能，能够实现表、字段等的模糊查询和存储类型、体量范围、条数范围等的筛选查询，查看数据资源、数据项集以及数据项之间的关系。 （6）实现服务资源目录功能，为服务提供者及服务使用者提供接入代理、路由及服务的透明访问等支撑功能，服务资源目录对象包括服务规约、服务资源、服务资源绑定的数据资源。 （7）实现服务资源应遵循服务规约进行创建和发布，一个服务资源只能遵循一个服务规约；一个服务规约，实现创建多个服务资源。 （8）实现服务资源目录可视化管理流程，实现服务资源	

		使用申请相关功能，完成服务目录服务的申请、审批功能，形成服务资源申请单。（9）实现应用资源目录管理相关功能，按照公安部大数据处理规范要求，完成全省业务应用系统的登记注册、报备审核等功能。（10）根据公安大数据处理规范中数据资源目录管理规程要求，完成数据资源目录管理的相关角色和职责、管理活动、管理工具等建设。（11）根据公安大数据处理规范中数据元管理规程要求，完成数据元注册、变更和停用等工作，完成代码标准注册、变更和停用等工作，完成数据元与数据项的对标工作。	
		数据管理-数据血缘： 应建设数据血缘管理系统，记载对数据处理的整个历史，包括数据的起源和处理这些数据的所有后继过程(数据产生、并随着时间推移而演变的整个过程)。通过读取大数据处理生命周期各环节的日志，实现数据血缘的可视化路径展示。通过数据产生、加工融合、流转流通到最终消亡等过程，构建形成数据相关继承关系集合，可以通过对接入数据、原始库、资源库、主题库、知识库、业务库等各类数据资源间和数据项间的继承关系进行描述和管理，可视化展现数据资源在各个环节间的继承关系。（1）采用图形化技术实现数据血缘关系多种图形可视化展现。（2）实现血缘关系管理，记录上下游数据资源编码、数据项编码和数据资源转换规则等数据血缘信息，并实现动态更新，包括资源血缘管理、实体血缘管理、字段血缘管理等功能。（3）实现血缘关系分析，对数据资源进行数据流向分析、溯源和变更影响分析，并提供数据血缘关系的图形化展现；包括数据资源数据流向分析、数据资源溯源分析、数据资源变更影响分析等。（4）实现血缘关系查询，按照数据类别、数据项和转换规则进行数据血缘查询，并向数据资源目录提供服务接口，包括数据类别查询、数据项查询、转换规则查询。实现地市数据血缘的对接和联动。	△
		数据管理-数据质量管理： 应建设数据质量管理系统，数据质量管理贯穿数据接入与数据处理的全过程，包括数据定义、数据读取、数据	一般

		清洗等环节。按照公安部大数据处理数据质量管理技术要求规范，需通过建立数据质量评估标准和管理规范，及时发现、监测定位、跟踪解决各类数据质量问题,形成数据质量问题的闭环处理。（1）根据质量评估要求，在数据定义阶段定义数据质量检核规则，并建设数据质量检核规则库。（2）提供质量检测数据采集，负责采集数据接入及处理环节输出的指标信息，源数据、各处理环节及存储数据的样例数据采集等。（3）质量检核，对数据按多种维度进行探查，并输出详细的数据质量检核报告，包括数据质量评估指标定义、数据质量规则制定、检核作业调度等。（4）发现及跟踪：实现根据数据质量检核报告、业务反馈信息发现和记录数据质量问题，实现数据质量问题的可视化管理、分析、跟踪、解决，实现分析、分类汇总并积累数据质量知识。（5）实现数据全生命周期的质量管理，形成数据质量问题的闭环处理。	
		数据管理-数据分类： 建设数据分级分类系统，提供数据按照数据来源、数据种类、数据属性进行资源级别的分类。数据分类是指针对数据来源、数据种类（数据集）、业务属性（数据项)等进行划分，构建科学合理的数据分类管理体系。（1）根据公安大数据处理中数据分级分类技术要求，对汇聚的各地市数据、业务数据、外部数据，开展数据分类工作，数据分类包括数据资源分类、数据字段分类、数据字段关系分类等。（2）实现数据资源分类，按照数据项集的属性对数据资源进行分类，属性包括数据组织一级分类、数据组织二级分类以及数据资源标签分类。（3）实现数据字段分类，从数据安全使用的要求对数据资源字段进行分类。（4）实现数据字段关系分类，建立字段与字段之间安全访问控制的访问推导关系。（5）实现数据分类可视化管理功能包括分类管理、数据授权管理、数据分类审核审批。	一般
		数据管理-数据分级： 1、通过数据分级，对涉及敏感内容、隐私内容、定位信息等内容的记录和字段进行分级别的访问限制，防止敏感	一般

		信息的扩散，杜绝手段滥用的风险。对数据内容的敏感程度或数据的开放范围进行划分，需构建完善的数据分级管理体系。（1）根据公安大数据处理中数据分级分类技术要求，实现数据分级。（2）根据公安大数据处理中数据分级分类技术要求，实现数据安全级别分级。（3）实现数据分级可视化管理功能包括分级管理、数据授权管理、数据分级审核审批。	
		数据管理-数据运维管理： 1、建设数据运维管理系统，全面掌握数据接入、数据流量、数据资源的总体情况和使用情况。（1）实现数据运维管理系统可视化界面构建，实现采集数据接入、处理、组织和服务等各项任务的状态信息情况查看，通过异常状态进行预警和处置，实现对各任务的实时监控和管理。（2）实现数据运维规则配置管理，包括实时采集配置、运行状态监控配置、预警配置、运维报表配置等功能。（3）实现数据运维数据采集，实现对来源数据以及接入、提取、清洗、关联、比对、标识、分发、入库等环节设置监控点，进行多维度信息的实时采集。（4）实现数据运维状态监控，包括来源数据的监控、数据接入及处理状态的监控、数据积压监测、数据心跳图、数据入库异常、数据服务接口监控等。（5）实现数据运维报表功能，包括数据资源报表、数据对账报表、数据有值率报表、数据标准化分析。（6）实现预警管理功能，包括数据接入异常、实时流量监控异常、批处理数据监控异常、运行状态异常，作业任务异常、数据质量异常、数据安全异常、数据备份异常和数据告警信息等预警管理功能。提供配置短信、邮件、公安内部邮件和即时通讯等多种方式报警。（7）实现运维日志审计功能，包括运维日志记录、运维日志查询、运维日志报表等功能。 2、实现数据运营管理系统可视化界面构建。（1）实现汇聚数据服务平台的服务能力，面向服务使用为用户提供服务。（2）实现服务平台注册功能，将省大数据平台、各市平台系统、各类资源和各个服务的相关接口地址、信息进行注册，实现各类资源、服务的统一汇聚，提供统一的服务目录体系运	一般

		营服务。（3）实现服务注册功能，将大数据平台中各类资源和服务注册或同步至运营平台，提供统一的服务目录体系运营服务。（4）实现各类资源和服务的发布，由服务管理发布至运营平台的服务目录，可视化运营平台能够提供的所有运营服务。（5）提供扩展服务属性的功能，允许服务运营管理者定义这些标签，通过给服务添加标签的方式来给服务进行分组，提供便于管理和搜索的运营服务。（6）实现服务变更功能，对服务目录上的服务进行更新操作，对服务进行变更时服务须为下架状态，提供服务变更的运营服务。（7）实现对更新和注销的服务进行下架处理功能，暂时或不再提供用户申请使用。提供服务下架的运营服务。（8）实现服务申请功能，用户申请使用运营平台服务目录中资源和服务的过程，包括服务（资源）申请，提供服务申请的运营服务。（9）实现对服务目录上的服务进行更新操作，对服务用户资源使用率较低时，可发起扩容变更或减少资源变更，包括变更申请、变更评估、变更审核、变更实施与验证和变更验收确认。提供服务变更的运营服务。（10）实现服务续期功能，对即将到期的服务与资源，发起续期申请，进行续期操作。提供服务续期的运营服务。（11）实现服务退订功能，包括服务退订申请，提供服务退订的运营服务。（12）实现服务评价功能，针对用户已申请的服务，实现用户对服务进行满意度待办评分进行评价。提供服务评价的运营服务。（13）实现服务质量管理功能，根据可用性、安全性、可靠性、响应性和可维护性的评价特征指标进行管理。提供服务质量管理的运营服务。（14）实现服务评价管理功能，对服务评价模板的管理、评价指标的设置，以及对用户评价数据的收集和汇总管理。提供服务评价管理运营服务。（15）提供可视化效能分析的运营服务。实现可视化效能分析功能，提供服务运营、质量的总体分析，并通过拖拽制作图表的方式对运营数据进行汇总、统计、分析并集中展现。（16）提供租户管理的运营服务。实现数据资源租户管理功能，使	

		用服务的省级警种部门和市级公安机关相关部门，通过运营平台的等级授权，成为运营平台的租户或租户下的某个用户。包括租户管理、租户用户、租户联系人、租户申请清单管理、租户申请的自助管理、租户的计量。（17）实现服务运营中心功能，提供用户自助运营管理，实现对运营平台服务的消费日志记录和审计。（18）实现服务目录功能，统一展示接入运营平台的大数据服务。（19）提供视图中心的运营服务。实现视图中心功能，主要包括应用视图、数据中心视图，通过视图中心查看数据中心的总体概况以及应用使用数据的概况。（20）开发大数据平台项目和产品管理系统，实现项目群全生命周期、任务事项审批流程和项目相关文件的管理，实现数据管理日常相关工作的可视化、流程化、标准化的管理。实现开发任务管理功能。（21）开发大数据平台运维运营 APP，实现移动化服务运营功能，在移动警务平台上发布。	
		数据管理-模型管理： 建设模型管理系统，平台通过模型框架引擎提供的个性化的、可配置的计算分析功能服务。（1）实现模型管理功能，预置的通用模型（如技战法模型、自然语言处理、多媒体信息处理等各类模型）。大数据平台新构建的模型及地市公安机关构建的模型进行统一注册和发布管理。实现全省模型共享，实现遵循标准的第三方模型导入。（2）实现算法管理，对基础算法库的管理，包括决策树、随机森林、逻辑回归、SVM、朴素贝叶斯、K 近邻算法、K 均值算法等的管理。（3）实现可视化模型构建及调试功能，可视化构建新模型或对已有模型调优，实现模型内部流程编排、模型数据组织、模型算子选择、模型参数调优等。（4）实现模型评价，建立对模型的评价指标和方法，提供反馈接口，并触发模型的迭代优化。（5）训练数据管理：实现对文本、图像、音视频等各类模型训练数据的离线提取、清洗、打标等处理，实现资源描述和管理、特征工程以及数据集版本管理。（6）实现模型纳管、上报、下发和模型适配功能。（7）实现模型管理可视化，提供模型	一般

		管理系统与数据建模系统、模型应用服务系统等其他关联系统接口对接。	
		数据管理-标签管理： 公安部大数据处理规范中技术要求建设标签管理系统，构建标签体系。 （1）实现数据标签配置功能，针对数据标签的打标规则和方式，实现标签配置。（2）实现通过人工、模型、机器学习等多种方式实现标签打标，使标签打标可视化管理。（3）实现标签管理功能，包括标签分类的创建、标签引擎、标签可视化、标签表的创建、标签的新增、修改、删除和查询等功能。（4）实现数据标签统计展示功能，实现数据量、更新状态、标签分类、标签更新时间等等维度的统计展示。 （5）实现标签分类功能，自定义标签分类，要素类型为标签分类的第一级，允许对分类进行延伸，允许子类的存在，标签分类实现编辑、删除操作。 （6）实现标签搜索功能，根据标签表某些字符或者全文快速检索，可实现模糊匹配。 （7）实现标签生命周期管理，包括创建生命周期管理、编辑生命周期管理、查询生命周期管理、审批生命周期管理、使用生命周期管理、评估生命周期管理、停用生命周期管理、下线生命周期管理、版本管理生命周期管理。 （8）实现标签模型管理，提供标签模型的定义，提供标签模型知识库的管理。 （9）按照公安部大数据处理规范中标签定义和分类要求，实现标签规则描述。	一般
		数据管理-授权访问机制： 1、建设数据授权管理系统，经过数据分级分类后，用户在使用数据时将根据自身权限使用规定范围内的各类数据。若需使用超出权限范围的数据，需经审批授权使用。对接零信任体系权限服务联动，完成以下功能： （1）实现数据获取安全功能，实现数据获取申请、审批等工作流程功能。根据的访问控制权限，实现数据的访问权限的鉴别。 （2）实现脱敏功能，实现数据脱敏规则、脱敏算法及脱敏任务的管理及应用，分为动态脱敏和静态脱敏。 （3）实现统一授权、签权和角色管理。角色分为省市两级管理员角色、领导角色、省市两级用户角色，省市	一般

		两级管理员实现角色的分级管理。 （4）大数据平台为一体化平台，统一集成各系统功能服务，实现统一用户登录服务。 （5）为山东省公安信息网大数据智能化安全体系（一期）提供审计日志数据。 （6）开发数据权限审批服务接口，实现通过接口形式对外提供服务。 2、建设数据开发管理系统，实现大数据平台大数据协同开发管理功能，提供多租户能力，用户可完成数据管理、脚本开发、作业开发、作业调度、开发运维监控等工作，并实现对应用服务测试环境管理服务和应用开发基础组件服务的对接管理。 （1）对接数据管理系统，完成数据开发任务中的可视化数据管理工作。 （2）实现脚本开发，构建在线脚本编辑器，提供多人协作进行 SQL、Shell、Python 脚本在线代码开发和调测。 （3）构建图形化设计器，提供拖拽方式快速构建数据处理工作流。预设数据集成、SQL、Shell 等多种任务类型，通过任务间依赖完成复杂数据分析处理。支持导入和导出作业。 （4）对接数据资源管理系统，提供在脚本开发和作业开发使用到的各种类型的资源统一管理。 （5）实现作业调度管理，持单次调度、周期调度和事件驱动调度，周期调度支持分钟、小时、天、周、月多种调度周期。 （6）实现数据开发运维监控，对作业进行运行、暂停、恢复、终止等多种操作管理，提供查看作业和其内各任务节点的运行详情功能，并对接数据运维运营系统。提供配置多种报警方式，作业和任务发生错误时可及时通知管理员和运维人员，保证业务正常运行。	
		数据服务-信息比对服务： 建设数据服务管理系统，实现数据服务接口的注册、授权、运维运营和监控管理。数据服务管理系统权限应与大数据平台的数据权限申请审批流程对接，保持权限一致。构建信息比对服务系统，基于大数据的信息比对碰撞分析应用是利用分布式计算技术，进行海量数据的碰撞比对，实现秒级结果输出，能够基于集中、分布存储的结构化数据和非结构化数据实现关联查询搜索、数据碰撞比对服务。根据公安部应用开发要求，基	一般

		于信息比对服务，开发信息比对应用，并建设相应的移动 APP 挂接到警务工作门户和移动警务平台。 （1）实现单表数据比对和多表比对功能，可自定义数据源进行比对。 （2）实现基于集中、分布存储的结构化数据和非结构化数据实现关联查询、碰撞比对服务。基于视频智能化应用系统实现图像比对服务。 （3）实现信息比对服务接口开发，并完成测试调用服务。 （4）实现数据服务接口，挂接到数据服务总线中开放服务。	
		数据服务-模型分析服务： 构建模型分析服务系统，根据业务需要利用基本算法，对数据进行统计、分析、规律性探索及预测等，并返回结果，以支撑应用层业务场景复杂、多变的需求。根据公安部应用开发要求，基于模型分析服务，开发模型分析应用，并建设相应的移动 APP 挂接到警务工作门户和移动警务平台。 （1）实现数据集碰撞类服务，根据条件中需要碰撞的字段，在一个或多个数据集中比对，按照交集、并集或差集进行计算，并返回结果。 （2）实现分析类服务，使用各种分析方法分析数据，以获取数据的统计分布情况，发现数据的内在规律性、识别其主要因素，或进行模型的参数估计、可信度评估等。 （3）实现预测类服务，利用各类已有模型、算法对数据进行计算，预测未知的变量或属性取值。	一般
		数据服务-数据推送服务： 1、构建数据推送服务系统，实现数据推送服务，完成公安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系统间信息推送等工作，主要包括数据汇聚、数据下发等功能。 （1）按照公安大数据处理规范标准提供数据推送服务，将需要推送的结果按照文件传输格式进行封装，通过数据传输通道周期性的将数据推送给目标平台或系统。 （2）按照公安大数据处理规范标准提供数据停止推送服务，对正在运行的推送服务进行停止推送。 （3）按照公安大数据处理规范标准提供数据推送回调服务，服务提供方通知服务请求方数据结果推送相关信息。 （4）按照公安大数据处理规范标准提供数据下载服务，数据资源推送可通过此服务	一般

		实现。 （5）按照公安大数据处理规范标准实现数据确认服务。 2、构建数据操作服务系统，实现数据操作服务，完成数据及数据表的增加、删除、修改等操作接口服务。 （1）数据增加服务，向指定资源增加数据，实现单条录入和批量导入。 （2）数据修改服务，对于指定条件范围的记录，对其指定字段值进行修改。 （3）数据删除服务，删除指定条件范围数据。 3、构建数据管理服务系统，实现数据管理服务，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，数据管理类服务包括数据资源目录管理服务和数据元管理服务。 （1）实现数据资源目录管理服务包括：注册服务、更新服务、查询服务、汇聚服务、下载服务等接口服务。 （2）实现数据元管理服务包括：数据元查询服务、代码标准查询服务、限定词查询服务、审批结果查询服务、数据元注册服务、数据元变更服务、代码标准注册服务、代码标准变更服务、限定词注册服务。 （3）按照公安部大数据处理规范中数据服务协议要求，按照接口服务传输协议、消息格式、接口方法以及消息语法要求，实现数据接口服务开发。 （4）按照公安部大数据处理规范中传输格式协议要求，按照文件、服务请求报文格式要求实现数据接口服务开发。 4、构建数据鉴权服务系统，实现数据鉴权服务，完成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敏感度、数据来源、数据种类、字段及字段关系分类四个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。 （1）请求方向服务提供方发起各类服务请求时，服务提供方根据请求用户警种部门、地市部门、身份、角色，对其进行身份鉴别、权限验证，并对其服务请求和资源访问权限进行鉴别。 （2）鉴权能力覆盖本地的全部数据访问行为。 （3）鉴权服务实现在服务调用之间进行权限验证。 5、实现数据服务总线系统，总线由请求受理、服务路由、协议转换、服务调用、管理及监控功能构成。	

		（1）实现请求受理功能，请求方提交服务请求报文，数据服务总线受理请求并鉴别请求方、服务使用者的令牌和服务访问权限，实现同步、异步等多种接入方式。（2）数据服务总线实现根据服务注册信息和挂载配置信息，确定报文的节点、总线传输路径并对请求报文和响应报文进行转换、传输。（3）实现协议转换功能，实现数据服务总线报文在不同消息协议、不同传输协议之间自动转换。（4）实现服务调用功能和返回服务响应功能，数据服务总线鉴别服务方令牌并进行路由和必要的协议转换，转发给请求方或由请求方异步获取。（5）实现数据服务总线监控功能，包括总线监控、服务监控、日志采集、会话跟踪。（6）实现管理和配置功能，包括节点管理、挂载配置等功能。（7）根据公安大数据处理规范数据服务总线的相关要求，实现报文格式要求，请求方和服务方应按照数据服务总线的报文格式和协议要求进行报文的封装与传输。（8）数据服务总线实现对请求方、服务方的令牌进行鉴别，并对请求方的服务资源访问权限进行鉴权。实现用户和权限管理，支持共建地市的多用户登录。	
		数据服务-查询搜索服务：构建查询搜索服务系统，实现查询检索服务，提供数据通用查询的功能，以预设或自定义的数据项为单一查询条件或组合查询条件，通过标准化的查询配置或服务接口调用数据，建立基于条件查询的分类分目查询功能和一键式查询功能，实现按要素分类查询或基于不确定关键字的一键式检索。根据公安部应用开发要求，基于查询搜索、语义识别服务、数据分析服务等数据服务和数据建模系统、知识图谱系统、机器学习计算支撑系统、视频智能化应用系统，开发多引擎数据搜索应用，并建设相应的移动 APP 挂接到警务工作门户和移动警务平台。（1）数据资源情况查询服务，对数据中心各类数据资源情况进行查询的服务。（2）通用数据查询服务，提供结构化数据查询，实现精确匹配、模糊匹配。（3）通用扩展查询服务，根据查询词的类型，通过字段扩展配置，用查询值在多	一般

		个同类字段进行查询，返回符合查询条件的全部同类字段数据信息。 （4）全文检索查询服务，基于关键词匹配或文本相似度匹配，在用户选定的数据库中查询符合关键词组合条件的数据。 （5）基于视频智能化应用系统实现图像搜索查询比对服务，输入图片或关键词检索，返回涉及类似场景的图片，以及对应描述的服务。（6）基于视频智能化应用系统实现音频检索查询服务，使用语音或文字，查询匹配相应内容的音频或文本服务。 （7）基于视频智能化应用系统实现视频检索查询服务，输入图片、关键词或视频片段，返回涉及相似场景的视频，以及命中的位置、场景描述等信息服务。 （8）与警种相关系统对接实现生物特征检索查询服务，提供声纹、人像、指纹、DNA 等生物特征的检索服务。 （9）实现数据服务接口，挂接到数据服务总线中，开放服务。 （10）在现有网络环境下，查询并发任务数不少于 500，数十亿数据量级的数据查询，响应时间不大于 5 秒。	
		数据服务-信息布控服务： 构建信息布控服务系统，实现信息布控服务，针对重点关注的信息进行布控关注，通过针对异构数据的多种流式计算引擎，灵活定制分类、标签进行属性标注，实现信息的分级、分类、分地域、分范围布控。根据公安部应用开发要求，基于信息布控服务，开发信息布控应用，并建设相应的移动 APP 挂接到警务工作门户和移动警务平台。 （1）实现信息布控功能，实现根据关键字进行布控。 （2）实现实时轨迹信息布控功能，实现按照轨迹等关键字进行布控。 （3）实现对象的分级、分类、分地域、分范围布控。 （4）实现集成图像、视频等多引擎布控服务。 （5）实现单个对象布控、批量对象布控服务。 （6）实现数据服务接口开发，并挂接到数据服务总线中，开放服务。 （7）在现有网络环境下，布控引擎支持并发比对任务不少于 500；当单任务不低于百万数据表布控，完成时间最大时间不大于 10 秒。	一般
		数据服务-背景核查服务： 通过多维度数据，构建背景核查服务系统，实现背景核查服务。	一般

		根据公安部应用开发要求，基于背景核查服务，开发背景核查、对象查证应用，并建设相应的移动 APP 挂接到警务工作门户和移动警务平台。 （1）构建核查服务字典内容项，核查内容为核查服务字典项中的内容。 （2）实现背景核查、对象查证服务，核查服务结果返回是或否等内容。 （3）实现数据服务接口开发，并挂接到数据服务总线中，开放服务。 （4）实现对象查证服务，针对对象开展查证的数据服务。 （5）实现可视化的参数配置和日志记录功能，可出核查报告。	
		数据服务-数据资源目录服务： 数据资源目录服务是大数据平台为上层应用提供整体服务能力的接口，能够提供标准化目录、标准化注册、标准化查询，同时提供元数据服务、数据对标等服务。 （1）数据字典查询服务，返回代码集包含的全部文件名称列表，根据用户输入的代码集文件名称，返回代码集文件内容。 （2）数据资源目录查询服务，包括省级资源目录查询、地市资源目录查询、数据资源目录数据集及统计信息查询。 （3）模型资源目录服务，包括模型目录模型注册查询、模型目录模型注册结果信息查询、模型目录模型已共享信息查询。 （4）标签查询服务，实现标签体系的分类、标签值等信息的查询。 （5）实现目录服务接口，挂接到数据服务总线中，开放服务。	一般
		数据服务-比对订阅服务： 构建比对订阅服务系统，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，在比中时将比对结果快速推送到告警模块。此服务根据输入的比对条件与结构化和非结构化数据进行匹配，并实时返回布控结果信息。按照公安大数据处理规范中比对订阅的相关参数规则要求开展比对订阅服务建设，开发比对订阅应用，并建设相应的移动 APP 挂接到警务工作门户和移动警务平台。 （1）比对订阅服务，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，并在比中时，实时返回比对结果信息。实现完全匹配、	一般

		模糊匹配、关键词匹配、正则匹配、多条件逻辑组合匹配、语义匹配、音频匹配、图像匹配等能力的扩展。（2）批量比对订阅服务，批量输入比对条件，使用完全匹配规则与结构化数据进行比对。（3）比对订阅状态查询服务，针对指定条件或规则，查询当前的信息比对订阅结果和比对订阅状态等。（4）中止订阅，取消已经提交的比对订阅申请或正在执行的比对订阅任务。（5）在现有网络环境下，支持并发比对任务不少于 500，单任务百万数据表与亿级数据表比对碰撞，完成耗时不大于 10 秒。	
		数据分析-热词监控： 建设数据分析系统，分析全省警情、案件等各类数据，对热词、业务标签等关键数据进行 7×24 小时分析，自动提供预警分析功能。开发数据分析应用，并建设相应的移动 APP 挂接到警务工作门户和移动警务平台。数据分析系统权限应与大数据平台的数据权限申请审批流程对接，保持权限一致。数据分析系统性能要求：在现有网络环境下，两张亿级以上的数据表关联计算，耗时不大于 60 秒；100 万条和 1 亿条的数据表进行倾斜关联计算，耗时不大于 5 秒；针对 1000 万条数据，可视化维度和指标并发查询数不少于 100，单任务响应时间不大于 5 秒。（1）通过大数据平台数据处理治理的结果数据和公安业务系统中的结构化数据或非结构化数据，实现关键数据预警分析功能。（2）实现公安关键数据库建设，实现关键数据库的增加和删除等功能，实现将非热词添加到热词榜。（3）实现关键数据黑名单功能：实现用户对低质量或者业务弱相关的关键数据推送结果进行“过滤”操作，提升关键数据探测模型的准确性和有效性。（4）实现关键数据 24 小时预警功能，对于命中的关键数据实现推送，基于关键数据探测结果和热度值形成关键数据排行榜并自动推送。实现预警信息自主订阅与推送功能。（5）实现关键数据内容展示功能，维度包括排名、关键数据热度，关键数据查看实现按照日/周/月/季级别查看。（6）实现榜单对比功能，实现添加多个不同时间段、不同行	一般

		政区划的关键数据进行比对分析。 （7）实现关键数据搜索功能，可根据输入的关键词进行智能匹配，提供预警接口和报表。 （8）实现热词同义词推荐，实现对挖掘监测的关键数据进行同义词推荐和聚类合并。 （9）提供事件、人物、物品和机构等指向性特征关键词抽取服务，提供符合标准的接口，能够对事件指向性特征关键词进行提取并形成新的关键数据如热词和业务标签等。	
		数据分析-热词态势： 通过语义挖掘等数据分析挖掘技术，提供热词等整体关键数据态势分析。 （1）实现关键数据趋势分析功能，对关键数据关联的数据时间与数据量进行统计分析。 （2）实现关键数据关联数据的同比增长率和环比增长率的分析和图像化展示。 （3）实现关键数据关联线索挖掘功能，实现多种形式的关键数据和关联线索之间的关联程度进行展示，依据距离、直观图形化判断关键数据关联度。 （4）实现关键数据类型占比分析功能，对热词关联的数据类型的占比统计分析，并进行图形化展现。 （5）实现热词、业务标签等关键数据位置轨迹相关区域分布分析功能，关键数据在各区域的分布情况统计，实现省市县三级下钻。	一般
		数据分析-热词分析： 通过大数据平台大数据分析挖掘引擎、知识图谱系统、机器学习计算支撑系统等技术工具，挖掘分析公安数据解决业务问题，实现多维下钻分析、多算法挖掘分析等针对热词等关键数据分析工作，并可通过接口调用共享分析结果。 （1）实现针对公安业务问题等关键数据趋势分析功能，对业务问题实现自定义时间内的数据趋势统计分析，实现折线图、柱状图等多种图形化展现，实现周、月、季度 3 种时间周期统计。 （2）实现公安业务问题的区域数据分析功能，对公安业务关键数据分析涉及到的省、市、县分布及排行情况进行统计分析，以条形图等形式展示分析结果。 （3）实现公安业务问题关联研判分析功能，对公安业务关键数据分析的突出数据及区域关联情况进行研判分析，以和弦图、旭日图等形式展示研判结果。 （4）实现公安业	一般

		务问题典型案例研判功能，对公安业务关键数据分析的典型案例进行增加、删除等操作。	
		数据分析-热词报告： 提供数据分析综合可视化展示工具，实现和弦图、桑基图等多种可视化展现方式，输出数据挖掘分析报告。 （1）实现数据分析报告模板功能，根据模板实现数据分析报告自动生成功能，模版包含但不限于标题、概述、关键数据统计结果、热点问题分析、结束语等内容。 （2）实现数据分析报告的综合可视化展示功能，包括但不限于曲线图、柱状图、条形图、和弦图、桑基图、旭日图等。 （3）实现数据分析报告在线预览功能，预览内容包括报告编号、分页预览、功能区、报告主体。预览实现缩放、旋转、下载、打印等基础操作。 （4）实现报告管理功能，实现新建报告、历史报告查看和管理等功能，以卡片的形式展示历史报告。	一般
		数据分析-热点监控： 按照公安业务需求基于公安全量数据对警种重点任务等特别是热点地区、热点事件、热点手法等热点关联关系数据进行预警分析。 （1）实现重点任务数据库搭建，包括但不限于重点任务地区库、重点任务事件库等重点库和关联关系库。 （2）通过大数据平台数据处理治理的结果数据和公安业务系统中的结构化数据或非结构化数据，实现重点任务库的关联关系分析与实时预警功能。 （3）实现重点任务预警信息自主订阅与推送功能，重点任务库的实时自动更新功能。	一般
		数据分析-热点态势： 实现重点任务的热点挖掘分析，提供态势变化、类型变化、时段变化等态势信息。 （1）实现态势模型搭建，实现热点态势模型。 （2）实现配置化分析功能，实现态势变化、类型变化、时段变化的个多维态势信息。 （3）实现预警关联功能，实现态势变化关联预警信息自主订阅与推送功能。	一般
		数据分析-热点分析： 通过大数据平台大数据分析挖掘引擎、知识图谱系统、机器学习计算支撑系统等技术工具，挖掘分析公安数据解决重点任务等热点数据分析问题，实现多维下钻分析、多算法挖掘分析等关键数据分析工作，	一般

		并可接口调用共享分析结果。实现对区域分布开展实时挖掘分析、多维分析、可视钻取，实时掌握重点任务数据挖掘分析结果。（1）通过全量数据的实时监测，实现重点任务数据库的自动识别。（2）实现针对重点任务数据的实时监测分析。（3）实现全量数据中提取重点任务行为数据多维分析。	
		数据分析-乱点分析：实现对重点任务地址数据问题即乱点分析功能。（1）实现重点任务地址数据挖掘功能，实现对文本等数据中的地点进行有效识别，包括不同的数据内容进行分类，实现时间和地点进行筛选功能。（2）实现地点自动推送功能及服务接口。（3）提供地址类、企业机构类实体识别服务，提供符合标准的接口，能够对地址类和企业机构类实体进行提取。	一般
		数据分析-热点报告：通过综合可视化展示工具，对重点任务数据分析报告进行多种可视化展现，包括和弦图、桑基图等，结果为输出分析报告。（1）实现重点任务数据分析报告生成功能，包括多种分析报告模板，助力一键快捷生成报告。（2）实现重点任务数据分析报告可视化展示功能，实现多种报告展示方式，包括但不限于和弦图、桑基图等。	一般
		数据分析-警情案件关联：实现警情数据和案件笔录数据的统一治理、关联，形成主题库、专题库。（1）根据文本数据识别人、物信息，筛选人、物关联关系等信息并构建专题库，文本数据包括但不限于警情数据和案件笔录数据。（2）实现对象关联功能，实现对人、号的实时关联。（3）实现对象检测功能，实现文本中的人、号等对象的实时检测。（4）实现报警分类识别服务，能够对报警数据分类进行提取，并生成报警数据接口服务。	一般
		数据分析-关系网挖掘：实现文本内与跨文本中的关系挖掘，形成关联关系。（1）针对文本数据，通过自然语言处理技术，从文本数据中提取关键要素及其相互关系、事件等相关特征信息。（2）实现关系关联展示功能。（3）提供实体之间的关系识别服务，提供符	一般

		合标准的接口，能够对实体之间的关系进行提取。	
		数据分析-隐藏线索发现： 对实体关联关系进行有效挖掘分析，发现隐藏线索等关联关系线索，并挖掘分析相似事件的处置结果，为事件的预警、布控和处置提供实时分析结果。 （1）实现无效关联筛选功能，利用算法对关联线索进行筛选提高线索关联挖掘的有效性。 （2）实现组合线索挖掘展示功能，提供多种形式展现模式。 （3）实现线索关联数据召回功能，根据已选中的线索组合进行关联数据召回，召回的数据以列表的形式展示，根据需求自主选择排序方式。 （4）提供线索融合功能，根据动态编辑，实时提供同义和近义线索推送，实现线索间的语义相似度计算。 （5）实现与数据建模系统对接功能，自动将选中的线索组合添加到数据建模系统。	一般
		数据分析-数据挖掘： 通过大数据平台大数据分析挖掘引擎、知识图谱系统、机器学习计算支撑系统和数据建模系统等技术工具，构建数据挖掘分析结果的智能分析模型，关联文本数据中的要素，自动形成人员知识图谱、案件串并图谱、进行警情扩线，辅助对警情和案情精准研判，挖掘潜在线索。 （1）实现数据档案功能，针对文本构建数据档案。 （2）实现人员关系挖掘功能，基于人员档案和关联关系的任务挖掘，并进行图谱形式的可视化展现。 （3）实现案件串并功能：通过文本中提取相关要素，自动形成案件串并。 （4）提供符合标准的接口，实现对以上内容提取。	一般
		数据建模-自主建模-数据源管理： 建设数据建模系统，利用大数据平台数据处理和治理的成果为数据源，实现自主建模数据源管理。数据来源方式包括数据库、外部文件、流式数据、数据接口等，提供数据预览，并实现数据源同步状态查看功能。实现与警务工作门户的对接。数据建模系统性能要求：在现有网络环境下，两张亿级以上的数据表关联计算，耗时不大于 60 秒；100 万条和 1 亿条的数据表进行倾斜关联计算，耗时不大于 5 秒；针对 1000 万条数据，可视化维度和指标并发查询	一般

		数不少于 100，单任务响应时间不大于 5 秒。（1）实现数据库来源管理，利用大数据平台数据处理和治理的成果为数据源，实现自主建模数据源管理。（2）通过 API 获取数据来源，实现数据资源的获取接入。（3）实现对接流式数据源，需具备数据源配置和数据表配置功能，完成流式数据的接入。（4）通过任务状态同步，实现数据源同步状态和同步记录查看功能，并支持新增数据源同步任务功能。（5）实现外部数据管理功能，提供数据上传的工作界面，通过拖拽及选择文件的方式，实现文件数据上传，数据类型包括但不限于 excel、csv 文件格式。实现上传数据资源在线预览和历史任意文件回滚和替换功能。（6）实现工作表设置，包括自动识别表头、配置字段类型、配置字段描述、数据去重配置等功能。（7）实现针对数据资源的数据分类管理、分类标签管理、数据备注管理等功能。（8）数据建模系统权限应与大数据平台的数据权限申请审批流程对接，保持权限一致。	
		数据建模-自主建模-可视化建模： 可视化建模应提供灵活多样的数据建模组件开展数据分析，实现单表自运算、多表比对运算等主要数据运算功能，并提供运算算子管理、SQL 脚本管理等功能。（1）对接算子管理系统，实现算子库管理功能模块，包括数据表自运算、多表比对运算等，实现数据可视化建模，针对不同算子实现可视化参数配置界面。省厅及各地市的算子统一在算子管理系统上注册、共享、使用。（2）提供自主建模的可视化画布功能，通过拖拽的形式构建模型，实现模型算子、数据资源、业务算子等建模要素的自由融合建模。针对数据结构，实现当前版本管理和历史版本对比。（3）实现 SQL 脚本运算、SQL 脚本语法校验、SQL 脚本格式化、SQL 脚本语法帮助、SQL 执行数据预览等功能，并且提供 UDF 函数功能，提供新增 UDF 函数扩展。（4）利用业务算子，实现将技战法进行抽象、封装，提供参数输入，条件筛选，结果输出功能。实现算子批量管理，包括但不限于发布、禁用、启用、删除、导出等功能。（5）	一般

		实现导入模型、编辑模型、删除模型、模型调试、复制模型、发布至模型超市、模型版本管理和模型更新的功能。更新模型要求按照多种更新模式，包括自动更新、定时更新、自定义更新和暂停更新。（6）实现一键布局、连线线型切换、显示隐藏节点注释、复制算子、高亮算子、算子颜色标记、节点注释、删除算子、算子预览数据、显示节点数据、画布缩放、鸟瞰图和常用算子等功能。（7）生成可供系统调用的接口服务，通过服务资源目录与模型超市对接。（8）构建模型租户管理功能，租户间实现数据隔离、模型隔离、结果隔离；实现省市两级租户管理。	
		数据建模-模型超市-模型档案： 建设模型超市，通过模型档案，让用户了解模型用途，选定模型，实现模型需求申请和相关审批功能。模型档案描述包括系模型的描述、模型使用的数据源、模型的应用场景、模型的创建民警、团队和单位、创建时间、模型更新时间、模型评比评分等。（1）实现业务模型需求申请功能，模型需求申请单自动进入模型审批流程，并实现流程管理。（2）实现省市两级建设完成的模型上传到模型超市进行共享展示功能。（3）实现模型上架和下架的管理能。	一般
		数据建模-模型管理-模型展示配置： 模型展示配置功能，对模型基本信息和模型使用情况的展示，实现模型的排名和多维维度的统计信息，可配置的展示信息包括模型名称、模型描述、关注人数、使用次数、评价次数、点赞次数、模型分类等信息。（1）实现模型概览、最新模型展示、最热模型展示和模型详情展示等功能，并实现各警种建模情况进行排名、各类标签模型数量排名、组织单位建模情况排名、高评分模型排名、用户建模情况排名等。（2）展示页可通过经典模型、推荐模型和全部模型等维度实现模型展示。（3）实现模型按标签和发布单位搜索功能。	一般
		数据建模-模型管理-模型复用配置： 在模型超市发布的模型，通过权限审批实现数据模型和可视化模型的复用。（1）实现不同用户间的数据模型的建模逻辑复用，可实现数据模型	一般

		的编辑功能。 （2）实现不同用户间的可视化模型展示界面复用，实现参数继承。	
		数据建模-模型管理-模型集中管理： 实现对所有公开发布的模型进行统一集中管理，利用标签的方式对模型进行有效管理并实现将用户发布的模型分类存放，实现按照模型名称关键字、模型分类关键字、模型描述关键字等搜索功能，实现与标签管理系统对接。 （1）提供模型卡片式列表管理，实现按照多种维度进行展现。根据用户关注模型标签、警种等维度为用户提供同标签模型推荐、同表模型推荐和同类模型推荐功能。 （2）提供模型标签管理功能，系统通过标签的方式对上架模型进行单个或多个标签打标展示，对模型进行有效管理。（3）提供模型推荐功能，根据不同用户的浏览和下载行为以及不同模型之间的关联关系为用户自动推荐其关注的模型。 （4）实现模型全文检索功能，根据模型名称、分类、简介等信息进行分类搜索。	一般
		数据建模-模型管理-模型共享管理： 模型共享管理是指用户通过模型申请、审批流程获取模型使用权限，实现模型共享管理。 （1）实现关注模型管理，提供关注模型的 URL 导出功能，并可实现取消关注模型功能。 （2）实现模型申请功能，通过流程管理功能实现共享模型的申请审批功能，审批结果包括已通过模型、未通过模型和授权模型。（3）实现待办任务管理功能，针对任务审批角色提供模型需求、模型发布、模型使用和成果反馈的待办任务管理等功能。	一般
		数据建模-模型管理-任务计划管理： 任务计划管理主要是用户建完模型后，可选择定时执行该模型。在定时执行页面用户可填写任务名称、任务描述、执行的时间规律输出结果，可供系统调取使用。 （1）建设模型定时运行功能，实现已建设模型按执行的时间规律（每天、每周、每月）、输出结果。 （2）提供数据建模结果表，界面化配置导出至目标数据源功能，实现新建导出任务、导出任务查询、新建导出数据源、导出数据源查询等功能。（3）实现模型任务列表管理功能，包括任务	一般

		的启动、停止、重命名、数据预览、定时频率调整等功能。	
		数据建模-建模可视化-在线分析： 建模可视化在线分析实现拖拽式设计，通过图表库、控件库、配置界面自由拖拽即可形成单表分析、可视化图形自由切换、可视化图形参数配置等功能。实现单表设计，将不同可视化图表的属性进行固化，通过选择配置的方式进行参数的快速设置，参数设置包括但不限于字体设置、颜色设置、预警条件设置、辅助线设置、缩略轴设置、数值设置、坐标轴设置、图表样式设置、图表备注、数据标注等。 （1）提供可视化分析画布，实现图表拖拽配置功能，根据拖拽设置维度、数值、颜色、数据筛选等控件配置可视化分析图表。维度和数值支持实时数据预览，并支持字段名称修改。 （2）实现可视化图表自由切换、维度指标适配、可视化图形适配等功能，自由切换图表库的可视化图表进行多维分析展示。 （3）实现配置字体设置、颜色设置、预警条件设置、辅助线设置、缩略轴设置、数值设置、坐标轴设置、图表样式设置、图表备注、数据标注、显示图内总计、显示标签、自动放大差异值、显示图表标签等参数。 （4）实现图表向下钻取、向上钻取和数据排序的交互分析功能。 （5）多维数据可视化图表之间可以根据某一条件进行联动，联动设置根据分析需求实现取消联动配置。 （6）要求提供图表的二度分析功能，实现通过框选的方式进行自主聚焦、任意维度的下钻、排除和表格展示功能。 （7）实现配置全局筛选、图内筛选、拖拽筛选和表达式筛选等多种筛选器功能。	△
		数据建模-建模可视化-图表库： 建模可视化图标库主要包括内置普通图表库、经纬度图表和自定义图表。自定义图表可实现开放式的多维数据展示，并要求提供自定义图表库。 （1）普通图表库包括但不限于表格、指标卡、计量图、簇状柱形图、堆积柱状图、折线图、百分比堆积柱状图、瀑布图、条形图、堆积条形图、百分比堆积条形图、对比条形图、面积图、堆积面积图、百分比堆积面积图、树	一般

		图、散点图、饼图、旭日图、地图、双轴图、漏斗图、词云、雷达图等。 （2）内置经纬度地图分析功能，经纬度地图分析功能包括但不限于支持气泡图、热力图、海量图、统计图、轨迹图、动态轨迹图等，并可在地图上进行多边形框选、半径全选查看选中区域数据，可在地图上进行多图层可见性设置，支持其他自定义方式，如自定义图标、热力强度、动态更新频率等。 （3）实现自定义图表库自由扩展功能，并将自定义图表库以页面形式，形成自定义图表超市，向用户共享。兼容主流第三方图表库。自定义图表可实现通过 JavaScript、Python 等语言进行图表自定义开发。 （4）实现 3D 柱形图、3D 折线图等多种 3D 可视化展示图形功能，并支持通过拖拽的方式设置 3D 图表的多方位展示。 （5）通过可视化仪表盘的导入和导出功能，实现可视化仪表盘的复用和迁移，并支持仪表盘隐藏配置。 （6）实现可视化仪表盘的分享功能，针对已分享的仪表盘，支持设置取消仪表盘分享功能。仪表盘分享方式包括但不限于免密分享和加密分享。 （7）可视化图表制作时，支持在图表画布使用数据资源添加计算字段和分组字段功能。	
		模型服务-**嫌疑研判模型： 建设模型应用服务系统，对接警务工作门户等相关系统，实现模型应用服务注册、管理等功能。根据业务需求，实现不少于 8 个**嫌疑研判类模型，并构建相关系统应用及服务。 （1）根据需求对**嫌疑研判类的相关信息筛选模型数据来源，开展**嫌疑研判类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**嫌疑研判及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**嫌疑	一般

		研判等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	
		模型服务-**可疑车辆分析预警模型： 根据业务需求，实现不少于 8 个**可疑车辆分析预警类模型，并构建相关系统应用及服务。 （1）根据需求对**可疑车辆分析预警的相关信息筛选模型数据来源，开展**可疑车辆分析预警类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**可疑车辆分析预警及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**可疑车辆分析预警等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-**人员挖掘模型集合： 实现不少于 8 个**人员挖掘类模型，并构建相关系统应用及服务。 （1）根据需求对**人员挖掘的相关信息筛选模型数据来源，开展**人员挖掘类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。（2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。（3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**人员挖掘及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**人员挖掘等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-**车辆预警监测模型集合： 实现不少于 8 个**车辆预警监测模型，并构建相关系统应用及服务。 （1）根据需求对**车辆预警监测的相关信息筛选模型数据来源，开展**车	一般

		辆预警监测模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。（2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。（3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。（4）实现数据模型的可视化分析展示，完成**车辆预警监测及相关警种的模型结果可视化展示。（5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。（6）实现**车辆预警监测等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	
		模型服务-盗窃类案件人案关联模型：实现不少于 8 个盗窃类案件人案关联模型，并构建相关系统应用及服务。（1）根据需求对盗窃类案件人案关联的相关信息筛选模型数据来源，开展盗窃类案件人案关联模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。（2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。（3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。（4）实现数据模型的可视化分析展示，完成盗窃类案件人案关联及相关警种的模型结果可视化展示。（5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。（6）实现盗窃类案件人案关联等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-驾车**模型：实现不少于 6 个驾车**类模型，并构建相关系统应用及服务。（1）根据需求对驾车**的相关信息筛选模型数据来源，开展驾车**模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。（2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。（3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。（4）实现数据模型的	一般

		可视化分析展示，完成驾车**及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现驾车**等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	
		模型服务-案件串并及嫌疑人挖掘模型： 实现不少于 8 个案件串并及嫌疑人挖掘模型，并构建相关系统应用及服务。 （1）根据需求对案件串并及嫌疑人挖掘的相关信息筛选模型数据来源，开展案件串并及嫌疑人挖掘模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成案件串并及嫌疑人挖掘及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现案件串并及嫌疑人挖掘等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-**团伙图谱分析模型集合： 实现不少于 6 个**团伙图谱分析模型类模型，并构建相关系统应用及服务。 （1）根据需求对**团伙图谱分析的相关信息筛选模型数据来源，开展**团伙图谱分析类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**团伙图谱分析及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**团伙图谱分析等相关警种模型与模型管理系统的对接，在模型超市和警务工作	一般

		门户中展示。	
		模型服务-**管控数据模型： 1、实现不少于8个**管控数据模型，并构建相关系统应用及服务。 （1）根据需求对**管控数据的相关信息筛选模型数据来源，开展**管控数据类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。（2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。（3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**管控数据及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的API接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**管控数据等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。 2、服务民生模型：根据业务需求，实现不少于15个服务民生模型，并构建相关系统应用及服务。 （1）根据需求对服务民生的相关信息筛选模型数据来源，开展服务民生模型集需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。（4）实现数据模型的可视化分析展示，完成服务民生模型结果可视化展示。（5）实现模型专题库和分析模型结果的API接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现服务民生模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-**人员再次作案分析模型： 实现不少于8个**人员再次作案分析预警类模型，并构建相关系统应用及服务。 （1）根据需求对**人员再次作案分析预警的相关信息筛选模型数据来源，开展**人员再次作案分析预警类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指	一般

		标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**人员再次作案分析预警及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**人员再次作案分析预警等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	
		模型服务-**地域研判模型： 实现不少于 8 个**地域研判预警类模型，并构建相关系统应用及服务。 （1）根据需求对**地域研判预警的相关信息筛选模型数据来源，开展**地域研判预警类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**地域研判预警及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**地域研判预警等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-**人员再犯罪分析模型： 实现不少于 8 个**人员再犯罪分析预警类模型，并构建相关系统应用及服务。 （1）根据需求对**人员再犯罪分析预警的相关信息筛选模型数据来源，开展**人员再犯罪分析预警类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**人员再犯罪分析预警及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的	一般

		API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**人员再犯罪分析分析预警等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	
		模型服务-**车辆活跃指数模型： 1、实现不少于 8 个**车辆活跃指数类模型，并构建相关系统应用及服务。 （1）根据需求对**车辆活跃指数类模型的相关信息筛选模型数据来源，开展**车辆活跃指数类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**车辆活跃指数及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**车辆活跃指数等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。 2、全息感知数据模型：根据业务需求，实现不少于 25 个全息感知类数据模型，并构建相关系统应用及服务。 （1）根据需求对全息感知的相关信息筛选模型数据来源，开展全息感知模型集需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成全息感知模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现全息感知类模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-**管控模型： 实现不少于 6 个**管控类模型，并构建相关系统应用及服务。 （1）根据需求对**管控的相关信息筛选模型	一般

		数据来源，开展**管控模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**管控及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**管控等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	
		模型服务-**关系人数据挖掘模型： 实现不少于 8 个**关系人数据挖掘类模型，并构建相关系统应用及服务。 （1）根据需求对**关系人数据挖掘的相关信息筛选模型数据来源，开展**关系人数据挖掘类模型及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现数据模型的可视化分析展示，完成**关系人数据挖掘及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的 API 接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**关系人数据挖掘等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	一般
		模型服务-**管控模型集合： 实现不少于 6 个**管控类模型集合，并构建相关系统应用及服务。 （1）根据需求对**管控的相关信息筛选模型数据来源，开展**管控类模型集合及相关警种的需求调研，输出构建模型所需的数据种类和实现思路。 （2）利用大数据平台的知识图谱、机器学习等技术，实现特征指标维度的提取。 （3）实现分析模型集的数据清洗治理，并按照业务逻辑和模型规则建设数据模型，实现数据预警预测分析研判。 （4）实现	一般

		数据模型的可视化分析展示，完成**管控及相关警种的模型结果可视化展示。 （5）实现模型专题库和分析模型结果的API接口封装，提供给其他业务警种和第三方系统进行调用。 （6）实现**管控等相关警种模型与模型管理系统的对接，在模型超市和警务工作门户中展示。	
		知识图谱-数据预处理-身份与行为关系提取：建设知识图谱系统，实现界面可视化，通过大数据平台数据治理的结果数据和公安业务系统中的结构化数据或非结构化数据，提取身份要素、行为要素和关系要素等，实现关系特征预处理。可提供其他业务警种和第三方系统进行调用，完成全息画像关系图谱构建及服务。知识图谱性能要求：在现有网络环境下，100个并发图谱检索查询，任意两个实体间的关系查询响应时间不大于5秒；100个并发3层关系扩展响应时间不大于6秒；千万级实体和关系数据导入时间不大于8分钟。 （1）实现实体定义、关系定义、标签定义、事件定义等功能。 （2）实现对实体分类、属性、名称、样式、颜色、尺寸等定义功能。 （3）实现对关系分类、属性、名称、样式、颜色、尺寸和方向等定义功能。 （4）实现知识数据接入功能，包括数据源管理、图数据接入、事件数据接入等。 （5）实现知识管理功能，包括实体管理、关系管理、标签管理、事件管理和字典管理等。 （6）实现实体提取功能，提取实体数据，并将实体所包含的属性信息一并提取。 （7）实现事件抽取功能，通过触发词识别原始数据中包含的事件，并建立实体与事件之间的关联关系。 （8）实现关系提取功能，提取实体与实体、实体与事件之间的关系。 （9）实现实体消歧功能，包括对同名、多名和缩写等多种实体语义的消歧。 （10）实现实体、关系、事件、属性等信息的存储。存储实体、实体与实体之间、实体与事件之间的关系、实体属性等数据的存储，支持千亿级数据资源的存储和分析。 （11）实现动态图谱分析功能，实现图谱的自定义分析功能，可按照用户实践经验，自定义分析实现不同时间范围、不	一般

		同关系属性，以及不同关系频次情况下的分析。 （12）实现关系分类功能，根据资源属性因素实现自然属性关系和社会属性关系的分类，根据数据实现直接、间接、疑似和时空关系的分类。	
		知识图谱-实体检索-对象检索： 实现对象直接检索、对象批量检索、语义检索、高级检索、关联检索、对象信息展示、检索结果聚类分析、检索结果上图分析、检索结果二次检索、检索结果排序等。 （1）针对对象检索，建设知识挖掘配置功能，对知识挖掘计算模型的配置，包含挖掘场景模板配置、挖掘场景管理、检查配置等一系列可视化配置管理，实现关系拓展、场景共享、自定义布局等功能。 （2）实现实体之间全部关系检索，同时支持对特定时间段内全部关系设置搜索范围。 （3）实现实体之间明确关系检索，如直接关系、间接关系、疑似关系、时空关系等。 （4）建设一度关系检索功能，可同时将多人之间的内部关系进行并行检索。 （5）建设二度关系检索功能，可同时将多人外部的共同联系人进行并行检索。 （6）建设知识挖掘功能，可针对任意对象进行无限关系挖掘扩展。 （7）实现基于图关系挖掘模板创建挖掘场景，提供图计算挖掘算法库，包括但不限于节点特征算法、路径分析算法、子图识别算法、社区划分算法、图嵌入算法等图计算算法。 （8）实现实体关联事件检索，一次性找出对象关联的所有事件。 （9）实现事件关联实体检索，一次性找出对象关联的所有实体。 （10）实现二次检索功能，可针对图谱中已分析结果，进行二次结果的检索。 （11）实现界面及接口服务。	△
		知识图谱-实体检索-全文检索： 使用全文搜索技术构建知识图谱全文数据搜索引擎，实现一键检索，命中结果分类展示、检索条数、模糊检索、范围检索、组合检索、筛选和二次检索、检索结果展示。对全文库中的关系数据进行全文搜索，辅助用户开展关系实战研判工作，为各级用户提供在海量关系数据中快速、准确获得和展现用户所需信息数据服务。	一般

		（1）实现关键词搜索方式，实现千亿级数据资源的全文检索。（2）实现组合查询条件搜索、模糊匹配搜索和精确搜索等功能。（3）实现通过输入单个、多个关键词，上传EXCEL/TXT/WORD 等文件进行批量搜索。（4）针对检索结果，实现新增条件，二次检索的功能。（5）实现对实体的相同属性分析，可根据用户需求或经验进行手工设定内容，自行设定实体关系范围、自定义时间范围、关系频次、自定义关系范围等。（6）提供快捷工具箱，包括图谱比例尺、多种布局方式、最大化、选中、取消选中点和线等工具。（7）实现在图谱内自定义标签创建，用于实现范围实体及事件的快速锁定。（8）实现图形化方式按照时间顺序查看目标实体的行为活动，可进行实体、关系、事件详情的快速浏览。实现时间轴、缩放方式功能，快速查看分析对象变化趋势。（9）实现时间矩阵功能，通过时间矩阵快速掌握事件在不同时间段的发生频率，并可根据发生频率快速范围级联锁定。（10）实现检索结果的单个或批量结果关注、保存、分享等功能。（11）实现图谱多种对外分享功能。（12）实现图谱历史保存功能，实现图谱的历史保存、返回条数、图谱历史缩略图、历史图谱快照等功能展示。（13）使用全文检索服务功能，实现对单个或多个关键字的全文检索服务，根据字段类型实现分词检索和模糊检索匹配。	
		知识图谱-实体检索-标签检索：实现单个标签检索、多个标签及文本进行组合检索，实现与标签管理系统的对接。（1）使用标签组合功能，实现标签组合查询结果的展示，并实现基于标签的二次检索。（2）实现动态检索配置功能，包括检索方式、检索资源、检索结果展示、检索标签配置、结果配置和对应的属性等功能。（3）实现标签检索功能，通过标签检索内容，实现对象标签检索工作。（4）实现标签组合功能，实现标签组合查询结果的展示及快速锁定。（5）支持自定义标签，可快速锁定用户关注实体。	一般
		机器学习-创建模型-聚类：1、构建机器学习	一般

		计算支撑系统，针对公安业务需求，提供相适应的机器学习算法，实现不少于 50 个基于机器学习的公安业务实战模型，实现和大数据平台的一体化联动，并实现实时自学习功能。（1）实现界面可视化。（2）模型创建，实现租户管理。（3）任务监控日志记录和参数配置。（4）通过机器学习算子实现机器学习模型调用。（5）针对分析维度开展统计性描述分析，包括但不限于计数、非空计数、去重计数、标准方差等反映数据离散程度和分布指标。2、通过创建模型聚类分析功能，实现对聚类模型开发的管理。（1）通过大数据平台的数据作为来源，实现聚类数据来源管理。（2）实现配置聚类分析字段功能，对分析数据进行过滤。（3）实现聚类模型信息管理功能，模型信息包括模型名称、聚类算法、类别名称和调参配置等。（4）实现自主参数调参功能，对聚类参数进行优化调整。	
		机器学习-创建模型-分类：通过创建模型分类分析功能，实现对分类模型开发管理。（1）通过大数据平台的数据作为来源，实现分类数据来源管理。（2）实现配置分类标签字段功能，对分类数据进行过滤。（3）实现分类模型信息管理功能，模型信息包括模型名称、分类字段名称、分类算法和调参配置等。（4）实现自主参数调参功能，对分类参数进行优化调整。	一般
		机器学习-创建模型-预测：通过创建模型预测分析功能，实现对预测模型开发的管理。（1）通过大数据平台的数据作为来源，实现预测数据来源管理。（2）实现配置预测分析字段功能，对预测数据进行过滤。（3）实现预测模型信息管理功能，模型信息包括模型名称、预测字段名称、预测算法和调参配置等。（4）实现自主参数调参功能，对预测参数进行优化调整。	一般
		机器学习-模型调试-小数据量运行：通过对小数据量运行模型调试，实现样本数据膨胀、特征选择计算等功能。（1）通过大数据平台的数据作为来源，实现小数据量来源管理。（2）实现配置关联规则分析字段功能，通过	一般

		关联规则对数据进行筛选过滤。 （3）实现关联规则模型信息管理功能，模型信息包括模型名称、关联规则算法和调参配置等。 （4）实现自动和手动两种方式调参，对关联规则参数进行优化调整。	
		机器学习-模型调试-调试结果数据查看：实现调试结果数据查看功能，通过查看参数，实现数据结果多方式展示。 （1）实现混淆矩阵和ROC 曲线展示方式查看训练结果信息。 （2）实现以表格形式展示训练的数据详情。 （3）实现查看模型的训练详情，包括使用算法及配置参数、衡量模型的准确度、召回率等。	一般
		机器学习-模型调试-运行日志查看：实现用户在组件调试过程中查看运行日志信息，对于在调试过程中正在运行的相关信息进行结果输出。 （1）实现在组件调试过程中查看运行日志信息。 （2）实现根据日志创建日期进行操作日志的检索。	一般
		机器学习-模型训练-数据拆分：通过数据拆分算子功能实现原有的业务数据集拆分为训练数据集和测试数据集。 （1）通过调用基础算法库中的相关算法，实现迭代训练。 （2）通过测试数据集对配置参数进行结果验证，实现预测数据质量的评估。	一般
		机器学习-模型训练-迭代训练：实现迭代训练数据预览和训练详情的展示功能。 （1）实现迭代模型数据预览，展示详细数据信息，并统计分类、聚类和预测的标识计算情况。 （2）实现查看迭代训练模型详情，展示模型使用算法，及推测值和真实值。	一般
		机器学习-模型训练-训练结果查看：实现用户对不同算法的训练结果进行查看，通过算法参数调整，实现模型算法“机器+人工”的训练模式。 （1）实现训练结果查看功能，在人工进行训练后，针对训练结果对模型进行编辑校正。 （2）实现训练结果可视化图表展示功能，训练结果开放服务接口调用。 （3）通过重新训练的功能实现模型更新。	一般
		可视化展示-个人信息-个人首页： 建设工作台系统，实现用户信息、工作任务、常用服务	一般

		等基本信息的展示，实现与警务工作门户的对接。（1）实现大数据平台相关的消息提醒功能。（2）实现个人工作任务的展示，包括已办工作任务和待办工作任务。（3）对接数据资源目录，实现数据使用权限的申请和审批功能。（4）对接服务资源目录，实现服务接口的使用申请和审批功能。（5）实现多级用户登录，主要包括省级和共建地市用户登录。（6）实现大数据平台租户的申请和审批。（7）在现有网络环境下，系统性能要求可满足不低于30000用户同时在线不少于2000并发的操作。（8）在现有网络环境下，系统功能操作响应时间不大于2秒，功能页面渲染加载时间不大于2秒。	
		可视化展示-我的数据-数据搜索：可对数据资源通过输入关键字的方式进行搜索，可实现模糊搜索，搜索到相应资源后可以查看具体的数据资源的字段详情信息。（1）实现数据搜索，不同用户搜索的结果数据按照权限展现不同的数据内容。（2）完成数据搜索的结果实现图形化展示等功能。（3）实现个人数据资源的搜索，展示数据在原始库、资源库、主题库、业务库等数据库中的分布情况。（4）实现对数据元的搜索，展示数据血缘情况。	△
		可视化展示-我的数据-数据分类：可按照编目系统已有的业务域如人、地、事、物、组织进行分类，同时也可以按照数据归属的警种来源进行分类。选择不同分类即可查看对应分类下的数据资源情况。（1）实现数据在原始库、资源库、主题库、业务库等数据库中的数据量、数据种类、更新周期等情况进行分类展示。（2）实现数据按照数据归属警种和数据来源进行分类展示。（3）实现数据分类查看功能，根据不同分类可查看对应分类下的数据资源情况。	一般
		可视化展示-我的模型-全部模型：可按照地市、警种、应用区域、最新上线、热门模型等维度对平台中已建的所有模型进行分类展示，并统计模型总量、使用量等信息。（1）对接数据建模平台，实现模型目录按照地市、警种的分类展示。（2）实现服务目录按照地市、	一般

		警种的分类展示。	
		可视化展示-我的模型-模型制作： 实现服务模型和服务接口的开发制作功能。（1）通过对接数据建模模块，实现拖拽式可视化服务模型创建。（2）实现数据治理和处理结果表的服务接口创建。	一般
		可视化展示-我的模型-模型发布： 实现模型和服务 API 发布和共享功能。模型的发布和共享是指将模型发布至模型超市进行展示，API 的发布和共享是指将服务 API 注册到服务资源目录中，并通过服务资源目录发布到服务总线。（1）实现模型和服务 API 发布申请、审批、上线、下线等功能。（2）实现模型发布后对模型进行运行情况监控。（3）实现服务 API 接口运行情况的监控。	一般
		可视化展示-我的应用-应用搜索： 实现平台内的各类应用搜索和集成功能。（1）实现按照应用系统分类和名称精准匹配和模糊匹配搜索。（2）实现数据治理日志的统一查询检索功能，包括集成，并可针对日志信息进行统计分析展示。（3）提供大数据平台各类系统及模块的集成，包括数据建模、知识图谱、数据分析等系统模块。	一般
		可视化展示-我的应用-全部应用： 实现大数据平台应用市场和应用访问情况。（1）实现应用列表，按照应用归属地市、警种、访问排行等维度进行分类展示。（2）实现申请我的应用功能，自定义我的应用列表。	一般
		可视化展示-我的战果-战果展示： 提供数据服务、模型服务和应用等使用情况多种维度的战果统计。（1）根据数据服务的使用情况，自动生成各类统计图表。（2）提供模型评价和使用统计功能，实现可视化图表，按照区域、用户、使用率、使用时间等维度进行排名。实现模型概览、最新模型展示、最热模型展示和模型详情展示等功能，并实现各警种建模情况进行排名、各类标签模型数量排名、组织单位建模情况排名、高评分模型排名、用户建模情况排名等。（3）实现数据资源展示大屏，包括但不限于使用 3D 折线图、3D 柱状	一般

		图、滚动图表和主分屏交互形式，直观展示数据治理过程信息、结果信息、数据处理、数据服务、数据应用等各阶段成果和使用情况的一体化展示。	
		公安部部标适配： 建设元数据管理系统。建设大数据系统，满足公安部云计算平台建设相关技术标准，在通用的大数据平台软件基础上开展包括但不限于接口定制化开发工作。 （1）实现数据元管理系统构建，实现界面可视化、多用户登录管理。实现任务监控日志记录和参数配置。实现公安部数据元对接，本地存储公安部数据元标准库，并开展数据元与数据项引用。 （2）根据公安大数据处理规范数据元管理规程要求，完成本地数据与部数据元对标工作。 （3）根据公安大数据处理规范数据元管理规程要求，实现数据元注册、数据元变更、数据元停用等工作。 （4）根据公安大数据处理规范数据元管理规程要求，实现标准代码管理，包括标准代码注册、标准代码变更、标准代码停用等功能。 （5）根据公安大数据处理规范数据元管理规程要求，实现数据元管理功能建设，包括数据元管理、数据元查询、标准代码管理、标准代码查询和数据元标准代码监控功能。 （6）按照公安部相关技术标准数据汇聚要求，通过部级数据资源上传和下发接收接口对接，实现向部级上报数据，接收部级下发数据。（7）完成数据治理实施标准制定工作，包括文档化部署步骤、数据库表命名规范、主题命名规范、脚本命名规范等实施有关的标准规范。（8）实现应用服务测试环境管理和应用开发基础组件建设并对外提供服务。应用服务测试环境管理，包括不限于实现快速部署测试环境、代码部署测试、代码质量分析、代码缺陷错误管理、测试介质管理、应用服务测试环境的登记注册、审核审批管理等功能。应用开发基础组件，需根据实际应用提供应用开发的基础组件和开发环境，适配公安大数据平台应用开发的 DevOps 可视化开发环境。构建大数据平台高可用的 DNS 域名解析服务。	一般
		集成服务要求： （1）集成规划设计：通过需	一般

		求调研及澄清、业务模块关系梳理、整体架构设计方案输出、云计算平台基础设施资源需求和大数据处理技术架构详细设计。（2）利用项目和产品管理系统集成项目管理：对项目进行统一协同管理，包括项目计划、资源管理、变更管理、质量管理、进度管控、风险管理、文档管理、项目验收等，确保项目高质量的按时、平稳交付。（3）数据实施：提供基于大数据平台的一系列设计、并协助开发和测试服务。实现相关系统的数据和服务接口对接工作。（4）集成验证服务：提供应用的集成验证服务，包含项目需求分析、集成验证方案设计、测试验证、集成验证等服务，以保证系统对接效率和质量。（5）业务上线支持：系统部署完成后，支撑和保障业务上线，同时对业务稳定性和连续性等进行评估，以保证整体业务快速上线。（6）质保期内，协助采购人完成制定省级行业大数据处理相关标准的工作。	
2.2	新一代移动警务部分（一期）	全省移动警务Ⅰ类区门户： 1、基础服务：包括首页管理、应用、组件、消息、系统及第三方接口管理等功能。 2、开发包服务：各应用模块可以通过开发包和客户端主程序交互，如获取会话信息、用户信息、平台时间等。 3、应用客户端程序：应用客户端程序指基于平台开发、发布的各应用模块的客户端程序，用户可以在客户端主程序界面上查询、下载、安装应用客户端程序。 4、应用开发者门户： 开发者注册：开发者注册信息包括开发者账号，开发者名称，开发者简介，联系人等开发者相关基础信息，由信通管理员进行审核，审批通过后可以在开发者门户系统提交应用发布的申请。 应用注册：应用注册信息包括应用 ID，应用名称，应用简介等应用模块相关基础信息，由信通管理员进行审核，审核通过后可以进行后续的开发和发布申请等操作。 应用发布：应用发布需要提供信息包括版本信息，应用截图等，由信通管理员进行审核，审核通过后自动发布。 5、管理员门户： 开发者管理：开发者管理主要包括开发者账号审核、开发者账号锁定、开发者账号注销等功能。 应用管理：包括应用审核、版本审核、应用下	一般

		架、应用注销、应用权限分配、版本权限分配、审批历史查询等功能。 特殊分类管理：系统可任意指定应用的特殊分类，以便客户端主程序能做不同的排版显示。 警员管理：包括用户管理、角色管理、权限管理。 基础数据管理：基础数据管理模块包括应用分类数据管理等功能。 应用商店管理：应用商店管理模块用于对客户端主程序进行管理，包括客户端主程序的发布和版本管理等功能。 统计分析：统计分析模块包括系统内各种信息的查询和统计功能,如应用评分排名统计；统计分析模块还支持生成各种报表，包括标准报表以及个性化定制报表等。 系统管理：平台管理系统相关管理功能，主要包括用户管理、日志管理等功能。 6、应用服务端程序：基于平台开发、发布的各应用模块的服务端程序，服务端程序一般和应用模块的客户端程序一一对应。 7、应用规范体系： 移动应用开发规范：明确应用开发必须遵循的一些技术规范和要求，并详细阐述移动应用平台提供的服务集及使用方法。 移动应用管理规范：明确了应用的上线审核流程，即应用必须满足移动应用开发规范，并通过应用功能、安全、稳定性等方面的测试，才具备上线发布的条件。 终端使用规范：主要明确了终端申请、发放、注销、补办及日常使用的流程。 8、日志管理：针对系统应用及功能的操作、使用过程等记录相关日志，主要包括终端行为日志、终端应用安装日志、终端应用使用日志、数据访问日志、后台管理日志。提供日志查看的功能，并提供系统日志及各类统计等功能，包括系统访问量等日常统计。	
		全国移动应用服务互联支撑体系互联： 1、网络配置：全国移动警务应用支撑互联互通业务需要通过公安信息网和公安移动信息网开展。各省级平台联网服务子平台（Ⅱ类区）接入公安移动信息网需要依赖网络设置。 2、部署升级：在不影响全省已有应用的前提下，对系统各区域应用支撑服务进行部署升级、迁移。 3、管理配置：在部级管理中心部署本地平台信息。在本级管理中心配置部级平台级联寻址	一般

		服务等相关信息。 4、移动应用及资源服务改造接入：包括开发者注册、服务资源改造接入、机制认证、协议认证、服务资源注册等功能。 5、应用改造接入：包括注册应用、申请资源、配置环境、开发应用、发布应用等功能。 6、应用对接联调：包括应用升级、资源申请、应用联调等功能模块。 7、统一授权：联网服务子平台（Ⅱ类区域），支撑Ⅱ类应用，其中管理功能可视情况确定部署位置。 8、全国互联：互联内容包括配置管理和寻址服务两个方面。 9、配置管理：省级平台互通接口开发、省级平台上报互通接口给部级配置中心、省级平台从部级配置中心同步互通接口。 10、统一认证：用户信息统一认证、应用信息统一认证、统一认证客户端功能开发。 11、应用市场：同步异地平台应用数据、本地平台显示异地应用数据。 12、服务总线：同步异地平台总线资源数据、服务总线客户端功能开发、服务总线服务端功能开发、服务总线异地接口转发功能。 13、统一权限：同步异地平台用户与应用权限数据、同步异地平台应用与接口资源权限数据、统一认证，资源寻址以及接口转发统一权限校验。 14、跨域改造：互联互通跨域资源同步、改造联调等。 15、日志管理：记录资源的调用行为。	
		全省移动警务视频融合系统： 1、视频会议：支持实现山东省公安机关实时大规模音视频交互，满足但不限于会议、会商、调度等各种远程多媒体视频会议需求。 用户注册终端支持不少于 12 万用户注册，不少于 500 路并发。 2、桌面会商： 通过桌面会商进行视频交流，还可在视频交流过程中共享文档、图片、视频等资料，实现各级各部门之间进行及时、充分的交流。 支持调度下级单位会场进行双向音视频互动。 平台支持视频监控国标 GB/T28181 协议、ONVIF 协议及 RTSP 协议。 支持在视频会议中调度视频监控图像入会。 支持扁平化调度，可跨级调度基层单位或一线现场。 支持分组和分级调度，支持调度前端快速查询、单呼、组呼。 支持对调度资源进行预案设置，调度时实现与网络视频电视墙的	△

		联动显示。 桌面会商终端支持警务通 4G、5G SIM 卡，无需接入有线网络即可接入移动信息网；桌面会商终端应配置 9 吋至 12 吋触控屏，无需遥控器，通过触控方式操作。桌面会商终端支持 4K30fps、1080P30fps、720P30fps、360P30fps、180P30fps 等分辨率。 3、远程培训： 各接入单位可基于移动警务视频融合平台进行远程培训应用。 培训管理平台分为课程前台与管理后台两部分：课程前台主要提供直课程观看、精品课程点播、培训资料归档、文件分享等功能；管理后台主要为管理员提供平台配置、人员管理、培训管理、文档管理、培训统计、系统设置等功能。培训平台支持基于音视频互动的培训课程创建与管理，可以进行课程安排、人员通知、报名管理、课后录像资源管理等。 培训过程中支持高清内容分享。培训过程中支持网络化巡课监课功能，可按课程类别进行筛选进行巡课监课，确保培训过程可管可控可监督。培训平台文档中心支持文件上传、下载与分享，分享的文件可由平台用户在前台页面进行预览、下载。 4、融合视频会议系统： 移动警务视频融合系统应支持 H.265、H.264SVC、H.264AVC 视频编解码，G.711、G.722 音频编解码。利旧现有视频会议系统，与现有移动警务视频会议平台兼容互通。 平台须对接现有移动警务系统，实现现有山东省公安厅移动应用服务平台“视频互联”APP 的接入。 5、融合视频监控系统： 支持监控国标 GB-T28181 协议、ONVIF 协议及 RTSP 流，通过获取监控设备码流，转换为标准码流后，传送到视频会议系统中。云视频平台可以在应急会议及会商会议过程中任意转发和调用监控视频，实现对一线现场情况全面掌控。	
		移动警务应用开发： 1、疫情核查：对接公安部疫情接口，制作疫情核查应用，包括确诊、疑似人员、密切接触者比对，车辆轨迹信息查询等功能。 2、多语种翻译：对接公安部语种翻译接口，制作多语种翻译应用，包括多个语种之间的互译：中文，英文，韩语，日文等；并支持语音翻译功能。 3、会议管理：制作警	一般

		务微信会议管理系统，会议通知编辑，参会人填报，签到、日常维护管理，显示当日会议签到情况等。	
		安全服务： 1、系统层安全渗透测试：针对主流操作系统进行渗透测试，主动发现操作系统存在的各种漏洞。 2、WEB 应用渗透测试：针对 WEB 常见的应用，重点测试由于安全设计不足和开发不规范所造成的隐患和漏洞。 3、对 APP 提供安全检测服务，重点测试信息泄露造成的隐患和漏洞。 4、根据公安行业安全检查和攻防演练工作要求，配合采购人完成年度安全检查、等保安全问题整改和攻防任务。 5、提供安全服务时限不少于 3 年。	一般
2.3	山东省公安信息网大数据智能化安全体系（一期）	安全管理中心-业务安全策略控制服务联动： 1、支持与环境感知服务联动，接收环境感知服务信息； 2、支持与认证服务联动，接收令牌和风险信息； 3、支持与权限管理服务联动，接收风险信息； 4、支持与审计服务联动，接收风险信息； 5、安全防护策略控制支持对多源、异构数据的多维度关联分析、研判；支持根据配置基线，进行智能推理、分析研判，生成决策结果。 6、安全防护策略控制支持基于决策结果进行服务的编排和调度，并支持无码化接入和对接；支持预置或自定义自动化脚本进行闭环处置； 7、通过安全策略控制的编排，协同联动安全大数据分析平台的其他功能模块，如推送模块，将管理策略分析结果或控制策略的执行反馈结果通过邮件或工单的形式推送给安全管理人员； 8、当策略即将到期时，能够自动下发提醒功能。	一般
		安全管理中心-安全管理中心级联： 1、通过数据流、工作流、指挥流、控制流等实现业务过程协同、组织过程协同、技术过程协同和数据过程协同； 2、全面提升省市级安全检测、安全防护、安全响应、安全处置、风险预警和态势感知能力，有效提升安全运营的效率和效果。 3、省厅和建平台的市公安局安全运维人员通过态势感知、安全风险评估、安全预警通报实现组织过程协同，从多个层面综合考虑以建立全方位的安全防护体系。 4、省厅安全管理中心可采集各地市数据中心内各类安全能力	一般

		日志等相关信息，实现在全省范围内的安全态势展现和风险管理，省市两级安全管理中心通过威胁情报共享实现数据过程协同，提升省市两级安全运营的效率和效果。 5、可依托安全管理中心的威胁情报库进行共享，持续提升省市级网络威胁检测能力，实现从被动防御变为主动检测，全面提高网络威胁防御能力。	
		零信任体系-认证服务联动： 1、认证支持部-省-市三级联动，部级认证主要为直接访问部级应用的用户提供身份认证服务 2、省、市级认证主要为访问山东省和建平台的地市本地应用的用户提供身份认证服务。 3、支持多种认证方式，包括 PKI、CA、动态口令认证等，要求支持认证方式可灵活配置扩展。 4、支持国密算法。 5、支持认证链管理，多种认证技术按策略进行认证链组合。	一般
		零信任体系-权限服务联动： 1、山东省厅和建平台的市局权限管理服务为本地提供权限管理服务，授权客体为本地资源； 2、部级权限管理服务可定义授权主体与客体映射关系或角色与授权客体的映射关系做为全局授权策略，全局授权策略可下发至山东省厅和建平台的市局，同时山东省厅和建平台的市局的部级权限管理服务对于全局授权策略不得修改，只可使用，以保证权限管理的一致性。 3、支持权限数据的准实时触发与自动同步，包含业务角色数据同步、业务角色分组同步、功能数据同步、菜单数据同步、角色功能关系同步、角色菜单关系同步、用户角色关系同步、角色互斥关系同步。 4、支持账号权限的自动回收与注销，包含离职权限回收、账号注销权限回收、调岗权限回收。 5、支持集中管理组织内所有用户、所有应用的系统权限，实现对权限控制相关的基础对象管理维护功能，包含菜单权限对象、功能权限对象、API 权限对象、关联用户、互斥对象、扩展属性、关联角色的管理维护。	一般
		零信任体系-业务审计服务联动： 1、支持给审计服务发送流程操作相关日志。 2、接收业务应用创建审批流程的请求； 3、支持业务应用查询审批流程列表； 4、支持业务应用查询	一般

		审批流程详情； 5、支持业务应用撤销审批流程； 6、支持业务应用删除审批流程； 7、可下发至山东省厅和建平台的市局，同时山东省厅和建平台的市局的部级权限管理服务对于全局授权策略不得修改，只可使用，以保证权限管理的一致性。	
		零信任体系-业务审批服务联动： 1、与认证服务联动接收认证服务的用户令牌；获取认证服务用户信息、组织机构信息。 2、与权限管理服务联动 通过权限管理服务判定审批流程是否命中白名单。 3、与审计服务联动 发送审批日志给审计服务，日志信息包含审批信息详情及审批人签名。 4、接收认证服务、权限服务、审批服务、各应用、各市局上报的日志。	一般
		零信任体系-可信环境感知服务： 1、支持对终端进行标识，标识应具备唯一、永久、防篡改、不可伪造等特性，支持感知公安安全U盘、公安 PKI_UKey 插拔。 2、支持漏洞风险感知：能够通过终端上安装的漏洞扫描软件扫描出当前系统上未修复的系统漏洞，以及漏洞的风险级别。 3、支持网络风险感知：具备对当前终端是否连接互联网、是否有无线网卡、是否开放共享服务、是否监听指定端口等网络变化进行风险性感知，对可疑行为实现日志审计并上报、告警和评估。 4、支持外设风险感知：具备对终端上外接新的设备的识别采集能力，并对新接入的外部设备进行风险感知分析，支持实时上报、告警和评估；具备对移动存储设备插拔、网络打印机输出、打开摄像头等外部设备变化进行风险感知分析，对可疑行为实现日志审计并上报、告警和评估。 5、支持安全配置感知：具备对主机的系统配置风险性感知，比如弱口令、权限变化、登陆注销事件、配置变更审计日志等进行风险感知，并对存在的风险项进行审计、上报、告警和评估；其中主要安全基线包括身份鉴别类、安全审计类、访问控制核心配置类、资源控制配置类、入侵防范类等。 6、支持恶意代码风险感知：具备对终端是否安装了防病毒软件以及从防病毒软件获得当前系统上存在的恶意代码风险；	一般

		具备感知防病毒软件的病毒库的更新状态。支持应用环境风险感知：能够检测到终端运行了指定的非法应用程序，同时能够感知到是否没有运行指定的必备应用程序；能够检测到是否存在指定的非法服务，同时能够感知到是否不存在指定的合法服务；能够检测到是否存在指定的非法注册表项，同时能够感知到是否不存在指定的必备注册表项。 7、支持系统应用类风险感知：包括但不限于 IE 主页相关项目、IE 菜单项、IE 核心配置、IE 外观配置、IE 常规设置、IE 浏览器图标配置、Internet 选项、用户样式表、重置 web 设置、About 协议、域名解析文件 Hosts、常用文件关联项、磁盘及文件夹配置、系统常用组件、系统启动配置、系统图标配置、任务栏及开始菜单、系统重要服务组件、组策略、显示属性、Web 桌面、网络驱动器、打印机设置、收藏夹快捷方式、桌面图标快捷方式、开始菜单快捷方式、桌面及资源管理器、快速启动栏快捷方式等项目；具备感知浏览器的安全级别和配置，具备感知浏览器的插件配置以及变化情况。	
		安全访问平台： 1、支持用户管理与认证功能，支持用户的新增，修改，删除。 2、支持对角色的管理，包括新增，修改，删除自定义角色 3、支持给成员授予不同的角色，支持用户角色自定义组合，支持基于角色的访问控制管理。 4、支持 HTTPS 安全访问方式。 5、支持自定义登陆超时设置，可以在无人操作时自动登出系统。 6、支持用户多次登录失败时，自动锁定账户。 7、支持通过 REST API 接口、SNMP、SYSLOG 等方式来对接安全设备的告警数据采集。 8、基本性能监控指标：CPU、内存、设备在线情况、设备连通性、设备响应时间等。 9、支持设备接口流量指标采集，如接口实际速率，接口利用率，接口带宽。 10、支持设备的业务指标的采集，如可信接入代理的 SSL 新建，并发，认证速率等。 11、支持性能监视设置和管理，支持采集对象、采集周期、采集状态的设置。 12、支持性能告警阈值设置，支持设置产生告警条件，设置自动恢复告警条件。 13、支持性能指标	一般

		自定义，提供用户定制采集指标的功能。定制指标用于性能管理采集监控实例的此指标数据。 14、支持告警展示，查询。 15、查看选定设备的健康状态，提供搜索功能快速定位到告警对象，查看详细告警信息。 16、告警按告警紧急程度分为紧急告警、重要告警、普通告警和信息类告警。 17、级别不同，告警显示颜色不同。可以根据告警等级进行告警筛选。 18、支持为不同的监控对象设置不同的通知规则，可以启用、停用规则，可以删除、修改规则。支持短信、邮件告警通知 19、支持配置邮件、短信网关来支持发送告警通知，支持邮件标题、内容、收件人、抄送人、密送人的自定义，支持短信内容、手机号码自定义，所有告警通知支持指定时间或时间范围的发送；支持告警发送的日志记录和搜索 20、支持告警支持批量认领、分配责任人、转移责任人、关闭操作。 21、支持告警转工单规则配置，通过设置设备对象类型、群组以及告警等级，选择工单模型，满足并不限于该规则的告警会自动生成工单并按照选定的工单模型流转到对应的责任人； 22、支持单个和批量告警手工转工单。 23、支持告警归并，同一类告警合并为一条。 24、支持告警屏蔽，提供告警屏蔽规则设定，通过告警源（产生告警的设备）、具体告警、时段的设定系统屏蔽告警的规则。 25、支持纳管各组件（当前设备为边界防火墙、可信接入代理、可信 API 代理、可信代理控制服务、认证服务、权限服务、环境感知代理、环境感知服务）上送告警的接收和展示，包括各使用率超限告警及链路可靠性告警。 26、提供默认显示首页，显示设备告警统计等关键指标。 27、提供可供定制的首页选项，通过首页的定制，用户自行添加或去除首页显示内容 28、支持自定义大屏展示整体方案中安全设备的整体运行情况，比如可以对安全访问平台当前的运行状态和历史的运行状态进行查看，了解平台的整体运行情况。 29、提供网元在线离线状态显示和刷新，网元故障信息的显示和刷新，链路故障状态的显示和刷新。 30、支持链路监测功能，通过链路	

		检测，监控链路的可用状态，支持业务故障快速定位。 31、支持设备的手动添加，或者批量导入。 32、配备不低于1000个设备资产管理License。	
2.4	山东社会治安动态全息感知网安全防护体系	视频监控共享平台： 1、软硬件一体化设备，配备千兆电口不少于6个，万兆光口不少于2个；（硬件） 2、镜像流量处理能力不少于20Gbps；（硬件） 3、支持资产发现和识别功能；（软件） 4、支持IP资源管理功能；（软件） 5、支持外设控制功能；（软件） 6、支持多维度的外联加固能力，能够根据外联服务器/外网域名定义外联探测地址，对仅连接外网时或同时连接内外网时分别自定义防护动作，如终端提醒、断开网络、强制关机等，并进行提醒信息自定义；（软件） 7、支持配备接入互联网的监测能力；（软件） 8、支持非授权外联管理功能，支持在不安装客户端代理的情况下，自动发现管理域内非授权外联的行为，上报设备的内网IP、外联时间；（软件） 9、内外网互联监测功能，自动发现管理域内同时连接内网和外网的设备，并上报设备内网和公网IP以及外联时间，可追溯外联前30天内的应用系统访问日志，并能在外联服务器上取证；（软件） 10、支持违规外联防护功能，支持不依赖客户端，对违规外联的设备实现定点阻断。同时，对于违规行为，支持通过网页访问跳转警示；（软件） 11、支持朔源取证功能，支持审计、记录网络边界和违规行为的网络流量，支持外联事件的核查取证。（软件）	一般
2.5	山东省公安厅“一门四通”项目（一期）	一门通晓-工作首界面： 警务工作门户面向全警，是各个应用系统的入口，根据不同警种不同级别用户的不同界面需求，对首页展现形式、内容进行定制，满足个性化的应用。平台门户包括模板定制、栏目定制、菜单定制、快捷功能定制、工作情况统计等功能。实现全省统一的登录鉴权中心，集成的所有应用登录统一在鉴权中心做身份认证，不影响业务系统不同位置的访问界面，实现一次认证，全网漫游。 构建移动门户，打通桌面应用和移动应用，实现PC端和移动端互通。打通警务微	一般

		信，实现警务微信端信息在 PC 端门户的提醒。包含用户登录、用户服务、授权服务、服务总线对接、日志服务、通知公告、消息服务等通用功能。 整合公安内部系统，汇聚关键数据并在门户集中展示；不需要再次进入业务系统，形成快速处理业务的能力；门户卡片来源于应用，应用建立完成后可以将应用生成门户卡片；应用删除时，同时将生成的门户卡片删除；门户快捷入口来源于应用，配置门户卡片的同时可以勾选同时生成快捷入口；应用删除时，同时将生成的快捷入口删除 汇聚各业务系统待办消息，可对接第三方系统；汇聚各日程系统的日程数据，可对接第三方系统；汇聚各任务系统的任务数据；汇聚公众号的数据；用户在终端上可以使用拖动的方式配置卡片和入口的排序。支持对接警务工作门户统一认证服务，获取凭证信息，校验后登录。 提供对于用户服务，支持对接 PC 端警务工作门户的用户服务，获取用户信息，并在业务功能内进行应用。	
		一门通晓-公告： 查看已读未读，公告也可和消息有阅读状态，显示已读/未读，并且支持部门统计；公告自动添加签名，支持编辑修改；公告可通过单独的应用消息推送到用户的会话列表页面，保证公告必达；支持上传封面图片；可设置文本样式，插入图片，表格，自动识别 URL 链接等等富文本编辑功能 支持公告附件上传，单个文件大小控制在 100M 以内。另外还需要在公告门户支持： 1、门户首页 建设半开放式门户首页，门户登录前展示门户通知公告、警务要闻、重要消息提醒等不涉密内容，并且列出所提供的主要办事事项，实现对门户功能的基本了解，登录后可自定义设置不同门户布局。 2、工作台页面布局 通过个人配置和机器算法结合实现“千人千面”，门户各功能模块可根据自身业务配置，用户根据不同角色、关注习惯自定义设置首页布局，并按照地域、警种部门实现不同风格、不同功能的工作台面，投标方案中提供领导、警种部门、派出所等三种以上不同用户的设计方案。 3、工作台内容定制 根据个人、警	一般

		种、使用习惯、浏览记录进行智能推荐，让门户展示更加贴近业务本身，成为用户的“专业秘书”，提升工作宽度和效率搭建基础服务，加深部门间协作。	
		一门通晓-共享服务： 包括常用工具集、模型等。 1、SSO（单点登录），在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统 2、自适应单点登录，不需要第三方系统供应商支持的单独登录方式 3、消息推送 第三方系统可将消息推送到门户 4、应用消息分类，推送的应用消息可自定义分类 5、帐号同步，提供 API 接口，可与第三方进行帐号同步 6、SDK，可通过 SDK 的方式把产品能力快速集成到用户的门户平台中 7、基于消息的交互，应用消息支持自定义模板，并可附上按钮，可直接在聊天界面完成复杂的工作流操作 8、Bot 能力，开放 Bot 能力给组织开发者使用 9、开放消息流入能力，开放向单人或者群发送实时消息的能力 10、开放消息流出能力，开放外部系统获取单人或群消息的能力 11、反向登录，可实现在第三方系统中沟通 12、插件，开放系统菜单（首页，会话界面、消息菜单），支持通过 URL、webhook 方式自定义消息长按菜单	一般
		一门通晓-文件传输： 1、离线文件传输，无论接收方是否在线，都可在单人会话或者群里进行离线文件传输 2、文件夹直接发送，PC 端文件传输支持发送文件夹 3、文件拖拽发送，PC 端支持文件拖拽进入会话窗口即可发送文件 4、局域网快传，单人会话支持点对点局域网快传文件/文件夹 5、文件已查收/未查收状态，文件也可和消息阅读状态一样，显示已查收/未查收状态 6、断点续传，文件传输支持暂停重启，且支持断点续传 7、文件预览，聊天中发送的文件在移动端可进行预览 8、文件上传下载记录，PC 端可显示用户上传下载的进度及记录	一般
		一门通晓-组织应用： 在新一代公安网下，基于云平台和大数据平台提供的能力，基于门户一期的统一认证、权限、消息等建设成果，增加警务工作门户的智能化程度。实现警务工作	一般

		门户对用户域应用、数据域应用、移动警务应用的统一接入管理，实现用户的无感知切换。实现应用的标签化管理，可通过标签快速检索查找到应用；实现应用不同维度的检索，包含地市、主题、警种等；根据使用习惯和应用评价，实现优质应用的推荐；实现全面应用详情档案，展示应用基本信息、使用评价信息、开发者信息等；实现应用的评价评分展示；根据不同维度实现应用的排名，如访问量、下载量以及评价得分等。 1、自有应用管理，组织用户可将自身的应用通过开放平台接入到门户中，并可针对每个应用进行可见范围设置 2、APP 应用接入，移动端工作台支持第三方 APP 接入唤起，并支持未安装应用提示下载 3、移动端 Hybird，支持上传 web 应用离线包的方式，提高应用页面的打开速度 4、工作台可配置，管理后台可对移动端工作台进行应用分类、应用排列、公告应用卡片等进行配置	
		一门通晓-其他： 1、字体大小设置，用户可根据自己的使用习惯来调整屏幕上的字体大小，方便查看 2、扫一扫登录，PC 端和 WEB 端可通过移动端扫码进行快速登录 3、多语言支持，客户端可根据客户语言要求支持相应语言	一般
		一门通晓-工作圈： 1、发布图文信息，支持文字、选择或拍摄图片发布到工作圈 2、发布本地视频，支持本地视频（限 30 秒）发布到工作圈 3、发布 URL 网址，支持输入 URL 网址直接转成卡片后发布到工作圈 4、发文时设置可见范围，发文时可选择谁可以看到当前发文 5、删除，支持删除自己的发文 6、对发文内容进行评论与点赞，可见联系人可以对发文进行评论和点赞 7、分享聊天中的 URL 至工作圈，支持将会话界面中的 URL 卡片分享到工作圈 为实现以上功能，要求实现： （1）数据模型管理，依托数据资源服务和应用服务，打造数据模型资源池，提供预设模型，也可以对接第三方数据模型，对模型进行整合管理。（2）模型订阅，实现模型的自定义订阅、模型分析数据的精准推送、模型的自主推荐。（3）模型分析轻应用，建设并支持模型的轻	一般

		应用服务，实现基础的数据赋能轻应用，供用户按需选择。 （4）智能助手，实现数据、模型、模块的主动推送、智能推荐。	
		一门通晓-多端在线管理： 手机通知管理，默认关闭，当收到新消息通知时，手机端不会再收到 Push；退出桌面端，将桌面端退出登录，跳转至登录界面，桌面端退出登录后，手机正常接收 Push 通知和声音。另外还要实现： 1、身份认证 为各个警务应用开发提供通用的、单一的终端用户登陆接口，通过实施单点登录功能，用户只需一次身份认证，就可以对所有被授权的应用系统进行访问，二次登陆时无需重复二次认证，提高信息系统的易用性、安全性、稳定性。简化用户的操作，保证同一用户在不同的应用系统中身份的一致性。 2、信息同步 实现 PC 端门户和移动端门户的信息共享和消息同步。 3、权限管理 支持对 PC 端和移动端门户权限的同步管理，权限分离管理，支持“分组织架构”权限管理，由指定组织的权限管理员分配所负责组织的权限管理。 4、消息中心 充分体现云计算、大数据的优越性，系统作为纽带，将各系统的多种消息进行统一汇总、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。	一般
		一门通晓-任务： 1、任务创建，输入任务标题、负责人、截止时间等信息快速创建任务 2、任务群，任务可直接建任务群沟通，任务新增成员可被自动拉入任务群 3、任务提醒，通过消息提醒通知相关人任务的进度变化 4、任务筛选，支持任务状态筛选、任务归属筛选、任务创建与截止时间筛选 5、任务动态，记录当前任务的操作动态，方便用户随时查看任务修改记录 6、任务重启，任务发起人可以将已完成的任务重新开启 7、子任务，支持添加子任务，子任务可支持无限级 8、任务架构树，展示整个任务的架构树，方便用户查看 9、任务搜索，任务可通过任务名称、发起人、创建人、参与人进行搜索 10、任务反馈，任务发起人、负责人、参与人都可以反馈任务，实时了解任务进展 11、任务催办，发	一般

		起人可催办任务负责人 为了实现以上任务，需要完成以下支撑服务： （1）工作提醒，实现相关业务系统工作提醒以及信息的集中展示。民警通过登录工作平台，就可以获取相关系统的提醒信息，各业务系统的提醒信息开放提醒接口，工作平台通过调用提醒接口获取民警提醒信息，为业务协作提供有效的帮助。（2）待办任务,警务工作门户是集中的、统一的入口，通过单点登录集成了各业务系统的功能，统一的待办任务服务，以服务的方式集成所有业务系统的待办任务，实现业务的协同。待办任务支持待办任务接入注册、待办任务接收、待办任务展示和待办处理等功能。 （3）通知公告，通知公告信息发布由信息拟稿、信息审核、信息发布、信息浏览功能组成。（4）个人画像,实现对民警个人信息的精确刻画，包含个人基本信息、个人系统使用信息、个人岗位职责、个人绩效考核、个人学习进度、个人数据贡献等信息。	
		一门通晓-工作日程： 输入日程名称、参与人、描述、结束时间、设置提醒等信息来创建日程；支持团队成员的日视图、月视图；查看日程详情时可以编辑日程、删除日程；支持搜索团队日程；日程详情上显示日程紧急程度、是否是私密日程、日程类型标签；日程参与者需要确认是否参与该日程；默认全员可见，可勾选仅参与人可见；用户可以在客户端设置关注我的日程联系人。 1、日程管理 （1）支持团队协作型日程工具日历共享、指派管理。（2）支持不同分组可管理查看不同日程安排。 （3）按选定时期，提供日程内容的展示。（4）安排指定日期的日程，可选择开启远程会议功能。 2、日程编辑 （1）支持安排日程时，可快速安排周期性重复的活动。（2）需支持安排活动时，可查看其他参与者的忙闲状态，但不能查看其具体的活动内容。（3）支持创建者可以在活动中预约视频线下会议室和设备，并可以查看会议室和设备的占用情况。 （4）需支持编辑已安排的日程，修改人员、时间、地点、备注等信息。 （5）支持取消已安排的日程。 （6）需支持复制一个	一般

		已安排的日程，带入参与人和资源，进行新日程的快速创建。 （7）支持可以将一个日程安排给指定的内部或外部联系人，并邀请他们参与活动。 （8）需支持系统将按照用户设置，在活动前提醒用户参与活动。 3、日程应用 （1）与手机日程应用同步，可以查看活动地点。 （2）与移动警务视频会议系统集成后，当安排了远程会议时，用户可以快速进入远程会议系统。 （3）支持可将本人的日程授权给他人进行管理和安排，应用于委托他人安排日程的场景。	
		一门通晓-搜索： 1、搜索人，可快速搜索组织下的具体成员，支持拼音搜索、英文名搜索、邮箱搜索、电话号码搜索、手机号码搜索。 2、搜索群，在桌面端或移动端可快速搜索群组。 3、搜索聊天记录，在桌面端或移动端可快速搜索聊天记录。 4、搜索应用，在桌面端或移动端可快速搜索应用，包括第三方业务系统。 5、历史搜索记录，将用户搜索的历史记录保存下来，方便用户下次搜索。	一般
		一门通晓-邮件感知： 对接邮件系统，当用户有新邮件时，给用户推送邮箱应用消息，方便用户查阅。	一般
		一门通晓-组织架构： 1、集群组织架构，可支持单云多组织、多云多组织的集群组织架构的展示 2、帐号管理，可添加、编辑、删除、停用组织成员的帐号 3、部门管理，可添加、删除、编辑组织中的部门，且支持部门排序 4、批量导入，可通过 excel 模板批量添加组织成员 5、域控同步，可通过域控同步实现组织架构的导入，目前支持单 DC、单域控、支持域控删除的帐号在后台停用不删除 6、角色权限管理，系统默认有云管理员、超级管理员、管理员、部门管理员、普通成员五种角色，用户可新增自定义角色及自定义权限。 7、导出组织架构，支持组织架构信息的导出 8、成员排序，可在后台调整成员在组织架构中显示的排序 9、一人多职，支持一个帐号在不同部门任职不同职位 10、分支隐藏，在组织架构中，可将本组织中的部门或成员隐藏起来，并可指定哪些成员才能看得到 11、组织	一般

		共享，在组织架构中，可将本组织中的部门或成员共享显示给其他组织；还可以设置本组织中的哪些部门或成员可以看到外部共享的组织 12、部门群，后台可快速创建部门群，当部门有成员添加或者删除时，部门群成员列表可自动同步 13、工作名片，组织架构的每个帐号都有工作名片，名片支持内部外部分享	
		一门通晓-组织个性化： 1、可对组织简称、logo、地址、官网进行快速设置； 2、管理员可在管理后台上传自定义图像； 2、管理员可自根据组织需求，自定义个人名片字段及排序； 3、可根据组织个性化的需求对 logo、名称等进行定制化设置。	一般
		一门通晓-组织群聊： 1、内部群，群聊范围限制在组织成员的群，组织人员离职会自动踢出群 2、群二维码，移动端可通过群二维码的方式添加群成员，满足线下当面加群的场景 3、群公告，群主或群管理员可在群里发送群公告，群公告会呈现独特的样式提醒群成员 4、群管理，群主可对群进行管理，包括入群验证开关、群新晋成员是否查看历史聊天记录、群管理员设定、群转让、解散群等 5、群聊天文件自动归档，针对群聊中出现的图片、文件消息进行自动归档，方便使用者查阅 6、群文件共享，每个群都有共享空间，方便群成员进行文件互相分享 7、群置顶，群会话可通过打开置顶开关，置顶在会话列表顶部	一般
		一门通晓-沟通升级： 1、消息阅读状态，消息可显示阅读状态：已读或未读 2、在线状态，随时随地了解接收方是否在线，以便于消息发送成功后得到及时反馈，支持移动端和 PC 端 3、消息云储存，消息采用云端存储的方式保存在用户服务器 4、消息草稿，用户未发送的消息，客户端保持草稿并提示 5、语音备注，语音消息可以备注自定义文本 6、@功能 组织群聊中，可@所有人、@单人、@多人（支持一次多选），消息通知不受消息免打扰影响 6、消息强通知，在普通消息和@消息的基础上，用更强烈的方式提示消息接收方，缩短信息反馈的速度；并可有短信落地 7、URL 卡片，自动识别 URL，用户可在聊天界面选择	一般

		以卡片的形式发送并展示 8、自动识别电话、邮箱，移动端可自动识别电话、邮箱，可直接调起系统邮件、拨打电话 9、消息引用，可引用他人消息内容进行发送，引用会自动带上发送人姓名和消息内容 10、消息撤回，2 分钟内自己发送的消息，可以进行消息撤回 11、消息撤回重新编辑，消息撤回支持增加重新编辑 12、消息收藏，可对喜欢或关注的消息进行收藏，客户端会有统一页面查看所有收藏信息，收藏可转发 12、截图，PC 客户端快捷按钮截取用户自定义的区域作为图片，并可对截图进行标注 13、远程协助，PC 端可远程控制其他电脑，方便用户异地协助 14、语音会议，支持 9 人同时语音通话，异地沟通轻松满足	
		一门通晓-短信： PC 端可通过对接短信应用对组织内外人员发送短信。	一般
		一门通晓-基础沟通： 客户端支持文字消息的收发；支持 90 秒长语音收发，播放支持暂停、拖拽；支持表情的收发；单人聊天和群聊天消息支持收发图片；客户端单人聊天和群聊天消息支持收发 3 分钟视频；客户端支持录制 30 秒短视频发送。	一般
		一门通晓-组织数据： 1、用户操作行为统计，可查询成员发送信息、登录、加入群聊、退出群聊等相关操作； 2、组织运营数据，可对组织成员登录率、消息数、在线时长、功能使用数、应用使用数等进行统计分析。	一般
		一门通晓-组织安全： 1、数字水印，管理员可在后台针对组织架构、名片、聊天界面开启或关闭安全水印； 2、混合加密算法，采用端到端的混合加密机制，同时使用了对称加密与非对称加密两种加密方式； 3、支持国密算法； 4、远程设备数据擦除，管理员可在后台针对任何一个帐号的移动设备进行远程数据擦除，保护敏感信息； 5、消息审计，可对员工的聊天记录进行消息（文字、图片、文件）审计； 6、文件不落地，开启后客户端传输的文件不可以被下载，只支持在线预览。关闭时，文件发起者可选择是否让文件只预览不被下	一般

		载； 7、预览水印，文件不落地的情况下，可开启预览水印开关，所有预览的文件会有水印保护； 8、敏感词监控，通过系统监控的方式对用户发送的消息进行敏感词过滤；保证互联互通环境信息传输的安全与纯净； 9、审计平台双密码，审计平台登录场景采用“登录密码+核准密码”双密码控制，双重保护消息审计安全； 10、截屏监控，在 APP 使用状态下，可记录用户对于 APP 页面的截屏操作，并将截屏图片汇总至审计平台； 11、群后台管理，可在管理后台针对组织内的所有群进行解散、变更群主的操作，支持搜索、排序、批量解散和自动解散。 12、指纹手势解锁，用户在设置界面开启指纹或手势解锁功能后，唤起 APP 时需要用户指纹或手势解锁。	
		一门通晓-互联互通： 1、跨组织沟通，支持单云下和多云下组织与组织之间的组织架构共享及沟通； 2、对外联系人验证机制，添加联系人时，需要对方验证后才能生效； 3、陌生人会话权限，隐私设置中增加陌生人会话开关权限，根据个人需求决定是否开启，避免陌生人骚扰； 4、名片字段管理，支持对内外的名片字段显示管控，设置哪些字段对外展示，哪些字段对内展示。	一般
		一门通晓-应用管理： 添加/移除应用，用户可选择性将应用通过应用商店添加至应用中心，也可移除应用中心不需要的应用，方便用户筛选、过滤所需应用；常用应用设置，用户可将应用设置在常用区域，方便用户快速进入；可选打开应用浏览器，打开第三方应用系统可控制打开浏览器；唤起 Native 应用，应用中心支持唤起 Native 应用；浏览器 IE 内核，PC 端打开第三方应用系统支持用 IE 内核打开。 1、用户机构管理 对用户、机构进行统一管理，并提供统一对外服务，负责用户机构的新增、修改、删除维护。 2、布局配置管理 对门户页面布局进行个性化设置管理，提供模板模型支撑，支持门户页面千人千面自定义布局。 3、权限管理 对门户模板、布局、工具等进行统一的权限管理。 4、运行管理 支持门户运行监控功能，对门户及门户接入应	一般

		用运行、故障情况进行统一监管。 5、日志管理 支持认证日志管理，实现用户认证行为的记录、查询。支持令牌日志管理，实现用户令牌、应用令牌验证行为的记录、查询。支持维护日志管理，实现管理员日常维护操作的记录、查询。 6、应用接入 实现用户域应用、数据域应用和移动警务不同应用之间的接入管理，按照标准的接入规范流程进行应用接入，并实现不同应用之间的标签化标识。 7、模块订阅 实现门户工作台首页的自定义订阅。 8、国产化适配 基于信创的要求，开展内网警务工作门户适配国产浏览器、国产中间件和国产数据库工作，包括页面适配调整、接口规范适配调整、应用组件适配调整等内容。 9、应用场景建设 围绕“人、地、事、物、组织”数据动态变化、风险预警等应用场景，实现“一标Ｎ实”数据按照区域、时间、部门等多维度可视化分析，统一归集到门户一体化工作桌面，满足并不限于基层基础工作对信息个性化定制、情报精准化推送的实战需求。	
		一门通办-通用微服务支撑： 建设业务协同服务大厅，打造协同服务应用中心，各警种业务系统通过服务大厅注册应用服务，协同服务应用中心统一管理，并统一对外提供服务，跨地市、跨警种业务服务调用依托协同服务应用中心完成。 1、服务大厅 （1）服务目录 梳理整合警种应用服务，整合注册进来的应用服务形成服务目录。 （2）服务详情 实现对服务详细信息的展示。 （3）管理控制台 把业务服务配置进服务大厅，为服务设置分类，并为不同的角色配置服务的访问权限，用户只需登录服务大厅，就能快速找到自己所需要的服务，无需再在各个系统之间进行繁琐的切换查找。用户可通过智能检索（支持首字母搜索、模糊搜索），快速查找所需服务；首页也可以显示近期热门申请服务，方便用户查找。 2、智能服务接入 （1）服务注册 各部门提供业务协同的基本情况和服务规约，基本情况包括业务系统情况、所属部门、数据内容、数据描述、数据密级、请求地址等相关信息，服务规约包括开发协议、服务规约描述、请求参数、	一般

		结果参数、共享数据项集等相关信息。 （2）服务发布 部门进行业务协同服务注册审核通过后，业务协同服务正式发布，对外提供开放使用。 （3）服务调用 实现对应用服务接口的调用。 3、智能服务开发 支持智能应用服务的开发指引、提供开发示例并进行 API 联调。 4、智能服务管理 （1）生命周期管理 实现对服务注册、发布、调用、关闭全生命周期的管理。 （2）服务监控 通过获取运行的服务实例来获取相应的服务状态，实时的了解服务的运行情况。服务状态监控包括运行的服务（状态包括：停用和启用），通过日志和异常日志来监控实际的吞吐量和异常率。	
		一门通办-知识中心支撑： 知识库构建，提供能支撑特定业务知识图谱构建的部分工具或完整的工具套件，套件需要包括完整的数据预处理、知识建模、知识抽取、知识融合、实体对齐等知识图谱构建工具。提取人、案、事、地、物、组织、证据、法规等要素对象，为服务社区警务办理、警情处置、案件侦查、执法办案等业务，构建知识图谱等形式的知识库。知识管理，主要包括知识目录管理、知识存储管理、知识上传共享、知识下载调用、知识更新等。知识服务，基于知识中心提供的业务知识图谱等知识能力，通过接口提供智能检索、智能预测、智能推理、智能问答推荐、关系分析、知识可视化等智能服务。实现图片、文字形式的经验交流和分享，提供交流渠道、评论反馈、搜索、置顶、热门、收藏等功能。可视化展示经验分享图文排版情况，并对用户分享经验和交流进行审核。打通民警与民警、民警与系统开发商、民警与领导之间信息传达交流和问题反馈的渠道，实现基层用户对系统问题、系统建议、心得交流等不同问题的多交流通道。 1、办事类需求归集 实现省市两级办事类需求的归集，支持民警常办、办事类事项的需求整理。 2、办事流程梳理 实现办事类事项的流程梳理、需提供材料整理，形成办事流程指引。 3、办事类接口对接 实现与省市、各警种部门办事类事项的接口对接。 4、线上办理 实现办事类事项的线上办理。 5、	一般

		办事后评价 实现对办事事项的事后评价，并整合对办事事项评价进行统计分析。	
		一门通办-微服务管理支撑： 微服务应用管理支撑，包括生命周期管理、应用限流、操作日志、服务治理（含服务限流、降级配置、服务熔断）、服务目录、接口服务、服务路由、访问控制、版本发布策略、应用编排等。镜像管理支撑，包括镜像仓库、镜像注册、镜像下载、镜像更新、镜像版本控制等。监控管理支撑，包括性能监控、应用监控、自定义指标监控、服务调用链跟踪、异常告警等。日志审计支撑，依托日志管理基础微服务组件，提供日志收集、日志分析、日志展示等功能，实现日志审计。	一般
		一门通办-API 网关支撑： 开发部署支撑，API 网关支撑“一门四通”微服务方式开发部署，面向开发者提供实现微服务架构的相关支撑，包括访问鉴权、应用授权、安全防护、服务注册、服务路由、API 调试、协议转换、数据转换、生命周期管理、负载均衡、服务监控、健康检测和 API 服务市场等。安全支撑保障，API 网关应具备高度的安全性、稳定性和可用性，能够以 API 方式开放基础组件微服务、通用业务组件微服务等服务能力，支撑应用功能组件的复用。API 网关依托公安云平台实现。	一般
		一门通办-系统对接支撑： 1、遵照国务院办公厅关于实现公安机关开具《无犯罪记录证明》“跨省通办”的政策要求，设计并建设《无犯罪记录证明》跨省通办功能，支撑全省无犯罪证明开具业务。 2、依据公安部警综资源数据汇聚要求对警种数据进行汇聚，对汇聚的警综资源数据进行规范和治理，保障警综资源汇聚的数量和数据质量。实现警综资源数据的对外共享，为警种业务系统提供数据服务支撑。基于业务数据实现数据的全方位展示和管理，主要包括全局展板管理、业务模块展板管理、自定义展板管理以及数据展板接入管理。3、服务支撑内容包括但不限于：数据汇集分发支撑，提供数据汇集的专用通道，支撑业务数据的向上汇集、向下分发。业务联动协同支	一般

		撑，遵循公安资源服务总线标准，支撑跨部门、跨层级、跨地区的业务联动协同。联动协同管理支撑，包括服务标准管理、联动监控和联动协同目录管理。联动协同节点支撑，包括联动网关、认证中心、节点管理、数据校验、权限管理和访问控制。（1）服务对接支撑 通过数据资源服务总线挂接的服务方，对接数据查询、信息核查、数据比对、数据交换和其它数据处理服务，实现数据的核查、比对、查询和复用功能。（2）消息对接支撑 能够接入相关业务系统的通知、公告、待办、预警、问题反馈、异常和其它消息，实现消息驱动、待办提醒和集中展示。（3）数据对接支撑 基于数据库数据传输服务、ETL 抽取工具、实时数据推送、数据交换服务等方式，实现系统间的数据传输和共享。（4）页面融合支撑 对于暂时无法上云且不能微服务化改造的业务系统，可通过解析页面内容和后台接口等方式，将相关页面元素与“一门四通”操作界面融合对接。	
		一门通办-智能服务开放支撑：（1）智能服务接入 实现服务提供商、应用的注册、审核。基于统一的服务接入标准和规范，提供更新服务目录、服务发布和服务调用管理功能。（2）智能服务管理 对服务的注册、审核、修改、发布、下架、删除等全生命周期进行管理。支持对服务调用过程的监测，可视化的展示服务的实时调用情况，生成服务统计报表。从应用效果、稳定性、性能等方面对服务进行全方面的评价。（3）智能服务开发 按照统一的服务开发要求和接口规范，提供服务的 API 接口使用文档、SDK 下载等开发指引，提供高频功能、典型场景等开发示例，提供测试测试接口、测试数据、测试用例、测试联调等支撑。（4）智能管理支撑 基于“一门四通”服务架构支撑业务应用与智能服务的融合调用和已有模块智能服务赋能改造，通过 API 网关实现智能服务的能力开放。提供多维身份认证、统一权限管理等支撑，提供故障检测、自动恢复等服务保障能力。（5）权限管理 实现不同业务办理权限的归集，实现对权限的	一般

		分级和分类管理。 （6）权限共享 支持权限自助申请，支持普通用户进行自助开通、变更、撤销等申请操作，跟踪权限审批过程。支持与审批服务进行对接，支持审批过程的跟踪与查询。支持提供前置页面，并且将此应用注册到资源目录中。支持与认证服务进行对接，完成应用级鉴权过程。 （7）异常鉴权预警 支持短时间频繁鉴权预警、持续越权访问预警、异常 IP 鉴权预警、异常时间鉴权预警，将预警信息进行统计分析并进行展示。 支持异常鉴权预警和风险处理，管理员发现异常情况时，可采取对应的措施对异常鉴权预警和风险数据进行相应处理，包含将权限进行周期性冻结，或者直接撤销掉权限。	
		一门通办-业务联动协同支撑： （1）数据汇集分发支撑 提供数据汇集的专用通道，支撑业务数据的向上汇集、向下分发。 （2）业务联动协同支撑 遵循公安资源服务总线标准，支撑跨部门、跨层级、跨地区的业务联动协同。 （3）联动协同管理支撑 包括服务标准管理、联动监控和联动协同目录管理。 （4）联动协同节点支撑 包括联动网关、认证中心、节点管理、数据校验、权限管理和访问控制。	一般
		一门通查-查询检索： 对大数据平台整合的数据、服务实现一站式检索，提供统一全文检索服务功能，可根据输入的检索条件，检索出所有满足条件的数据条目，速度达到千亿级数据查询秒级响应。建设超级搜索框，聚合部、省、市、县（区）众多的搜索引擎，实现一次输入，一站式鉴权，多次搜索，结果一个出口。支持检索词纠错能力，当用户输入错别字时给出正确的检索词提醒。支持检索提示，在输入检索关键词时提供相近词、同音词等提醒功能，基于动态输入提醒，辅助用户选择合适的搜索词。 提供检索结果排序、热门检索关键词、检索结果导出、检索语法提供、检索信息提示、检索历史展示、检索帮助、检索结果关联以及系统 UI 设计等能力，实现对检索整体功能体验的提升。支持结果根据人员、物品、案事件、地址、组织等维度进行分类展	一般

		现。支持对检索结果按信息类别、地域、时间等条件进行筛选和二次检索。支持按列表查看检索结果和视图查看结果，支持切换展示样式。支持提供检索结果的命中条数展示、统计等，支持查看检索结果详情页面等功能。支持检索结果导出，提供批量 Excel 导出功能，可以导出展示的当前页数据，也可以按分页导出检索的所有结果集数据。支持通过词库管理功能对搜索词库进行管理，包括功能词汇发现、热词管理、拼音词管理、百姓体词管理、敏感词管理。支持对功能词、热词、拼音、百姓体、敏感词进行浏览、导入、修改、删除等管理。对标电脑端“一门通查”功能，实现移动端同步无差异性应用，支持对接语音识别接口，实现语音搜索。 1、关键字检索。支持输入汉字、数字、字母等任意关键词进行精准、模糊检索，支持多种关键词的混合查询，根据业务需要选择要检索的范围，选择某类信息，比如：人员、车辆、案件等进行关键词检索。 2、范围检索。支持范围检索，可选择特定范围的数据资源进行特定范围的数据检索，支持用户自定义勾选需要检索的范围数据进行范围检索。 3、组合检索。实现任意组合多个筛选条件进行组合检索。 4、地理检索。对接应用 PGIS 地图，基于地图指定时间范围和空间范围，任意选择需要检索的资源（可以选择某类，也可以选择多类资源中的部分资源），然后在选择的时间、空间和资源范围内进行检索。 5、高级检索。支持数据资源属性自定义配置的检索查询，可以基于关联检索配置信息表对检索结果进行关联检索，支持检索结果属性聚类、维度下钻统计挖掘。 支持逻辑运算组合检索、通配符检索、姓名同音、模糊音检索、身份证号转换检索、时间段检索、年龄段检索等。 6、图像检索。通过对接省厅已有的图像检索服务，实现系统的图像检索功能。通过对上传包含人脸的图片，进行智能化人脸识别比对，实现身份落地查询的检索方式，以达到让用户快速实现对线索图片的身份确认。 7、文本检索。支持对文本搜索内容中语义内容的识别，实现对公民身份号码、车牌号码、	

		手机号码、案件编号、警情编号、航班号、车次号、酒店实体、网吧实体、机场实体、车站实体等内容的识别。 8、标签专搜。实现对各类对象的标签式快速查询检索。	
		一门通查-批量检索： 支持通过点击上传导入或拖拽 excel 表格、TXT 文本、DOC 文档进行识别，实现以文件形式的查询方式，自动从文件中提取批量检索要素，对档案资源、关系资源、轨迹资源等执行批量检索。 当批量检索身份证号、手机号等代表人员唯一信息时，可以直接以 word 方式导出被批量检索人员的档案，包括人员基本信息，同住人员、同行人员、亲密度等排行信息。 提供对两个或多个区域内，数据碰撞分析功能，发现其中隐藏的共同线索。支持对接 PGIS 平台，支持通过数据关联展示目标基本信息。 提供支撑海量数据的知识图谱，基于图谱中人、地、物的属性、关联信息自动进行数据筛选分析，支持以搜索或标签筛选方式从大量信息内容中快速获取所需内容。并进行基于标签和要素标识的多种数据类型的碰撞比对，从而起到全链管理的效果。 数据筛选分析：提供对知识图谱中实体的多维属性联合筛选比对，根据搜索条件和筛选条件智能判断相似度，并根据相似度返回筛选结果。 数据碰撞比对：提供基于知识图谱的多实体碰撞比对，实现多种实体的多级关系碰撞比对，从而发现满足碰撞关系范围内的目标实体。 信息比对服务是根据输入的批量资源信息，在已有数据资源范围内开展确定维度的信息查询和展示业务。可实现 100 万以内的关注人员姓名、身份证号信息与省厅、各地市动态数据（日增量数据）的定时比对，并定时将比对结果反馈给任务发起者。	一般
		一门通查-关系分析： 建设关系亲密度计算模型，结合资源库的亲属关系、同行（各种人员轨迹数据，包括手机轨迹数据、人脸轨迹数据、车辆轨迹数据、火车轨迹数据、飞行轨迹数据等）、同住、同案等关联数据，按设定的规则自动分类计算人员关系亲密度，排名优先的关系人展示在最前排或着重显示。 实现同户人、历史同户人，同地址，民航（铁路）同	一般

		订票、同换票、同乘，网吧同行，住宿同行，同出入境，同案分析，同监所分析，公路客运同行分析，同车违章分析，同服务处所分析，多人关系分析，多同关系小贴士，关系人综合分析等功能。 1、人员关系分析 提供基于单个线索值，以及多个线索值之间的人员关系扩线分析功能； 支持根据人员身份证号进行关系分析，并以图形化展示人与人之间的关系，人员节点位置可拖拽自定义摆放； 人员关系分析支持多种方式，包括：同户、同行、同住、同单位、同行、同上网、同学、同交通违章、同案、通联等； 支持查看人员关系形成的数据详情，以及各节点人员基本信息； 支持对两人之间最短关系路径的醒目展示，或对关系层级进行范围筛选； 人员关系分析图支持树形、环形等多种自动排列功能；支持对关系分析图的保存、修改、删除、发送。 2、要素关系分析 提供对人员与房屋、单位、车辆等要素的关系分析展示功能。 支持根据人员身份证号信息进行关系分析，并以图形化展示人员与要素之间的关系，各节点位置可拖拽自定义摆放。 支持查看形成人员、要素关系的数据详情，以及各节点基本信息。 支持对关系要素的扩线，实现人员间关系通过此要素的二次关系分析。 支持关注要素节点设置，实现以此节点为中心，展示上下各一级人员关系信息。 支持对扩线产生的人员节点发起人员关系分析。 关系分析图支持树形、环形等多种自排列功能。 支持关系分析图的保存、修改、删除等。 3、伴随分析 （1）人人伴随 基于人像、电围等数据，提供人与人的伴随发现分析功能。 支持根据人像、身份证号，对时间段内，与目标人员同时出现的人员进行分析，分析结果以伴随频次进行排名展示，并能够通过数据关联展示人员信息。 （2）手机伴随 提供基于手机号、IMEI、IMSI 的手机伴随发现分析功能。 支持根据手机号、IMEI、IMSI 三类线索值，进行伴随分析，能够通过线索值，对时间段内，与其同时出现的线索信息进行分析，分析结果以伴随频次进行排名展示，并能够通过数据关联展示线索的人员信	

		息。 （3）人车伴随 提供基于车牌号，人员、车辆的伴随发现分析功能，根据伴随分析的线索值类型不同，分为以人找车、以车找人两种类型。 支持根据手机信息、车辆信息，发起伴随分析，通过卡口设备与电围设备的关联配对设置，实现分析数据时间段内，伴随出现达到要求频次的线索信息，并能够通过数据关联展示线索的人员信息、车辆信息、机动车所有人信息。（4）活动规律分析 基于对目标线索日常活动轨迹的汇总归并，实现其活动规律展示，并对下时段出现位置进行概率推算。 支持对目标出现位置频次、时段热点位置，以图表的形式进行统计排名，并对下时段出现位置进行百分比展示。 支持通过数据关联展示目标基本信息。	
		一门通查-轨迹分析： 1、轨迹查询 提供对人、地、事、物、组织等要素轨迹信息查询以及活动轨迹的动态展示功能，支持轨迹点位的信息展示、目标基本信息查看；对接 PGIS 地图，实现普通地图、卫星图等多种样式切换功能。 2、点位分析 提供对目标位置进行区域范围设置，对其周边半径范围内各类要素分布进行展示，包括房屋、单位、人员、设备，并对不同类型要素进行图标差异化标识，提供对详细数据的调用功能；支持标注半径范围内的要素进行分类统计。 3、轨迹找人 在电子地图上进行活动轨迹绘制，并在指定时间段内对绘制轨迹周边人员信息进行展示，通过身份证号或手机号进行筛选。	一般
		一门通查-云家谱： 基于关系挖掘能力，构建云家谱分析功能。通过对户籍人口、户籍人员变动、婚姻登记等数据进行治理，支持根据父系关系、母系关系、同一地址关系、三代以内关系等多种限定条件筛选出不同层级的血缘关系，并通过可视工具清晰地展现血缘关系图谱。方便民警结合技战法工具对**人员进行“以亲属找人，以家找人”。具体支持姓氏分布、年龄分布、人口迁移情况、家族图谱等功能。	一般
		一门通查-个人电子档案： 建立“一人一档、一车一档、一案一档、一址一档、一企一档、	一般

		一址一档、一房一档”，并相互打通，打造可以实现信息无限关联的信息圈。 1、一人一档 人员电子档案包括个人基本信息、社会信息、个人互联网信息、个人活动轨迹信息展现、关系人信息、人脸数据和人员综合时空分析展现，从而刻画出该人的信息。电子档案支持多种展现方式：同一电子档案中支持图片、表格、关联图、时间轴、饼图、柱状图、折线图、色温图、关联图标、网吧同行分析图、宾馆住宿分析图、火车座位图和飞机座位图等多种展现方式。 2、一车一档 实现对各种车辆活动的动态管控，以“一车一档”的方式集中展现车辆动态管控过程中的信息展现，包括车辆的基本信息、卡口信息、违章信息、所属人等信息，可以清楚地反映了车辆分析研判和关注管理的全过程，达到“以车管人”的目的。主要内容包括基本信息、出行轨迹、违章信息等功能。 3、一案一档 案件档案包括案件信息关联汇总、案件统计信息、阶段案件信息统计、案件简要信息、嫌疑人基本信息、案件涉及的公民身份证号、案件涉及的人名、案件涉及的通讯号码、案件涉及的车牌号、案件涉及的银行卡号、案件涉及的 QQ 号等。 4、一址一档 基于公安“一标三实”等相关标准地址数据，以标准地址库为基础，构建标准地址档案，围绕地址为核心，整合该地址相关的人、地、事、物、组织等相关信息等。包括地址基础信息和关联信息等内容。 5、一企一档 为每一个目标企业进行多维度画像，从基础信息、工商数据、企业涉案数据、关系人员信息、互联网信息等方面进行详细分析。立体式展现企业所属行业、经营情况、上下游关系等内容。 以上电子档案服务都可以通过 API 的方式对外提供服务。 6、一机一档 通过手机全息档案手机概览模块，系统支持将手机号基本信息、机主信息、使用人信息、物品关联信息、落脚点信息、通联规律信息、关系分析信息、活动区域信息、行为分析信息、话单分析信息进行集中式展示，便于用户对手机的重点概要信息进行便捷掌握和研判。 7、一房一档 住宅全息档案功能旨在为警务人员提供全维度	

		房屋信息描述，提供信息内容涵盖公安关注的人、地、物、事等多维度，通过房屋全息档案功能，能够帮助民警快速了解房屋住户、周边环境、关联的案事件、车辆、物流快递等信息。房屋全息档案模块主要功能包括：房屋概览信息、登记信息、关联案事件信息、门禁出入信息、车辆、物流信息等。	
		一门通查-智能个人中心： 实现用户的历史记录、使用统计情况、个人关注详情、经验交流、最新消息通知、我的检索、经验交流、最新动态、在线用户、背景标引、水印显示等功能。（1）历史记录：保存近期的检索记录，方便查看工作历史。 （2）使用统计：以图表形式统计用户近期的系统使用情况，并进行同比/环比的比较分析。 （3）个人关注详情：记录用户的个人关注情况，包括关注中，和已取消的关注，支持关注人员的取消关注和已取消关注人员的再次关注。 （4）经验交流：可以查看其它用户提交的问题和答复信息，用户也可以提交问题、回答问题。 （5）最新消息通知：包括关注人员的最新消息提醒和系统的广播消息通知等。 （6）最新动态：展示系统数据资源增加、更新情况，展示系统功能更新情况。 （7）在线用户：在线用户信息显示用户姓名、登录时间、所属组织机构等信息，支持根据姓名查找系统注册用户，管理员用户支持用户角色筛选功能。（8）背景标引：将违法犯罪、在逃、涉枪、涉爆、吸毒等背景标签添加到人员信息中进行展示。（9）水印显示：为了防止用户随意泄露系统数据，在检索结果列表页、细览页等界面都添加背景水印，水印内容是当前用户的身份证号和姓名。（10）我的收藏：系统支持结果收藏，用户可以将原始资料、档案、图片等结果集存储，作为再次分析的数据来源，可查看当前用户所有收藏的结果集。并支持用户对结果集进行碰撞比对分析。 （11）帮助：支持当前用户下载功能帮助手册，方便用户了解各功能点使用方法。 大屏可视化。围绕“一门通查”数据资源、应用情况、服务共享情况、资源运行情况、安全风险评估等内容，建设大屏可视化相	一般

		关功能，实现“一屏观全局”。	
		一门通查-数据资源管理： 按照公安部相关标准规范，开展数据资源接入、处理、组织、共享和管理，建设相关的数据按照相关标准具有反哺第三方应用的能力。 1、数据源接入适配 为满足数据接入索引库，支持适配不同来源数据，包括支持适配连接 ORACLE、Mysql、Greenplum、PostgreSQL、达梦数据库、Hive 等主流数据仓库。 2、数据资源接入 支持从不同数据源读取数据。支持创建、修改、删除数据接入作业。 3、数据资源处理 对各类需要接入索引库的数据资源按照业务需求进行转换、整合、标引、冗余，完成数据索引化。 4、数据接入调度 根据各类数据资源对实时性的要求不同，支持对数据接入作业进行接入策略设置及启停调度。 5、索引库建库 根据不同数据来源及结构，构建索引库实例及表结构，包括根据集群及服务器内存情况设置实例数、分片、副本、刷新时间、日志写入方式、自动拆分索引等参数及索引表结构创建。 6、数据资源分发 经过索引化处理的数据进行分发、入库存储，形成完整的索引库。 7、API 接口服务 针对已建设完成的全文索引库，构建全文索引服务接口，对上层应用提供全文索引库中各类数据资源的检索 API 接口。包括：各类资源的简项检索 api、详细项检索 api、资源目录 api、分类统计 api、命中数量 api、全文检索 api 等。	一般
		一门通查-后台管理： 管理模块需要支持各种常用的关系数据源，支持可视化配置数据模型，提供应用模型管理能力，完成检索资源的注册和管理功能，并进行统一身份认证管理。支持系统后台管理各项能力，形成组织机构、用户和角色、权限等管理功能。 1、数据源管理 支持各种常用的关系数据源，同时也支持 Hadoop Hbase、MPP 等大数据架构的数据库类型。 2、数据模型管理 支持可视化配置数据模型，包括查询的脚本、查询条件、数据项等，查询条件和结果，可以支持模板定义。支持数据模型依赖纳入连接的数据源，同时支持依赖分层解耦提供的 api 接口作为数据来源。	一般

		3、应用模型管理 为满足系统管理员配置业务分析模型来配置资源通用应用需要，支持应用模型配置功能，系统提供可视化的配置工具，通过可视化点击等操作，配置应用模型所依赖的数据模型、查询分析条件、输出项等。 4、检索资源注册 系统支持对底层提供的检索库表或 api 接口进行模型化配置，封装成成熟的检索服务。支持将检索服务资源在线注册，注册的内容包括资源基本信息、访问敏感等级、业务分类、更新频率、数据关联关系，数据项的引用标准、代码、日期格式、访问敏感等级等。通过规范化的资源注册采集元数据信息，包括数据的技术属性、业务属性、管理属性等等。资源在注册之后，可在搜索系统提供数据服务。 5、检索资源管理 支持对注册的检索资源的注册情况进行编辑、删除，对不同的角色进行访问授权控制。	
		一门通查-管理模块： 1、统一认证 用户或角色必须通过统一用户身份的认证（登录）和用户的授权，并根据用户的权限，对用户的功能权限进行控制。 2、用户管理、角色权限管理 对接统一用户服务，提供用户信息管理功能，管理员可方便的增加、查看、编辑和删除记录的用户，还可以更改用户角色。 支持针对系统账号权限的管理，包含角色新增、编辑、删除管理、权限映射、角色缓存管理、申请权限列表等模块。 支持用户分权限级分类管理，根据用户登录情况支持动态调整，按需分配。 3、组织机构管理 对接统一组织机构服务，支持组织机构的新增、编辑和删除等，并在平台进行展现。	一般
		一门通查-安全运维运营： 遵循国家信息安全等级保护相关规范以及国家保密管理和密码管理的有关要求，建立健全“公安网+数据服务”安全保障体系。按照信息系统安全等级保护要求构建数据存储环境、应用系统环境、运行管理机制，确保数据安全和公民个人数据合法应用。安全保障体系要与应用系统同步建设，对所建安全保障体系要进行重点保护、实施动态调整。提供的软件产品需具备防止网页被篡改的能力、防止系统数据被盗取等防止黑	一般

		客攻击的能力，并提供详细的技术安全防护架构说明，保证系统安全。	
		一门通查-外部接口： 对接部、省、市、县（区）公安部门、大数据局等政府部门，以及社会企业建设的查询服务接口，实现相关资源的检索请求，检索结果集成到“一门通查”界面中。 按照微服务架构建设“一门通查”，具有分层解耦能力，支持以 API 接口的形式发布并应用到大数据平台，为其他的业务系统提供标准的接口和服务。包括但不限于根据业务场景构建的基础检索、轨迹类服务、档案类服务、关系类服务以 API 的形式注册到服务总线，供其他平台调用。	一般
		一门通考-考评： 通过汇聚信息系统的运行日志、用户应用日志、授权用户清单、业务数据、民警的主观评价等要素，建设全省应用系统评价指标体系，经模型分析、数理统计，可视化展现该信息系统的应用活力，实现对信息系统建设的评价结果。通过统计民警登录使用信息系统的次数、核心业务功能模块的应用次数，以及民警在信息化系统应用评价、功能优化、成果分享、实战技巧等方面提出的“金点子”意见建议的数质量，对民警的信息化实战应用进行全面刻画，客观反映民警的信息化应用活跃度和实战能力。通过对基础信息采集工作，设置评价指标，包括但不限于关键业务数据增长率、完整率、规范率等基础评价指标，**人员管控和案件侦破等专项工作的贡献率指标，以及关键业务数据缺失率和错误率扣分指标，实现对基础信息采集工作的考评。设计建设全省公安信息化综合水平评估功能模块，支撑全省公安信息化综合评估。投标方案中要提供对应用系统评价、民警应用能力评价、基础信息采集评价和全省公安信息化水平综合评估设计方案。 1、考评内容目录化，实现考核内容目录化，支持按照目录进行浏览、查询、统计等应用。 2、考核结果可视化，支持按照单位、个人、条线业务等条件，按照日、周、月、季度、半年、年的维度，以图表等方式实现考评结果的可视化。 3、配置业务流程模式，建设系统业务流程模型，支持根据自身业	一般

		务特点认定相应的业务模型。 4、考核关系设置，在系统中设置针对不同岗位人员的不同的考核关系，可自动取得组织结构中的岗位、职位等级，也可根据考核中的自身应用，重新设置。 5、考评维度设置，考核系统中评价人员的评价维度，不同类型的人员可设置不同的考核维度。 6、评分方式，针对绩效评价中使用的评分方式进行设置，支持众多常用的评分方式，并可根据企业自身的实际情况，配置个性化的评分方式。 7、权限方案，满足多样化的权限控制方案，支持针对不同人员，不同考核周期及不同考核类型的不同权限功能。 8、考核周期，支持不同的考核周期，并且不同的考核项目考核周期均不相同。 9、指标体系设置，持将考评所需要的考评指标在系统中存储，以便重复引用；支持指标进行分类管理，针对不同人员、不同类型、不同考核中进行应用。具体功能包括设置考核指标维度、设置具体指标、设置不同的分类、制定不同的考核分类、制定考核方案、确定分配规则等。 10、量化考核，支持与其他业务模块实现数据集成，而且对来自于其他系统的数据提供多种方式进入系统参与绩效评价，包括 EXCEL 导入、数据集成方案等等。 11、量化考核流程，"业务数据抽取：系统可根据相应的考核周期、指标，提取相应的考核数据，保证绩效评价的公平、公正。 12、目标分解：目标层层分解，落实到人，使目标切实可行 13、目标更改：如果突发性、不可抗拒原因，可对目标进行适当调整，以达到最好的激励效果。 14、流程处置，参与考评的人员，可直接在系统中参与打分；系统自动批量计算绩效评价结果，系统计算后获得绩效评价结果排名，如对绩效考评结果有疑义，可启用变更审计流程；系统支持员工对绩效结果进行审诉业务处理；系统支持对全业务流程的进程查看。 15、绩效评估，绩效评估可自动获取服务系统或者其他业务数据，可通过平台通用的函数、SQL 语句设定取数规则，同样 EXCEL 数据可自动导入系统中，参与计算，以便保证绩效评价的真实有效。 16、统计分析，统计分析提供有关绩	

		效评价的查询统计和分析报表，可由用户来使用 BI 工具提供的报表、图表、多维分析等工具进行，也可查看系统中所设置的绩效结果报表。 17、在线调查与评估。系统管理员可以发布调查问卷，调查问卷可以同时发布多条信息，管理员发布了问卷之后，问卷选择的参与人员，可以看到该问卷，并对问卷进行作答，后台应设有多种分析方式。 18、实现对全省典型应用案例、联合创新课题等评选活动的全流程信息化支撑，功能包括但不限于材料上报、过程评选、结果公示、统计分析和系统管理等功能。	
		一门通考-在线学习： 1、上岗认证、能力提升培训，支持在线创建学习地图，能自动推送课程认证课程，并根据在岗时间或测评成绩开启能力提升培训地图。 2、专项必修课，结合新应用上线、专项能力提升培训项目，支持按岗位下发学习课程，终端进行线上学习、学习完成后自动推送考试及满意度测评，学习期间民警可进行课程内容提问与讨论互动。 3、自选课题，民警可根据自身岗位条件，在线选择课程库中的内容进行学习，并可同时进行作业、课程自测、笔记、查阅课程相关资料和查看同学、教师等信息。 4、组建班级，管理后台能够实现“拉群派送课程” 或者“组建专班”开展线上培训功能； 5、防挂机设置，需要用技术手段防止挂机学习。 6、在线学习的测试，在线学习应具备学习前测试、学习中单元测试、学习完成结业测试三项测试功能，且均能按题目类型、按题型导出进行线上或线下分析，以获得学习者的基本能力素养。考试完成后民警可查看自己的试卷，订正题目，查询错题正确答案。 7、移动终端在线学习 在线学习功能可实现 PC 与手机端同步应用。	一般
		一门通考-在线考试： 1、学习完成自助考试，民警必修课题、学习地图学习完成后自动推送考试试题，民警可通过个人账号查看考试成绩，错误题目核对。 2、在线考试后台，可以实现通过选择岗位、姓名、单位 、区域、等多种筛选模式选择在线测试对象；考试试题库应包含试题模块、难度系数、试题分值等信	一般

		息。学习地图、必修课题可在后台有管理员对测试试卷进行匹配。 3、测评能力分析，能够分析测评完成人员的岗位、单位 、区域 、模块等要素的考试分值关系；可由管理员对试题库进行配置导出自己需要的试题进行线下考试；可在线监控考试民警状态，安排进入失败的民警重新考试，禁止考试；能够实现系统对选择、判断的自主判断功能。 4、民警参加考试，民警登录进入系统后，可以看到当前需要参加的考试，点击后进入正式考试，并在重要位置提醒民警考试注意事项。 5、在线考试功能延展，为了增加终端学习的趣味性，考试功能需增加以倒计时答题、互动 PK 答题等趣味功能。可由后台设置答题后的抽奖环节以强化民警的学习兴趣在线测试功能延展：非考试型在线测试，可布置线上作业，民警可通过视频上传、文件上传等多种模式进行作业互动，部分课程可设置作业完成后获得证书。	
		一门通考-在线直播课堂： 1、在线直播课堂，可实现后台直播授课，终端线上学习互动，实现一对多的培训模式。讲师可通过后台设置共享 PC 屏幕、手机屏幕、摄像头、分享白板、摄像头与 PC 屏幕同时分享等功能。直播间可设置直播助教，助教或讲师可发送参训签到的随机指令（也可系统设定规则签到规则），以防止民警端挂机行为。讲师和助教可以看到民警提问，并能通过视讯回答问题。系统自动对民警的问题进行记录汇总，供讲师后期查看 。2、规模覆盖，单个项目应可以同时容纳多人模式进行同时视频观看、语音互动培训。 3、直播复习，对直播的视频进行存档，提供在线编辑剪辑工具，自助分割成线上课件，可对内容进行自选课题复习。	一般
		一门通考-课程管理与发布： 1、课件制作：提供课件制作工具，可对视频文件进行剪辑、PPT 与视频文件的打包发布等功能。 2、课程保密性管理：支持对课件进行可见群体设置。3、课程发布：支持 office 文件、PDF、视频文件、H5、长图、国产办公软件等发布，支持定向发布及一键群发功能，且应通过技术手段保证文件的保密（禁止下载选项）及客户的顺	一般

		利查看、学习。 4、讲师评价，民警在完成学习后，可对讲师进行评价，评价至少包含实用性、讲师讲课能力等信息。 5、课程答疑区，民警在学习过程中可针对专项课题在答疑区提出问题，后台管理员与课程所对应讲师可以对问题进行解答。	
		一门通考-线下培训过程管理： 支持根据岗位、区域等因素选择参训人群，支持线下培训报名、课前学习、在线签到、课程复习、考试等功能。	一般
		一门通考-知识分享： 每个民警可有独立的申报优秀话术与案例的入口； 每个民警可有独立的申报优秀成果的窗口；支持组织与策划相关的答题竞赛、技能视频竞赛、个位能力展示等多样化的分享竞赛机制。通过分享与评比深度挖掘终端的优秀人才与优秀案例。	一般
		一门通考-讲师管理： 设置讲师数据库，包括讲师个人资料，主讲课程及平台课程民警关注量，评价排名，通过以上数据可实现讲师能力分析，并组织民警对优秀讲师进行投票提问等多样化的讲师互动活动。	一般
		一门通考-知识共享平台： 后台可上传相关通知与文件包，方便终端学习与查阅，文件包可包括 office 文档、视频、pdf 文档、压缩文件包，共享平台文件可以授权下载到本地。	一般
		一门通考-信息数据库： 实现培训、考试类信息的存储、计算和应用。	一般
		一门通考-积分商城： 1、积分商城，民警通过培训记录获得积分奖励，根据获得的积分，换取对应的奖品。民警可以按照积分值的范围查找奖品，可以查看获得积分的方式。 2、首页通知及排名，首页显示最新的学习通知、系统功能更新等通知内容。首页进入后显示优秀民警排名，可设置积分榜排名、学时榜排名、专家榜排名等信息。 3、在线调查与评估，系统管理员可以发布调查问卷，调查问卷可以同时发布多条信息，管理员发布了问卷之后，问卷选择的参与人员，可以看到该问卷，并对问卷进行作答，后台应设有多种分析方式	一般
		一门通考-权限管理： 系统设置管理员，由管	一般

		理员进行设定分级管理权限，管理权限包括人员配备管理模块、人员培训管理模块；管理员角色定义系统管理员：对系统的所有内容可进行编辑，并可对下级管理员权限进行新增、删除、变更增减项等操作。	
		系统改造对接-情报平台： 按照“一门四通”对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括： 1、待办任务对接。实现待办任务、通知通报内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。 3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	一般
		系统改造对接-执法闭环系统： 按照“一门四通”对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括：1、待办任务对接。实现待办任务、通知通报内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	一般
		系统改造对接-禁毒系统： 按照“一门四通”对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括： 1、待办任务对接。实现待办任务、通知通报内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。 3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	一般
		系统改造对接-出入境系统： 按照“一门四通”对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括：1、待办任务对接。实现待办任务、通知通报	一般

		内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	
		系统改造对接-基础要素管控： 按照“一门四通”对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括：1、待办任务对接。实现待办任务、通知通报内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	一般
		系统改造对接-警务保障系统： 按照“一门四通”对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括：1、待办任务对接。实现待办任务、通知通报内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	一般
		系统改造对接-人事系统： 按照“一门四通”对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括： 1、待办任务对接。实现待办任务、通知通报内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。 3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	一般
		系统改造对接-交通管理： 按照“一门四通”	一般

		对接要求，推动系统的微服务化改造，实现基于“一门四通”的对接应用，主要包括： 1、待办任务对接。实现待办任务、通知通报内容的梳理、对接集成。 2、信息提醒对接。实现到期提醒、超期提醒的梳理和流程对接。 3、待办工作平台。实现门户待办工作至业务办理界面研发，以及过程的跳转。 4、考评内容建设及对接。实现对应考评内容的增、删、改、查、统的可视化，并与门户实现对接集成。	
2.6	图像信息综合应用平台人像聚类归档模块	视图应用支撑： （1）应用数据优化评价：对视图数据进行进行统计分析和评价。 （2）安全管理模块：按照公安部的相关要求，为平台提供安全保障。 （3）大数据平台服务支撑：大数据平台服务支撑，为警务大数据平台提供数据和接口服务，为移动警务平台提供数据和接口服务。 （4）地理信息系统对接：地理信息系统对接，提供基于 PGIS 地理信息系统的数据和应用对接。 （5）运维监控对平台进行监测管理。	一般
		**人员数据管控模块： （1）轨迹汇聚：接收地市汇聚的轨迹数据，在省厅平台进行存储。轨迹数据包括比中轨迹和聚类轨迹数据。 （2）轨迹查询：轨迹数据查询，提供地市汇聚的全量轨迹数据的浏览、查询、筛选功能。 （3）轨迹上报：轨迹数据上报，将地市的轨迹数据推送到部平台,获取人员身份信息，对数据进行存储。转发人员身份信息到地市平台。 （4）特征值接收：与部视综平台对接，支撑 16 个地市不同厂商的特征值的接收、同步、存储。 （5）数据对账：数据对账，实现对地市的特征值接收、汇聚轨迹数据进行数据统计和对账。 （6）特征值分发：与地市视综平台对接，完成注册、保活、订阅接口，并将未解密的特征值转发到地市平台。	一般
		聚类归档： （1）档案实名化：系统自动对创建的非实名档案与底库中的实名信息进行碰撞比对，实现非实名档案的实名化。无法实名化的档案，系统会定期进行多次的实名化。 （2）档案汇总统计：定时对系统中产生的档案进行汇总统计，可按时间、人员类别、区域、风险等级方式对档案进行汇总统计。	△

		（3）以图搜档：通过上传人脸或人体照片，以图片方式进行档案的搜索。按档案的关联程度进行排序。 （4）路人数据接入管理：路人数据接入管理，对需要聚档的人像卡口数据进行接入、参数配置管理。（5）离线聚档：支持 24 小时内完成不少于 1000 万人脸抓拍图片与不少于 1 亿档案库碰撞聚档。 （6）档案存储管理：对系统中产生的档案进行存储管理，支持一年的数据存储能力。 （7）结构化信息档案检索：通过姓名、身份证、人员类别、属性、活动时间、活动区域等结构化信息进行档案的检索。 （8）档案自动标签：系统自动根据个人档案中的轨迹信息进行标签化处理，包括人员类别、活动时段、活动区域等信息。 （9）底库管理：对聚档的实名底库进行导入管理，对底库照片进行特征值、结构化信息、照片进行管理。支持亿级底库的导入。 （10）“一人一档”档案建档：通过档案的形式展示人员的基本信息、标签信息、轨迹信息、同行人员、活动区域、活动时段、车辆信息、MAC 信息。 （11）档案碰撞分析：按上层业务系统需要提供档案的碰撞分析能力，包括排序、检索、同行、频次、时空碰撞等能力。 （12）轨迹查看：对聚档后人员的轨迹进行检索、查看、浏览。可在 PGIS 地图中完整还原人员的活动轨迹，可查看每个轨迹点的小图、场景图、时间、地点等轨迹信息。 （13）动态索引优化：对档案的多重优化后的数据，重新进行动态索引，提高档案的检索速度。要求亿级档案检索速度不超过 2 秒。支持对地市汇聚的档案进行二次聚档。 （14）聚档任务管理：对需要进行聚档底库、区域、点位、时间段、阈值、任务工作时间、优先级进行设置。（15）自定义标签管理：可自定义标签，比如是否**人员、人员类别、数据来源、工作性质、联系方式等标签信息。标签可以由数据导入时通过 Meta 信息导入。 （16）实时聚档：对接入的路人抓拍人像进行实时比对和关联，将同一个人的轨迹信息实时放入个人的档案中。 （17）多维数据融合管理：系统支持将多个维度的信息进行关联，使个人画	

		像更加丰富、立体。如关联车辆、关联人员、MAC 信息等，需提供具体设计方案。（18）档案去重：系统自动对重复的档案，重复的轨迹进行去重，去除重复、低质量的数据。（19）外部 Meta 数据导入管理：支持对聚档的底库数据导入相关的人员信息数据，包括联系方式、地址、户籍、证件号、人员类别等附加信息。（20）档案合并：系统实现对多份相似的档案自动进行合并，将多份档案归并到一份档案中，重新组合形成的档案特征信息。包括实名档案和非实名档案的合并。	
		视图数据治理：（1）前端资源治理：支持对接入的点位基础信息进行检测分析，对时间、经纬度、场所类型、设备名等基础信息进行治理，保证点位基础信息的准确性和可用性。基础数据治理模块对建档入库的全量资产档案数据进行校验，校验规则包括：数据唯一性、信息完整性、档案合规性、档案准确性等。模块支持设备编码治理、设备名称监测治理、监控点位类型监测治理、摄像机功能类型监测治理、经纬度监测治理、摄像机位置类型监测治理、设备状态监测监测、MAC 地址及 IP 地址监测治理。（2）数据质量评估：支持对数据治理过程中发现的质量问题进行评估，生成评估报告。支持图形、列表方式对系统内视频图像设备基础信息、视频图像数据、**人员人像轨迹数据、视频流数据等 4 类视图数据治理成效进行统计展现。（3）数据清洗：对汇聚的各类数据进行校验，对收集的各类元数据、数据内容进行人工校验和基于标准规范的自动化校验，区分出噪声数据和重要数据。（4）视图数据质量检测：支持对接入的图片进行检测分析，发现图片无法调取、清晰度差、无法发现人脸、俯仰角过大、左右偏转角过大、人脸两眼间距过小等图片异常情况并处理。按照公安部相关要求，治理视频图像设备（包括视频监控和车辆卡口、人员卡口、微卡口等抓拍设备）基础信息、图像数据、**人员人像轨迹数据、视频流数据等 4 类视图数据。	△
		共性应用模型：（1）单点登录：数字证书登录，支持用户绑定数字证书的登录，实现数字	一般

		证书单点登录。（2）日志管理：可查看系统用户登录、操作、管理的详细日志信息。（3）图像调优：用户可以提高在图片模糊不清情况下的比对准确率。（4）组织机构管理：可对系统用户的组织机构进行维护管理，支持按组织机构代码导入。（5）用户权限管理：可按用户、用户组、组织机构设置用户使用的资源和功能的权限。可设置查看、操作、管理的细化操作权限。（6）n:N 交叉比对：指对两个人脸图像数据库进行匹配比对，得出两个数据库中图片特征值高于设定阈值的人像对。（7）布控报警：当布控人员出现在布控摄像头画面中时，立即进行报警。（8）1 比 1 身份核验：通过输入一张查询照与一张证件照，系统进行 1:1 比对并返回相似度分数，完成人证核验。（9）卡口监控：系统具备对人像卡口进行监视管理。（10）资源管理：支持静态资源库的导入、建库、统计管理，支持导入的离线视频库的管理。（11）1 比 N 静态比对：支持利用本地静态人像库或与本地联动的更大规模的人像资源库，确认某张照片人像的真实身份。结果按相似度排序，支持结果导出。（12）路人结构化检索：支持通过结构化信息对路人库进行筛选，方便实战中找到特定类型的路人。（13）路人以图搜图：用户上传一张类证件照，在人像库中进行检索。（14）布控任务管理：用户可以发布、管理布控任务。（15）一机一档：对接入系统的卡口进行管理，维护点位、类型、编码、区域、参数等信息。支持接入的卡口状态查看，对异常的卡口进行标记。支持前端视频图像感知设备资产档案管理，提供资产采集建档，数据查询导出、基础数据质量检测、资产分级分类管理、资产管理效能分析、资产共享同步、系统管理、多维度数据统计分析等功能。（16）战果管理：用户录入战果信息，上级部门可以查看下级部门录入的战果。（17）同人多帧检索：一次性上传多张照片，通过一次性给系统提供更多信息，从而提升检索结果准确率。（18）离线视频分析：对离线视频文件进行分析，截取出视频中出现人脸照片。	

		对外接口服务（聚类归档模块）： （1）对外接口服务（聚类归档模块）：档案对外接口调用，支持大数据等第三方平台获取聚档后的人员档案信息。支持单条调用和批量调用，接口可按功能和调用频次进行限制。	△
		集群维护管理（聚类归档模块）： （1）集群维护管理（聚类归档模块）：对聚档应用使用的硬件资源进行配置和维护管理，可实时监控聚档任务完成情况，聚档集群服务器的负载情况，辅助运维工作。	一般
		专业应用模型： （1）个人关系分析：系统可以生成查询个人关系图，图中包括同行关系、亲属关系等。 （2）时空碰撞分析：支持选定多个时空范围进行碰撞分析，找出在多个地点范围内出现的活跃度最高的目标人员。 （3）人员摸排分析：支持输出案发前在附近出现过的人及轨迹信息。 （4）宏观态势分析：通过可视化界面，展现整体的治安态势。展现整体的治安态势，用于查看系统接入的各类设备资源数据、各类人员分布数据、以及聚档后的各类统计数据，可以实时监控区域内各类风险人员出现的位置，便于直观获取宏观数据辅助决策。主要用于可视化展示，以及日常用于查看抓拍统计、设备统计、静态库等宏观数据统计，对于风险指数、风险人员、风险事件进行实时监控和预警。宏观态势主要提供如下功能： •风险指数风险分布实时更新 •风险人员、风险事件实时预警 •显示实时抓拍数量和汇聚档案数量。 •显示设备数量及对应地图点位。 •显示静态库数量、类别及库大小。 •显示区域内的人口结构，如**人口、外来人员、实有人口的统计数据。 •显示**区域各类风险人群（即**人口）的统计数据及**人员的实时行踪。另外，系统支持地图缩放、设备筛选、区域框选、**人员定位报警等功能。 •通过可视化界面，展现整体智慧安防小区建设情况，包括各地已建设数量、接入联网数据等。 （5）同行关系分析：根据时空信息分析同行人员，包括同行次数、区域、时间、人员等信息。	一般
		专题应用模型： 1、治安应用模型：**人员群	一般

		体关系分析、治安关注特定人员群体关系分析、**人员窝点发现模型、**监控。（1）疑似**行为监控：多名**标签人员在敏感时间相继进入同一治安热点区域即报警，及时发现。（2）**窝点发现模型：多名**人员在敏感时间内出现即预警。及时发现异常聚集的**人员和聚集地点。（3）治安关注特定人员群体关系分析：对治安关注特定人员进行关系网的分析，挖掘群体中的小团伙或核心联络人等有价值的线索。（4）**人员窝点发现模型：多名**人员同时出现于同一特定区域即报警，及时发现**人员窝点，提供研判线索。（5）**监控：通过摄像头捕捉路人进行聚档，对**在无家人陪同的情况下独自外出的情况进行预警。2、**应用模型：栖息地分析、窝点分析、徘徊分析、同行反查、落脚点分析、在逃追踪。（1）栖息地分析：查询目标对象的落脚点/栖息地。用于分析**或者**人员的栖息地，研判人员位置信息。（2）窝点分析：通过分析特定关注人员多次出现在某摄像头下，研判**、**等场景的窝点。支持根据窝点附近人像卡口报警的时间进行筛选。（3）徘徊分析：通过摄像头抓拍，分析案发地附近可疑的徘徊人群，推送相关业务系统。（4）同行反查：对遮挡面部信息的**，通过找出与**同行的面部清晰的同行人，查询该同行人的历史抓拍，找到**未遮挡面部的照片，从而利用同行人确认**的身份。（5）落脚点分析：根据**（可通过关系人辅助研判）的历史时空信息研判出**的落脚点，进行核查或蹲点，也可以根据落脚点进行精准布控，提高抓捕效率。（6）**追踪：对标签为全国**的人员，出现即报警，及时发现**人员，掌握行踪。3、**应用模型：感知发现**人员、**对象关系分析、**团伙分析、**团伙分析。（1）**人员感知发现：在重大活动现场以及机场、火车站等**场所，对高危标签人员进行感知发现、及时预警。（2）**对象关系分析：基于**对象的个人档案库和**人员库，分析**对象的个人关系。（3）诈骗团伙分析：通过摄像头捕捉路人进行聚档，基于聚档数据和诈骗人员库，找出诈	

		骗团伙个人关系，及时发现诈骗团伙。 （4）**团伙分析：通过摄像头捕捉路人进行聚档，基于聚档数据和传销人员库，找出**团伙个人关系，及时发现**团伙。 （5）**特定关注人员管控：通过摄像头捕捉路人进行聚档，基于聚档数据和**特定关注人员库，实时发现**关注人员行动轨迹和出行规律，对其进行管控。 4、**应用模型：建设**关注人员库、**人员库，通过技战法模型提供研判辅助。 （1）特定人群发现预警：发现特定人员，实时预警排查，掌握特定人员的实时活动轨迹，进行无感知管控。 （2）**关注人员监控：在敏感时间、敏感区域出现即预警，及时发现。 （3）****人员在本区**区域出现预警模型：****人员在敏感时间出现在**区域即预警，及时发现****人员，分析作案可能，提供案发后抓捕方向。 （4）**人员长时间内异常聚集模型：多名****人员长时间在同一小区异常聚集即预警，及时发现可疑的异常聚集事件。 （5）**人员短时间内异常聚集模型：多名****人员短时间在同一小区异常聚集即预警，及时发现可疑的异常聚集事件。 （6）**人员聚集预警模型：多名**人员在敏感时间聚集即预警，及时发现异常聚集的**人员和聚集活动。	
		视图解析： （1）关键点定位：关键点定位用于对人脸、人体位置、水平角度、垂直角度、偏仰角度等信息的获取。 （2）人像自动矫正：通过关键点定位信息，自动对图像进行矫正。 （3）人脸模型库管理：1、对解析的人脸模型库进行管理，支持模型库的更新、切换、加载、导入功能。2、支撑省厅实现全省各家静态库统一查询及展示。 （4）视图数据接入管理：对接入的监控摄像机的点位、参数进行配置和管理。 （5）人像提取：从图片中提取人脸、人体小图，实现“抠图”功能，将小图、坐标等进行存储。 （6）解析任务调度管理：对 500 万张/天的请求进行任务管理，将解析任务分发到不同的硬件解析单元（GPU 卡）进行解析。 （7）图像质量检测：判断图像中是否有符合解析的元素。包括人脸尺寸、人体尺寸、角度、清晰度是否达到解析标准。	一般

		（8）特征向量提取：获取可用于比对的人脸特征值。单条特征值小于1k。 （9）解析数据入库存储：写入高速缓存，结构化信息存储到数据库中转存到视图库中、非结构化信息存储到视图库存储系统中。（10）人脸属性提取：包括年龄、性别、眼镜、帽子、墨镜、口罩等。	
		视图库对接： （1）图片流接入：图片流接入：支撑省厅与全省16个地市的视图库系统或市局视综平台进行对接，实现视图库的数据汇聚，推送人脸或人体小图、大图数据。2、接入能力：支撑省厅接入6万路人像卡口，并对接入设备及数据进行检测管理。 （2）部平台对接：与公安部视图库系统实现对接，完成向公安部推送视图数据，向公安部提供分布式身份确认、分布式轨迹查询、分布式布控功能。 （3）视图库考核模块：按公安部对视图库考核的要求开发省级视图库考核模块，对地市接入的视图数据数量、数据质量、接入稳定性。 系统运维检测模块：对视图库数据上传稳定性、视图库接口功能稳定性进行检测，确保山东省级视图库接口功能及数据上传稳定可靠，对系统异常情况进行自动检测和异常情况的自主修复，并进行故障报警，对无法自主修复的问题进行人工干预处理。	一般

3、货物明细

（1）货物一览表

序号	货物名称	数量	单位	是否强制节能	是否核心产品	是否接受进口
3.1	山东新一代公安信息网建设——交换机	10	台	否	否	否
3.2	山东新一代公安信息网建设——网络智能管理平台	1	套	否	否	否
3.3	山东新一代公安信息网建设	2	台	否	否	否

	——路由器Ⅰ					
3.4	山东新一代公安信息网建设——路由器Ⅱ	3	台	否	否	否
3.5	#大数据中心（数据域部分）——数据分析智能工具	1	套	否	否	否
3.6	新一代移动警务部分（一期）——核心交换机	1	台	否	否	否
3.7	新一代移动警务部分（一期）——汇聚交换机	4	台	否	否	否
3.8	新一代移动警务部分（一期）——万兆下一代防火墙	2	台	否	否	否
3.9	新一代移动警务部分（一期）——万兆三层交换机	2	台	否	否	否
3.10	新一代移动警务部分（一期）——探针	1	台	否	否	否
3.11	新一代移动警务部分（一期）——视频安全传输系统（万兆）	1	套	否	否	否
3.12	新一代移动警务部分（一期）——单向安全传输系统（万兆）	2	套	否	否	否
3.13	新一代移动警务部分（一期）——抗	2	台	否	否	否

	DDOS					
3.14	新一代移动警务部分（一期）——WEB 应用防火墙	1	台	否	否	否
3.15	新一代移动警务部分（一期）——安全准入系统	1	套	否	否	否
3.16	新一代移动警务部分（一期）——智能流量管理器	1	台	否	否	否
3.17	新一代移动警务部分（一期）——物理服务器扩展升级	8	台	否	否	否
3.18	新一代移动警务部分（一期）——移动云计算超融合软件升级	4	套	否	否	否
3.19	新一代移动警务部分（一期）——移动云计算安全网络防护	2	台	否	否	否
3.20	新一代移动警务部分（一期）——移动云计算服务器主机安全管理	300	点	否	否	否
3.21	新一代移动警务部分（一期）——移动警务数字证书 USB-KEY	100	个	否	否	否
3.22	新一代移动警务部分（一	2	台	否	否	否

	期）——应用安全认证网关					
3.23	新一代移动警务部分（一期）——发证安全接入网关	1	套	否	否	否
3.24	新一代移动警务部分（一期）——证书从目录服务	1	套	否	否	否
3.25	山东省公安信息网大数据智能化安全体系（一期）——后端接入防火墙	2	台	否	否	否
3.26	山东省公安信息网大数据智能化安全体系（一期）——VPN 网关	2	台	否	否	否
3.27	山东省公安信息网大数据智能化安全体系（一期）——入侵防御	5	台	否	否	否
3.28	山东省公安信息网大数据智能化安全体系（一期）——前端接入防火墙	2	台	否	否	否
3.29	山东省公安信息网大数据智能化安全体系（一期）——可信 API 代理	4	台	否	否	否
3.30	山东省公安信息网大数据智能化安全体系	1	套	否	否	否

	（一期）——可信代理控制服务					
3.31	山东省公安信息网大数据智能化安全体系（一期）——可信接入代理	2	台	否	否	否
3.32	山东省公安信息网大数据智能化安全体系（一期）——可信运维代理	1	台	否	否	否
3.33	山东省公安信息网大数据智能化安全体系（一期）——数据中心防火墙	2	台	否	否	否
3.34	山东省公安信息网大数据智能化安全体系（一期）——数据交换前置防火墙	7	台	否	否	否
3.35	山东省公安信息网大数据智能化安全体系（一期）——数据交换后置防火墙	4	台	否	否	否
3.36	山东省公安信息网大数据智能化安全体系（一期）——数据防泄漏	2	台	否	否	否
3.37	山东省公安信息网大数据智能化安全体系（一期）——	2	台	否	否	否

	日志审计					
3.38	山东省公安信息网大数据智能化安全体系（一期）——深度威胁检测	2	台	否	否	否
3.39	山东省公安信息网大数据智能化安全体系（一期）——漏洞扫描系统	1	台	否	否	否
3.40	山东省公安信息网大数据智能化安全体系（一期）——网页应用防火墙	2	台	否	否	否
3.41	山东省公安信息网大数据智能化安全体系（一期）——设备准入控制	2	台	否	否	否
3.42	山东省公安信息网大数据智能化安全体系（一期）——隔离与交换系统-数据交换	1	套	否	否	否
3.43	山东省公安信息网大数据智能化安全体系（一期）——隔离与交换系统-视频交换	1	套	否	否	否
3.44	山东省公安信息网大数据智能化安全体系（一期）——高级威胁检测	1	台	否	否	否
3.45	山东省公安信	1	台	否	否	否

	息网大数据智能化安全体系（一期）——高级未知威胁检测					
3.46	山东省公安信息网大数据智能化安全体系（一期）——可信环境感知代理	1	套	否	否	否
3.47	山东省公安信息网大数据智能化安全体系（一期）——环境感知代理客户端	1	套	否	否	否
3.48	山东省公安信息网大数据智能化安全体系（一期）——部门间信息共享系统	1	套	否	否	否
3.49	山东省公安信息网大数据智能化安全体系（一期）——认证服务	1	套	否	否	否
3.50	山东省公安信息网大数据智能化安全体系（一期）——权限服务	1	套	否	否	否
3.51	山东省公安信息网大数据智能化安全体系（一期）——业务审计服务	1	套	否	否	否
3.52	山东省公安信息网大数据智	1	套	否	否	否

	能化安全体系（一期）——业务审批服务					
3.53	山东省公安信息网大数据智能化安全体系（一期）——安全管理服务	1	套	否	否	否
3.54	山东省公安信息网大数据智能化安全体系（一期）——安全识别服务	1	套	否	否	否
3.55	山东省公安信息网大数据智能化安全体系（一期）——安全检测服务	1	套	否	否	否
3.56	山东省公安信息网大数据智能化安全体系（一期）——安全防护服务	1	套	否	否	否
3.57	山东省公安信息网大数据智能化安全体系（一期）——安全响应服务	3	套	否	否	否
3.58	山东省公安信息网大数据智能化安全体系（一期）——资产管理	1	套	否	否	否
3.59	山东省公安信息网大数据智能化安全体系（一期）——安全大数据	1	套	否	否	否
3.60	山东省公安信息网大数据智	1	套	否	否	否

	能化安全体系（一期）——态势感知					
3.61	山东省公安信息网大数据智能化安全体系（一期）——云安全管理平台	1	套	否	否	否
3.62	山东省公安信息网大数据智能化安全体系（一期）——应用安全防护服务	3	套	否	否	否
3.63	山东省公安信息网大数据智能化安全体系（一期）——日志审计服务	1	套	否	否	否
3.64	山东社会治安动态全息感知网安全防护体系——IPS	3	台	否	否	否
3.65	山东社会治安动态全息感知网安全防护体系——交换机	2	台	否	否	否
3.66	山东社会治安动态全息感知网安全防护体系——入侵防御系统	2	台	否	否	否
3.67	山东社会治安动态全息感知网安全防护体系——加解密媒体设备（C级）	1	台	否	否	否
3.68	山东社会治安	1	台	否	否	否

	动态全息感知网安全防护体系——安全隔离网闸					
3.69	山东社会治安动态全息感知网安全防护体系——数据库	2	套	否	否	否
3.70	山东社会治安动态全息感知网安全防护体系——数据库审计	1	台	否	否	否
3.71	山东社会治安动态全息感知网安全防护体系——服务器	32	台	否	否	否
3.72	山东社会治安动态全息感知网安全防护体系——用户认证设备	1	台	否	否	否
3.73	山东社会治安动态全息感知网安全防护体系——省级视频密钥管理系统	1	套	否	否	否
3.74	山东社会治安动态全息感知网安全防护体系——综合审计系统	1	台	否	否	否
3.75	山东社会治安动态全息感知网安全防护体系——网络数据交换系统	1	套	否	否	否
3.76	山东社会治安动态全息感知	20	台	否	否	否

	网安全防护体系——视频专用智能钥匙					
3.77	山东社会治安动态全息感知网安全防护体系——视频可信鉴定设备（B级）	1	台	否	否	否
3.78	山东社会治安动态全息感知网安全防护体系——视频安全接入系统	2	套	否	否	否
3.79	山东社会治安动态全息感知网安全防护体系——视频安全设备身份证书注册模块	1	套	否	否	否
3.80	山东社会治安动态全息感知网安全防护体系——视频安全设备身份证书申请模块	1	套	否	否	否
3.81	山东社会治安动态全息感知网安全防护体系——视频密钥管理设备	2	台	否	否	否
3.82	山东社会治安动态全息感知网安全防护体系——视频应用保护网关	1	台	否	否	否
3.83	山东社会治安动态全息感知网安全防护体系——视频数	2	台	否	否	否

	据安全密码设备					
3.84	山东社会治安动态全息感知网安全防护体系——视频监控共享平台升级改造	1	套	否	否	否
3.85	山东社会治安动态全息感知网安全防护体系——视频目录系统	2	台	否	否	否
3.86	山东社会治安动态全息感知网安全防护体系——设备认证设备	1	台	否	否	否
3.87	山东社会治安动态全息感知网安全防护体系——边界安全访问控制网关	1	台	否	否	否
3.88	山东社会治安动态全息感知网安全防护体系——防火墙	5	台	否	否	否
3.89	山东社会治安动态全息感知网安全防护体系——防病毒网关	1	台	否	否	否
3.90	山东社会治安动态全息感知网安全防护体系——集中监控与审计系统探针系统	3	台	否	否	否
3.91	山东社会治安	1	台	否	否	否

	动态全息感知网安全防护体系——集中监控与审计系统监管系统					
3.92	图像信息综合应用平台人像聚类归档模块——**人员比对应用系统	1	套	否	否	否

（2）详细配置表

序号	货物名称	指标需求	重要程度
3.1	山东新一代公安信息网建设——交换机	交换容量≥380Tbps，包转发率≥115200 Mpps；≥4 个业务槽位，≥8 个交换网板插槽，且支持网板 N+M 冗余；	一般
		风扇框冗余设计，≥3 个风扇框；	一般
		电源模块支持双路输入，且支持 AC 和 HVDC 混合供电；	一般
		主控引擎与交换网板硬件分离，主控板故障或者更换不影响整机转发性能；支持信元交换，跨板转发不丢包；	△
		支持端口聚合，802.3ad；支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术；	一般
		支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议；支持路由协议多实例、策略路由；	一般
		支持 PQ、DRR、PQ+DRR 等队列调度方式，支持 ACL、CAR、Remark 等动作；	一般
		支持集群或堆叠多虚一技术，实现单一界面管理多台设备；	一般
		支持缓存的微突发状态统计；支持 VXLAN over IPv6，支持 IPv6 VXLAN over IPv4；	一般
		支持二层到四层的 ACL，支持 IP/ARP/ICMP 安全；	一般
		支持单播、组播和广播风暴控制，支持 DHCPv4 Server、Relay 和 snooping；	一般

		支持 VxLAN OAM: VxLAN ping, VxLAN tracert；支持配置回滚；支持 Ansible 自动化配置；	一般
		支持通过命令行、中文图形化配置软件等方式进行配置和管理；	一般
		支持 BootROM 升级和远程在线升级，支持 ZTP 技术，配置自动下发，支持 RADIUS 用户登录认证；	一般
		实配：双主控，≥4 电源，≥4 块交换网板，≥48 个万兆光口，≥30 个万兆单模模块（10KM），≥18 个万兆多模模块（0.3KM）。	△
3.2	山东新一代公安信息网建设——网络智能管理平台	总体要求 1.1 协同管控：满足公安部制定的网络综合管理体系相关标准和要求，须实现网络感知、网络资源综合管理，网络管控，智能分析、网络保障、网络运营等功能，需开放南北向接口，实现上下级网络综合智能管理系统的对接，对接现网的基础网管系统、公安网终端准入管控系统、智能网络流量分析系统平台等，实现综合管理、基础网管、网络流量分析、终端准入管控系统和认证系统用户统一登录，实现全部网络资源的管理与分析； 1.2 流量分析能力整合：对接现网智能网络流量分析系统平台及 10G 流量采集器、40G 流量采集器，建设完善智能网络流量分析系统平台及流量采集器双平台方案部署，完成数据交换及功能调用，实现对骨干网络节点和汇聚网络节点的网络流量采集分析，实时监测各条链路负载状态的，包括平均比特率、峰值比特率、带宽利用率、会话数等；实时监测展现网络服务质量，包括平均延迟时间、丢包率、重传率等；实时监测展现业务服务性能，包括平均返回时间、零窗口率、无应答率等；实现流量异常告警、定位和提供相应数据依据；支持上述指标数据存储时间不小于三个月。协同实现 10G 流量采集器、40G 流量采集器的流量处理、报文存储、并发用户数、并发会话数、新建会话数等能力；或配置≥6 台同等性能的 10G 流量采集器和≥2 台同等性能的 40G 流量采集器及网络流量分析平台实现以上功能（10G 流量采集器性能要求：最大流量处理能力≥10Gbps；最	△

		大报文存储性能≥2Gbps；最大并发用户数≥5万；最大并发会话数≥300万；最大新建会话数≥10万/秒硬盘容量≥4T，万兆SFP+光接口≥2个,千兆电接口≥4个；40G流量采集器性能要求：最大流量处理能力≥40Gbps；最大报文存储性能≥4Gbps；最大并发用户数≥20万；最大并发会话数≥500万；最大新建会话数≥40万/秒，硬盘容量≥30TB，万兆SFP+光接口（含光模块）≥4个，千兆电接口≥4个）； 1.3终端准入管控能力整合：对接现公安网终端准入管控系统，升级现公安网终端准入管控系统功能，实现新一代公安信息网络终端准入管控功能，扩容新一代公安信息网网络终端准入功能及相应功能授权，整合数据共享与服务联动，实现公安厅所有入网设备进行准入管理，实现对入网设备的可知、可管、可控和可溯源，设备类型覆盖PC终端、哑终端（包括但不限于打印机、摄像头等）、网络设备、安全设备、服务器等，管理规模不低于现网已采购终端准入管控系统管控能力；	
		统一管理功能 1.1统一架构：微服务容器化部署，支持服务弹性扩展，支持更大规模的管理能力；系统支持高可用集群； 1.2统一权限管理：基于角色的权限控制方案，支持菜单和操作的权限控制，支持细分资源增删改查的权限控制； 1.3统一拓扑展示：实现统一展示网络设备、链路、终端和流量信息；实现链路的增加、修改、删除、合并、隐藏等；支持目录-视图-云图多级管理网络设备、终端资源；支持集群、分组等分组展示；支持拓扑背景图设置；支持网络拓扑和资源数据的联动；支持自定义拓扑节点类型、图标等；支持拓扑节点关联告警状态，可自定义哪些告警影响节点状态；	一般
		网络资源管理 1.1网络拓扑：须实现网络拓扑的自动发现和动态更新，可发现设备及其链路关系；支持网络拓扑信息的手工编辑：支持将设备加入不同的自定义视图管理，支持在拓扑上增加修改链路、支持将设备纳入不同的云图、分组进行呈现；支持分层展示和拓扑下钻能力；支持网络运行状态展示，具备设备资源	一般

		状态、告警、网络性能、链路流量等指标的呈现； 支持查看网元和链路详情；支持拓扑背景图设置，支持图片或者 GIS 地图； 1.2 链路管理：须实现通过手工、批量导入、数据采集方式获取链路信息，包括链路 ID、状态、左右节点 IP、名称、左右接口索引、MAC 地址和名称等信息；可自动从监控模块同步链路信息；可自动识别链路和设备的连接关系； 1.3 运营商专线管理：支持通过手工、批量导入等方式获取专线信息，包括链路左右节点、运营商、带宽、价格、报障方式、线路编号等信息； 1.4 资源维护：须实现资源总览功能，对资源进行类型和实例进行统计，并支持分层展示；支持资源全文检索；支持资源的增删改查、导入、导出；支持资源的锁定和解锁；锁定配置项，锁定期间不可变更该配置项；解锁后可正常变更；支持资源的二维码打印；支持资源关系拓扑查看；支持资源审计，当资源属性发生变更后，可通过流程审批决定是否变更资源属性或立即变更资源属性，可发送资源变更告警；支持到期时间提醒和告警；支持资源基线化，资源属性和基线不一致时，可记录变更；可将资源属性恢复至基线；支持手工设置资源之间的关系，如设备主备、链路主备； 1.5 资源自定义：须实现自定义资源属性及属性关联；资源属性可设置属性名称、英文缩写、所属分组、数据类型、最大长度、缺省值等；资源数据类型支持文本、文本区域、下拉文本、属性下拉文本、整数、小数、IP 地址、MAC 地址、日期/时间、附件、密文、表格、表单、URL 等；实现自定义资源类型，可设置资源属性、属性分组、可设置属性是否主键、是否必选、是否写入二维码、是否在标签页展示、是否提供高级查询以及属性排列顺序；支持设置属性关联，即类型 A 的属性 A 的值从类型 B 的属性 B 中获取；支持自定义关系类型和资源间关系，系统预置常见关系，如连接、依赖、部署、运行、包含、成员关系等；可导入、导出资源属性、资源类型、资源关系定义信息；可设置资源类型和关系是否自动同步以及同步数据的来源； 1.6IP 资源管理：	

		支持 IP 地址生命周期管理，具备 IP 地址规划、分配、变更、回收、使用状态监控等功能； 1.7 配置信息：实现网络设备配置备份、查看、基线化、比较、导出等操作；支持按照设备或区域周期性自动备份配置，并将备份报告发送至邮箱；支持设备配置审计：和上一次发生变更或和基线不一致时发送告警；将设备配置恢复至基线；支持设备配置部署：配置片段、配置文件、CLI 脚本、TCL 脚本部署；支持参数化部署，不同设备使用不同参数进行部署；支持设备配置库，系统预置大量常用配置片段； 1.8 设备软件管理：支持设备软件库，支持从本地或设备导入设备软件；支持升级设备软件、升级设备 Boot ROM 文件；支持将任何类型的文件上传到设备；	
		网络资源-多维展示 1.1 多维展示：支持大屏元素自定义设计，支持常见的图表、图片、文字、时间等组件，并且可以设计各组件的数据源和展示方式；大屏数据源配置：静态数据 JSON 格式通过 API 获取 GET 或者 POST 方式获取或者通过过滤器中的 JavaScript 代码调用 API 实现；系统默认提供网络设备、告警、拓扑、终端、流量信息等大屏元素；支持领导、普通管理者、运维人员、查看员等多维度大屏视图；	一般
		网络态势 1.1 网络设备管理：支持 SNMP v1、v2c、v3 协议管理设备；支持手工增加设备；支持自动发现设备，立即或周期性执行；支持设备基本信息展示：设备标签、管理状态、IP 地址、掩码、sysOID、类型、系统名称、联系人、位置、设备型号、最后轮询时间、接口数量、运行时间、系统描述等；支持接口信息展示：展示接口状态、接口描述、接口别名、最后改变时间、光/电口、IP 地址等；支持设备导入、导出、管理、取消管理、删除、修改基本信息等；支持设备常用操作：Telnet 或 SSH 至设备、打开设备 Web 网管、Ping 和 Tracert 设备；支持设备可达性状态探测：当设备不可达时会发出不可达告警，设备状态变为红色，当可达后，发出可达告警，设备状态变为正常，支持设备告警接收； 1.2 设备支持：支	一般

		持主流厂商设备；支持自定义支持设备：通过自定义设备厂商、设备系列、设备型号、设备类型等内容，实现对设备公有 mib 信息获取；1.3 网络设备监控：支持设备 CPU、内存、响应时间、不可达比例监控；支持接口收发速率、带宽利用率、丢包率等指标监控；支持显示监控实时数据和历史监控数据，支持数据的图形化展示，支持最近两小时、最近一天、周、月、自定义时间监控数据查看；支持五级阈值告警，当性能指标超过阈值时根据不同的阈值发送不同级别的告警，支持五级告警阈值：数值型支持大于、小于、等于、大于等于、小于等于，字符型支持包含、不包含，支持配置触发次数；支持自定义监控模板，关联监控指标和阈值设置；	
		应用感知： 1.1 实现建立应用特征库的能力，包括：应用名称、应用服务器 IP 地址、URL 地址、端口号等；支持基于特征库识别应用流量，支持灵活的应用分组和对比监控；支持应用活跃度分析，识别热点和僵尸应用；支持基于应用历史健康度，预测应用健康度变化趋势；支持 HTTP 应用分析：包括 HTTP 状态码、页面传输时间、响应时间分析；支持 HTTPS 应用解码分析：通过上传私钥解析 HTTPS 报文；支持应用间访问关系梳理；支持将协同完成一个功能的多个应用定义成业务；支持业务仪表盘功能：提供业务质量监控的全局视角；支持业务健康度评估、流量异常检测，基于历史健康度预测业务健康度变化趋势；支持业务拓扑呈现：使业务的组成、关键指标、告警状态一目了然；支持业务多段分析：通过多段对比分析，缩小故障定位的范围，提高问题处理的效率；支持业务 HTTP 分析：包括 HTTP 状态码、页面传输时间、响应时间分析；	一般
		用户感知： 1.1 支持用户流量分析，统计任意用户组内用户流量、包数，具备任意用户组的用户流量排名、包数排名；支持用户组查看终端列表，包括查看终端上下线流量、流速、会话数、0 窗口数、包数等；用户组分不同终端类型分析，包括用户终端、服务器、摄像头	一般

		等；支持用户关键指标回溯，如重传率、丢包率、时延、TOP 应用；支持用户查看会话列表；支持某个用户在某一个时间段在某一个链路上的流量分析（包含用户流量，以及访问的应用流量等指标）详情；支持查询结果的导出；	
		智能分析 1.1 故障定位：形成系统故障定位能力集，并支持随版本升级扩展。通过内置多指标阈值或动态基线匹配规则，自动发现网络中存在的故障；对于发现的故障及时触发告警提示，给出原因分析、排障过程，并提供处理建议；对故障进行归纳与总结，按故障分类进行汇总呈现，给出故障新增和关闭趋势分析；支持将已知高频故障排查方案自定义编排及固化成故障排查流程，实现多设备分步骤的端到端故障排查场景和设备群组（如主备冗余）的故障排查场景；支持 python 脚本实现单步故障排查操作自定义；故障定位范围至少覆盖现网核心设备，包括但不限于：骨干节点和汇聚节点设备等。 1.2 合规检查：支持周期性或一次性设备合规检查，合规特性 100+。检查范围至少覆盖现网核心设备，包括但不限于：骨干节点和汇聚节点设备等。报告支持 word、Excel、pdf、html、国产办公软件格式。可自定义合规场景；支持违规信息总结报告生成；支持自定义配置变更的流程编排，能应对多设备分步骤的端到端配置变更场景；支持 python 脚本实现单步配置变更操作自定义； 1.3 容量规划：支持流量带宽历史数据统计和趋势数据分析，以时间、阈值等维度进行容量预测；支持基于容量预测数据，给出推荐建议；	△
		告警管理 1.1 系统告警：支持接收设备发送的告警；支持系统自动产生告警：系统会定期检测网络设备不可达/可达状态，并发送告警；系统会自动生成性能阈值告警；支持活动告警和历史告警查看；支持告警的恢复、确认、删除、打印、备注和导出等操作；支持告警转发至邮箱、收集、微信和流程等；支持声光告警提示；支持重复告警计数；支持设备 Trap 浏览和 Trap 升级成告警规则定义；支持	一般

		Trap 定义修改：修改 Trap 描述和级别等；支持 Trap 过滤：重复、闪断、未知 Trap 和未管理设备 Trap 过滤，或自定义 Trap 过滤规则；支持 Trap 转发至其他系统；告警自动处理规则统一管理：自动调整级别，支持根据告警重复次数和持续时间，修改告警级别；支持自动确认、告警每 5 分钟邮件或短信通知等。支持设备告警级别的颜色设置；支持设备告警保存时长； 1.2 组合告警：针对复杂场景下的告警关联分析，实现精准化的告警上告，例如：某个设备的 cpu 利用率过高和接口流量过高告警关联分析，上告“xx 设备性能负载异常”告警；告警具有告警源、告警类型、告警参数等属性，通过合理设置组合告警规则，过滤出满足条件告警，按照聚合方式进行组合告警上告，压缩告警的同时，提供场景化故障分析；1.3syslog 管理：支持 syslog 接收和信息展示；支持 syslog 导出；支持匹配 syslog 信息，将 syslog 升级成告警；	
		报表管理： 1.1 支持报表模板自定义设计，支持报表模板的发布、修改、删除；支持周期报表生成（天、周、月、季度、半年、年），支持多种格式的报表，*.xls、*.csv、*.pdf 等；可以设置周期数据开始日期和报表失效日期；支持周期报表发送到邮件：对生成的报表可以指定策略，使用 Email 转发给指定的地址；支持报表信息查看；系统预置报表：总体运行状态报表（网络设备）、设备通断统计报表、网络设备运行性能报表、资源告警统计报表、资源可用性报表、资源监控统计报表等；	一般
		流程管理： 1.1 支持自定义流程，用户可根据实际需求自定义流程方案；系统预置事件管理、问题管理、变更管理等流程方案；支持工作任务台，提供待办工单、已办工单、新建工单、工单委托等功能；支持操作员流程工单自助台，仅进行流程工单处理操作；支持服务级别管理，主要用于衡量流程指定阶段的处理时间，当时实际时间和设定时间不一致时，会启动邮件通知、修改处理人等升级策略；支持工单处理：接单、转派、挂起、驳回、撤回、委托、会签、关联等操作；支持工单和资源库关	△

		联，实现资源的变更入库等操作；支持工单和知识库关联，用户可以自定义知识分类，将各种经验总结或者流程工单中的知识归档到知识库中，方便后续查阅。流程工单中也可以通过关键字自动搜索知识库，返回结果可以给工单处理做参考；支持数据字典，流程表单编排时可选择数据字典中的数据项作为表单字段内容；	
		网络管控 1.1 网络调控：支持通过各管理域内的网管进行操作，包括接口配置、基础路由配置、设备堆叠和集群配置、链路聚合保护等功能； 1.2 支持针对业务需求，通过路由调整，实现对网络流量路径的调度；	一般
		网络运营-业务保障 1.1 自定义保障拓扑：创建自定义保障拓扑，将保障相关设备、链路加入该拓扑；可实时查看设备基本信息、可达性等；可实时查看链路的可用性、通断状态等；1.2 网络巡检：支持周期性或一次性设备巡检，巡检特性。巡检内容包括硬件、软件、安全及网络状态四大维度，巡检范围至少覆盖现网核心设备，包括但不限于：骨干节点和汇聚节点设备等。支持主流厂商的设备；支持巡检告警总结报告生成，支持巡检明细数据的明细报告生成。报告支持 word、Excel、pdf、html、国产办公软件格式。可自定义巡检场景及部分参数告警阈值；支持网络设备技术公告风险检查。技术公告内容定期进行更新； 1.3 网流业务保障：支持重要活动保障配置，包括保障事件、保障对象(链路、设备、业务)、保障时间、保障人员等；支持对保障范围内链路、设备、业务进行实时监控，支持定期生成活动报告；支持对活动保障期间重点文件的统一管理； 1.4 流量考核：支持对链路带宽利用率、流量趋势、流量存储周期、任意窗口、流量排序、源目的 IP 流量统计、流量趋势预测进行考核；支持系统自检考核指标；支持在线浏览报告、并下载报告；	一般
		网络运营-运营服务 1.1 运营服务：支持北向 Rest 接口，可提供基础网管、准入管理和流量等数据获取和功能调用；	一般

		系统管理 1.1 操作员管理：支持配置操作员名称、密码、姓名、操作员全称、认证方式、手机号、所属组织、关联租户、附加信息等参数；支持操作员的禁用和启用。禁用操作员后，该操作员信息不会删除，但是无法再次登录；支持查看在线操作员，支持强制下线在线操作员；操作员分权管理：基于权限、角色、组织的操作员分权控制，实现系统各功能权限的增删改查细粒度控制，以及资源分权控制；操作员安全：支持用户名+密码和验证码双因子认证；支持 http 和 https 访问；支持 LDAP、RADIUS 等认证方式；支持配置账号密码有效期；支持配置密码策略；支持操作员闲置时长配置；支持基于 IP 和子网的系统访问控制； 1.2 系统管理：支持自定义系统 LOGO、图标和标题、版权信息、登录页背景图等；支持操作日志、系统日志、运行日志的查看和导出； 11.3 备份恢复：支持集群配置备份恢复：支持定时备份、手工备份和手工恢复；支持应用数据的备份和恢复：立即备份、定时备份和手工恢复；	一般
		配置一套基础网管平台，配置不少于 5000 设备管理授权；	△
		支持手工增加设备；支持自动发现设备，自动发现设备任务可立即或周期性执行；	一般
		支持设备基本信息展示：设备标签、管理状态、IP 地址、掩码、sysOID、类型、系统名称、联系人、位置、设备型号、最后轮询时间、接口数量、运行时间、系统描述等；	一般
		支持接口信息展示：展示接口状态、接口描述、接口别名、最后改变时间、光/电口、IP 地址等；	一般
		支持设备导入、导出、管理、取消管理、删除、修改基本信息等；	一般
		支持设备常用操作：Telnet 或 SSH 至设备、打开设备 Web 网管、Ping 和 Tracert 设备；	一般
		支持设备可达性状态探测：当设备不可达时会发出不可达告警，设备状态变为红色，当可达后，发出可达告警，设备状态变为正常；	一般
		支持主流厂商设备；	一般

		支持自定义支持设备：通过自定义设备厂商、设备系列、设备型号、设备类型等内容，实现对设备公有 mib 获取；	一般
		在网络维护期间支持网络设备挂牌。挂牌后，可以选择是否继续采集监控数据、是否产生 Trap、Trap 是否升级告警、告警是否转发；	一般
		支持设备 CPU、内存、响应时间、不可达比例监控；	一般
		支持接口收发速率、带宽利用率、丢包率等指标监控；	一般
		支持显示监控实时数据和历史监控数据，支持最近两小时、最近一天、周、月、自定义时间监控数据查看；	一般
		支持五级阈值设置，当性能指标超过阈值时根据不同的阈值发送不同级别的告警。支持五级告警阈值；	一般
		支持自定义监控模板，关联监控指标和阈值设置；	一般
3.3	山东新一代公安信息网建设——路由器Ⅰ	交换容量≥310Tbps，包转发能力≥76800Mpps；单槽位转发性能可达 2T，线速转发不丢包；	一般
		整机业务载板插槽≥16 个(全尺寸业务卡槽位，非子卡槽位)，配置板卡采用子母卡设计；	一般
		冗余交流电源，支持高压直流供电方式；支持双风扇槽位冗余，设备散热方式采用前后风道散热方式；	一般
		支持 IPv4 和 IPv6；支持 RIP、OSPF、IS-IS、BGP 等路由协议；支持 L2VPN、L3VPN、EVPN 等 VPN 技术；	一般
		支持 LDP LSP、RSVP-TE、SR-TE 等 MPLS 技术；支持 VXLAN、GRE 等隧道技术；支持智能隧道 CBTS 功能；	一般
		支持基于硬件的 BFD 故障探测技术，支持最小发包间隔 5ms；支持全面的快速重路由 FRR 功能：	一般
		支持 5 级 H-QoS 调度；	一般
		设备支持 100GE/40GE/25GE/10GE/GE/FE 等接口模块；	一般

		支持 VRRP、Eth-Trunk、E-Trunk、ECMP、UCMP 等可靠性技术；	一般
		支持 Telemetry 高速数据采集技术，可实现大数据分析对专线质量进行追踪；支持 SRv6 技术，提供向下一代极简网络演进功能；	一般
		考虑安装及日常维护方便，所有主控板、交换网板和业务板全部是前插板；	一般
		嵌入式电源系统，实现交流输入转换为稳定的 48V 直流输出，支持 2kW 整流模块，最大输出功率 4kW；支持热插拔，系统高度 1U，支持标准 19 英寸机架或嵌入式机柜等多种安装方式；系统可适应宽范围交流输入，具备智能化蓄电池管理、远程监控等功能；支持空开热插拔；支持电源模块热插拔；智能化蓄电池管理和电池保护；支持环境监控，可通过干接点、串口或网络接口实现远程管理；	一般
		本次配置：双引擎、四交换网板、配置≥8 块电源，万兆光接口板≥48 个，为保证业务可靠性，需要不少于 2 块业务板分散部署，配置≥20 块万兆单模 10KM 光模块,配置≥8 块万兆单模 40KM 光模块，嵌入式直流电源系统×2	△
3.4	山东新一代公安信息网建设——路由器 II	交换容量≥160Tbps，包转发能力≥38400Mpps；单槽位转发性能可达 2T，线速转发不丢包；	△
		整机业务载板插槽≥8 个(全尺寸业务卡槽位，非子卡槽位)；配置板卡采用子母卡设计；	一般
		冗余交流电源，支持高压直流供电方式；支持双风扇槽位冗余，设备散热方式采用前后风道散热方式；	一般
		支持 IPv4 和 IPv6；支持 RIP、OSPF、IS-IS、BGP 等路由协议；支持 L2VPN、L3VPN、EVPN 等 VPN 技术；	一般
		支持 LDP LSP、RSVP-TE、SR-TE 等 MPLS 技术；支持 VXLAN、GRE 等隧道技术；支持智能隧道 CBTS 功能；	一般
		支持基于硬件的 BFD 故障探测技术，支持最小发包间隔 5ms；支持全面的快速重路由 FRR 功能：	一般
		支持 5 级 H-QoS 调度；	一般

		设备支持 100GE/40GE/25GE/10GE/GE/FE 等接口模块；	一般
		支持 VRRP、Eth-Trunk、E-Trunk、ECMP、UCMP 等可靠性技术；	一般
		支持 Telemetry 高速数据采集技术，可实现大数据分析对专线质量进行追踪；支持 SRv6 技术，提供向下一代极简网络演进功能；	一般
		考虑安装及日常维护方便，所有主控板、交换网板和业务板全部是前插板；	一般
		配置双引擎、双交换网板、配置≥4 块电源，配置≥2 块 12 口万兆光接口板，配置≥6 块万兆多模光模块，≥6 块万兆单模光模块 40KM,≥8 块万兆单模光模块 10KM。	△
3.5	#大数据中心（数据域部分）——数据分析智能工具	#数据分析智能工具： 1、提供数据分析智能工具，实现态势感知、时空分析、虚实对应、独立分析、全局扩线等智能工作功能，整合调用大数据平台各类数据资源和服务资源以数据分析智能工具应用系统形式对外提供服务，数据分析智能工具安装部署及后续扩展使用时无授权数量限制。 （1）提供时空分析功能，实现时空大数据可视化展示、时空轨迹分析应用等。利用现有 PGIS 体系和时空数据资源，构建时空轨迹分析体系，时空分析与数据分析、对象分析组合使用，实现对数据的深度挖掘，并对外提供服务，时空分析在 5000 个节点图上作战进行地图展示时，响应时间不大于 5 秒。 （2）提供关系分析功能，实现添加关系、关系扩展、关系展示布局、关系收回、关系演变、事件还原、关系筛选等功能并对外提供服务。 （3）提供行为分析功能，以轨迹时间轴方式展示与关系要素信息等行为联动分析。提供基于时间点、时间段、行为类型等维度开展自主分析并对外提供服务。 （4）提供多维分析功能，按照多种标签作为分析维度条件，实现多种标签进行组合查询，开展以标签为元素的多维分析并对外提供服务。 （5）提供全息画像功能，实现人员画像、车辆画像、手机画像、组织画像、案事件画像以及全息画像的可视化配置。提供全息画像可视化配置功能，对画像展示内容进行自定义增、删、改配	△

		置。按照展示内容的差异性，支持包括但不限于基本信息、普通栏目、统计栏目、轨迹栏目、相关栏目、引用栏目、同关注栏目的呈现并对外提供服务。（6）提供数据分析项目空间管理功能，实现数据、要素、关系、权限等的项目内容管理。根据不同数据分析场景，提供个性化配置功能并对外提供服务。	
3.6	新一代移动警务部分（一期）——核心交换机	框式交换机，模块化设计，可扩展交换容量设计；双主控、双电源、冗余风扇；	一般
		默认配备 48 个 10/100/1000Base-T 自适应端口以太网电接口板，24 个 100/1000Base-X 以太网光接口板，2*48 端口万兆以太网光接口板，配套 24 个 eSFP 千兆多模模块，96 个 10G 多模光模块；	一般
		专用双机冗余模块和线缆。	一般
		和现有移动信息网核心交换机组建双机冗余互备	一般
		交换容量≥19.84Tbps，包转发率≥2880Mpps，6 个扩展业务槽；	一般
3.7	新一代移动警务部分（一期）——汇聚交换机	10GE 光口≥48 个，40GE/100GE 光口≥6 个，10GE 多模光模块≥48 个，配置 40GE 堆叠高速线缆≥1 根；	一般
		支持冗余电源，电源槽位数≥2 个，配置电源个数≥2 个，风扇框个数≥4 个；	一般
		支持灵活的前后/后前风道设计；	一般
		交换容量≥4.8Tbps，包转发率≥2000Mpps；	一般
		IPv4 路由表项≥40K，IPv6 路由表项≥40K；	一般
		支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议；	一般
		支持 VxLAN 功能，支持 BGP EVPN；	一般
		支持 SNMPv1/v2c/v3，支持 RMON；	一般
		支持基于 MAC/协议/IP 子网/策略/端口的 VLAN；	一般
		支持 G.8032（ERPS）标准环网协议；	一般
		支持支持 IGMP Snooping；	一般
3.8	新一代移动警务部分（一	GE 电口≥12；GE 光口≥8；10GE 光口≥4，支持 USB3.0，配置 10GE 多模模块≥4 个，GE 单	一般

	期）——万兆下一代防火墙	模模块≥4 个；	
		支持配置双电源，三风扇，风扇支持热插拔；	一般
		支持前后风道；	一般
		吞吐量≥20Gbps，最大并发连接数≥800 万，每秒新建连接数≥20 万，配置 IPS 入侵防御功能（永久授权），配置威胁防护特征库升级授权≥3 年；	一般
		IPSec 吞吐量≥20Gbps，SSL_VPN 吞吐量≥2Gbps，SSL 代理吞吐量≥3Gbps，IPS 吞吐量≥8.8Gbps；	一般
		支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议；	一般
		能够基于 IP、IPv6、MAC 地址、时间进行访问控制策略控制;支持自定义安全策略，安全策略组功能；支持策略冗余/命中分析；	一般
		支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议；	一般
		支持全面 NAT 功能，对多种应用层协议支持 ALG 功能，包括 ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS 等；	一般
		支持对 HTTPS，POP3S，SMTPS,IMAPS 加密流量代理解密后，并进行内容过滤，审计，安全防护；	一般
		支持 DNS 过滤，提高 WEB 网页过滤的性能；	一般
		支持 U 盘升级。	一般
3.9	新一代移动警务部分（一期）——万兆三层交换机	GE 电口≥24 个，10GE 光口≥12 个，配置 10GE 多模模块≥8 个；	一般
		支持可拔插冗余电源，电源槽位≥2 个；	一般
		采用前后风道方式；	一般
		交换容量≥2.56Tbps，包转发率≥660Mpps；	一般
		支持静态路由、RIP v1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+；	一般
		支持 DHCPv4/v6 client/relay/server/snooping；	一般
		支持策略 VLAN，支持 MUX VLAN；	一般
		支持 PIM DM、PIM SM、PIM SSM，支持 IGMP v1/v2/v3 及 IGMP v1/v2/v3 Snooping 及 IGMP	一般

		快速离开机制；	
		支持 DHCP Snooping 等安全特性；	一般
		支持 Telemetry 技术；	一般
		支持 MACSec 加密技术。	一般
3.10	新一代移动警务部分（一期）——探针	4 个千兆 RJ45 网口，电源：工业电源	一般
		采集通用网络设备的运行状态，包括 CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等。	一般
		采集服务器的运行状态，包括 CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等。	一般
		采集通用安全设备的运行状态，包括 CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等。	一般
		采集专用安全设备的运行状态，包括 CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等，专用安全设备的业务日志信息。	一般
		采集系统本身的业务运行日志、管理员管理操作日志以及系统告警信息等。	一般
		支持对采集的数据按照后台系统提供的规则进行数据清洗、整理、抽取、归一、统计、分析等基本数据处理。	一般
		支持省厅移动警务平台的统一运维系统，并支持数据上报、分析与管理。	△
3.11	新一代移动警务部分（一期）——视频安全传输系统（万兆）	由用户认证服务器、隔离设备、设备认证服务器三部件组成；	一般
		安全通道最大带宽:7Gbps；	一般
		高清最大并发数（4Mbps）:1750 路；标清最大并发数（2Mbps）:3500 路；视频数据误码率<0.5%；视频流传输时延<50ms；	一般
		支持信令双向传输，视频数据双向传输，对内外网数据均有安全检查机制；	一般
		基于零反馈单向传输硬件和双芯普通模块实现视频数据双向传输；	一般
		支持基于公安数字证书、用户名/密码方式的身份认证机制；	一般
		支持多种数据检查，包括数据源、病毒木马及	一般

		关键字扫描（C/S 客户端模式）等；	
		支持多种协议格式检查，包括视频信令协议格式（SIP）、视频传输协议格式及主流视频监控公司的私有协议视频信令协议格式等；	一般
		支持对视频资源的访问控制，能够对用户、设备的细粒度授权访问管理；	一般
		支持流量审计、设备访问审计、告警审计等多种日志审计与告警功能，支持与集中监管与审计系统联动；	一般
		支持国标模式多个下级域平台对应一个上级域平台的汇聚业务；支持国标模式一个下级域平台对应多个上级平台的共享业务；	一般
		同时支持 C/S 客户端模式和平台级联模式；	一般
		支持 GB/T 28181-2011 标准的平台对接；	一般
		支持 GB/T 28181-2016 标准的平台对接。	一般
		支持省厅移动警务平台已建的级联上报系统，按照公安部移动警务规范要求，纳入省、部监控平台统一监控、审计与管理。	△
3.12	新一代移动警务部分（一期）——单向安全传输系统（万兆）	由导入前置机、隔离设备、导入服务器三部件组成；	一般
		吞吐量≥2.5Gbps(ftp-cc 模式)；	一般
		文件传输性能（5KB 小文件）:3000 个/秒（ftp-cc 模式）；	一般
		支持任务数≥32；	一般
		数据库到数据库交换记录数:3000 条/秒；	一般
		支持 FTP 协议。	一般
		支持 SAMBA 协议。	一般
		支持 NFS 文件服务端至服务端（SS）传输模式；	一般
		支持对病毒扫描功能，能够将病毒文件禁止传输。支持抗 DDOS 攻击功能。	一般
		支持防止非法用户采用 SQL 注入手段入侵系统。	一般
		支持白名单功能，阻止不匹配的设备连接。	一般
		支持文件自动重传功能；	一般
		支持对文件数据的加密、解密；支持 15 种文件格式的检查、关键字内容过滤；	一般
		支持国产数据库、Oracle8i、9i、10G、11G、	一般

		12C 和 SQL Server2000、2005、2008、MySQL5.6 及以下版本数据库同步，包括同构全量、增量同步和异构全量、增量同步。其中，异构支持不同表名、不同字段名和不同字段类型的数据同步（同步的字段类型须相近，源端字段长度须小于或等于目标端字段长度）；	
		支持业务服务器 IP 地址绑定的接入认证；支持导入前置机和导入服务器间的唯一性认证；	一般
		支持系统管理员、安全管理员、审计管理员三级权限；	一般
		支持管理界面以用户名/口令方式访问；支持鉴别失败处理机制及超时重鉴别机制；	一般
		支持业务流量统计功能；支持对通道故障进行报警；	一般
		支持数据业务监控、安全审计与告警以及运维监控管理和上报监管。	一般
		支持省厅移动警务平台已建已建的级联上报系统，按照公安部移动警务规范要求，纳入省、部监控平台统一监控、审计与管理。	△
3.13	新一代移动警务部分（一期）——抗 DDOS	配置双电源模块，电源支持热插拔；	一般
		严格前后风道；	一般
		配置 3+1 冗余风扇，风扇支持热插拔；	一般
		主机：GE 的 Combo 口≥8 个，GE 电口≥4 个，10GE 光口≥10 个，配置外置 bypass 设备，10GE 多模模块≥22 个，配置 IPS 入侵防御功能（永久授权），配置特征库升级授权≥3 年；	一般
		检测吞吐量≥18Gbps；	一般
		每秒新建连接数≥50 万，最大并发连接数≥2000 万；	一般
		支持双机热备，支持主主部署模式、主备部署模式；	一般
		支持 SYN Flood、SYN ACK、UDP Flood 等 DDoS 防护，支持 HTTP Flood、 HTTPS Flood 等应用层 DDoS 防护；	一般
		支持对 SMTP、POP3、HTTP、FTP 协议实现病毒扫描检测；	一般
		支持≥6000 种的应用识别能力；	一般

		系统预定义入侵防御签名库数量不得少于10000条且具备CVE和CNNVD编号的签名条目数不得少于8000，支持用户自定义签名规则，支持正则表达式；	一般
		支持静态路由、策略路由，OSFP、BGP、ISIS等路由；	一般
3.14	新一代移动警务部分（一期）——WEB应用防火墙	专业性WEB应用防火墙设备及专业性WEB应用防火墙资质，而非NGAF、NGFW、UTM设备配置模块；	一般
		GE电口≥2个，GE光口≥4个,10GE光口≥4个，支持1+1冗余电源，配置电源个数≥2个，10GE多模光模块≥4，GE多模光模块≥4个，配置特征库升级授权≥3年；	一般
		网络吞吐量（Mbps）≥10Gbps，HTTP应用层吞吐≥8Gbps，HTTP最大并发连接数≥50万，HTTP最大新建连接数≥4万，TPS每秒事务处理数≥6万，业务时延小于<50ms；	一般
		支持多条链路数据的防护，防护网段数量不限，站点数量不限制；支持旁路部署；	一般
		支持WEB缓存、WEB压缩、WEB访问审计、负载均衡，高性能白名单安全识别模块、自学习建模模块、智能攻击者锁定模块、应用层CC防御模块。	一般
3.15	新一代移动警务部分（一期）——安全准入系统	MGMT接口≥1个，GE接口≥4个，GE光口≥4个，10GE光口≥2个；Bypass接口2组；RJ45串口≥1个， MGMT(RJ45)≥2个；	一般
		支持冗余电源；	一般
		应用层吞吐量≥8G，最大接入终端数≥10000，并发视频终端数≥2000；	一般
		支持符合公安部标准要求的智能手机型、便携式微型计算机型和5G物联网扩展智能设备等多形态警务终端的接入管控；	一般
		支持扩展基于国产密码算法的密钥系统的联动认证；	一般
		支持部署模式：网桥模式、路由模式、旁路模式、混合模式、支持主/备、主/主 HA、分布式部署、集群部署；	一般
		支持管理方式：WEB管理、SSH管理、Console管理、网管策略；	一般

		支持资产管理方式：IP/MAC 绑定、终端特征绑定、账号密码认证、一机一档；	一般
		支持入网审批功能：入网设备事前审批；	一般
		支持终端准入功能：基于 IP、MAC、接入设备特征、应用协议等多重属性自动注册准入；发现私接/仿冒/非法接入行为即时报警，并记录痕迹；	一般
		支持防火墙功能：状态监测防火墙、协议识别，允许系统认可的应用协议通过，阻断其它应用协议。	一般
3.16	新一代移动警务部分（一期）——智能流量管理器	设备支持 48 个 10GE（光口）SFP/SFP+可插拔光模块（兼容万兆光模块、千兆光模块、千兆电模块，自定义输入/输端口数量）；	一般
		自适应千兆速率；总监控流量达 480Gbps 输入+480Gbps 输出，共 960Gbps 吞吐量。	一般
		流量分发：按照用户指定的特征对镜像流量进行分类，转发到目的端口，实现一分多的流量分发。	一般
		流量聚合：将输入的多条镜像流量汇聚在一起，转发到一个或者多个目的端口，实现多路流量的聚合分析。	一般
		流量分流：将输入镜像流量，按照用户指定的 hash 策略，分别送往不同的端口，这些端口属于同一个分流组。	一般
		流量去重：对输入的多个重复镜像流量进行处理，仅保留 1 个镜像流量，其余的丢弃。	一般
		流量截取：对镜像流量的数据包截取，能按照 64 字节、128 字节自定义传输数据包长度。	一般
		流量 IP 地址过滤：按照 IP 地址规则，对输入的每个镜像流量进行匹配，若符合规则即为命中。命中后可以将该流量转发或者丢弃，取决于用户配置。	一般
		流量协议过滤：按照协议规则，对输入的每个镜像流量进行匹配，若符合规则即为命中。命中后可以将该镜像流量转发或者丢弃，取决于用户配置。这里的协议可以是 L2~L4 低层传输协议，也可以是 L5~L7 高层应用协议。	一般
		流量清洗：对指定特征的流量进行丢弃处理，最多支持 4K 条五元组清洗配置策略，且不影	一般

		响设备线速采集性能。	
		流量统计：对设备上每个端口每种特征的输入、输出流量进行统计，如报文数量、字节数量、吞吐量、错包等。	一般
		流量上报分析：支持将预处理的流量上报省厅已建设的网络全流量安全分析系统，进行深度流量分析和安全检测。	一般
3.17	新一代移动警务部分（一期）——物理服务器扩展升级	支持现有服务器硬件扩展。 每台扩展系统盘 2 块 240G SSD,数据缓存盘 2 块 960G SSD,1 个 4 口万兆光 PCIE 网卡（含 4 个 10G 多模光模块和 OM3-3M 光纤 4 对）	一般
3.18	新一代移动警务部分（一期）——移动云计算超融合软件升级	配套超融合虚拟化软件包含计算、存储、网络虚拟化和升级维护服务 3 年;	一般
		支持计算虚拟化、存储虚拟化、网络虚拟化功能；兼容 INTEL XeonE7-4809V2/XeonE7-4809V4 CPU；内存虚拟化支持≥512GB；存储虚拟化支持≥8*900G SAS 硬盘，支持固态硬盘数据加速功能。超融合虚拟机可以实现物理机的全部功能，如内存、CPU、网卡、存储，可以指定单独的 MAC 地址等。	一般
		采用分布式管理架构，去中心化，管理平台不依赖于某一个虚拟机或物理机部署，由多台物理服务器组成分布式存储集群，通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out 架构），扩容过程保证业务零中断。	一般
		支持部署虚拟分布式交换机、虚拟路由器、分布式防火墙，提供≥100 个虚拟路由器，≥100 个分布式交换机的永久授权，虚拟机数量授权不限。每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括 Windows、Linux，并且支持国产操作系统。	一般
		支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加 CPU 和内	一般

		存资源，确保业务持续高效运行。	
		支持对超融合平台的硬件进行监控和大屏展示，包含 CPU，内存，网卡，硬盘，存储，RAID 等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议 。	一般
		支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员。	一般
		为避免主机假死导致系列问题发生，支持识别假死主机并标签化为亚健康主机，并提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险。	一般
		在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。	一般
		主动探测业务系统，实时监控业务可用性，监控策略包括 HTTP、FTP、POP3、SMTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障。	一般
		存储虚拟化要求配置按 CPU 个数的存储虚拟化授权；支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用 License 激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能	一般
		支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性；支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中 IO 性能占用导致对业务的性能造成影响；支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性。	一般
		支持条带化功能，实现分布式 raid0 的性能提	一般

		升效果，并且支持以虚拟磁盘为单位设置不同的条带数。	
		为了便于部署关键业务系统，虚拟存储可支持 Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度。	一般
		支持以磁盘为单位创建分卷，可将集群内固态硬盘组成一个高性能全闪存存储池，满足高性能应用需求，将固态硬盘和机械硬盘组成一个大容量混合存储池，满足普通应用需求，以更低成本灵活满足不同业务对存储性能容量的不同需求，并降低故障影响范围；支持在同一个存储池（卷）内，针对不同的虚拟机或虚拟磁盘设置不同的副本数，灵活地满足用户的可靠性需求。	一般
		支持坏道扫描功能，由用户设置扫描的时间段定期对集群的硬盘进行扫描，及时发现潜藏的坏道；支持智能坏道预测，准确识别出接下来会出现坏道的硬盘，实现故障前预测并处理，规避故障风险 。	一般
		支持硬盘容量预测功能，并可根据客户设置的阈值进行容量告警，为用户扩容提供指导，并避免使用过程中突然出现容量不足问题 ；支持智能预测硬盘寿命，并预估硬盘剩余可使用时间，进行实时预警，提醒用户在寿命到期之前可实现在对业务无影响的情况下安全更换硬盘 。	一般
		支持对虚拟机或虚拟磁盘设置不同的缓存 QoS 能力，区分出高性能虚拟机、普通性能虚拟机和低性能虚拟机。	一般
		支持针对虚拟机或虚拟磁盘设置数据分布策略，当采用副本聚合策略时，可以保证以性能优先为原则，实现 IO 本地读效果，当采用副本散列策略时，可以保证虚拟机以分布均匀优先为原则，打散分布均匀在各物理主机上。	一般
		支持单节点的一块或多块缓存盘（SSD）拔出后，集群内所有的虚拟机正常运行未出现中断，其中一台虚拟机硬盘拔出前后磁盘读写（IO）性能少幅下降，或几乎没有下降。	一般
		支持云安全功能：超融合自带分布式防火墙，并可扩展支持云安全服务（包括云堡垒机管	一般

		理、云漏扫、系统安全加固、日志审计等安全组件）。	
		支持与部级、省级移动警务 II 类区安全感知平台联动，无需二次开发，实现当发生僵尸网络、勒索病毒、挖矿安全事故时，实现自动隔离中毒云主机，并提供故障前一刻的业务安全状态供恢复，将安全事故损失最小化。云安全联动支持将病毒虚拟机进行关机或挂起，避免挖坑云主机消耗整个平台的性能。	一般
3.19	新一代移动警务部分（一期）——移动云计算安全网络防护	2U 标准设备，CPU：2 颗 Silver 4210R 2.40 GHz（10C），内存：≥3*32GB DDR4 2666，系统盘≥1*128GB SATA SSD，缓存盘≥1*240GB，数据盘≥2*4TB，标配盘位数≥8，冗余白金电源，≥6 千兆电口。支持双机备份，保障安全组件高可用。	一般
		云安全主机本次共提供 5 个安全组件的通用授权，包括虚拟下一代防火墙、虚拟运维安全管理（堡垒主机用户授权不小于 100）、虚拟日志审计（日志审计不小于 150 点）、虚拟 WAF、虚拟负载均衡功能，保障业务的高安全性。	一般
		支持虚拟安全扩展，可通过追加授权方式扩展云安全服务功能，包括虚拟 IPS、虚拟上网行为管理、虚拟 SSL VPN、虚拟数据库审计、虚拟漏洞扫描、终端安全检测与响应、虚拟 WAF、网页防篡改等独立的安全组件。	一般
		支持集成第三方生态产品以扩充平台安全能力。	一般
		支持云计算平台安全联动功能，支持超融合云计算平台安全联动，实现当发生僵尸网络、勒索病毒、挖矿等安全事故时，实现自动隔离中毒云主机，并提供故障前一刻的业务安全状态供恢复，将安全事故损失最小化。云安全联动支持将病毒虚拟机进行关机或挂起，避免挖坑云主机消耗整个平台的性能。	一般
		支持省级移动警务 II 类区安全态势感知平台一键下发安全策略到下一代防火墙和终端安全检测与响应功能模块进行联动处置；同时支持安全组件与公安部本级移动警务平台数据审计系统对接，不需要二次开发，可支持上报安全	一般

		监测数据。	
		支持联动安全感知能力，可联动部、省移动警务平台态势感知平台最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则，能够及时的进行安全防护，全面保障业务的安全。	一般
		支持独立的 Web 应用防护规则库，具备独立的僵尸主机识别特征库。	一般
		支持在系统界面上以滑尺方式动态分配安全组件的性能规格，同时支持已分配组件规格的动态变更和授权回收，回收后的授权可以分配给其他用户和其他类型的安全组件使用。平台能够提供处理性能灵活分配的安全组件，单组件应用层最大吞吐量可达 7Gbps（单向），最小可达 5Mbps(单向)。	一般
		支持基于云平台整体视角的安全运营中心，能够统一监测和收集安全事件，从移动警务联网子平台维度实现安全风险统一管理，并且能够通过大屏进行投放，展示安全资源池的运营情况。	一般
		支持基于移动警务联网子平台视角的安全运营中心，能够统一监测和收集各安全组件的日志，从业务系统维度实现安全风险统一管理，并且能够通过大屏进行投放，实现市级移动警务联网子平台安全集中可视化。	一般
		支持以月、周为单位定期生成市级移动警务联网子平台的 PDF 安全报表，包括业务的风险情况，及运维人员的服务情况，提升移动警务联网子平台的服务感知。支持在平台首页上显示安全感知平台的威胁中心信息摘要。	一般
		支持在首页整体展示全部业务系统的风险状态，包括业务风险分布、风险业务 TOP5、安全事件列表（包括失陷事件、攻击事件和漏洞事件）等。	一般
		平台侧界面支持在首页监测安全资源池集群状态（包括总计算资源、总内存资源及总存储资源）和安全风险状态，安全风险能够体现全部业务的风险分布。	一般
		支持分布式部署多套安全资源池的集中运维，在主节点上可集中查看分支节点的资源利用率	一般

		（包括 CPU、内存、磁盘利用率），并对授权池服务到期，网络故障以及主机资源不足的节点进行集中告警，支持在主节点上直接管理分支节点。	
		平台侧界面支持安全组件分配功能，管理员可直接为云平台分配安全资源，同时完成关键安全资源的策略初始化。	一般
		支持移动警务联网子平台安全资源的服务链配置，通过灵活选择源、安全服务节点和目的，完成安全路径的自定义，安全服务节点的先后顺序可灵活调整。	一般
		支持对安全组件单独升级，交付最新功能版本，无须对平台软件进行升级。支持批量升级平台安全组件，提高运维效率。	一般
		支持通过 netconf 协议接管交换机，自动配置引流策略，同时支持跟随移动警务联网子平台业务变化，自动更新对应交换机的策略。	一般
		支持对云安全服务平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。	一般
3.20	新一代移动警务部分（一期）——移动云计算服务器主机安全管理	服务支持云化部署，并支持通过云安全服务平台进行统一的服务管理。支持云虚拟机和物理机系统安全加固，本次提供不少于 300 点系统安全加固授权，病毒库更新持续不少于 3 年。	一般
		支持与省级移动警务 II 类区安全态势感知平台进行安全联动，支持管理员在安全感知平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置；支持将主机安全加固系统采集终端资产信息（包括操作系统、硬件、软件、账户、监听端口、运行进程等）上报省级移动警务 II 类区安全态势感知平台，并由省级移动警务 II 类区安全态势感知平台统一组织主机资产的可视化呈现。	一般
		支持管理员在省级移动警务 II 类区安全态势感知平台管理界面下发一键隔离指令，对终端所有连接进行阻断，防止病毒进一步扩散。	一般
		省级移动警务 II 类区安全态势感知平台检测到某主机访问僵尸网络恶意域名时，联动主机安全加固系统定位到该主机上发起恶意域名访	一般

		问的具体进程、及其进程链信息，并且省级移动警务 II 类区安全态势感知平台根据主机安全加固系统返回的举证信息，联动主机安全加固系统对恶意进程进行处置。	
		支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到省级移动警务 II 类区安全态势感知平台进行分析和展示。	一般
		支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端。	一般
		支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录。	一般
		支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示。	一般
		支持资产登记功能，支持录入本终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，并可设置哪些为必填项，以便于进行终端资产管理。	一般
		支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户。	一般
		支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议。	一般
		支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔	一般

		离。	
		支持对服务器重要目录进行权限控制，仅允许配置的可信进程操作该目录并提供配置指引；提供基于可信鉴定方式的进程防护方式，通过人工智能自学习机制，自动建立信任进程名单，阻断非可信进程的运行并提供配置指引，同时支持通过模板和手动的方式添加信任进程。	一般
		基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。	一般
		支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截。	一般
		支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息	一般
		一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、SSH 策略检测、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。	一般
		支持对操作系统停更的系统提供专项防护，包括 0day 漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；支持对已停止更新的操作系统的全网一键清点，管理员可快速筛选出全网已停止更新的操作系统的数量和具体的终端；支持基于应用、端口和账号的清点，可辅助客户进行已停更操作系统的风险识别。	一般
		支持基于 IP（组）、服务和角色维度进行配置项设置，并且支持对配置项的备份以及恢复操作。	一般
3.21	新一代移动警务部分（一期）——移动	高速通讯接口，内置智能芯片，具有智能 IC 卡操作系统的所有功能，用户存储空间为 64K，用于安全存储个人信息、密钥、数字证	一般

	警务数字证书USB-KEY	书。	
		支持公私钥算法及其密钥对生成，可实现签名/验证、身份识别功能，支持摘要算法。	一般
		支持国家安全密码管理委员会批准的国产密码算法 SM1、SM2、SM3、SSF33 算法，实现加密解密算法。	一般
3.22	新一代移动警务部分（一期）——应用安全认证网关	网络接口：6 个千兆电口，可扩展支持光口（不含光模块），冗余电源	一般
		最大新建连接数（SM2）：5000 次秒；每秒交易数(TPS)：25000 次/秒;最大并发连接数：10000;最大流量：1000Mbps。	一般
		支持兼容移动警务 PKI 系统为移动应用系统提供基于数字证书的身份认证与访问控制服务。	一般
		支持多种认证策略方式、使用的协议、加密强度、以及是否传递相关信息等进行满足不同的公安业务需要。	一般
		支持多应用类型，对 B/S、C/S 应用进行安全防护。	一般
		支持多服务功能，支持创建多个 SSL 服务，保护不同的应用服务，也支持同一个 SSL 服务保护多个应用服务。	一般
		支持认证服务正反代理连接模式，自定义数据流向，同时支持多种协议类型及多个认证服务，可根据业务实际需求可灵活多变支持。	一般
		支持证书信息绑定，将信息绑定到 cookie、URL 和 HTTP 的位置，也可绑定文件类型，支持自定义，显示对绑定内容和站点列表的查看。	一般
		支持应用访问控制策略管理，灵活的角色白名单规则设置，基于角色类型、角色信息属性等；与应用进行关联绑定，通过对应用类型、应用 IP、应用端口、授权角色进行权限策略统一下发管理。	一般
		支持与省厅 PKI 系统平台兼容对接，同步获取证书 CRL 吊销列表及黑名单，对用户证书有效性验证。提供黑名单服务配置、LDAP 服务配置、黑名单上传下载配置、黑名单自动更新、黑名单管理服务。	一般
		支持与移动警务证书服务兼容，能够解析由省	一般

		厅移动警务证书系统签发的证书信息，进行认证鉴别服务。	
		支持与省厅认证平台兼容对接，同步认证策略至本地，实现认证策略一致性，跨域访问认证。	一般
3.23	新一代移动警务部分（一期）——发证安全接入网关	含 2 台服务器密码机和 2000 套移动警务智能手机终端可信根(芯片类型)组件。	△
		服务器密码机规格：网络接口：RJ-45 10/100/1000Mb x3,双模块冗余电源，MTBF 大于 50000 小时;	一般
		服务器密码机 SM1 算法加解密速率：500Mbps	一般
		服务器密码机 SM4 算法加解密速率：900Mbps	一般
		服务器密码机 SM2 密钥对产生速率：30000 对/秒	一般
		服务器密码机 SM2 签名速率：30000 次/秒；SM2 验签速率：20000 次/秒	一般
		服务器密码机 SM2 算法加密速率（256 字节）：15000 次/秒；SM2 算法解密速率（256 字节）：22000 次/秒	一般
		服务器密码机 SM3 计算 Hash 速率（4K 字节）：900Mbps	一般
		服务器密码机随机数产生性能：30Mbps	一般
		服务器密码机,密钥生成采用由国家密码管理局批准使用的双物理噪声源生成随机数，可生成各类对称密钥（SM1、SM4 等）和非对称密钥（SM2 等）	一般
		服务器密码机密钥安全存储，设备内部支持 500 个对称密钥和 200 个非对称密钥的安全存储	一般
		服务器密码机密钥销毁，支持通过管理界面删除指定的对称或非对称业务密钥，也支持销毁全部业务密钥	一般
		服务器密码机密钥更新，支持各类对称密钥和非对称密钥的更新	一般
		服务器密码机密钥备份与恢复，采用基于密钥分割的方式备份密钥和安全数据，保障备份数据的安全性	一般
		服务器密码机采取高强度的密钥分割算法，只有满足最少数量的管理员才能进行恢复操作，	一般

		备份密钥可恢复到相同型号的其它加密机设备中	
		服务器密码机多级密钥管理体系，支持主密钥/密钥保护密钥/数据加密密钥三级密钥保护模式，以及主密钥/数据加密密钥二级密钥保护模式	一般
		服务器密码机全面支持国产密码算法以及常用国际密码算法，包括 SM1、SM2、SM3、SM4 等	一般
		服务器密码机提供符合《GB/T 36322-2018_信息安全技术 密码设备应用接口规范》的标准化接口，接口支持 C、Java、Python、Go 等主流编程语言，便于应用厂商进行开发和集成	一般
		移动警务智能手机终端可信根支持具有可信执行环境（TEE）和安全芯片（SE）功能的专用移动警务终端，通过移动警务 PKI 空中发证功能向安全芯片（SE）签发国密证书，提供原厂技术承诺。	一般
		移动警务智能手机终端可信根支持遵循国密规范标准 SDK 接口	一般
		移动警务智能手机终端可信根支持国密 SM2、SM3、SM4 密码算法支持和密钥管理	一般
		移动警务智能手机终端可信根支持符合 GB/T 1466.1 标准的多模国密可信根证书签发，满足用户要求，对新机型适配。	一般
3.24	新一代移动警务部分（一期）——证书从目录服务	在线精确查询时间（百万级）：单线程响应时间＜1 毫秒，50 线程响应时间＜20 毫秒	一般
		在线模糊查询时间（百万级）：单线程响应时间＜130 毫秒，50 线程响应时间＜300 毫秒	一般
		吞吐量 100 万条目：≥2500 次/秒（50 线程精确查询）	一般
		最大并发连接数＞1000	一般
		支持国密 SM2 算法数字证书，CRL 及目录服务地址等证书目录数据对外发布，支持主从部署模式及级联同步功能	一般
		支持 LDAP V2、V3 标准，支持标准的 LDIF 格式	一般
		支持 PKI 的相关标准，支持 X.509 V3 标准	一般
		支持主从结构，支持一主一从，一主多从多种布署方式	一般

		提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力	一般
3.25	山东省公安信息网大数据智能化安全体系（一期）——后端接入防火墙	1、主控板、接口板和业务板分离，实配双主控，除两个主控板外，整机业务扩展插槽≥4，双电源； 2、10GE 光口≥24 个，100GE 光口≥2 个，配置 10GE 多模光模块≥24 个，100GE 多模光模块≥2 个； 3、防火墙吞吐量≥120Gbps，IPS 吞吐量≥36Gbps，整机最大并发连接可扩展到≥4.8 亿，整机每秒新建连接数可扩展到≥1200 万； 4、支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议、IPv6 over IPv4 隧道、6RD 隧道等。	一般
3.26	山东省公安信息网大数据智能化安全体系（一期）——VPN 网关	1、交换容量≥200Tbps，包转发率≥48000 Mpps； 2、业务槽位数≥4，交换网槽位数≥2，且支持网板 N+M 冗余； 3、本次配置 40GE-QSFP+端口≥20 个，万兆光口端口≥48 个，配置 40G 多模光口模块≥16 个,万兆多模模块≥20 个，配置双引擎、2+2 冗余电源，满配交换网板。	一般
3.27	山东省公安信息网大数据智能化安全体系（一期）——入侵防御	1、千兆电口≥4 个，千兆光口（含光纤模块）≥4 个，万兆光口（含光纤模块）≥4 个，双电源； 2、IPS 检测吞吐量≥12Gbit/s，每秒新建连接数 ≥25 万，最大并发连接数≥1000 万； 3、准确检测并防御针对操作系统、应用、服务器等各种漏洞的攻击，支持 0 day 攻击防护。	一般
3.28	山东省公安信息网大数据智能化安全体系（一期）——前端接入防火墙	1、主控板、接口板和业务板分离，实配双主控，除两个主控板外，整机业务扩展插槽≥4，双电源； 2、10GE 光口≥24 个，100GE 光口≥2 个，配置 10GE 多模光模块≥24 个，100GE 多模光模块≥2 个； 3、防火墙吞吐量≥120Gbps，IPS 吞吐量≥36Gbps，整机最大并发连接可扩展到≥4.8 亿，整机每秒新建连接数可扩展到≥1200 万； 4、支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议、IPv6 over IPv4 隧道、6RD 隧道等。	一般
3.29	山东省公安信息网大数据智能化安全体系（一期）——	1、支持 HTTP/HTTPS API 数量≥1024，最大吞吐量≥20Gbps，加密吞吐量（包括国密）≥5Gbps，并发连接数≥50000； 2、支持加密流量解密、检查与控制、令牌检查与控制、协	△

	可信 API 代理	议格式检查与控制、业务应用访问权限检查与控制、日志记录和报送； 3、系统部署支持多活模式； 4、系统能够提供定期冷备机制，在集群部署或双机热备部署下，出现故障或意外造成数据错误时，可启动定期备份的冷备系统和数据恢复机制，确保极端情况下，系统仍然可用； 5、系统能够支持业务系统的 URL 封装转换保护和封装访问认证，使业务系统真实的 URL 不暴露在外，外部无法随意访问和根据 URL 追踪到业务系统应用服务器，避免业务系统暴露而遭到攻击； 6、系统能够支持屏蔽业务系统内部的功能，避免系统内部的重要业务暴露到外部网络，要求有友好用户体验的配置界面和截图； 7、支持 IP Hash 负载均衡模式，能够按照访问 IP 地址进行负载分配； 8、支持 Round Robin 负载均衡模式，能够按照访问次数进行轮询负载； 9、支持 Session Sticky 负载均衡模式，能够按照会话粘合度进行负载分配； 10、系统应有负载均衡能力，确保系统在进行集群部署时多台应用服务器能够多节点分担分流，确保系统能够在高强度并非和大用户的时候，能够继续稳定运行； 11、系统能够提供业务系统访问的 TLS 传输安全保护能力，能够将所有从外部访问的业务系统进行 TLS 隧道安全加密传输； 12、提供 HTTP/HTTPS 两种方式，根据业务系统实际情况自动卸载 SSL，完成 HTTP 接口支持； 13、支持 Socket、Websocket 协议转换； 14、提供多种映射策略，包括：客户端过滤、时段过滤、IP 地址过滤等，同时支持黑白名单两种方式； 15、系统支持国密 SM2、SM3、SM4 算法。	
3.30	山东省公安信息网大数据智能化安全体系（一期）——可信代理控制服务	1、支持用户授权数≥50000，并发授权数大于等于 10000； 2、支持代理跨网跨域访问认证服务； 3、支持代理跨网跨域访问权限服务； 4、支持与认证服务、权限服务间加密通信； 5、接收并转发用户发起的认证请求，参与完成认证过程； 6、支持向用户返回用户令牌和应用令牌； 7、会话管理：支持会话管理，可查看和强制终端会话； 8、权限判定：支持为可信接入代理、可信 API 代理提供权限判定；	△

		9、权限变更订阅：支持订阅授权服务的权限变更服务，实时获取最新权限； 10、权限管理联动：支持与权限管理联动，获取应用、API 等权限列表； 11、日志审计：支持记录策略判定日志，包括用户、终端信息、时间、目标应用/API 等信息，并支持日志上报；12、高可用性：零信任服务不对用户侧提供服务，降低了网络暴露面，有效缓解网络攻击；13、支持运用缓存技术，提高鉴权性能，以支撑大用户量高并发访问； 14、支持全面记录用户日志，实现访问可控，实时追踪，事后溯源，包括网关日的浏览和查询、日志保存策略管理 15、支持应用服务的管理，包括应用名称、是否强制 https、应用域名和后台应用服务器映射关系、应用访问证书配置、访问地址和端口、访问域名、应用使用协议、是否开启 Web 防护 16、支持对应用进行分类，实现应用分类的增、删、改、查，以便于应用的管理。 17、须提供安全特征管理，包括安全关注点、安全策略和安全特征点，同时通过设置访问者 IP 黑名单，阻止特定 IP 访问企业应用； 18、风险感知和分析：支持和终端环境感知、行为分析等风险分析平台联动，实时接收风险通报，并结合代理会话状态、权限列表、访问日志等信息进行综合分析，实时变更权限，实时撤销风险会话； 19、须提供与认证服务联动完成身份验证的设置，包括验证跳转 URL、验证特定参数、验证完成特征、身份特征过期时间等 20、支持在认证过程中与风险引擎相结合，在出现风险的时候进行风险预警，并根据风险控制策略对用户进行二次增强认证或禁止访问等。	
3.31	山东省公安信息网大数据智能化安全体系（一期）——可信接入代理	1、标准机架式设备，冗余电源，千兆电口≥2 个，万兆光口（含光纤模块）≥20 个；40G 光口（含光纤模块）≥4 个，网络吞吐量≥80Gbps，最大用户并发数≥10000； 2、支持加密流量解密、协议格式检查与控制、令牌检查与控制、终端身份检查与控制、用户访问检查与控制、日志记录与报送。	△
3.32	山东省公安信息网大数据智	1、标准机架式硬件设备，双电源。配置千兆电口≥4 个，万兆光口（含光纤模块）≥2	一般

	能化安全体系（一期）——可信运维代理	个，设备可管理授权数≥500； 2、支持 DB2、oracle、mysql、sqlserver、国产主流数据库协议代理运维； 3、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，可自动完成授权； 4、支持 ssh、telnet、rlogin、rdp、vnc 协议的 H5 运维； 5、支持批量登录字符设备。	
3.33	山东省公安信息网大数据智能化安全体系（一期）——数据中心防火墙	1、主控板、接口板和业务板分离，实配双主控，除两个主控板外，整机业务扩展插槽≥4，双电源； 2、10GE 光口≥24 个，100GE 光口≥2 个，配置 10GE 多模光模块≥24 个，100GE 多模光模块≥2 个； 3、防火墙吞吐量≥120Gbps，IPS 吞吐量≥36Gbps，整机最大并发连接可扩展到≥4.8 亿，整机每秒新建连接数可扩展到≥1200 万； 4、支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议、IPv6 over IPv4 隧道、6RD 隧道等。	△
3.34	山东省公安信息网大数据智能化安全体系（一期）——数据交换前置防火墙	1、千兆电口≥4，千兆光口（含光纤模块）≥4，万兆光口（含光纤模块）≥4，配置双电源， 2、吞吐量≥10Gbps，最大并发连接数≥400 万，每秒新建连接数≥20 万，配置入侵防御、防病毒模块、URL 查询升级授权； 3、支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议、IPv6 over IPv4 隧道、6RD 隧道等。	一般
3.35	山东省公安信息网大数据智能化安全体系（一期）——数据交换后置防火墙	1、千兆电口≥4，万兆光口（含光纤模块）≥20，40G 光口（含光纤模块）≥4，配置双电源， 2、吞吐量≥80Gbps，最大并发连接数≥2500 万，每秒新建连接数≥80 万，配置入侵防御、防病毒模块、URL 查询升级授权； 3、支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议、IPv6 over IPv4 隧道、6RD 隧道等。	一般
3.36	山东省公安信息网大数据智能化安全体系（一期）——数据防泄漏	1.2U 标准机架式设备，双电源；内存≥64G，硬盘≥6T；千兆电口≥2 个；检测能力≥1G；2.文件识别能力：识别常见的办公文件类型并提取内容，包括 office、wps、pdf 文档等；识别压缩文件并递归解析，包括 zip、rar、7z、gz 等；可防止压缩炸弹，不受压缩层数限制；识别打包类文件，包括 tar，war 等；识别图片类文档并实现 OCR，包括 jpg，png，	一般

		tiff，bmp 等；识别音频文件，包括 mp3，wma 等；识别视频文件，包括 mp4 等；识别常用的源代码文件，包括 java，c++，pyton 等；识别常用的图纸设计文件，包括 AutoCAD，SolidWorks 等。 3.内容匹配能力：能够设置关键字间距进行识别；能对正则表达式命中的内容，再做匹配检查。正则表达式命中的内容能否重复，可以选择。支持密级标识在文档头的情况，可以对文档首段的内容使用正则表达式进行匹配。 4.地址范围匹配：源 IP 段范围限定，目的 IP 段范围限定，源 ip 段和目的 IP 段 ；发件人集合限定，收件人集合限定，发件人和收件人集合限定。 5.策略选项：服务器中保存的安全策略方便管理。 6.网络流量识别能力：SMTP, HTTP, FTP ,SMB ,POP3, IMAP 等；139 邮箱等 http 协议的 webmail 邮件；统计网络流量和数据包情况，实时展示到页面；单台网络流量监控设备应支持千兆网卡接入，支持光口和电口连接。 7.系统管理：可定制的风险仪表盘，用直观的图表同时显示多个报告。可点击报告，查看事件细节；对系统管理用户进行锁定，开启，禁用功能，用户密码可以重置；系统内部数据库敏感信息加密。 8.事件管理：查看事件的时间、状态、严重程度(严重等级分为“高”、“中”、“低”三级)；按策略组、策略、IP、邮箱地址、组织机构、文件类型、文件大小等属性，结合时间属性统计。	
3.37	山东省公安信息网大数据智能化安全体系（一期）——日志审计	1、标准机架式硬件设备，双电源，标配千兆电口≥4 个， console 口≥1 个，内存≥32GB，磁盘容量≥4T（RAID5），EPS≥10000/秒，配置日志源许可≥200 个；2、支持日志收集； 3、支持日志分析； 4、支持三维关联分析； 5、支持建立安全评估模型； 6、安全分析场景：内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等 5 大类的安全分析场景。	一般
3.38	山东省公安信息网大数据智能化安全体系（一期）——	1、千兆光口（含光纤模块）≥2 个，千兆电口≥2 个，万兆光口（含光纤模块）≥2 个，吞吐量≥5G，冗余电源； 2、支持流量威胁检测能力； 3、支持流量分析记录能力，能够对	一般

	深度威胁检测	网络通信行为进行还原和记录，以供安全人员进行取证分析； 4、支持文件还原分析能力。	
3.39	山东省公安信息网大数据智能化安全体系（一期）——漏洞扫描系统	1、标准机架式硬件设备，双电源。配置千兆电口≥4 个，硬盘≥1T。配置系统、软件漏洞检测模块，Web 应用漏洞检测模块，数据库扫描模块，提供≥512 个 IP 授权。 2、扫描对象：支持 Windows 系列操作系统、Linux 主流操作系统、Unix 主流操作系统和国产操作系统，支持 Web、FTP、电子邮件等应用系统等扫描策略。 3、支持弱口令扫描。 4、支持指纹识别。 5、支持日志自动审计。 6、支持漏洞策略库。 7、支持 Web 扫描。 8、支持数据库扫描。	一般
3.40	山东省公安信息网大数据智能化安全体系（一期）——网页应用防火墙	1.产品必须为专业性 WEB 应用防火墙设备及专业性 WEB 应用防火墙资质，而非 NGFW、UTM 设备，不限防护网站数量。2U 标准机架式设备，硬盘≥2T，双电源，配置千兆电口≥6 个（含 2 组硬件 BYPASS 模块），千兆 SFP 业务光口≥4 个，万兆光口≥2 个（含万兆多模光模块，应用层吞吐量≥8Gbps，HTTP 最大并发连接数≥50 万，HTTP 最大新建数≥4 万。 2.支持透明串接、反向代理、旁路镜像等多种部署模式部署，支持链路聚合，支持集群模式、主-主模式、主备模式、硬件 BYPASS、软件 BYPASS，内置 SSL 硬件加速卡，实现对 HTTPS 的加解密，提供设备对 HTTPS 的处理性能；3.支持保护站点快速向导配置部署，支持自动发现网络环境中存在的 Web 业务系统，记录服务器的 IP、Port、域名等信息，支持透明串接和旁路反向代理下的 HTTPS 业务的安全防护。 4.支持 HTTPS 站点 SSL 算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果。 5.支持客户端安全防护，插入特殊的 HTTP 报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options、X-Content-Type-Options、X-XSS-Protect、Content-Security-Policy 等。 6.系统内置机器学习安全引擎，通过机器学习可以对用户 web 业务系统建立安全的访问模型，学习的内容包括 URL、参数、参数类型、参数长度、cookie 等信息，支持设定学习的周	一般

		期，需要学习的域名信息，可以设定可信任的客户端 IP，不可信的客户端 IP 以及不学习的 URL 信息，内置通用的机器学习模型，无需对现网业务进行学习，通过与云端联动，数据模型可实现自动更新。 7.支持细粒度检测检测条件，可基于 URL、请求头部字段、目标 IP、请求方法等多种组合条件进行检测，检测指标可通过 URL 访问速率和 URL 访问集中度、请求离散度三重检测减少误判率；检测的客户端对象可支持 IP、IP+URL、IP+User_Agent 多种算法，客户端 IP 支持应用层字段解析，并支持自定义检测字段功能。 8.支持报表导出为 Word、pdf、html 等多种格式，支持定时报表，并发送到管理员邮箱，支持攻击事件、告警等级、被攻击服务器 IP、攻击者 IP、攻击入口等不同报表模板，支持对不同报表模板进行组合生成多维度报表。	
3.41	山东省公安信息网大数据智能化安全体系（一期）——设备准入控制	1、千兆网口≥6 个、RJ45 接口≥1 个，加密吞吐量≥2.6Gbps、新建连接数≥4000、最大并发连接数≥4100； 2、支持设备入网注册、接入认证、入网合规检查等功能,实现接入设备的身份验证，杜绝非法设备接入数据交换服务区； 3、支持资产管理，包括位置管理、机构管理、人员管理、证书管理、设备管理及终端管理； 4、支持多种认证方式，包括：用户名/密码、证书认证、MAC 认证，支持多因子融合认证； 5、支持提供灵活、丰富的策略管理与授权管理，根据具体要求制订合理的安全策略和权限控制； 6、支持 802.1x、SNMP 与 DHCP 等多种准入控制技术，能够满足在复杂多样网络环境下的准入控制； 7、支持对终端的合规性检查； 8、支持能够对终端进行持续的实时监控； 9、支持提供统计报表； 10、支持查询终端资产基本情况、终端软硬件变动情况、终端合规性检查情况和终端接入报警情况； 11、支持对管理员的操作行为审计，支持事件追溯与责任认定； 12、支持终端合规性与设备入网情况记录，系统自动记录全网的终端合规性检查情况与设备入网情况； 13、支持三员分立管理； 14、支持系统管理，管理员的授权管理，密码策略自定义，支持登录	一般

		失败次数限制； 15、支持数据备份和恢复。	
3.42	山东省公安信息网大数据智能化安全体系（一期）——隔离与交换系统-数据交换	1、由前置集群及后置集群构成； 2、单台设备网口配置千兆电口≥2 个，万兆光口≥2 个； 3、整体通道吞吐量≥40Gbps； 4、支持 Sql Server、MySQL、Oracle、达梦（DM）、人大金仓、南大通用、PostgreSQL 等数据库同步服务，各种数据库之间的异构数据转换，支持文件实时同步； 5、支持 FTP、SFTP 等文件同步服务； 6、支持 Kafka 消息交换； 7、支持外侧数据交换服务与系统互相认证，应用/数据服务与内侧数据交换服务互相认证后，进行请求服务或指令交换； 8、通道支持访问控制，有效阻断不明来源数据的接入； 9、针对各类业务数据，进行按需过滤，例如类型过滤，文件扩展名过滤等； 10、支持任务传输异常中断、安全策略触发的报警功能； 11、支持对网络内终端、服务器等设备基于 IP 和 MAC 等信息的注册和认证，拒绝非注册设备的访问请求； 12、数据交换前置机与后置机通过不同类型的通道面向不同类型 的数据，并且每个通道独立管理，实现了数据交换的逻辑隔离，并且通道支持访问控制，有效阻断不明来源数据的接入； 13、支持文件类型、大小、传输带宽、传输频率、时间等策略的安全控制； 14、管理口与业务口分离，增强配置信息抗干扰能力； 15、支持负载功能，多设备负载配置，系统中任意设备故障或宕机不影响任务的正常运行，具备极高的系统可用性；且可以通过负载模式提高边界交换的性能。	一般
3.43	山东省公安信息网大数据智能化安全体系（一期）——隔离与交换系统-视频交换	1、由单向光闸集群构成，单台设备网口配置千兆电口≥4 个，万兆光口≥4 个； 3、整体通道吞吐量≥40Gbps； 4、配合数据交换集群实现实时文件、数据、消息、指令等交换功能； 5、支持文件、数据库的单向传输： 6、支持 FTP、Samba、NFS、专用客户端等多种方式的文件单向传输 7、支持文件类型过滤 8、支持多文件并发传输 9、支持多级目录（128 级） 10、支持中文文件名，长文件名（255 字符） 11、支持 LINUX、WINDOWS 病毒查杀及病毒文件隔离功能 12、支持异构不同数据库之间的数据交换，现在支持 Oracle、MS SQL	一般

		Server、DB2、Sybase、国产常用的数据库之间的单向交换。 13、支持对交换的数据进行内容的过滤，根据用户的定义内容黑名单对数据库中的数据进行过滤，对不符合的数据不进行交换 14、支持对数据库数据中的大字段进行格式检查。查看大字段中有没有木马和病毒的特征码的判断和大字段数据的数据具体的文件格式是不是符合要求。 15、管理口与业务口分离，增强配置信息抗干扰能力。	
3.44	山东省公安信息网大数据智能化安全体系（一期）——高级威胁检测	1、千兆电口≥4，千兆光口（含光纤模块）≥4，万兆光口（含光纤模块）≥4； 2、清洗能力≥10G； 3、支持对 SYN Flood, SYN-ACK Flood，ACK Flood, FIN/RST Flood, TCP Malformed，TCP Connection Flood, TCP Malformed, TCP Fragment Flood, UDP Flood, UDP Fragment Flood，ICMP Flood，Other Flood，各类 UDP 反射放大的识别和阻断； 4、支持基于会话检测防御各类连接耗尽和异常连接攻击，包括基于源并发会话、新建会话防御 TCP 连接耗尽，Sockstress、TCP 重传、空连接等异常连接攻击防御； 5、支持基于被动防御、CNAME 认证防御针对 DNS 授权服务器的虚假源 Flood 攻击；支持基于源限速、域名限速防御真实源 DNS Flood 攻击；支持 DNS 报文合法性检查功能，至少 3 种 DNS 防御种类； 6、持针对 WEB 网站的 CC 攻击防御能力，支持基于重定向、Cookie、JavaScript 认证防御 HTTP Get/Post Flood（CC 攻击）；支持基于验证码的高强度挑战认证防御机制防御 CC 攻击。 7、支持对 HTTPS 应用的精细化防护，支持基于源认证防御针对 443 端口的 Flood 攻击；并基于行为分析防御场景 TLS 加密高频访问攻击。 8、支持 IPV4/IPV6 共栈 DDoS 攻击防御。	一般
3.45	山东省公安信息网大数据智能化安全体系（一期）——高级未知威胁检测	1、硬件规格：标准机架式设备，冗余电源≥千兆光口（含光纤模块）2 个，千兆电口≥2 个，万兆光口（含光纤模块）≥2 个，文件检测能力≥10 万/24 小时； 2、文件处理，支持对文档类、可执行类、脚本类、多媒体类、移动应用类、压缩类等文件进行检测； 3、动态检测，支持文件执行过程中所有动作得记录，	一般

		能否发现执行过程中的异常及截图，支持对动态行为能够进行威胁情报深度匹配，支持监控文件、进程、网络、注册表等操作相关的系统和内核调用接口； 4、漏洞检测，可通过沙箱检测文件运行期间是否出现漏洞利用行为，支持识别堆喷射、异常控制流跳转等漏洞利用攻击过程，利用已知漏洞攻击行为中的异常攻击代码，实现未知威胁检测； 5、支持风险数据包保存功能，可存留会话的请求和相应数据包，帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置 wireshark 组件在线预览风险数据包 6、支持解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW V9 等协议报文（HTTPS、SMTPS、POP3S、IMAPS 加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号； 7、支持 WEB 特征攻击风险白名单配置，白名单颗粒度可达到 WEB 特征类别、WEB 特征规则和 HTTP 方法 8、支持对 HTTP、IMAP、SMTP、POP3、Redis、Telnet、FTP 等协议的弱口令检测 9、支持自定义 HTTP 登录行为的用户名获取来源，包括但不限于请求头、URL、Cookie、POST-body；支持自定义配置状态码、返回内容与登陆成功/失败状态的绑定关系 10、支持主流协议的暴力破解，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态 11、支持对内网主机进行主机威胁分析，详细展示具体的威胁等级、威胁次数、攻击开始时间、攻击结束时间、威胁性指数统计等 12、持 WEBSHELL 检测，可检测访问 webshell 的行为，包含具体对应的 URL、返回码、返回数据包内容等，可显示一句话类 webshell 后门是否植入成功 13、具备 DNS 协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连 C&C 域名、DNS 返回详情、恶意主机明细等行为。 14、支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP 流量、DNS 流	

		量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示 15、具备元数据外送至第三方平台的能力，支持以 KAFKA、FTP、SFTP、SYSLOG 数据接口输出审计信息、会话应用识别信息、会话应用流量统计信息、传输层流量统计、应用层统计信息、登录行为统计信息和文件检测信息。	
3.46	山东省公安信息网大数据智能化安全体系（一期）——可信环境感知代理	1、系统需满足公安部《GA DSJ 300-2019 公安大数据安全 总体技术框架》、《GA DSJ 350-2019 公安大数据安全 安全访问平台技术设计要求》等规范文档中对环境感知代理的要求，通过采集用户终端设备属性、可信环境信息，实现对终端可信环境的状态和变化的实时感知； 2、具备环境感知内容进行管理和配置，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； 3、能够对物理机环境的可信状态和云桌面环境的可信状态的联动感知，能支持国内主流厂家云桌面的可信环境感知; 4、具备感知发现终端中恶意行为,感知终端上的高危漏洞，高危端口、高危进程和服务，及时发现终端当前的已知风险； 5、具备可信环境感知数据上报接口，支持对终端环境感知评估结果的历史记录查询；6、具备对终端系统配置风险采集，包括弱口令、权限变化、登陆注销事件、配置变更审计日志等进行风险感知，并对存在的风险项进行审计、上报、告警和评估；其中主要安全基线应包括身份鉴别类、安全审计类、访问控制核心配置类、资源控制配置类、入侵防范类；7、支持级联部署、支持集群部署、支持国产化服务器部署，windows 和国产化终端以及信创终端统一管理、支持国产数据库部署。 8、支持对终端进行标识，标识应具备唯一、永久、防篡改、不可伪造等特性，持感知账户锁定阈值、重置账户锁定计数器、账户锁定时间等变化； 9、支持感知是否正在违规外联；10、支持对用户终端和服务器分别进行感知评估； 11、支持终端环境数据采集汇总、分析后统一上报环境感知服务，实现对终端可信环境的状态和变化的实时感知； 12、支持级联	一般

		部署、支持集群部署、支持信创环境部署。	
3.47	山东省公安信息网大数据智能化安全体系（一期）——环境感知代理客户端	1、支持不少于 50000 点终端环境感知代理客户端； 2、支持漏洞风险感知； 3、支持网络风险感知； 4、支持恶意代码风险感知； 5、支持应用环境风险感知； 6、支持系统账户风险感知； 7、支持应用环境风险感知； 8、支持物理环境风险感知； 9、支持硬件配置变化风险感知； 10、支持系统关键对象风险感知； 11、支持系统环境风险感知； 12、支持用户行为风险感知； 13、支持感知终端是否安装规定的防病毒软件；14、支持感知关键系统补丁是否安装； 15、支持感知是否开启了 WIFI、是否开放共享服务； 16、支持采集终端环境数据，并统一上报环境感知服务； 17、环境感知代理客户商注册时支持与 PKI 证书联动，读取 PKI 证书里的持有人信息； 18、具备对终端进行标识，标识具备唯一、永久、防篡改、不可伪造等特性； 19、可采集硬件信息，包括 CPU、内存、磁盘、ip、mac、操作系统等信息，并上报至控制中心； 20、客户端程序目录下的相关文件均是不可以被篡改、注入、拦截、恶意终止，保证客户端程序本身的可信； 21、终端可信环境状态的传递应基于国密算法，确保数据传输过程中的真实性和不可伪造性； 22、具备感知公安安全 U 盘、公安 PKI_UKey 插拔；23、支持感知终端硬件资产变化，比如摄像头是否被移除或者禁用； 24、支持感知代理客户端预注册审核，安装完成感知代理后要经过管理人员审核通过才可正常使用； 25、具备对各种终端安全监测的日志进行实时上报和告警； 26、支持感知终端外部接口发生变化，必须且不仅限于 USB、红外、蓝牙、1394、串并口等； 27、支持感知终端 IP 地址变化、MAC 地址变化、网关变化和 DNS 地址变化等； 28、客户端上支持展示注册人员姓名信息； 29、客户端上支持展示补丁安装情况信息； 30、客户端上支持展示终端环境评分结果； 31、客户端上支持展示网络通信是否正常。	一般
3.48	山东省公安信息网大数据智	1、通过数字证书的方式进行身份验证，登录进部门间信息共享系统。 2、门户展示，能够	一般

	能化安全体系（一期）——部门间信息共享系统	提供可添加附件的公告公示栏； 3、提供平台可用数据服务介绍等功能。支持个性化展现功能，来自不同部门、不同权限的用户看到不同的展示信息，也只能访问有权限的不同应用，系统提供外网门户功能，门户布局美观； 4、提供基于拓扑结构的图形化设备状态展示； 5、管理界面增加资源目录、用户中心、日志管理等模块； 6、支持平台资源集中管理、服务发布等门户系统功能。 7、支持所有注册资源、接口程序、配置信息实现一键式配置，减少操作流程，提高操作便捷性； 8、共享服务平台具有数据查询、统计分析、通知公告、个人工作台、地图形式展现、数据质量监管、数据关联查询、碰撞比对等功能，支持用户自助申请资源功能，支持省市级联部署； 9、首页可查看本省地图及资源目录的图形化界面； 10、共享服务平台内各服务器设备状态监管； 11、可对注册的设备进行状态监测和管理； 12、能够支持共享平台对外的统一接入门户，首页统计平台服务情况，监控服务器目前cpu、内存、磁盘使用情况。 13、可以查看资源详情，支持用户根据资源的不同字段申请服务，由内网管理员审批，发布服务； 14、通过平台管理系统的审核后，实现公安内网用户使用由外部接入单位共享的各类数据资源； 15、提供设备注册功能，设备注册后按照区域进行使用； 16、部署于内网和外网应用服务区。建立资源目录，资源目录中包含引入的外部社会信息资源和公安内部数据资源； 17、资源目录按照人员、物品、场所、组织、案事件、其他进行分类，在资源目录列表中可以查看资源名称、资源别名、服务器名称、网络位置、所属部门、资源业务类别、资源类型等内容； 18、能够通过资源目录实现服务注册、服务引用、服务封装发布等功能； 19、能够在页面进行数据资源的增删改查等操作； 20、能够查看资源详情，支持用户根据资源的不同字段申请服务，由内网管理员审批，发布服务； 21、能够支持资源审批管理，对于内外网接入共享平台的数据资源应首先通过审批，通过审批后的资源才可进行共享。 22、	

		部署于内网和外网应用服务区。提供质量判别标准，对采集的外部单位数据的质量进行判断，依据标准进行监测、分析，统计质量有问题的数据，并提示系统管理员进行处理； 23、与内外网共享服务引擎配合工作，实现对整个共享服务平台内各个应用服务器的配置管理； 24、支持数据的去重，设置去重字段，将重复或有疑义的数据识别出，单独处理； 25、设置数据质量判别标准，支持根据预定义的标准对数据质量进行判断，将问题数据标记； 26、增加统计维度、统计深度，可以从部门、资源要素、地市等多角度进行统计，统计时间支持自定义； 27、统计分类包括平台访问量、数据采集量、数据共享量、数据质量分析、数据比对结果等； 28、系统提供数据接入情况等统计分析，并支持多种展示方式，同时支持数据打印、导出； 29、统计分析数据支持级联上报，在省级平台可以将全省各地市的数据统一进行分析。 30、支持对外提供共享接口服务或调用第三方服务接口，满足接口查询的大并发以及低延迟使用，实现作为外单位和公安网之间接口访问，提高对外数据共享与引进的效率和灵活性； 31、系统可以自动生成服务接口规范文档，并提供 PDF 格式下载； 32、能够实时将数据库里的数据发布成 restful 和 webservice 接口，其他单位用户可根据业务需求调用相关接口获取数据，从而达到数据共享； 33、能够实时把外部单位的 restful 和 webservice 接口引入内网供各警种部门使用； 34、能够把第三方接口提供给外单位查询，提供方式不仅限于 webservice 可同时支持 restful； 35、支持接口服务统一接入、经过认证后进行数据交换，包括数据库、文件、消息、HTTP/HTTPS、Socket 等； 36、支持自助发布 DCP 服务，也可根据需要，利用 WSDL 直接进行定制化开发。 37、能够进行关联查询，对查询结果进行关联展示； 38、支持人口信息核查、支持以服务方式开放外部单位调用； 39、支持提供单个或多个身份证号码对人员基本信息核查功能； 40、支持通过安全数据交换系统的数据接口发送数据	

		查询等请求，和安全数据交换系统保证兼容性； 41、可以针对资源，设置和已有的在逃人口库等进行比对，出现预设字段重合则认为比对成功，支持报警。 42、支持外部用户服务审批管理；43、提供共享平台的外部单位用户申请资源服务的审批功能； 44、可以查看资源详情，支持用户根据资源的不同字段申请服务，由内网管理员审批，发布服务；45、能够在页面添加用户，可对用户的门户使用权限和服务权限进行控制，不同用户具有不同的权限。 46、能够支持服务授权，不同用户对服务的调用次数和时间进行授权。 47、支持统一身份认证、集中审计、痕迹查询等功能。 48、在日志查询页面可以配置日志回滚策略，保留不少于 30 天，分为按时间回滚和按条数回滚，管理员可按照实际情况设置。49、能够对用户调用服务日志进行记录，并可在页面进行展示和查询，同时可对日志保存天数和条数进行配置； 50、能够提供流量、日志安全审计方面的数据支撑。	
3.49	山东省公安信息网大数据智能化安全体系（一期）——认证服务	1、支持用户授权数不少于 50000，并发授权数不少于 10000； 2、允许使用多种用户名登录。 3、多次认证错误后，提示输入验证码，继续认证错误后一定次数后锁定统一用户。4、支持失败显示验证码次数、失败锁定次数及失败锁定时长的自定义. 5、支持管理员对锁定用户进行解锁。 6、支持首次登录强制修改密码。 7、支持密码口令认证技术，支持密码复杂度可配置，由数字、大小写字母、符号等多种元素组成，长度可设定，并提供定期更换、更换前提醒、历史密码不允许重复等密码策略。 8、口令信息应进行加密存储和加密传输等安全保护。 9、支持在用户认证通过后，创建会话、并返回至用户。支持在服务端对令牌进行集中管理，包括签发、撤销、格式转换、验证和更新等。 10、支持在内存中集中保存和管理会话与令牌。在系统失效时，可从存储中恢复。支持独立部署会话库和认证服务。 11、支持双因素认证。 12、可以对应用设置安全级别，根据安全级别，支持针对指定的应用进行多因素认证。 13、支持登录页面	△

		的自定义，针对应用系统登录页面的个性化定制。 14、支持全局注销，即注销统一认证服务的同时注销认证过的所有应用系统。15、支持采用 OAuth、SAML、WS-Federation 等标准协议实现 SSO。成熟的商用套件通过配置即可集成（EBS、SAP、SharePoint 等）。 16、支持多种集成方式，例如协议模式、代理模式、代填模式。 17、支持 B/S、C/S 应用的 SSO 集成，支持跨浏览器应用 SSO 集成。 18、支持自定义认证链，即用户在完整的认证过程中按顺序执行的认证流程。 19、支持串行认证链。	
3.50	山东省公安信息网大数据智能化安全体系（一期）——权限服务	1、支持用户授权数不少于 50000，，并发授权数不少于 10000； 2、支持从一个身份数据源回收身份数据（如用户、机构），也支持将分散在多个应用系统中的身份数据回收并聚合为平台权威身份数据，保证身份数据的完整性、权威性； 3、支持从上游权威身份系统同步机构数据； 灵活扩展组织机构的属性定义，并支持定义多值属性； 4、可以根据不同的组织机构类型进行组织机构专有属性的定制；灵活配置从上游权威身份系统回收的组织机构属性及其映射关系；5、支持对敏感字段的加密存储，加密方式支持国密算法，并支持自定义加密算法； 6、基于组织机构的用户查询；支持批量操作，并支持预导入功能；对已删除的机构支持查询和导出； 7、支持人员多组织机构树； 支持从上游权威用户系统同步用户数据；结合用户入职、兼职、调岗、借调、离职等不同业务场景实现用户账号的全生命周期管理； 8、用户组（静态组和动态组）管理，以及用户组内人员及权限灵活管理；9、扩展用户的属性定义，并可以定义多值属性； 10、支持密码策略，同时可以根据需求制定多套密码策略，并支持根据不同的用户范围同时启用不同的密码策略； 11、支持弱口令管理，配合用户密码策略一起使用，当用户密码策略中启用弱口令后，弱口令中列出的系列简单口令都不准使用； 12、支持批量操作功能，并支持预导入功能。通过预导入功能，能够对即将导入数据进行合规性检查，又能够	△

		对导入数据进行预览； 13、具有应用系统的基本管理（增、删、改、查）功能；支持应用对象建模，包括账号、机构、组、角色、资源； 14、可灵活扩展应用的属性定义，并支持定义多值属性； 15、根据应用需要，选择不同的组织机构树进行供应，为应用配置同步的组织机构属性映射，为应用配置同步的帐号属性映射； 16、具有应用账号的回收功能，即主动从应用系统获取账号到统一身份管理及认证平台中，并与用户相关联，检查是否有孤儿等不合规账号存在； 17、支持应用账号的新增、绑定、解绑、启用、禁用、删除操作； 18、新增账号时，能为不同类型的用户设置灵活的有效期； 19、可手动为用户分配应用账号； 20、根据用户职位和机构的变化，自动调整或撤销用户的应用权限； 21、通过定义权限分配策略，自动分配应用账号。策略分配支持全部和自定义条件，自定义条件支持用户类型、组织机构、用户组，支持用户属性粒度级别的自定义条件； 22、针对一人多账号问题，要求提供基于菜单权限和数据权限的授权，严格控制不同账号的权限； 23、支持按照省、市机构的分级管理，管理员可以将自己可管理的身份子集管理权限再分配，实现统一存储，分级管理； 24、支持操作日志管理，支持按照操作用户、时间等条件查询日志； 25、支持操作日志的批量导出； 26、提供外部接口，并提供接口调试界面、支持自定义开发接口。	
3.51	山东省公安信息网大数据智能化安全体系（一期）——业务审计服务	1、配置与审计主服务通信得采集服务地址，用于跟审计主服务进行规则，应用，采集服务相关信息得同步。 2、每当规则相关信息以及应用相关信息修改时，都会通过采集服务表及时得与采集服务进行通信，以防数据不一致得情况发生。当采集服务自启动时，会自动扫描数据库中得数据，重新加载。能够将非标准的日志内容转化成为标准日志。 3、对审计日志字段进行相关过滤配置，可对审计规则中得每一个字段进行规则配置，包括（等于，不等于，包含，不包含）等规则信息 4、根据认证得维度进行报表展示，根据不同的时间范围展	一般

		示不同得报表。 5、根据应用访问得维度进行报表展示，根据不同的时间范围展示不同得报表。 6、根据应用得鉴权授权维度进行报表展示。 7、根据产生得告警分类进行报表以及列表展示。 8、可以根据某一特定得值，进行分词查询，查询到得内容进行高亮显示 9、支持日志完整性校验、完整性校验告警、非法日志告警。日志在保存之前要求进行哈希处理，系统存储原文以及哈希值。在查询日志或设定的定时扫描任务进行日志的完整性校验。校验过程为重新把原文进行哈希，将校验的哈希值和原来存储的哈希值进行比对，比对结果一致则校验通过，不一致则证明数据不完整，不完整将触发告警。 10、根据身份标识、事件时间、事件动作、源地址、目的地址、是否处置进行日志查询，能够自动根据选择时间展示各个时间段的日志量 11、能够通过身份标识、事件时间、告警类型、告警级别、等条件进行告警查询，能够进行告警溯源，并可以进行条件查询以及处置告警。 12、设置可触发告警条件得日志规则，目前告警类型分为四种，(休眠账号，异地登录，频率异常，敏感词)，可根据不同得类型设置不同得触发条件，主要功能增删改查。 13、为规则设置中告警类型为敏感词得规则提供选择条件，目前敏感词可设置为精确匹配以及模糊匹配 14、对接第三方应用（业务安全策略控制），进行推送告警以及规则。 15、为规则设置提供选择，主要功能增删改查 16、对日志查询中得数据进行归档配置，周期间隔，执行时间，以及保留日志得天数。到达时间后将日志进行保存 17、对通过归档配置中保存得日志进行查询。 18、配置可不进行告警产生得条件。主要功能增删改查 19、主要为了记录一些常识或知识点问题记录等，方便问题排查，主要功能增删改查 20、由身份系统提供得机构信息。 21、由身份系统提供得用户信息。 22、主要对应用进行增删改查，可配置当前应用是否显示在审计系统当中。 23、向业务安全策略控制服务 24、推送的告警以及规则历史 25、对推送历史中失败得告警以及规则，配置重发机制。	

		26、可根据不同纬度进行报表展示。 27、接口形式收集查询日志。	
3.52	山东省公安信息网大数据智能化安全体系（一期）——业务审批服务	1、支持查询登录人相关已起草申请的所有审批流程，支持通过审批类型等条件进行查询操作，如任务审批、权限审批等。 2、支持查询登录人相关需要待办理的所有审批流程，支持通过审批类型等条件进行查询操作，如任务审批、权限审批等。 3、支持查询登录人相关已经审批完成的所有未办结的审批流程，支持通过审批类型等条件进行查询操作，如任务审批、权限审批等。 4、支持查询登录人相关已经审批完成的所有已办结的审批流程，支持通过审批类型等条件进行查询操作，如任务审批、权限审批等。 5、支持查询登录人相关的所有审批流程，支持通过审批类型、流程状态等条件查询，查询流程范围支持分级策略，如管理员可以看到全部所管辖机构内的相关流程。 6、支持审批流程详情展示，包含审批请求类型、审批标题、审批内容、提请人员ID、提请人员姓名、提请人单位 ID、申请人单位名称、创建时间等。 7、支持导出所有流程信息。 8、支持导出勾选的流程信息。 9、用户对具体任务进行审批操作，对需要审批的内容进行核查，可以审批通过并填写审批意见，同时可以选择审批流程的下一步审批人员，将审批流程流转到下一步。 10、用户对具体任务进行审批，并对内容进行核查，可进行驳回操作，驳回到上一步提交人。 11、支持批量处理多个流程 12、展示待办理的数据，可针对流程信息进行审批。 13、展示当前管理员已经办理过得流程信息。 14、支持为权限系统不同类型的审批流程进行流程定制，支持系统内部流转权限审批流程，可自定义配置流程节点和审批单人员，流程配置支持WEB 页面拖拽画流程。 15、支持根据不同需求定制特殊审批角色，支持不同节点自动选择办理人进行审批。 16、支持为对接应用配置办结通知地址、应用编码等信息。 17、支持以日志的形式记录审批流程处理相关的行为 18、支持以日志的形式记录审批任务操作相关的行为。 19、支持以日志的形式记录审批请	一般

		求处理相关的行为。 20、支持系统访问所产生的日志进行实时记录，并提供日志数据的查询操作，导出等操作功能 21、提供对常用数据的字典项进行维护功能，如包括审批类型管理、任务类型管理等，支持通过数据字典基础信息进行查询操作。 22、提供对系统的功能配置进行维护功能，支持对平台配置、数据同步配置等信息的查询操作。 23、提供系统异常日志文件的下载功能。 24、提供对系统管理人员进行维护与权限设置操作，支持配置下级权限管理员权限。 25、提供对系统的定时任务进行统一管理操作。 26、审批服务支持接收认证服务的用户令牌。支持获取认证服务用户信息、组织机构信息。 27、支持向权限服务提供权限申请与变更服务。支持将审批结果发送至权限管理服务。	
3.53	山东省公安信息网大数据智能化安全体系（一期）——安全管理服务	一、服务注册模块： 1、通过提供标准的对接模板，支持不同类型安全服务完成快速注册。服务标准模板包括但不限于服务名称、服务版本号、服务所属资产类型、服务所属厂商、服务联动方式、服务开发者邮箱、服务类型、服务开发语言等。 2、支持 HTTPS、HTTP、SSH、JDBC、LDAP、LOCAL、SMTP、SOAP、TCP、SOAP OVER HTTPS 十种联动方式。 3、支持 Java、Python 两种服务开发语言。 4、支持快捷制定服务实例参数 key 以及参数值，默认参数包括但不限于主机地址、端口、是否启用 HTTPS 等，支持自定义参数制定。 5、支持将平台已注册的标准服务快捷添加至模板中。支持便捷开发。 6、支持将未注册的服务自动化注册至平台，通过在线安装的方式可自动化完成服务注册。 7、支持将未注册的服务人工注册至平台，通过人工导入服务安装包，可快捷完成服务注册。 8、支持第三方服务注册至平台。支持手动将第三方服务注册至平台。支持自动化将第三方服务注册至平台。支持第三方服务类型包括但不限于安全识别服务目录、安全防护服务目录、安全检测服务目录、安全响应服务等。 9、支持已注册的第三方服务从平台注销。支持手动或自动化将已注册的第三方服务进行注销。 10、服务注册	一般

		后，需通过服务发布进行启动服务。服务启动后方可进行服务调度。 11、服务发布并使用后，对于闲置或无需再次使用的服务进行注销回收，减少平台资源占用。 二、服务目录模块： 12、提供安全防护体系中的安全识别服务目录、安全防护服务目录、安全检测服务目录、安全响应服务，以及零信任体系中的认证服务目录、权限管理服务目录、业务安全策略控制服务目录、环境感知服务目录、业务审计服务目录。 13、目录内容包括但不限于服务类型、服务名称、服务接口、服务描述、服务实例等信息。 14、提供资产识别、漏洞扫描、基线核查和代码审查的安全服务。安全识别服务目录包括但不限于获取资产列表、防篡改获取资产列表、基线漏洞扫描、数据库漏洞扫描、检查依赖漏洞等安全服务。 15、提供网络访问控制、网络入侵防御、WEB 应用防护、恶意代码防护的安全服务。安全防护目录包括但不限于入侵检测系统服务、添加或删除扫描目标网站等服务。 16、提供流量异常检测和蜜罐系统的安全服务。安全检测服务目录包括但不限于上传流量包、删除流量包等服务。 17、提供安全事件抑制、安全事件取证和攻击溯源的安全服务。安全响应服务目录包括但不限于文件检测、流量包分析内容、沙箱检测等服务。 18、提供认证服务。认证服务目录包括但不限于二次认证、锁定用户、撤销令牌等认证服务。 19、提供权限管理服务。认证服务目录包括但不限于撤销权限、冻结权限、降级权限等认证服务。 20、提供业务安全策略控制服务。业务安全策略控制服务目录包括但不限于获取弱点策略列表、获取弱点策略聚合信息、获取微隔离策略列表等服务。 21、提供环境感知服务。环境感知服务目录包括但不限于沙箱检测、扫描恶意文件等服务。 22、提供业务审计服务。业务审计服务目录包括但不限于日志审计、启动分析任务等服务。 支持对安全服务进行分类，分类标准包括但不限于能力模板、IPDR、安全运营等。 23、支持对安全服务进行分级。支持分级自定义。支持基于安全服务分级进行查询。 支持对安全	

		服务的分类进行查询，分类标准包括但不限于能力模板、IPDR、安全运营、厂商、实例类型等。 24、支持对安全服务的分级进行查询。分级类型包括但不限于高、中、低、未知等。支持通过服务名称、服务描述、服务 URL、服务状态等对安全服务进行模糊查询。 三、服务接口模块： 25、支持北向接口与安全管理中心联动，实现安全策略的编排、处理结果的同步。 26、支持设备级北向接口和标准级北向接口开发。标准级北向接口标准化程度更高，可适配更多服务实例。设备级北向接口只可适配某厂商某种特定的服务实例。 支持南向接口对接各项安全能力服务并与之联动，实现安全规则的下发和处理结果的上报。 27、支持接口标准化。通过标准、统一的接口，提供安全服务能力的调用、配置和管理，保障服务的有效性和高可用性。 28、提供配置管理接口。支持服务实例配置管理。支持服务目录配置管理。支持服务编排配置管理。 29、提供策略编排接口。支持编排能力接口管理。支持编排能力接口调用。支持接口调用结果反馈至平台。 30、提供能力调度接口。包括但不限于设备服务接口、标准服务接口、剧本编排服务接口等。 31、提供信息查询接口。支持服务目录信息查询。支持服务实例信息查询。支持服务接口信息查询。 32、提供数据上报接口。支持数据源接入海量告警数据。支持服务调度结果上报。 33、支持对安全服务接口进行分类，分类标准包括但不限于能力模板、IPDR、安全运营等。 34、支持对安全服务接口进行分级。支持分级自定义。分级类型包括但不限于高、中、低、未知等。 35、支持对安全服务接口的分类进行查询，分类标准包括但不限于能力模板、IPDR、安全运营、厂商、实例类型等。 36 支持对安全服务的分级进行查询。分级类型包括但不限于高、中、低、未知等。 37、支持接口调用使用多种协议支持。包括但不限于 HTTPS、HTTP、SSH 等。 四、服务调度模块： 38、支持根据安全管理中心下发的策略进行服务编排。支持将安全服务平台中囊括的所有安全服务作为剧本编排元	

		素编写至不同类型的剧本中。 39、支持服务编排引擎调度不同类型的服务目录。通过服务编排将各种服务有效组合在一起，实现自动化或半自动化服务调度流程。支持剧本完成服务调度任务。 40、支持服务调度结果反馈至编排工作流或平台。通过服务调度结果反馈机制，洞察调度有效性以及成功或失败的具体原因。 41、支持服务目录下添加多个服务实例。支持对服务实例进行全生命周期管理。包括但不限于服务实例的注册、编辑、启用/禁用、注销等。 42、服务实例分类管理： 支持服务实例的标签化管理，支持通过标签对服务实例进行分类查询。标签类型包括：能力模板、IPDR、安全运营、厂商、实例类型及其他自定义标签类型。支持标签自定义管理。支持标签的灵活使用。 43、服务实例注册管理： 支持人工注册服务实例，通过填写服务实例的注册参数，将服务实例注册至对应的服务目录中，即可进行服务实例的调度与使用。支持注册参数必填与不必填。支持注册参数类型为密码型、输入型、布尔型等。支持注册参数密码不可见。支持注册参数复用性。支持服务实例不可重复性。 44、服务实例权限管理： 支持将服务实例的权限与用户进行绑定，对于无权限的服务实例，平台支持发起鉴权服务。支持服务实例权限与平台角色进行绑定，绑定后，该类角色下的用户均具有该服务实例的使用权限。权限管理可对敏感服务实例进行保护，有效降低误操作带来的未知损失。支持服务实例与权限进行解绑。 45、服务实例使用管理： 支持服务实例的启用/禁用。启用服务实例即可对该实例进行服务调度，禁用服务实例可禁止调度该实例。支持服务实例启用禁用的可视化展现。 46、服务实例健康监控管理： 支持对每一个安全服务目录下的服务实例进行健康监控。支持监控结果可视化展示。支持对健康设备进行搜索过滤。 47、服务实例卸载管理： 支持对已注册的服务实例进行快速卸载。 48、支持第三方对不同类型的服务进行调度。支持第三方不登陆平台即可进行服务调度。支持通过平台用户赋予第三方用户权限，	

		支持不同权限的第三方用户进行服务调度。 49、支持第三方服务调度结果反馈。支持结果反馈至第三方使用者指定的 IP 和端口。	
3.54	山东省公安信息网大数据智能化安全体系（一期）——安全识别服务	1、提供云上漏洞识别能力，包括：支持网站/系统/数据库/基线各 1000 个 IP； 2、支持主机、基线、网站、数据库扫描，并具备弱口令扫描功能，提供多种弱口令扫描协议，包括 SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP 等协议进行弱口令扫描，允许用户自定义用户、密码字典；授权扫描许可不少于 500。 3、厂商漏洞策略库不低于 40000 条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与国内 CNNVD 漏洞库标准兼容。 4、提供扫描操作日志自动审计功能，用户可以根据操作内容、操作账户、操作 IP、操作开始时间、操作结束时间等自定义日志审计规则。并将审计结果发送到指定邮箱当中，用户可自定义审计结果发送的频率和时间； 5、提供采用 SMB、SSH、Telnet、SNMP 等协议对 Windows、Linux 系统进行登录授权扫描。 6、提供 Web 应用漏洞扫描功能，支持国内外常见第三方组件扫描。 7、支持识别国内外主流 Web 应用防火墙品牌及被扫描目标对象的网站响应状态，能根据不同的响应状态直观呈现不同颜色标识。 8、支持常用的授权数据库漏洞扫描。	一般
3.55	山东省公安信息网大数据智能化安全体系（一期）——安全检测服务	1、支持主流数据库审计，支持非关系型数据库审计；支持不少于 16 个数据库实例，不少于 32000TPS。 2、支持对 SQLserver 2005 以上版本采用通讯加密的数据库，可以导入证书的方式实现审计解密。 3、支持数据库请求和返回的双向审计，支持返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小。 4、支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告。 5、支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义敏感数据掩码规则，支持自定义。 6、可自定义审计策略，审计策略不少于支持 18 个条件；查询条件易于使用，审计查询条件均为非正则表达式形式进行，支持	一般

		采用部分匹配模糊查询方式检索审计日志。 7、支持基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询。 8、系统提供内置多种报表模板库，报表支持生成多维度综合报告，支持 HTML、PDF、PNG 等格式的报表导出。 9、支持对数据库自动建模及智能对异常行为告警功能；可基于账号、IP 地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警。	
3.56	山东省公安信息网大数据智能化安全体系（一期）——安全防护服务	提供云上网页防篡改防护能力，包括： 1、支持不少于 50 台服务器(Windows/Linux)网站防护； 2、支持常见关系型数据库和非关系型数据库； 3、采用先进内核驱动、WEB 核心内嵌和实时触发机制结合，基于特征码、模糊Hash、脚本虚拟机动态检测 Webshell。 4、支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 5、支持在同一种操作系统下，网站路径相同，可通过规则模板，用模板统一将规则下发到各监控端。 6、支持实时防护网站常见的SQL 注入攻击、XSS 跨站攻击、Web 容器及应用漏洞攻击，智能检测并防御 CC 攻击，保证网站正常服务能力。支持策略验证、Cookie、JS 脚本混合验证、抗图片识别工具的干扰色图片验证。 7、支持多种日志级别，日志导出，支持邮件，Syslog，短信，SNMPTrap，平台等多种告警方式。 8、智能检测并防御 CC 攻击，保证网站正常服务能力。防护分为高中低三级，主要进行策略验证、Cookie 验证、JS 脚本混合验证、抗图片识别工具的干扰色图片验证； 9、一键启停所有对监控端的保护； 10、支持将容器镜像内目录保护后，任何以该镜像创建的容器内的目录都被保护的功能。 11、提供云上主机安全防护能力，包括：1、提供不少于 300 个主机防护授权；2、支持账户暴力破解防护；3、支持恶意程序检测；4、支持关键文件变更检测；5、支持漏洞	一般

		检测； 12、支持对 CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对 CPU、内存达到一定阈值时客户端进行熔断。13、支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露 14、违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意 IP，支持黑名单告警和阻断。 15、支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意 IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置。 16、提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。支持白名单设置 17、支持流量画像，支持全网流量可视化。	
3.57	山东省公安信息网大数据智能化安全体系（一期）——安全响应服务	提供云上网页防护与响应能力，包括： 1、新建不少于 50000 连接，并发不少于 500000 连接，防护流量不少于 500Mbps；不限 IP/端口/域名； 2、能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括 SQL 注入、命令注入 、Cookie 注入等）、跨站请求伪造等应用攻击行为；防护流量不少于 500Mbps，HTTP 最大新建数不少于 50000，HTTP 最大并发数不少于 500000。 3、能够识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷;支持对 HTTP 请求分割攻击和 HTTP 响应报文截断攻击的防护，支持 HTTP 协议规范性检查，检查 HTTP 报文合法性，检查 HTTP 报头是否有缺失或为空，检查请求报文是否畸形检查 HTTP 报头长度，防止缓冲区攻击;支持第三方组件漏洞防护，包括 WEB 容器漏洞（Nginx、IIS、Tomcat 等 WEB 服务器漏洞）、开源 CMS 漏洞（Kuwebs、phpcms、TRS WCM、JBR-CMS、DeDeCMS 内容管理系统漏洞）、WEB 服务器插件漏洞。 4、内置机器学习安全引擎，通过机器学习对用户 web 业务系统建立安全的访问模型，学习的内容包括 URL、参数、参数类型、参数长度、匹配频率等信息，支持设定学习的周期、学习的域名、学习的 URL 等信息，可设定阀值，当达	一般

		到一定阀值后执行告警或者阻断。 5、按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP 的访问。	
3.58	山东省公安信息网大数据智能化安全体系（一期）——资产管理	1、支持信息资产管理：支持信息资产的发现、注册、标记、梳理和管理；支持管理资产分类；支持监控安全域、Web 业务系统、服务器、终端、安全设备等网络实体类型。 2、支持管理资产分类，包括但不限于主机、应用、终端、服务器、网络设备、安全设备、外设，支持拓扑图的增加、修改、删除、导入、导出，支持创建不少于 50 个业务或网络拓扑，支持建立平面拓扑和 3D 拓扑。 3、支持监控安全域、Web 业务系统、服务器、终端、安全设备等不少于 5 种网络实体类型。 4、支持对资产进行监控，并根据资产访问关系进行自动分析，实现实体间网络互访关系的多级钻取，支持不少于 10 跳的流量关联关系分析，支持通过端口、协议、异常访问类型过滤关联关系。 5、支持通过拓扑中各个节点的安全态势状况进行计算，对拓扑所对应的业务系统进行整体健康程度的详细量化评判。 6、支持漏洞管理：支持接收内部、外部提交的漏洞，支持漏洞分类分级管理。 7、支持不少于以三种形式展示全量资产规模及资产间相互访问关系，包括但不限于三维球面体、二维平面图、星空图等。 8、持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录 9、支持拓扑图的增加、修改、删除、导入、导出，支持创建不少于 50 个业务或网络拓扑，支持建立平面拓扑和 3D 拓扑。支持通过拓扑中各个节点的安全态势状况进行计算，对拓扑所对应的业务系统进行整体健康程度的详细量化评判。 10、支持监控安全域、Web 业务系统、服务器、终端、安全设备等不少于 5 种网络实体类型。 11、支持卡片和按列展示 web 业务系统，可查看 web 业务系统的网络速率、访问次数、访问成功率、7 天告警情况等。 12、支持从已有的资产平台同步资产信息，支持资产信息的导入、导出； 13、支持资产指纹变更对比，形成资产变更历史记录，展示资产变	一般

		更对比字段变化，资产异常告警、漏洞的统计。 14、支持展示资产画像，对资产进行监控，并根据资产访问关系进行自动分析，实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持通过一键溯源进行威胁关系的自动拓展。 15、支持对资产进行监控，支持多层访问关系全自动分析、展示。查看资产供给链情况、告警时序、风险详情并直接处置威胁风险，并识别风险的威胁方向、告警、攻击链、威胁等级、告警次数、最近异常发生时间等。16、支持图形模式、列表模式和按访问方向、访问类型查看当前资产的访问关系图，统计展示当前资产访问内网 IP 目标数量、被来源内网的 IP 访问数量、访问了互联网的 IP 目标数量、被来源互联网的 IP 访问数量。 17、支持生成资产行为画像，展示访问流量变化趋势、访问次数变化趋势、访问来源 TOP10、访问目标 TOP10。	
3.59	山东省公安信息网大数据智能化安全体系（一期）——安全大数据	1、在云平台、网络、终端、云平台、边界、业务应用、数据等实体的关键部位采集相关数据； 2、支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据； 3、支持通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息； 4、支持接入文本格式、CVS 等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理； 5、支持通过云端对接、本地导入或手动编辑的方式，接入威胁情报数据； 6、包含安全数据探查、安全数据定义、安全数据读取和安全数据对账四个数据接入流程，分别完成认识数据、元数据结构定义、获取数据、数据质量核对效验；7、日志采集方式应支持但不仅限于 Syslog、kafka、ftp、部署代理等 4 种方式； 8、支持采集异构设备的日志数据，实现包括但不限于安全类、网络类、应用服务器类、操作系统类等不少于 4 大类、50 种设备的日志接入采集； 9、支持接入应用服务器的性能类数据，	一般

		包括但不限于 CPU、内存和磁盘的性能告警数据； 10、内置解析规则支持厂商不少于 200 家，支持解析日志设备型号不少于 2000 种，无需配置解析规则与设备日志对应关系，自动完成解析； 11、支持数据探查，可对数据源进行取样操作； 12、可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息，不少于 30 个字段； 13、具备同时保存事件原始日志数据和标准化后日志数据的能力； 14、支持对安全数据处理规则的定义，包含但不限于安全数据提取、安全数据清洗、安全数据关联、安全数据比对、安全数据标识和安全数据分发等数据预处理流程； 15、支持数据处理任务管理功能，可对独立的数据处理任务做到增、删、改、查等操作； 16、安全数据组织是安全数据存储的形态，安全数据存储可根据安全大数据的业务需求建立相应的存储库，包括原始库、资源库、主题库、业务库、知识库、业务要素索引库等； 17、安全大数据相关的原始库、资源库、主题库、知识库、业务库等均可在本地数据资源目录注册，各级数据资源目录汇聚到部级数据中心，汇总后再分发到各地数据中心； 18、全数据治理包括数据标准管理、元数据管理、数据质量与监控管理、数据共享与服务管理，为安全数据分析提供高质量的数据支撑； 19、支持数据质量监控包括但不限于：提供质量评估指标定义、提供数据质量检测规则管理、提供数据质量检测指标数据采集、计算，以及指标对比； 提供数据质量检测结果展示； 20、支持数据对账功能，可提供在自定义时间段里，对数据提供方和数据接入方数据的完整性、一致性、正确性进行核对和检验； 21、提供安全数据的访问和管理能力，包括原始库、资源库、主题库、业务库、知识库、业务要素索引库，元数据、数据资源目录等数据服务； 22、支持通过服务令	

		牌限制用户访问数据的权限； 23、安全数据分析根据安全业务需求，利用安全分析技术，对数据进行统计、分析、规律性探索及预测等，支撑安全应用业务场景复杂、多变的需求，平台应内置包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的安全分析模型； 24、模型可通过串并联方式组合编排，前一个模型的输出可以作为后一个模型的输入，支持分析模型编排层级不少于 10 层； 25、安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容； 26、支持对安全日志里 200 个以上字段进行任意形式的逻辑与或非形式组合建模，字段包括但不限于应用协议、目的 IP、目的主机名、目的端口、目的用户名、数据流方向、情报 IOC 等，运算方式包括但不限于等于、不等于、大于、小于、大于等于、小于等于、属于、不属于、存在、不存在，并能根据组合方式自动生成运算表达式； 27、支持在安全模型列表一键查看模型产生的异常记录或安全告警。 28、平台内置不少于 8 种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常、域名请求数异常等特定场景条件下的安全态势异常； 29、支持自定义部署 AI 机器学习模型，允许用户选用的高级机器学习算法不少于 4 种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险； 30、建立 24 小时巡查机制建设。对公安民警的行为数据进行全面采集，通过用户行为基础特征提取，结合业实际业务需求，为各警员建立行为基线，形成符合实际业务场景的警员异常行为检测模型，以 24 小时为单位，进行异常行为实时监测，及时发现疑似违规行为并进行短信提醒。通过建立常态化巡查机制，并结合内部管理制度，规范民警的业务系统使用和查询行为； 31、建立警员全息画像，运用大数据技术，汇总各警员相关的历史、档案、行为数据，从而	

		描绘出各警员的信息全貌。从个体特征维度、群体属性维度两个方面对用户画像进行全面的分析，直观展示各警员访问及使用业务系统的行为轨迹，为警员异常行为分析提供直观的决策依据； 32、安全日志查询权限的下放，每个地市可以查询自己本市警员的全省应用系统查询行为。	
3.60	山东省公安信息网大数据智能化安全体系（一期）——态势感知	1、支持基于资产信息，按照区域、类型、重要程度等，结合安全事件、漏洞信息进行多维度分析；支持形成资产类型分布、资产弱点、资产健康度、资产风险分布等分析数据，进行态势展示； 2、支持对数据分布、访问行为、数据流动等信息进行多维度分析；支持形成包括数据泄露风险、越权操作、异常访问行为、异常流量等分析数据，进行态势展示； 3、支持 基于漏洞和基线核查信息，结合应用系统，区域资产等基础数据，进行多维度分析；支持形成在不同区域、系统和资产上的脆弱性分布以及排名等分析数据，进行态势展示；4、支持基于网络攻击、恶意代码等数据进行多维度分析；支持形成横向威胁扩散、病毒蔓延趋势、攻击路径等分析数据，进行态势展示； 5、支持按照安全事件时间段，对事件攻击链分布、事件级别、事件类型、区域分布等对公安信息网中发生的安全事件进行多维度分析；支持形成安全事件的不同区域事件分布对比、安全事件发展趋势等分析数据，进行态势展示； 6、支持基于公安信息网中的违规流量信息、违规访问行为、违规事件分布信息等进行多维度分析；支持形成违规主体、违规事件类型、违规行为对象、处置状态等分析数据，进行态势展示； 7、支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，提供不少于 10 块大屏展示界面，支持大屏轮播，可自定义选择播放大屏及轮播时间间隔； 支持可视化图表类型不少于 15 种，包括但不限于时序图、饼图、柱状图等； 8、统计类图表支持展示升序或降序的 TOP5 到 TOP100，可针对数据中任意字段的计数、平均值、求和、最大值、最小值、唯一值	一般

		等不少于5种算子的统计结果配置可视化图表； 9、可视化图表可通过拖拽配置组装成仪表盘，仪表盘不少于7种布局类型，仪表盘展示时支持时间范围自定义选择。 10、支持对云平台、数据、应用、网络、边界、终端等的日志信息进行记录和安全审计，支持对安全审计模型、算法、规则等进行分析，发现攻击行为、违规异常等并告警； 11、支持对特权用户的操作行为进行审计，支持对用户行为、用户画像等进行分析，发现异常并告警； 12、支持根据告警规则，生成安全审计结果； 13、支持对信息资产进行安全风险评估，基于信息资产，以资产的脆弱性包括漏洞、弱配置等进行安全风险评估，支持在安全管理中心下发漏洞扫描、配置核查扫描任务； 14、支持用户自定义编辑报告模板，根据实际的业务需求自定义统计分析的指标对象，生成有针对性的分析报告，安全分析中的所有字段内容，都可以作为报告的统计对象，并自定义时间范围实现报告导出 15、内置深度威胁分析、攻击者取证等2个以上报告模板，报告订阅支持通过邮件方式在设定时间点发送日报、周报、月报到不同邮箱，可配置订阅规则数量。 16、支持根据安全风险评估过程中发现的安全风险进行预警；支持基于威胁情报、高危漏洞进行安全风险预警； 17、支持建立安全风险预警指标规划，根据不同的安全风险类型、影响范围进行风险预警定级。	
3.61	山东省公安信息网大数据智能化安全体系（一期）——云安全管理平台	1、支持以软件形态在通用X86或ARM服务器上部署，通过虚拟化技术构建安全资源池向用户提供云安全能力，安全能力支持弹性扩容、按需分配； 2、安全资源池支持集群化部署，利用分布式存储技术为虚拟化安全能力提供高可用和动态迁移特性，同时支持硬件节点扩展，快速提升集群规模； 3、支持使用云平台提供的虚拟化资源部署云安全管理平台及安全产品，无需进行云外流量牵引，避免对云平台网络改动过大和占用额外的硬件服务器资源； 4、能够利用虚拟化资源为用户提供一站式安全解决方案，不少于包括下一代防火墙、web应用防火墙、堡垒机、综合漏洞扫描、数据库	一般

		审计、日志审计、主机安全（EDR）、APT 等安全能力； 5、支持用户认证统一，被授权的用户可以直接通过管理平台登录到各个安全产品，包括下一代防火墙、web 应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全（EDR）、APT 等所有安全产品，无需二次认证； 6、支持用户通过管理平台一键开通任意安全产品，安全产品成功开通后可自动获取计算、存储等虚拟化资源实现自动化部署和激活； 7、安全产品支持试用开通功能，试用产品具备全量产品功能但不消耗产品授权，提升用户体验 8、云安全中心具备租户视角，支持以安全态势大屏和 dashboard 方式展示租户的安全情况，包括资产总数、风险总数、风险资产 TOP 排名、安全风险 TOP 排名、防护事件 TOP 排名等信息； 9、支持按照业务系统及单个资产两种维度展示资产的风险状态，包括高危资产及已失陷资产； 10、具备风险管理模块，租户可统一查看系统中存在的风险总数、高危风险及 WEB 安全事件，并支持基于安全产品及风险类型进行筛选查询； 11、具备日志查询模块，支持统一查看系统内产生的安全日志，日志支持按照搜索语法进行搜索，并支持根据时间进行自定义筛选； 12、支持三权分立安全原则，系统内置多种身份角色，包括系统管理员、业务管理员、安全审计员、操作员等，并支持身份角色自定义 13、支持设置临时成员，可自定义账号有效期，到期后成员将被自动踢出租户团队 14、支持自定义角色权限，可根据业务需求对角色权限进行细粒度分配 15、安全产品支持以通用授权许可的方式进行开通，管理平台只记录许可总数，授权许可将根据产品种类及规格进行按需扣减消耗，支持两个许可合并激活一个高规格的安全产品 16、支持以许可文件包的方式批量导入许可，通过扩展许可数量的方式扩展资源池可激活的安全产品数量 17、支持通过管理平台查看物理机和安全虚拟机的资源占用信息，包含资源 ID / 别名，CPU 使用率、内存使用率、磁盘使用率，网络流入流出速率，并用可视化图表的方式展示 CPU、内存、	

		磁盘占用趋势，网络总流入流出速率趋势；18、支持告警条件自定义，管理员可自定义告警时间、告警阈值、告警持续时间，支持通过邮件方式发送告警信息； 19、内置工单中心，默认提供服务申请、主机登录审批等多种业务类型的工单供租户选择，支持租户自定义工单流程，如审批节点及审批人员 20、支持管理员后台创建工单模板并发布给所有租户，供租户直接调用模板使用 21、支持对工单进行分类统计查看，包括已办工单、待办工单及租户内部所有工单 22、支持通过升级包的方式对管理平台进行升级，并支持版本回退 23、支持对安全组件的特征库进行后台统一更新，如漏洞扫描、主机安全的特征库，管理员通过上传特征库文件，勾选需要升级的安全产品，即可完成一键更新 支持管理员自定义平台 logo 和名称，支持用户自定义更换自己的用户头像； 24、云安全管理平台应具备良好的适配性，可与华为云、浪潮云进行对接。	
3.62	山东省公安信息网大数据智能化安全体系（一期）——应用安全防护服务	提供云上统一运维审计服务能力，包括： 1、支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，客户端工具支持不少于 3000 资产管理，不少于 3000 并发字符。 2、可以通过 socks5/http/ssh 等代理协议连接管理异地云资源区中私有网络的云主机 3、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 4、支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；支持发送方式，包括邮件、FTP、SFTP 等 5、支持自动密码恢复、手工验证密码、密码强度控制等，不少于支持使用常见浏览器打开堡垒机的 Web 页面直接调用 mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX 等运维客户端工具。 6、支持 ssh、telnet、rlogin、rdp、vnc 协议的运维，无需本地运维客户端工具。 7、支持通过堡垒机页面直接调用本地 windows 的 plsql、sqlplus、sqlwb、ssms、mysql.exe 等数据库	一般

		客户端工具。 8、审计数据支持通过SFTP/FTP 方式自动归档，并在页面中可以查询哪些数据是否归档，可以设置归档成功之后自动删除数据，归档后的数据可以用专用播放器离线查看。 9、支持保存 SSH 的 sz/rz 命令（zmodem）传输的原始文件，支持保存SFTP/FTP 传输的原始文件。	
3.63	山东省公安信息网大数据智能化安全体系（一期）——日志审计服务	1、支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集，支持使用代理(Agent)方式提取日志并收集，支持不少于 500 个日志源的采集。 2、采用解决方案包上传对产品进行功能扩展，无需要代码开发。 3、支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器。 4、支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等。5、支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V 等；支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展 6、支持基于内存的实时关联分析，跨设备的多事件关联分析；支持自定义条件都事件进行聚合 7、具备安全评估模型，评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。 8、支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析。 9、支持FTP、SAMBA、NFS 和 FILE 等多种方式的远程服务器日志备份方式。 10、支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。	一般
3.64	山东社会治安动态全息感知网安全防护体系——IPS	1、配置要求：≥4 个千兆光口，≥4 个千兆电口，≥12 个 SFP+万兆光口； 2、吞吐量≥40Gbps； 3、支持防范各种应用层攻击；4、系统预定义入侵防御签名库数量≥7500；5、支持≥4000 种的应用识别能力。	一般
3.65	山东社会治安动态全息感知	配置要求：10GE 光口≥48 个，40GE 光口≥6 个,配置 10GE 多模光模块≥48 个，40GE 多模	一般

	网安全防护体系——交换机	光模块满配，全端口激活；交换容量≥2Tbps，包转发率≥1500Mpps；支持静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、IS-IS、IS-ISv6、BGP、BGP4+等路由协议；支持 VXLAN 功能。	
3.66	山东社会治安动态全息感知网安全防护体系——入侵防御系统	1、配置要求：≥4 个千兆光口，≥4 个千兆电口，≥12 个 SFP+万兆光口； 2、吞吐量≥40Gbps； 3、支持防范各种应用层攻击； 4、系统预定义入侵防御签名库数量≥7500； 5、支持≥4000 种的应用识别能力。	一般
3.67	山东社会治安动态全息感知网安全防护体系——加解密媒体设备（C级）	1、标准机架式机箱，网络接口≥4 个千兆网口 2、支持全码流加密，视频加/解密网络时延≤500ms，时延抖动≤50ms；3、支持 SM1、SM2、SM3、SM4 等国密算法;支持 C 级前端视频解密，支持视频及音频加密传输； 4、支持国产化操作系统和 CPU； 5、支持系统配置备份/恢复、日志审计等系统管理功能； 6、支持日志审计系统管理； 7、支持国产化操作系统和 CPU。	△
3.68	山东社会治安动态全息感知网安全防护体系——安全隔离网闸	1、网口配置千兆电口≥4 个，万兆光口≥4 个， 2、应用层数据传输率≥4Gbps； 3、提供多种主流数据库的单、双向数据交换； 4、可以同时发送和接收多个数据库中的多个表； 5、数据传输可选 SSL 加密，链路安全。	一般
3.69	山东社会治安动态全息感知网安全防护体系——数据库	1、符合 SQL 标准；符合标准的访问标准；支持.NET、Eclipse、JBuilder 等开发环境；支持 WEBlogic、TOMcat、东方通等中间件。 2、支持扩平台操作系统如：Windows\linux 及国产操作系统； 3、支持三权分立；支持独立审计； 4、支持双机热备及故障恢复机制； 5、支持 SQL\DB2\ORACLE 等数据库兼容； 6、大型通用关系型数据库系统，采用成熟的关系数据库模型，支持 SQL 语言，提供多种符合标准的数据访问接口，适合政府行业应用需求。	一般
3.70	山东社会治安动态全息感知网安全防护体系——数据库审计	1、配置要求：≥4 个千兆电口，≥2 个千兆光口（含光模块），双电源； 2、SQL 处理能力≥40000EPS，数据库数审计能力≥20 个； 3、支持主流数据库审计； 4、支持无须在被审计数据库系统上安装任何代理即可实现审计； 5、支持 IPV4/IPV6 双栈审计； 6、支持	一般

		数据库请求和返回的双向审计； 7、支持对数据库自动建模及智能对异常行为告警功能。	
3.71	山东社会治安动态全息感知网安全防护体系——服务器	1、国产化 CPU≥2 颗，每颗 CPU≥32 核心，主频≥2.6GHZ，内存：≥256G；硬盘：≥3*4T，2 块 SSD 硬盘≥960G；RAID 卡：≥1 块，支持 RAID0,1,5,10； 2、网口：千兆网口≥4 个，万兆光网口≥2 个；配置冗余电源，配置标准机架导轨。 3、支持国产化操作系统	一般
3.72	山东社会治安动态全息感知网安全防护体系——用户认证设备	1、标准机架式机箱，网络接口≥4 个千兆电口，支持 SM2、SM3、SM4 等国密算法; 2、支持基于数字证书的视频用户身份认证、单点登录，身份认证≥450 次/秒，并支持配置多张证书链，验证不同类型的用户证书； 3、支持多种认证策略方式、使用的协议、加密强度、以及是否传递相关信息等进行控制满足不同的需要，支持 URL 级别的访问控制，对于不同用户、不同角色实现不同的控制，包括对加密视频的播放、回放、下载、删除等操作； 4、支持认证服务连接模式正反代理、协议类型、数据流向，定义多个服务，根据业务实际需求可灵活配置，自动更新和动态更新黑名单，包括 LDAP、HTTP、手工上传等多种方式更新，采用三权分立管理方式，不同管理员负责不同的管理功能； 5、支持国产化操作系统和 CPU。	一般
3.73	山东社会治安动态全息感知网安全防护体系——省级视频密钥管理系统	1、密钥托管容量≥40 万对；存贮容量≥40 万对； 2、支持国产密码 SM1/SM2/SM3/SM4 算法； 3、支持视频对称密钥产生、存储、备份与恢复、更新、销毁和撤销的生命周期管理；4、支持视频加密密钥 VEK、视频密钥加密密钥 VKEK、视频导出传输密钥 VETK 的管理；5、支持密钥使用授权，保障密钥安全使用；6、支持机构管理； 7、支持兼容对接部级根视频对称密钥管理系统，负责省级二级视频对称密钥管理服务； 8、支持视频密钥加密密钥 VKEK 更新周期≤1 天，视频加密密钥 VEK 更新周期≤1 小时； 9、支持 VKEK 存档管理；10、支持平台视频服务托管； 11、支持平台视频服务接入管理； 12、支持国产化操作系统和 CPU。	一般
3.74	山东社会治安	1、标准机架式硬件设备，双电源标配；≥4	一般

	动态全息感知网安全防护体系——综合审计系统	个千兆电口，1 个 console 口；内存≥16GB；2、EPS≥10000/秒，资管管理数≥200； 3、支持 Syslog、SNMP Trap、HTTP、SFTP 协议日志收集； 4、支持网络安全设备、交换设备、路由设备、操作系统、应用系统、虚拟环境等的日志收集； 5、设备类型的解析规则≥5000 种； 6、支持≥200 个厂家的设备的接入。	
3.75	山东社会治安动态全息感知网安全防护体系——网络数据交换系统	1、 由前后置 2 台服务器构成，配合隔离网闸实现数据交换，单台设备：网口配置≥2 个千兆电口，≥2 个万兆光口（满配光模块）；2、 吞吐量≥4Gbps； 3、 支持主流数据库的同步，可实现异构数据库同步，对数据库所在操作系统无任何要求； 4、 数据库支持多种同步方式； 5、 支持数据库、文件之间的模糊格式同步交换； 6、 支持 FTP 协议的文件传输；7、 支持文件自动重传功能； 8、 支持业务服务器 IP 地址绑定的接入认证； 9、支持管理界面以用户名/口令方式访问；支持鉴别失败处理机制及超时重鉴别机制； 10、支持业务流量统计功能；支持对通道故障进行报警； 11、 支持系统管理员、安全管理员、审计管理员三级权限； 12、支持数据业务监控、安全审计与告警以及运维监控管理和上报监管。	一般
3.76	山东社会治安动态全息感知网安全防护体系——视频专用智能钥匙	1、硬件（USBKey），芯片容量≥256KB；SM2 算法密钥对生成时间≥2 对/秒；签名速度≥30 次/秒；验签速度≥20 次/秒。 2、支持 SM1、SM2、SM3、SM4 算法； 3、支持证书写入功能，支持前端设备认证功能，支持用户认证功能，支持信令认证功能； 4、支持 USB2.0 及以上版本接口； 5、数字证书格式支持 X.509 v3。	一般
3.77	山东社会治安动态全息感知网安全防护体系——视频可信鉴定设备（B 级）	1、标准机架式机箱，网络接口≥4 个千兆电口； 2、支持国产密码 SM1/SM2/SM3/SM4 算法； 3、视频可信鉴定≥2000 次/秒；并发数≥3000； 4、支持证书解析，获取证书中的主题信息及扩展项信息； 5、支持视频文件验证； 6、支持对视频鉴定结果生产鉴定报告；7、支持对鉴定报告进行签名、验签； 8、支持对鉴定报告进行管理； 9、支持国产化操作系统和 CPU。	一般

3.78	山东社会治安动态全息感知网安全防护体系——视频安全接入系统	1、由视频接入认证服务器、视频用户认证服务器、视频安全隔离设备组成；单台设备：≥2 个千兆电口，≥2 个万兆光口（含模块）；视频安全隔离设备：整机≥4 个千兆电口，≥4 个万兆光口（含模块）； 2、吞吐量≧8Gbps 3、高清最大并发数（4Mbps）：≥1700 路； 4、标清最大并发数（2Mbps）：≥3500 路； 5、视频数据误码率<0.5%； 6、视频流传输时延<50ms。 7、支持信令双向传输，视频数据单向传输，对内外网数据均有安全检查机制； 8、基于零反馈单向传输硬件实现视频数据单向传输； 9、支持对登录视频安全接入系统的管理员进行基于口令认证方式的身份认证，对管理员的登录地址、登录超时、远程登录进行限制。 10、支持证书认证功能，建立快速安全的通道，并对通信数据集进行加密，保障传输安全。附 20 只公安数字证书配合业务调试； 11、对设备信息进行匹配，只有符合要求并注册的设备才可接入网络，对不可接入的设备及时阻断并告警。 12、支持多种数据检查，包括数据源、病毒木马(数据小于 1.4KB)及关键字扫描（C/S 客户端模式）等； 13、支持多种协议格式检查，包括视频信令协议格式（SIP）、视频传输协议格式及主流视频监控公司的私有协议视频信令协议格式等； 14、支持对视频资源的访问控制，能够对用户、设备的细粒度授权访问管理； 15、支持流量审计、设备访问审计、告警审计等多种日志审计与告警功能，支持与集中监管与审计系统联动； 16、支持国标模式多个下级域平台对应一个上级域平台的汇聚业务；支持国标模式一个下级域平台对应多个上级平台的共享业务； 17、支持数据安全检查，如数据源检查，网络包格式检查，防止异常分片包的攻击行为； 18、支持敏感信息扫描，对内网出去的数据进行扫描检查并告警，对敏感信息进行及时阻断，预防信息泄露风险； 19、支持病毒木马扫描，对来自外网的不可靠数据进行隔离阻断，杜绝安全风险； 20、支持视频编码协议检查，对诸如 H.264、MPG4 等视频编码协议进行白名单方式和黑名	一般

		单方式检查，并进行及时阻断和告警； 21、支持视频传输协议检查，对诸如 RTSP、RTCP、RTP 等视频传输协议进行白名单方式和黑名单方式检查，并进行及时阻断和告警；22、支持视频控制信令格式检查，对诸如 SIP、SDP 等视频控制信令格式进行白名单方式检查，并进行及时阻断和告警。 23、对审计管理员进行日常审计管理，包括：一般日志消息的审计、告警信息的审计、流量信息的审计、设备访问情况的审计。 24、对审计管理员进行报表化的管理，包括：管理员的登录情况、用户的访问情况、设备被访问情况；25、同时支持 C/S 客户端模式和平台级联模式； 26、支持 GB/T 28181-2011 标准的平台对接； 27、支持 GB/T 28181-2016 标准的平台对接。	
3.79	山东社会治安动态全息感知网安全防护体系——视频安全设备身份证书注册模块	1、注册管理证书≥40 万张，在线服务并发数≥1000，单次请求处理时间≤1 秒； 2、支持国产密码 SM1/SM2/SM3/SM4 算法； 3、支持视频身份证书的注册、更新、废除等生命周期管理； 4、支持灵活的策略配置机制，可自定义证书策略； 5、支持与部级视频安全密钥服务系统兼容对接，向部级系统请求证书的签发，实现设备、平台及用户身份证书的注册管理；6、支持注册多域名的站点证书； 7、支持安全登录机制； 8、支持操作员权限按指定域、权限域、证书类型细分授权； 9、支持三权分立管理，管理员权限相互制约，按系统管理员、操作员、审核员等不同角色授权管理；10、支持国产化操作系统和 CPU。	一般
3.80	山东社会治安动态全息感知网安全防护体系——视频安全设备身份证书申请模块	1、在线申请并发数≥1000；单次请求处理时间≤1 秒； 2、支持国产密码 SM2/SM3/SM4 算法； 3、支持签发国密证书，并可以使用数字证书登录系统； 4、支持批量导入和模糊查询人员数据； 5、支持与视频安全身份证书注册系统兼容对接，实现设备、平台身份证书的申请、审批审核、证书下发等； 6、支持与警务云统一用户管理系统兼容对接，获取用户可信身份信息进行证书申请； 7、支持对视频前端设备整机离线、介质在线、整机在线三种发证模式； 8、支持批量申请证书； 9、支持审批	一般

		审核业务流程灵活调整； 10、支持用户证书、平台证书和设备证书完整生命周期管理； 11、支持本级范围证书发证量统计，可地图区域化可视化展示； 12、支持查看证书操作的历史记录； 13、支持查看各类证书的统计概况； 14、支持查看最新发证趋势； 15、支持查看最新需要待办的事项； 16、支持国产化操作系统，国产数据库和 CPU。	
3.81	山东社会治安动态全息感知网安全防护体系——视频密钥管理设备	1、标准机架式机箱，网络接口≥2 个千兆电口； 2、视频密钥分发速度≥1000TPS，平均无故障时间 MTBF≥30000 小时； 3、支持国产密码 SM1/SM2/SM3/SM4 算法； 4、支持密钥管理，包括：密钥产生、密钥存储、密钥的安全使用和密钥备份恢复等； 5、支持周期性随机检测功能； 6、支持实时随机检测功能； 7、支持密钥支撑管理服务，对使用的对称密钥进行管理； 8、支持视频密钥的安全生成、存储、分发和查询等； 9、支持现有和历史 VKEK 的存储和检索； 10、支持日志审计； 11、支持国产化操作系统和 CPU。	△
3.82	山东社会治安动态全息感知网安全防护体系——视频应用保护网关	1、标准机架式机箱，网路接口≥4 个千兆电口； 2、最大新建连接数≥3000；并发连接数≥10000；SSL 加密流量≥0.8Gbps； 3、支持国产密码 SM1/SM2/SM3/SM4 算法； 4、支持 USBKEY 证书的强身份认证； 5、支持国密 SSLVPN 技术规范； 6、支持单双向证书认证； 7、支持与部级视频应用保护网关上下级联，采用双向认证链路加密服务，保护视频密钥安全传输； 8、支持对连接数、应用访问情况、系统资源占用等信息进行统计； 9、支持管理员三权分立； 10、支持系统备份恢复； 11、支持国产化操作系统和 CPU。	一般
3.83	山东社会治安动态全息感知网安全防护体系——视频数据安全密码设备	1、标准机架式机箱，网络接口≥2 个千兆电口； 2、256 位 SM2 密钥对生产≥350 对/秒；256 位 SM2 签名速度≥700 次/秒，验证速度≥180 次/秒；加密速度≥130 对/秒；解密速度≥220 对/秒；SM1 算法加解密速度≥280Mbps；SM4 算法加解密速度≥135Mbps；SM3 杂凑算法≥200Mbps。 3、支持国产密码 SM1/SM2/SM3/SM4 算法； 4、支持设备初始化和设备自检，设备物理安全防护； 5、支持批	一般

		量生成设备准入信息； 6、支持采用双物理噪声源生成随机数，生成各类对称密钥和非对称密钥； 7、支持密钥安全存储，密钥位于内置的加密硬件中，须与授权管理员的 USBKey 进行密码运算才能够提供服务； 8、支持各类对称密钥和非对称密钥的更新； 9、支持采用基于密钥分割的方式备份密钥和安全数据，保障备份数据的安全性； 10、支持密钥存储采用安全芯片实现密钥的存储，保证密钥的安全；11、支持多级密钥管理体制和权限分离的设备机制，确保密钥安全和设备管控安全； 12、物理分割的工作服务端口和设备管理端口；13、支持具备基于安全 IC 卡的密钥备份、恢复机制； 14、支持产生随机数，随机数符合国家密码管 理局颁布的《随机数检测规范》； 15、支持多进程、多线程调用密码服务接口。 16、支持管理用户采用三权分立的模式，保障设备的安全访问； 17、支持对设备 CPU/内存资源的使用率、当前并发连接数量、服务进程状态等进行实时监控； 18、支持审计管理员对密码设备的管理操作行为进行审计； 19、支持多机并行及负载均衡，满足大压力、高并发的稳定性。	
3.84	山东社会治安动态全息感知网安全防护体系——视频监控共享平台升级改造	1、流量分析系统（一台）：采集口≥4 个千兆口，管理口≥2 个千兆口；流量实时采集和分析性能≥2000Mbps；支持实时捕获并保存网络中的全量通讯数据包；支持原始通讯数据包回放，能提供服务端离线数据包导入模式，回放分析界面和功能与实时采集链路的相同；支持统计分析所有 TCP 会话的通讯流量信息；支持 DPI 深度报文分析处理； 2、流量管理系统（一台）：万兆光接口数量≥48；自适应千兆速率；总监控流量达 480Gbps 输入+480Gbps 输出，共 960Gbps 吞吐量；支持流量分发、流量聚合、流量分流、流量去重、流量过滤、流量清洗、流量统计等功能。 3、全省全息感知巡检服务（一套）：具体服务内容包括：1）按照公安部科信局全国公安机关网络安全检查工作的要求，常态化开展全省安全监测运维工作；2）每天对全省全息感知网内的软硬件设备资产实现在线自动化安全抽查；3）每月完	一般

		成全省全息感知网全覆盖检查 1 次；4）每年不少于 4 次的全省全息感知网内安全检测；组织全省及时修复部局下发的安全隐患；5）提供可视化展示服务，展示全省全息感知网安全态势；6）构建厅本级安全防护、监测、管理和应急处置体系，对重大安全问题的响应和处理，24 小时内解决安全事件；7）为各地市公安局和直属公安局提供专业的全息感知网安全检查工具，支持其完成自查工作；8）按照省厅要求，每年提供不少于 1 次的安全技术培训服务。9)按照公安部和省厅要求，提供监测、安全配置建议和考核等报告。10)按照公安部和省厅要求，提供资产总览展示、管理、告警、盘点、生成报告等可视化展示能力。11)按照公安部和省厅要求，提供全网安全风险检测、展示、分析、预警、生成报告等可视化展示能力。	
3.85	山东社会治安动态全息感知网安全防护体系——视频目录系统	1、管理容量：可达十万级条目； 2、精确查询：10 万条目，单线程<1ms，50 线程<10ms；3、模糊查询：10 万条目，单线程<60ms，50 线程<100ms； 4、引用：宽度超过 50，深度超过 12 级； 5、吞吐量：10 万条目，50 线程，精确查询>10000 次/秒，模糊查询>500 次/秒； 6、复制：从目录服务器的宽度>100，深度>7 级；子树复制的最小粒度为条目；7、全库统计条目及子树统计条目，响应时间<1 秒。 8、最大连接数：1024。 9、支持 LDAP V2、V3 标准，支持 X.509 V3 标准；10、支持与部级视频目录系统兼容对接，同步本省范围证书信息列表； 11、支持导入/导出； 12、支持分页异步读取数据； 13、支持对数字证书、公共密钥、数字签名进行存储和管理。 14、支持存储、发布和管理设备证书信息和 CRL 信息； 15、支持提供证书查询、CRL 查询、权限查询等功能； 16、支持匿名、用户名/简单密码、用户名/摘要密码等多种身份认证方式； 17、支持基于策略语句的访问控制； 18、支持对访问目标的定义可基于条目位置基于条目过滤条件； 19、支持根据 LDAP 身份认证信息为用户或用户组授予相应的访问权限； 20、支持管理的粒度可达到	一般

		条目/属性级，可通过限制 IP 来控制允许访问目录服务器的客户机； 21、支持对于主体的授权，可基于主体的位置特征、主体的属性特征进行策略授权； 22、支持 SSL 和 TLS 实现的安全通道，实现信息传递的私密性保护，满足高安全性的需要； 23、支持全库统计条目及子树统计条目； 24、支持 Schema 的扩展，可实现用户自定义 Schema 文件的载入，用户自定义对象类和属性的加入； 25、支持用户对索引项的扩展，自定义索引项的索引类型； 26、提供图形化的客户端，辅助管理员对目录服务器进行数据管理； 27、提供备份/恢复工具，帮助管理员实现数据灾难恢复； 28、支持 7×24 小时的可用性。	
3.86	山东社会治安动态全息感知网安全防护体系——设备认证设备	1、标准机架式机箱，网路接口≥4 个千兆电口； 2、设备身份双向认证时间延迟≤400ms； 3、支持国密算法； 4、支持基于数字证书的方式对本域安全前端进行身份认证； 5、支持对设备进行单向或双向设备身份认证； 6、支持实现 SIP 信令处理认证和 SIP 路由； 7、支持将设备信息发布到视频目录系统中； 8、采用三权分立管理方式，不同管理员负责不同的管理； 9、支持日志审计； 10、支持国产化操作系统和 CPU。	△
3.87	山东社会治安动态全息感知网安全防护体系——边界安全访问控制网关	1、端口配置≥2 个千兆电口、≥2 个万兆光口（含光模块）； 2、加密宽带吞吐量≥2.6Gbps； 3、支持国产密码 SM2/SM3/SM4 算法； 4、支持单双向认证选择功能，可以设置是否需要提交证书； 5、支持自动更新黑名单、动态更新，不需要重新启动服务； 6、支持多站点证书，不同的服务可以拥有不同的站点证书； 7、支持多证书链功能，一个 SSL 服务中可同时配置多条证书链，验证不同用户证书； 8、支持可以创建多个 SSL 服务，保护不同的应用服务，也可以采用同一个 SSL 服务保护多个应用服务； 9、支持 B/S 应用和 C/S 应用，将资源划分为 web 资源、C/S 资源、地址段资源等多种方式； 10、支持 DNS 穿透功能，外部客户端可以直接使用内部域名访问应用； 11、支持系统客户端策略的统一下发，用户无需对客户端进行任何配置；12、支持采	一般

		用穿透模式和证书转换模式实现对原有https应用的灵活信息传递； 13、支持终端信息注册和管理，基于终端硬件信息准入认证，只能访问被网关保护的网络，无法同时访问其他网络； 14、支持客户端进程控制，控制客户端中哪些应用进程必须存在或者哪些进程不允许存在，哪些应用进程才能通过访问； 15、支持细粒度的访问控制，对于web资源支持基于正则表达式匹配的URL过滤，支持基于文件扩展名、类型的内容控制； 16、支持黑名单和白名单策略模式，可以进行灵活设置； 17、支持系统备份恢复功能，保证系统瘫痪时的快速恢复； 18、支持性能检测功能，对CPU、内存、磁盘容量、连接数、进程等资源情况的收集，便于系统的维护和问题定位。	
3.88	山东社会治安动态全息感知网安全防护体系——防火墙	1、≥4个千兆电口，≥8个万兆光口（含光纤模块），≥2个40G光口（含光纤模块 ），配置≥1T的存储容量，配置双电源； 2、吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万，配置入侵防御、防病毒模块、URL查询升级授权； 3、支持IPv6协议栈、IPV6穿越技术、IPV6路由协议、IPv6 over IPv4 隧道、6RD隧道等。	△
3.89	山东社会治安动态全息感知网安全防护体系——防病毒网关	1、支撑国产平台，具有多重病毒过滤技术、虚拟化病毒分析技术等应用基础； 2、10/100/1000BASE-T接口：≥6个（支持2对Bypass接口）； 3、SFP/GBIC端口：支持Bypass光口，要求支持光口、电口灵活扩展，可扩展到不少于12个光口； 4、HTTP杀毒吞吐量≥950Mbps。	一般
3.90	山东社会治安动态全息感知网安全防护体系——集中监控与审计系统探针系统	1、网口配置：≥4个千兆电口 2、应用吞吐量≥3Gbps； 3、支持 SYSLOG SNMP v2/ v3、Telnet、ICMP 协议方式进行数据和信息采集； 4、支持对网络设备负载及运行状态进行实时监控； 5、支持级联上报功能。	一般
3.91	山东社会治安动态全息感知网安全防护体系——集中监	1、网口配置：≥4个千兆电口 2、应用吞吐量≥3Gbps； 3、能够提供安全接入平台不同层次的信息注册和管理功能； 4、提供对接入终端的查询统计； 5、提供整个平台总拓扑视	一般

	控与审计系统监管系统	图； 6、能够实时看到各种业务当前的运行状态，能够实时监控各种设备当前运行状况。	
3.92	图像信息综合应用平台人像聚类归档模块——**人员比对应用系统	按照公安部要求实现**人员在省厅端的比对应用功能： 1、通过省厅转发平台完成部级2000 万**人员特征接收和同步； 2、对**人特征值存储和本地入库管理，特征数据存储容量不低于 2000 万条； 3、按公安部要求实现安全认证和特征安全解密； 4、按比中轨迹方式对路人数据进行比对预警； 5、提供预警数据浏览、存储、检索； 6、连接上级平台上传轨迹信息并获取人员身份信息，上传报警轨迹时间不得晚于照片抓拍时间 2 小时，需具备数据每日稳定上传部级平台的保障机制,确保数据每日上传部级平台； 7、提供基于聚类档案的**人员实名化能力供聚档平台调用。	一般

4、服务要求

序号	服务要求	指标需求	重要程度
4.1	项目实施要求	所有硬件在签订合同后 60 个自然日内完成供货、安装部署并投入使用；所有软件在签订合同后 270 个自然日内完成试运行；项目整体在365 个自然日内验收合格。	△
		投标人中标后要开展需求调研，细化相关方案，经双方讨论确认后生成需求报告再组织工程实施。	一般
		投标人负责所有采购范围内软件、硬件的开发、交付及实施调试等工作。	△
		投标人应提供合理的实施方案，包括项目进度计划及保证措施，并提出实施策略、项目管理方案、实施进度、实施范围、项目验收方案、系统测试方案、系统发生故障时的应急预案、技术支持及培训方案、实施部署方案及售后服务方案等。	△
4.2	总体架构要求	新一代公安信息网建设部分： 网络综合管理系统，应实现对现有智能网络流量分析系统平台和终端准入管理系统的对接服务，实现登录界面统一、策略联动下发、数据协同共享、告警统一呈现。	△
		大数据中心（数据域部分）： 依据《山东省政务信息系统项目管理办法》（鲁政办字	△

		[2018]37 号）第三十二条要求，优先采购自主可控的业务应用软件。（1）大数据平台系统建设应当遵循统一的 UI 风格。（2）大数据平台各应用系统要基于移动警务平台开发相应的警务移动端应用 APP,要求适配各类警务移动终端。（3）大数据平台安全访问和数据交换要按照公安大数据规范性技术文件要求利用安全基础设施进行开发建设，确保全程用户可信、业务应用可信、服务可信、数据交换可信。山东省公安信息网大数据智能化安全体系（一期）未建设完成之前，数据处理工作先期在用户域进行建设，建设架构均采用分层解耦模式，便于后期迁移进数据域。（4）大数据平台建设使用 PaaS 组件需适配山东公安云计算组件，如有特殊组件需求，需投标人提供相应的软件授权和安装服务。（5）必须满足公安数字证书登陆。（6）采用 WebServices 等 Internet/Intranet 接口技术标准。（7）采用访问控制、提交信息过滤等多种安全手段，提高系统安全性。（8）系统应具有跨平台性，支持多种 Linux 操作系统，支持多类型数据库及主流国产数据库、主流国产中间件，支持目前主流的分布式数据库。（9）全面的浏览器兼容（火狐浏览器、谷歌浏览器、360 浏览器、IE10、IE11 及以上等主流浏览器），分辨率自适应。（10）实现基于微服务架构的管理方式，对 API 接口采用分层解耦的方式进行快速开发，提供支撑实现微服务架构的相关功能。将基础组件微服务、通用业务组件微服务等服务内容以 API 的方式进行开放，实现 API 数据接口的管理以及应用功能组件的复用。	
		山东省公安信息网大数据智能化安全体系部分：（1）为确保本次所招标山东省公安信息网大数据智能化安全体系（一期）中零信任服务相关产品的先进性、产品间系统对接及厂商服务能力，要求所投可信环境感知代理、可信运维代理、可信 API 代理、可信应用代理及安全访问通道其他安全设备产品须实现紧密联动，统一策略管理。（2）本次招标采购的山东省公安信息网大数据智能化安全体系（一	△

		期）数据交换通道要求具备统一衔接和综合利旧能力。（3）本次招标采购的山东省公安信息网大数据智能化安全体系（一期）相关模块应符合公安部大数据安全规范（GA DSJ300/350/351/352 等），后续标准变更后投标人应对该系统免费变更升级。	
		社会治安动态全息感知网安全防护体系（一期）部分：社会治安动态全息感知网安全防护体系（一期）省级视频密钥管理系统、视频安全设备身份证书申请模块，需支持与省厅统一用户机构管理系统兼容对接，实现视频密钥机构的管理和获取用户可信身份信息进行证书申请。	△
		“一门四通”部分：（1）依据《山东省政务信息系统项目管理办法》（鲁政办字[2018]37号）第三十二条要求，优先采购自主可控的业务应用软件。（2）要求部署在采购人指定位置，投标人需要对系统部署所需资源进行估算，提供资源估算方案。（3）架构支持前后端分离技术、分层解耦、微服务管理和协同应用服务，满足公安部的新技术要求。（4）基于微服务架构的管理方式，对 API 接口采用分层解耦的方式进行快速开发，提供支撑实现微服务架构的相关功能。将基础组件微服务、通用业务组件微服务等服务内容以 API 的方式进行开放，实现 API 数据接口的管理以及应用功能组件的复用。（5）软件架构要求具备开放性，提供完整规范的开发接口，能够满足主流平台的快速开发要求。（6）采用 J2EE 的技术架构、全 B/S 结构，三层（多层）技术应用、XML 技术及其应用。（7）采用 WebServices 等 Internet/Intranet 接口技术标准。（8）采用访问控制、提交信息过滤等多种安全手段，提高系统安全性。（9）系统应具有跨平台性，支持 Linux 和 Windows 操作系统，持多类型数据库及主流国产数据库、主流国产中间件，支持目前主流的分布式数据库。（10）全面的浏览器兼容，分辨率自适应。	一般
4.3	系统性能指标要求	（1）稳定性指标：系统保证 7×24 小时不间断运行。（2）处理时间（指从发送 HTTP 请	一般

		求给WEB服务器，到WEB服务器发送过来第一个字节的间隔时间，即网站处理访问请求的时间差）小于等于100ms。	
		大数据中心（数据域部分）： 投标人应按照公安部所下发的大数据处理相关规范要求对标建设，以实现公安部要求的完整省级公安大数据平台功能并包含共建地市部分大数据平台功能。系统架构应满足高可用性、高可靠性、分层解耦的要求，各系统和组件在用户域和数据域分别实现统一界面登录，按照平台要求实现统一授权管理。随着用户数的增长及功能应用的增长，软件系统随硬件性能的调整而保持相对的稳定性。数据服务接口调用并发数不少于500。大数据平台的接口和数据服务要求通过域名访问的方式提供服务，域名命名需符合山东省公安厅域名命名管理要求。	一般
		“一门四通”部分： （1）吞吐量指标：同时在线用户数不小于5000个，根据在线用户数，可动态扩展。用户登录认证并发数不少于1000个，根据在线用户数，可动态扩展。（2）一体化业务协同性能：支持并发数不少于2000。平均响应时间延时不大于300ms。（3）业务性能指标：系统响应时间：单一条件查询不大于3秒；组合条件查询不大于5秒；关联查询不大于8秒。系统满足实时业务处理的要求，1000万行单表有索引的数据复用响应时间不大于3秒。事务处理指标（1000用户同时在线情况下），简单事务处理（主要指各类信息录入、修改、主要页面平均响应时间等）不大于3秒。	一般
4.4	知识产权要求	本项目所开发软件的知识产权包括专利权、著作权等，归投标人和采购人双方共享，申请知识产权相关费用由投标人承担，包含在总报价内。未经采购人同意，投标人不得以任何方式向第三方披露、转让和许可有关的技术成果、计算机软件、关键技术、秘密信息、技术资料和文件等项目相关信息。投标人就本项目开发的软件等内容（不包含第三方商业软件），应向采购人提供全部源代码和文档（注释语句不少于30%），采购人可无限制使用该软件。投标人使用的第三方及其他软件的价格应在投标	一般

		报价中包含，未写明的出现问题由投标人承担责任。投标人应保证采购人使用该系统及服务或其中的任何一部分时，免受第三方提出的侵犯其知识产权的索赔或诉讼，如有任何上述指控，投标人应与第三方交涉并独自承担可能发生的一切法律责任和费用。	
4.5	资料要求	实施前提供系统最新版本完备准确的工程技术资料。投标人根据项目进展和合同要求，按照系统工程、软件工程方法，按时提供相关文档及技术成果。文档必须满足国家标准、行业标准、建设单位和监理单位的要求。 各阶段投标人应提交的文档包括但不限于： （1）项目管理类：项目计划文档，软件配置管理计划，文档编制规范，软件质量保证计划，项目变更控制文档，项目验收计划，项目总结报告等。（2）软件开发类：总体方案规划报告，需求调研计划，需求调研材料，软件需求分析报告，软件概要设计说明书，软件详细设计，项目测试大纲，项目测试报告，软件开发编码规范等。 （3）组织实施类：系统部署实施计划，部署实施方案等。 （4）系统管理与维护类：运营手册，运维手册，各类管理员手册，用户操作手册，用户培训手册等。	△
4.6	安全保密性要求	投标人必须遵守与采购人签订的保密协议，未经采购人书面许可，投标人不得以任何形式向第三方透露本项目标书以及本项目的任何内容，保证对工程实施过程中产生的各类技术文件、信息以及由采购人、监理单位提供的所有内部资料、技术文档、数据和信息予以保密。项目建设符合网络信息安全等保2.0三级要求，采用国产密码技术进行保护，通过建立完善的安全保障体系、安全防护体系及安全管理体系保障项目安全可靠运行。	一般
4.7	软件测评要求	开发类软件应按照有关国家和行业标准进行严格的单元测试、集成测试和用户接受测试等，投标人应配合相关单位实施安全等级保护测评工作，及时发现问题并整改，之后采购人组织系统验收。验收测试中产生的问题，投标人须及时解决。当主要指标及性能达不到规范要求时，将再做系统测试，并按合同有关条款处理，直到采购人认为有条件通过验收为止。	一般

4.8	培训要求	投标人需提供有效的、切实可行的培训计划，为用户提供技术和应用培训（含教师、课程讲义），列明培训时间、培训对象、内容、培训方式等。投标人需要对全省各级公安机关相关人员、技术人员、业务骨干等多层次进行培训，业务骨干、技术人员集中培训至少 2 次以上，视频培训按需进行。投标人应根据项目实际需要，向用户提供全面的软硬件的安装、集成、维护操作、故障排除及使用培训，使用户能够尽快地熟悉系统的性能和使用方法，具备独立进行管理、故障处理、日常维护使用等工作能力。培训时间、地点由用户指定。	一般
		大数据中心（数据域部分）： 投标人为采购人提供不少于 200 人的大数据处理技术认证培训，培训时间不少于 5 天，提供培训视频大于 30 个学时，提供培训 PPT 大于 20 个；提供不少于 20 人的原厂大数据认证培训，原厂培训时间不少于 10 天，提供参加原厂最高级认证考试，相关费用由投标人承担，包含在总报价内。	一般
4.9	质保要求	（1）质保期限三年。 （2）质保期内，投标人免费为用户进行版本升级更新，如遇标准规则变化等特殊情况，须配合提供版本升级更新和部署方案调整服务，采购人指定驻场办公场所或由投标人提供就近办公场所；质保期外，投标人须提供售后服务的维护方案及其他服务等。 （3）软件支持服务：软件更新授权 7×24。 （4）硬件支持服务：备件先行 7×10×ND（下一自然日到达/送达）、故障件提取；硬件更换 7×10×ND（下一自然日到达/送达）、问题处理 7×10×ND（下一自然日到达/送达）。 （5）远程支持服务：热线受理 7×24、远程问题处理 7×24、智能保障、在线技术支持 7×24。 （6）快速响应服务：对于紧急的问题在 2 小时内到达现场，当天处理。此类问题包括：服务器系统、应用系统严重错误等。 （7）故障处理服务：所有故障应在 24 小时内完成修复；同一设备运维期内连续 3 次出现同一故障的，投标人应负责免费更换成熟的不低于同档次设备。 （8）定期环境检修服务：在系统投入运行后，投标人应派出	△

		技术人员提供至少每季度一次的定期巡检，以确保软硬件系统的正常稳定运行。在现网出现大规模调整和升级的情况下，根据要求提供不定期的日常巡检。主要工作内容包括：收集用户使用信息，对网络环境的检查、清理，解答用户疑难，通报开发方近期相关项目的应用经验等工作，并将结果及时反馈客户。（9）功能优化服务：在完成所有建设内容后，投标人应根据巡检报告和采购人需求，提供功能优化方案，每年对系统提供不少于 1 次的功能优化。（10）在重大会议期间，可根据需要提供保障服务：派出经验丰富的技术专家，进行现场或远程的保障服务，协助用户对系统进行现场安全值守，对系统的运行状况进行实时监控和日志分析。	
		大数据中心（数据域部分）： 质保期内应提供原厂现场服务、大数据平台运营运维服务、数据治理服务、数据处理服务、数据管理服务、模型开发服务、模型算法调优服务、数据开发服务和数据接口开发服务、大数据平台二次开发服务等服务内容，以上服务费用包含在总报价内。	△
4.10	人员要求	投标人应承诺组建本地化项目实施团队，明确负责人及组成人员（投标文件中列明人员名单、职务、工作职责、联系电话等）并承诺保证人员稳定，负责项目实施建设、交付和后续运行维护，按时保质保量完成相关建设并提供高质量的后续服务。在项目开发周期内，投标人应提供不少于 50 人的驻场开发人员，并须保持人员稳定，如出现人员调离等原因调整的，须及时将调整人员信息报送采购人并征得采购人同意；采购人有权提出更换驻场技术人员。项目组团队人员配置科学合理、分工明确，至少应包括项目经理、技术负责人、测试负责人、系统分析师、系统设计人员、软件开发人员、测试人员、配置管理员、质量保证员、用户培训人员、部署实施人员、运行维护人员等角色。除驻场人员外，投标人还应具备一定规模和专业的二线支持团队，系统升级和系统集中使用期间，二线支持团队应根据要求进行驻场服务。	一般

		在项目质保期内，投标人应提供驻场技术服务人员 57 人，负责包括新一代公安信息网建设部分、大数据中心（数据域部分）、新一代移动警务部分、公安信息网大数据智能化安全体系部分、社会治安动态全息感知网安全防护体系部分、“一门四通”部分、图像信息综合应用平台人像聚类归档模块部分的驻场运维服务工作。	★
		新一代公安信息网建设部分： 本服务为针对该项目的新一代公安信息网建设部分所提供的驻场运维服务，服务不单独列预算，含在整体预算里。 要求驻场人员 2 人，负责整个项目的统筹与具体运维管理工作。	△
		大数据中心（数据域部分）： 本服务为针对该项目的大数据中心（数据域部分）所提供的驻场运维服务，服务不单独列预算，含在整体预算里。 在质保期内，在省厅现场派驻 22 名技术服务人员，具体要求如下： （1）项目经理（1 人）：负责梳理整体数据资产及治理情况，制定数据治理计划并分解工作任务及里程碑，为数据治理产出及质量负责。 （2）大数据算法工程师（2 人）：负责设计、训练和测试机器学习、深度学习算法模型，并进行各警种实战业务场景进行算法模型调优。负责数据收集、整理和分析，并设计模型的校验方案。利用机器学习计算支撑系统构建基于机器学习的公安业务实战模型。 （3）数据开发工程师（8 人）：负责完成数据的接入、处理、治理的相关数据及接口服务开发工作。 （4）数据分析工程师（4 人）：负责收集业务侧用户需求，完成数据服务、数据赋能的相关数据、模型、业务算子等开发及服务工作，对数据治理提出相关需求建议。 （5）前端开发工程师（1 人）：负责前端框架设计与开发，与后端程序技术团队有效配合，完成功能的开发工作。 （6）UI 设计工程师（1 人）：负责系统界面、服务应用化的界面设计及美工。 （7）软件开发工程师（3 人）：负责在维保期内采购人需求变更及特殊任务对应的软件功能的设计、应用开发和 APP 开发。 （8）大数据平台数据库管理员和平台运维人员（2 人）：熟悉	△

		主流 Linux 操作系统、数据库、云计算平台和大数据组件 Hadoop、Spark 和 Flink 等。	
		新一代移动警务部分： 本服务为针对该项目的新一代移动警务部分所提供的驻场运维服务，服务不单独列预算，含在整体预算里。 提供驻场人员 2 人（1 人负责设备运行及安全服务，1 人负责软件系统维护和升级）。要求如下：（1）提供不限次数上门服务，根据用求完成年度安全检查和攻防任务。（2）提供包括但不仅限于系统升级、安全策略配置、系统安全扫描、安全日志分析、系统安全加固，并提供安全应急服务和重大安保服务。	△
		公安信息网大数据智能化安全体系部分： 本服务为针对该项目的公安信息网大数据智能化安全体系部分所提供的驻场运维服务，服务不单独列预算，含在整体预算里。 驻场人员 14 人：项目负责人 1 人，负责整个项目的运维协调管理；安全管理中心 3 人；零信任体系 5 人；安全防护体系 2 人；安全访问与数据交换通道 3 人。要求如下：（1）负责整个项目的统筹与具体运维管理工作；（2）具备网络安全设备日常维护经验，具有相关的网络攻击和防御技术与经验；（3）提供 5×8 现场安全技术支持服务，7×24 技术支持。	△
		社会治安动态全息感知网安全防护体系部分： 本服务为针对该项目的社会治安动态全息感知网安全防护体系部分所提供的驻场运维服务，服务不单独列预算，含在整体预算里。 驻场人员 9 人：项目负责人 1 人，负责整个项目的运维协调管理；安全认证体系 2 人；安全防护体系 2 人；安全检测体系 4 人（其中防止违规外联能力 1 人，流量管理能力 1 人，全省全息感知巡检服务 2 人）。要求如下：（1）负责整个项目的统筹与具体运维管理工作；（2）具备网络安全设备日常维护经验，具有相关的网络攻击和防御技术与经验；（3）提供 5×8 现场安全技术支持服务，7×24 技术支持。	△
		“一门四通”部分： 本服务为针对该项目的“一门四通”部分所提供的驻场运维服务，服	△

		务不单独列预算，含在整体预算里。 在质保期内，驻场人员 4 人：“一门通晓”需提供 1 人，“一门通办”需提供 1 人；“一门通查”需提供 1 人，“一门通考”需提供 1 人。负责整个项目的统筹与具体运维管理工作，包括软件的调试、日常维护以及技术培训等相关服务。	
		图像信息综合应用平台人像聚类归档模块部分： 本服务为针对该项目的人像聚档归档模块所提供的驻场运维服务，服务不单独列预算，含在整体预算里。 驻场人员 4 人：包含项目经理 1 人，负责整个项目的运维协调管理；数据治理与组织 2 人；专业应用服务 1 人。要求如下： （1）负责整个人像聚档归档模块的统筹与具体运维管理工作； （2）团队人员均需具备视频智能化建设项目建设和维护经验； （3）提供 5×8 现场技术支持服务。	△

5、其他要求

序号	其他要求名称	其他要求	重要程度
5.1	交钥匙工程	本项目为“交钥匙”工程。	一般
5.2	信创适配	所有软件应适配信创环境。	一般