

用户需求书

项目名称: 上海市公安局智能体构建及测评工具子系统
建设项目

责任单位: 上海市公安局科技信息化总队

目录

一、 背景与现状概述	5
二、 目标与任务	5
三、 设计方案	7
(一) 业务流程、数据和数据流分析	7
1、智能体构建流程	7
2、 测评流程	7
(二) 功能和性能需求	7
1. 智能体运行	7
2. 智能体构建	12
3. 应用管理	15
4. 扩展工具	16
5. 知识库工具	34
6. 评测中心	43
7. 通用知识库	48
8. 产品软件采购（智能体平台）	51
9. 其他	51
四、 技术性能指标及配置要求	53
五、 进度安排	55
六、 实施要求和技术服务要求	56
(一) 质量保证期	56
(二) 培训要求	56
(三) 运维人员要求	57
七、 招标方案、投标单位资质要求及投标书应答要求 ..	57
(二) 投标单位资质要求	58

(三) 关于转让和分包的规定	58
(四) 投标书应答要求	58
(五) 知识产权及保密要求	59
八、 项目验收	576

一、背景与现状概述

2023 年以来，人工智能大模型浪潮持续涌动。国内外一大批创新企业和高校院所加大研究力度，纷纷推出各自的大模型产品。国内 10 亿参数规模以上的大模型数量已超 100 个，大量高质量模型百花齐放，助力中国成为全球人工智能发展的领头羊之一。

上海市公安深入科技领域研究探讨新技术，结合国内大模型浪潮，结合国家公安部科技部推进科技兴警三年行动计划，加强上海公安重大业务需求科技支撑能力，聚焦智慧警务基础支撑，运用人工智能、大模型等新技术，结合公安业务场景打造示范级应用场景，赋能各警种业务使用。

各类大模型结合业务使用的需求不断涌现，为进一步提升大模型在公安领域的高效使用，实现对各大模型有效管理，创新式实现公安大模型管理标准与规范，形成上海市公安统一模型管理范式。

为便捷、规范上海公安大模型应用建设，减少共性功能的投资，本次拟统筹建设大模型智能体基础功能及相应可视化功能，为全市公安大模型应用构建提供智能体及模型测评等基础功能。

二、目标与任务

（一）主要目标

基于模型赋能平台、算力纳管平台的建设成果，构建覆盖市-区两级的智能体应用开发与生态体系。聚焦解决应用构建效率低、成果实用性不足、协作缺乏规范等核心

问题，通过技术迭代与机制创新，实现警务智能应用从"可用"到"好用"的跨越，打造支撑人工智能背景下的警务应用核心基础设施，形成可复制、可推广的警务智能应用建设范式。

目标一：智能体应用构建效能提升

构建可视化、低代码的智能体应用开发框架，集成既有的大模型能力（大模型、知识库、基础问答等），实现大模型应用中通用功能模块的即拖即用。

目标二：智能体应用服务能力进阶

通过平台提供的基础调优能力，为智能体应用在问答类场景的准确性进行进一步提升。

目标三：生态共建机制构建

制定相关技术规范，涵盖设计、开发、运营全周期标准，并特别明确市区两级数据接口协议、安全防护要求及业务协同流程。

（二）建设任务

主要完成智能体、工具箱和评测中心在内的软件开发以及智能体平台的产品购置与集成。

1、智能体是由产品软件智能体平台及智能体权限管理、智能体应用中心等知识开发内容组成，为全局智能体应用构建提供基础能力。

2、工具箱主要包括知识库构建等通用工具，知识问答场景模型调优工具以及基本的工具注册管理服务。

3、评测中心主要由评测中心基础能力、评测任务管

理、评测数据集管理 3 部分构成。

三、设计方案

（一）业务流程、数据和数据流分析

1、智能体构建流程

智能体以用户域为主导，聚焦于满足市局业务场景的应用需求。基于业务场景定位开展需求分析，通过工具集成、环境准备、智能体设计与开发，完成测试验证，实现智能体的部署与发布以及基于发布的智能体开展监控优化等整体构建流程。

2、测评流程

测评流程需包含但不限于算力测评流程、模型测评流程、应用测评流程。需满足基于评测目标和具体的业务场景，开展环境准备、功能测试、性能测试，并开展用户实践以及评测结果分析、迭代优化等工作。

（二）功能和性能需求

1. 智能体运行

功能清单如下：

层级	二级功能	三级功能	四级功能
智能体运行	智能体应用中心	服务订阅	订阅可视化
			事件订阅
			标签订阅
			分级订阅
			事件通知

			智能体行为绑定
			触发条件定义模块
			订阅源异常处置模块
			订阅源动态解绑
		应用广场	应用分类展示
			应用检索与筛选
			应用详情查看
			应用复制导入
			应用评分与评论
			应用权限管理
			应用收藏管理
		用户智能体管理	我的智能体管理
			权限控制
			数据偏好设置
		在线辅导工具	提示词优化辅导
			系统操作辅导
	智能体管理	智能体交互确权	权限验证及实时管控-双重校验

1.1. 智能体应用中心

1.1.1. 服务订阅

1.1.1.1. 订阅可视化

智能体编排平台内，提供可视化订阅配置界面，对不同类型的消息推送订阅服务进行定制化开发，并通过多渠道推送通知。

1.1.1.2. 事件订阅

智能体编排平台内，对于消息推送按事件类型订阅，涉及事件订阅内容为针对资源告警、审批消息、版本更新、服务状态变更、消息通知等内容。

1.1.1.3. 标签订阅

智能体编排平台内，系统支持智能体根据业务需求，按“知识问答”“数据分析”等功能标签自主订阅，精准匹配所需服务能力，无需冗余配置，高效获取对应功能支持，适配多样化使用场景。

1.1.1.4. 分级订阅

智能体编排平台内，按照用户不同角色权限划分，分级订阅权限控制，针对审批消息、资源告警等与权限相关的消息进行分级订阅。

1.1.1.5. 事件通知

智能体编排平台内，针对资源告警、审批消息、版本更新、消息通知、服务状态变更等事件，在智能体应用中心中实现消息推送功能。

1.1.1.6. 智能体行为绑定

智能体编排平台内，系统支持将智能体订阅的内容与其实时行为策略深度绑定，订阅内容更新时可自动触发对应策略调整（如更新发布至智能体广场，则推送消息弹窗），确保智能体行为与订阅需求精准同步，提升响应效率。

1.1.1.7. 触发条件定义模块

智能体编排平台内，内置规则引擎，允许用户自定义订阅触发条件，支持按事件类型筛选，实现订阅事件与执行逻辑的自动化关联。

1.1.1.8. 订阅源异常处置模块

智能体编排平台内，对订阅服务增加保活机制，对长时间未更新或频繁报错的订阅源并自动尝试重连。

1.1.1.9. 订阅源动态解绑

智能体编排平台内，系统支持智能体根据任务场景变化，由用户灵活对现有订阅关系执行动态解绑操作，停止接收其推送消息，也可按需重新订阅所需内容，无需复杂流程。

1.1.2. 应用广场

1.1.2.1. 应用分类展示

按功能类型（如知识问答、数据分析等）对发布上线的智能体应用进行分层级分类展示。

1.1.2.2. 应用检索与筛选

支持关键词搜索、标签过滤等方式快速定位目标应用。

1.1.2.3. 应用详情查看

提供智能体应用的功能介绍、演示文档、作者信息等详细信息。

1.1.2.4. 应用复制导入

当用户具有智能体的使用权限后，可在应用广场中复制智能体导入目标空间。

1.1.2.5. 应用评分与评论

允许用户对使用过的智能体应用进行评分和留言。

1.1.2.6. 应用权限管理

区分公开应用、专业应用、专属应用，支持发布者设置应用的运行及复制权限。

1.1.2.7. 应用收藏管理

允许用户对应用广场内对感兴趣的智能体应用收藏以便后续查看。

1.1.3. 用户智能体管理

1.1.3.1. 我的智能体管理

智能体应用中心提供用户对不同开发阶段的智能体进行管理，其中涉及项目开发、发布、上线三个阶段控制。

1.1.3.2. 权限控制

智能体发布/上线可选择发布至项目空间/应用广场，其应用广场内对应权限为：仅查看简介、可运行、可创建副本，并由对应权限审批者进行审批。

1.1.3.3. 数据偏好设置

指定智能体优先使用的数据源（即知识服务节点优先预设个人知识库），从而对智能体使用数据进行偏好设置。

1.1.3.4. 在线辅导工具-提示词优化辅导

通过提供操作指引的方式，提供提示词优化辅导，从而指引用户在构建的提示词可以精准传递用户意图，以便大语言模型理解。

1.1.3.5. 在线辅导工具-系统操作辅导

通过提供操作指引的方式，提供系统操作辅导，使用户快速获得系统操作的辅导建议，从而快速的学会系统操作，减低用户学习成本。

1.2. 智能体管理

1.2.1. 智能体交互确权

1.2.1.1. 权限验证及实时管控-双重校验

智能体主动发起交互过程中，将同步开启系统权限与用户授权双重校验机制，确保交互操作合规且安全。

2. 智能体构建

功能清单如下：

层级	二级功能	三级功能	四级功能
智能体构建	智能体权限管理	智能体权限审批	人工申请
			分级审批节点设计
			审批决策支持
			审批操作及意见
		智能体权限架构设计	
		资源分级管控	业务分类

			生命周期状态分类
			单位职能分类
			资源权限管控
		组织架构/角色 权限模型支持	多级警务组织架构建模
			警务角色权限矩阵
			三维权限体系

2.1. 智能体权限管理

2.1.1. 智能体权限审批

2.1.1.1. 人工申请

可对智能体发布上线至智能体广场进行人工申请。申请基于分级审批节点逐级传递。

2.1.1.2. 分级审批节点设计

对发布上线至应用广场及智能体广场内的运行、复制权限进行审批节点细分。

2.1.1.3. 审批决策支持

在审批或查阅环节，需完整展示申请的全部详情，具体涵盖智能体名称、简介、智能体作者、作者所在单位、审批内容等信息，确保信息全面透明。

2.1.1.4. 审批操作及意见

在审批流程中，需根据实际情况完成通过或驳回的审批动作，并按照审批结果对申请人进行消息推送告知。

2.1.1.5. 智能体权限架构设计

对智能体未发布、已发布、已上线三种状态，结合所属的单位/项目空间，针对不同用户角色对智能体的权限架构细分。

2.1.2. 资源分级管控

2.1.2.1. 业务分类

系统可有效支撑业务维度的资源分类管理，针对工具类应用、知识库文档、应用广场内应用等多类型资源，能依据不同业务场景下的资源属性与用途，精准划分至对应业务资源类别，提升资源调用效率。

2.1.2.2. 生命周期状态分类

系统支持智能体资源从创建初始化、上线发布、日常运维优化，到版本迭代更新，再到下线注销的全生命周期管理，确保各阶段资源配置合理、运行稳定且符合业务需求。

2.1.2.3. 单位职能分类

系统支持按组织架构对资源进行精细化分类管理，可针对不同分局、不同下属单位的业务属性与使用需求，将各类资源精准划分至对应主体，方便各单位高效调取、管理专属资源。

2.1.2.4. 资源权限管控

系统支持对工具、知识库、大模型、应用广场内应用等多类型资源，按用户个体、角色群体、组织层级维度，批量完成权限授予操作，也可按需批量收回相关权限，提升权限管理效率。

2.1.3. 组织架构/角色权限模型支持

2.1.3.1. 多级警务组织架构建模

在智能体权限管理模块中，其组织架构 / 角色权限模型可支持市、区等多级警务组织架构建模，同时能顺畅接入警务4A系统，实现权限数据同步，保障警务权限管理合规高效

2.1.3.2. 警务角色权限矩阵

提供标准角色库直接选用与自定义角色按需设置功能，可对智能体及资源库内进行权限管控，适配警务权限管理需求

2.1.3.3. 三维权限体系

从角色、资源、操作三个维度交叉控制访问权限，角色定身份、资源定范围、操作定行为，实现细粒度的权限精准管控，确保权限分配贴合实际使用场景且管控严谨

3. 应用管理

功能清单如下：

层级	二级功能	三级功能
应用管理	应用计量	用量统计（调用/时长）
		资源消耗计量（CPU/内存/模型 token 数/网络流量）
		实时数据监控
	应用流控	流量阈值设置
		过载熔断保护
		实时流量监控

3.1. 应用计量

3.1.1. 用量统计（调用/时长）

实时记录应用调用次数与使用时长，按对象、时段等维度分类统计，生成量化结果。

3.1.2. 资源消耗计量（CPU/内存/模型 token 数/网络流量）

实时监测应用模型 token 消耗及网络流量，按对象、时段等维度统计，生成量化数据

3.1.3. 实时数据监控

实时采集应用调用、资源消耗等数据，监控关键指标动态，展示用量与消耗状态，触发异常预警。

3.2. 应用流控

3.2.1. 流量阈值设置

支持按应用维度，对其调用大模型次数进行流量阈值设置，并可按组织、角色、用户维护进行设置。

3.2.2. 过载熔断保护

实时监测应用负载状态，当请求量或资源占用超阈值时自动触发熔断，暂停接收新请求，待恢复正常后逐步放行。

3.2.3. 实时流量监控

实时监测应用请求量、大模型调用量等流量数据，并纳入流控系统统一管理。

4. 扩展工具

功能清单如下：

层级	二级功能	三级功能	四级功能
扩展工具	通用工具	标准问题文本转SQL	表格上传模块
			表格问答模块
			数据提示词模块
			表格处理-代码生成与执行模块
		语音识别工具（接入）	
		OCR 解析工具（接入）	
		文本知识转脑图	文档上传模块
			脑图提示词模块
			脑图问答模块
			脑图代码生成及预览模块
			脑图总结
			可视化预览
			导出模块
		数据生成图表工具	
		代码解释器	代码生成模块
			代码执行模块
			代码预览模块
			语法检查模块
			错误提示模块
			代码复制模块
			代码导出模块
			跨平台运营模块

			交互执行模块
			脚本执行模块
		跨站搜索	目标网页配置与爬取范围设定
			网页内容智能抓取与解析
			爬取数据实时清洗与去重
			用户搜索 query 解析与意图识别
			网页资源索引构建与更新
			搜索结果排序与精准展示
		过程/临时数据处理工具	暂存数据库结构配置与参数设定
			临时数据实时入库与分类存储
			多格式文件上传与解析适配
			暂存数据安全导出与格式转换
			过期数据自动清理与空间释放
	工具注册管理	Function call	工具管理模块
			调用决策模块
			执行控制模块
			结果处理模块
			监控与调试模块
		模型上下文协议 (本期 MCP)	MCPserver 模块
			MCPclient 模块
			MCPHost 模块
			上下文信息存储
			上下文状态更新

			共享与传递
			可视化模块
		工具 API 调用	API 注册模块
			请求构建模块
			异步请求模块
			响应解析模块
			错误重试模块
			日志记录模块
	通用工具	应用调优工具 (知识问答)	调优工具可视化模块-RAG 流程 配置模块
			调优工具可视化模块-RAG 组件 配置模块
			调优工具可视化模块-RAG 输出 验证模块
			调优工具可视化模块-RAG 结果 发布模块
			调优工具流程编排引擎
			知识场景化关联工具
			预检索分类工具
			检索调优工具
			后检索调优工具
			生成优化工具
		应用调优测试工 程 (知识问答)	全链路数据追踪模块-流程节点 追踪子模块

			全链路数据追踪模块-节点变量 监控
			全链路数据追踪模块-全链路审 计日志子模块
			人工标记模块-交互式标记面板
			人工标记模块-数据导入
			人工标记模块-标记关联
			人工标记模块-多轮对话标记支 持
			人工标记模块-批量标记
			人工标记模块-数据导出
	业务工具	人员信息问数	人员信息关联数据查询业务思维 链
			人员信息多轮问答对话流调优
			人员信息元数据治理整合
		车辆信息问数	车辆信息关联数据查询业务思维 链
			车辆信息多轮问答对话流调优
			车辆信息元数据治理整合
		人脸信息问数	人像轨迹关联数据查询业务思维 链
			人像轨迹多轮问答对话流调优
			人像多模态解析模块
		驾照信息问数	驾驶证照信息关联数据查询业务

			思维链
			驾驶证照信息多轮问答对话流调
			优
			驾照多模态解析模块

4.1. 标准问题文本转 SQL

4.1.1 表格上传模块

支持上传多文档格式（xls/xlsx/csv 文件等），对输入表格进行内容解析和预处理，确保符合大模型的输入要求。

表格问答模块

提供通过文本进行数据包类相关的问答的基础能力。能够基于对自然语言的理解，转化为对于表格内数据的问答功能。

数据提示词模块

可编辑数据问答的提示词模板，引导模型进行推理生成。

表格处理-代码生成与执行模块

基于模型能力与数据表格，支持生成对应的 Python, sql 等代码并执行获得处理后的表格结果。

4.2. 语音识别工具（接入）

接入公安现有语音识别工具。

4.3. OCR 解析工具（接入）

接入公安现有 ocr 工具，接入后，可在线完成校验，并在线编辑，并保存到新的文档。

4.4. 文本知识转脑图

4.4.1. 文档上传模块

支持上传多文档格式（doc、docx、xls、xlsx 文件等），对输入文档进行内容解析和预处理，确保符合大模型的输入要求。

4.4.2. 脑图提示词模块

提供可编辑脑图的提示词模板，引导模型进行推理生成。

4.4.3. 脑图问答模块

提供通过文本进行脑图生成类相关的问答的基础能力。

4.4.4. 脑图代码生成及预览模块

基于模型能力与输入文本，生成对应的 xml/markdown 内容并执行获得结果，支持在对话框里预览代码解释器并展示 xml 代码/markdown 内容。

4.4.5. 脑图总结

支持调用大模型能力进行脑图解读，生成总结文本。

4.4.6. 可视化预览

基于脑图文件前端渲染可视化的脑图并于对话框内进行展示。

4.4.7. 导出模块

支持脑图源文件（.mm/.md）和图片（.jpg）导出。

4.5. 数据生成图表工具

基于开源工具进行接入。并优化其参数动态适配图表、下钻的效果。支持趋势图、柱状图、饼状图。

4.6. 代码解释器

4.6.1. 代码生成模块

支持用户可在对话框输入文本，借助大模型生成 Python3、js 等代码

4.6.2. 代码执行模块

能够读取并逐行解析源代码，将其转换为机器指令后执行，实现代码所定义的功能。

4.6.3. 代码预览模块

支持在浏览器展示代码解释器结果。

4.6.4. 语法检查模块

在代码执行前或执行过程中，依据特定编程语言的语法规则，检测代码是否存在语法错误。

4.6.5. 错误提示模块

当检测到代码中的语法错误、运行时错误等问题时，向开发者提供详细的错误信息，指出错误位置和可能原因。

4.6.6. 代码复制模块

支持用户复制代码解释器内的代码内容。

4.6.7. 代码导出模块

支持用户一键导出对应的代码文件（.py/.js 等）。

4.6.8. 跨平台运营模块

能够在不同的操作系统（如 Windows、Linux 等）和硬件架构上运行，保证代码的可移植性。

4.6.9. 交互执行模块

允许开发者在交互式环境中直接输入代码并立即执行，快速查看执行结果，便于代码测试和实验。

4.6.10. 脚本执行模块

支持执行包含一系列命令和操作的脚本文件，实现批量处理。

4.7. 跨站搜索

4.7.1. 目标网页配置与爬取范围设定

支持自定义目标网页地址及爬取深度、范围，预设规则过滤无关页面，确保爬取聚焦有效资源，适配多样化需求

4.7.2. 网页内容智能抓取与解析

自动抓取网页文本、图片等内容，解析 HTML 结构提取关键信息，适配动态加载页面，保障内容获取完整性。

4.7.3. 爬取数据实时清洗与去重

对抓取数据进行格式校验、冗余剔除，去除重复内容及无效信息，净化数据提升可用性。

4.7.4. 用户搜索 query 解析与意图识别

接收用户搜索关键词，解析语义意图，识别核心需求，转化为精准检索条件，提升搜索匹配度。

4.7.5. 网页资源索引构建与更新

对爬取数据建立结构化索引，实时更新资源库信息，优化索引结构，支撑快速检索响应。

4.7.6. 搜索结果排序与精准展示

实时捕捉过程中的动态数据，采集关键指标、状态变化等信息，确保数据实时性与完整性，为临时数据处理提供即时支撑。

4.8. 过程/临时数据处理工具

4.8.1. 暂存数据库结构配置与参数设定

支持自定义库表结构、字段属性及存储规则，配置数据有效期参数，为临时数据提供适配的存储框架，保障存储规范

4.8.2. 临时数据实时入库与分类存储

接收动态数据实时写入暂存库，按类型手动分类归档，监控存储状态，确保数据临时留存的及时性与有序性。

4.8.3. 多格式文件上传与解析适配

支持各类格式文件上传，自动解析内容结构并提取数据，适配不同文件类型，保障上传数据准确导入暂存库。

4.8.4. 暂存数据安全导出与格式转换

支持数据按需求格式导出，加密处理敏感信息，记录导出日志，保障数据导出安全合规及跨场景复用。

4.8.5. 过期数据自动清理与空间释放

依据配置规则识别过期临时数据，自动执行清理操作并释放存储空间，维持暂存库高效运行，避免资源占用冗余。

4.9. 应用调优工具（知识问答）

4.9.1. 调优工具可视化模块

依托智能体构建平台底座能力做二次开发，搭建可视化调优操作界面。

4.9.1.1. RAG 流程配置模块

基于智能体构建平台提供可视化 RAG 画布，拖拽组件即可快速搭建 RAG 链路，依托模块化组件快速搭建调优路径，完成问答类业务应用优化。

4.9.1.2. RAG 组件配置模块

可单独配置 RAG 全流程各组件参数，灵活调试、优化组件运行性能。

4.9.1.3. RAG 输出验证模块

从准确性、内容相关性、信息安全性三个维度校验 RAG 输出答案。

4.9.1.4. RAG 结果发布模块

支持将调试完成的 RAG 能力嵌入智能体构建平台的智能体

workflows, and call its release module to implement online release.

4.9.2. 调优工具流程编排引擎

复用智能体平台能力, 编排 RAG 调优组件, 实现支持顺序、分支判断、循环三种可执行的流程结构。

4.9.3. 知识场景化关联工具

依托知识库平台实现业务目录树的梳理与生成, 支持把知识点挂载至对应目录节点, 同时为知识片段批量添加自定义标签。

4.9.4. 预检索分类工具

依托业务目录树、知识标签提前锁定检索范围; 自动解析用户问句意图、提取关键信息; 整合多轮对话上下文合并为完整查询; 拆分复杂问题为多条适配知识库检索的简易问句。

4.9.5. 检索调优工具

兼容 BM25 关键词检索、向量语义检索、混合检索三种方案; 通过问句改写、扩充同义 / 近义词优化知识召回效果。

4.9.6. 后检索调优工具

对多渠道检索返回结果做二次打分重排, 优化内容排序优先级。

4.9.7. 生成优化工具

根据检索到的知识库内容, 自动匹配提示词模板, 调用大模型生成问答答案。

4.10. 应用调优测试工程（知识问答）

4.10.1. 全链路数据追踪模块-流程节点追踪子模块

依托智能体平台生成问答全链路数据流向图谱，直观展示每个节点处理细节；支持 API 编排、绑定智能体应用流程两种搭建方式。

4.10.2. 全链路数据追踪模块-节点变量监控

提供应用测试所需查看及汇总的各处理节点的入参、出参信息，以及节点调用的知识库、大模型、提示词、重排算法等底层能力的监控页面。

4.10.3. 全链路数据追踪模块-全链路审计日志子模块

生成符合合规要求的审计日志，满足监管机构的数据追溯需求。

4.10.4. 人工标记模块-交互式标记面板

左侧显示原始问题及系统回答，右侧提供预设标签（正确 / 错误 / 部分正确 / 无关），支持自定义标签（如 "需多文档融合" 包含过时信息 "）。

4.10.5. 人工标记模块-数据导入

支持本地 excel 文件导入后，作为测试集进行全链路测试。

4.10.6. 人工标记模块-标记关联

针对长文本回答，支持划词标记（如选中 "2023 年政策" 标注 "时间错误"），自动关联知识库对应条款。

4.10.7. 人工标记模块-多轮对话标记支持

处理上下文依赖场景（如 "刚才的问题再详细点"），显示历史对话链并标记上下文关联错误（如忽略前一轮提到的关键条件）。

4.10.8. 人工标记模块-批量标记

支持 Excel/CSV 批量导入未标记数据，自动预填充置信度高的标签（如系统回答与标准答案完全一致时标记 "正确"），人工仅需审核。

4.10.9. 人工标记模块-数据导出

支持标记后的数据和原数据进行 excel/csv 格式导出。

4.11. 业务工具

4.11.1. 人员信息问数

4.11.1.1. 人员信息关联数据查询业务思维链

支持汇集人员信息问数涉及的关联数据表，构建警务常用数据查询思维链。

4.11.1.2. 人员信息多轮问答对话流调优

支持完成人员关联信息多轮问答对话流程优化。

4.11.1.3. 人员信息元数据治理整合

支持结合业务场景，完成相关数据表表结构适配调整与元数据整合治理。

4.11.2. 车辆信息问数

4.11.2.1. 车辆信息关联数据查询业务思维链

支持汇集车辆信息问数涉及的关联数据表，构建警务常用数据查询思维链。

4.11.2.2. 车辆信息多轮问答对话流调优

支持完成车辆关联信息多轮问答对话流程优化。

4.11.2.3. 车辆信息元数据治理整合

支持结合业务场景，完成相关数据表表结构适配调整与元数据整合治理。

4.11.3. 人脸信息问数

4.11.3.1. 人像轨迹关联数据查询业务思维链

支持汇集人像轨迹问数涉及的关联数据表，构建警务常用数据查询思维链。

4.11.3.2. 人像轨迹多轮问答对话流调优

支持完成人像轨迹信息多轮问答对话流程优化。

4.11.3.3. 人像多模态解析模块

支持对接集成人像比对、人像多模态识别模块能力。

4.11.4. 驾照信息问数

4.11.4.1. 驾驶证照信息关联数据查询业务思维链

支持汇集驾驶证照信息问数涉及的关联数据表，构建警务常用数据查询思维链。

4.11.4.2. 驾驶证照信息多轮问答对话流调优

支持完成驾驶证照信息多轮问答对话流程优化。

4.11.4.3. 驾照多模态解析模块

支持接入驾驶证照多模态识别模块能力。

4.12. 工具注册管理

4.12.1. Function call

4.12.1.1. 工具管理模块

实现智能体构建平台内的工具的标准化定义、动态注册与高效检索，支撑工具的灵活扩展

4.12.1.2. 调用决策模块

基于用户意图与上下文，判断是否调用工具、调用哪个工具及生成调用参数。

4.12.1.3. 执行控制模块

保障工具调用的高效性、可靠性与可扩展性，处理复杂任务的依赖与并发。

4.12.1.4. 结果处理模块

将工具返回结果整合到对话流程中，提升生成内容的准确性与用户体验。

4.12.1.5. 监控与调试模块

实时追踪工具调用状态。

4.12.2. 模型上下文协议（本期 MCP）

4.12.2.1. MCPserver 模块

①服务注册与发现。管理 MCP 服务节点的注册、发现，确保客户端与宿主环境高效连接。②请求路由与调度。解析客户端 / 宿主的请求，根据上下文状态动态路由至目标模块。③服务治理。监控服务健康状态，支持服务熔断、限流、版本管理，保障平台稳定性。

4.12.2.2. MCPclient 模块

①客户端 SDK/API。提供多语言开发工具包，封装基础通信协议，简化客户端接入。②用户交互接口。提供前端界面或 CLI 工具，供用户主动查询、修改上下文参数。

4.12.2.3. MCPHost 模块

①宿主环境管理。管理物理 / 虚拟宿主设备的资源分配与状态监控。②设备接入网关。支持多种协议接入外部设备，实时采集上下文数据。③任务调度引擎。基于上下文状态分配计算任务，优化宿主设备利用率。

4.12.2.4. 上下文信息存储

自动存储并管理模型运行时的上下文信息，确保信息不丢失。

4.12.2.5. 上下文状态更新

根据用户交互与模型输出，实时更新上下文状态，保持信息的一致性。

4.12.2.6. 共享与传递

在模型调用不同工具或服务时，自动传递必要的上下文信息，确保交互的连贯性。

4.12.2.7. 可视化模块

在调试区提供上下文信息的可视化界面，便于用户运行调试。

4.12.3. 工具 API 调用

提供 API 调用工具能力

4.12.3.1. API 注册模块

用户可注册外部工具的 API 信息,包括 API 地址、请求方法、参数格式、认证方式等

4.12.3.2. 请求构建模块

根据 API 要求，支持发送 HTTP 请求进行调用，包括设置请求头、请求体等。

4.12.3.3. 异步请求模块

支持异步 API 调用，提高应用响应速度，同时处理多个并发请求。

4.12.3.4. 响应解析模块

在节点中解析 API 响应，提取有用信息，并转换为应用内部可用的数据格式。

4.12.3.5. 错误重试模块

在 API 调用失败时，提供重试机制，确保任务的可靠性和稳定性。

4.12.3.6. 日志记录模块

记录 API 调用的详细日志，包括请求时间、响应状态、错误信息等，便于问题排查和性能优化。

5. 知识库工具

功能清单如下：

层级	二级功能	三级功能	四级功能
知识库工具	知识采集	全文检索知识库接入	标准化数据对接
			高性能数据通道
			检索增强能力
			安全可信交互
			弹性扩展架构
		跨知识库知识迁移工具	知识转换与适配模块-结构转换
			知识转换与适配模块-权限迁移
			冲突检测与解决模块-逻辑冲突识别
			冲突检测与解决模块-冲突消解策略
			知识融合与整合模块
			验证与评估模块
			版本控制与日志模块
	知识处理	文本切分工具	字符切分

			按符号分割
			按段落分割
			按标题/结构分割
			语义切分
		文档知识库自动 归类打标工具	文档/知识自动分类
			基于提示词自定义打标
			标签图谱化工具
	知识管理	知识目录构建/ 检索工具	知识目录自动构建工具
			知识目录全视图工具
			知识目录检索工具
		知识间关系管理 工具	多知识关联关系管理工具
			相似问效果评估工具
		知识图谱工具 (开源接入)	工具集成
			多线程并行生成图谱
			多图谱维护-版本控制
			多图谱维护-冲突检测
			增量图谱生成-增量数据识别
			增量图谱生成-增量合并算法
			增量图谱生成-增量触发模块
			图谱检索
		文档元数据管理 工具	元数据提取
			元数据变更管理
			元数据检索
	知识服务	知识检索服务	自适应检索策略

			检索策略支持
		知识共享工具	开放授权接口
		知识质量评估工具	知识淘汰归档工具
			冲突知识识别工具
			重复知识识别工具
		知识溯源工具	

5.1. 知识采集

5.1.1. 全文检索知识库接入

5.1.1.1. 标准化数据对接

支持 RESTAPI、gRPC 等多种协议接入，提供 JSON/XML/YAML 格式自动转换能力，内置元数据映射引擎实现字段级精准对接。

5.1.1.2. 高性能数据通道

依托批量写入接口 + Netty 异步传输实现海量文档高速同步，自带智能路由、动态限流管控。

5.1.1.3. 检索增强能力

内置语义检索引擎，支持近义词扩充、向量检索、结构化 + 全文混合检索，优化字段权重加快检索响应速度。

5.1.1.4. 安全可信交互

采用加密传输，实现字段级权限控制，自动识别并脱敏信息。

5.1.1.5 弹性扩展架构

支持水平集群扩展，自动处理分片平衡与故障转移，提供冷热数据分层存储策略。

5.1.2. 跨知识库知识迁移工具

5.1.2.1. 知识转换与适配模块-结构转换

自动识别源库与目标库的数据模型、字段、存储格式差异，通过规则 / 引擎把表格、XML、图谱等数据转为目标库适配格式。

5.1.2.2. 知识转换与适配模块-权限迁移

保留并适配源知识库中的访问控制策略（如用户权限、角色分组、文档可见性等），将其映射至目标知识库的权限体系。

5.1.2.3 冲突检测与解决模块-逻辑冲突识别

通过字段约束校验、语义识别，排查跨库迁移带来的数据重复、实体歧义、关联矛盾等问题。

5.1.2.4. 冲突检测与解决模块-冲突消解策略

提供自动化或人工干预的冲突解决方式，如按优先级保留数据（源库 / 目标库优先）、合并互补信息、通过语义相似度匹配消除歧义，或标记冲突待人工审核，确保迁移后数据的一致性与准确性。

5.1.2.4. 知识融合与整合模块

将迁移的新知识与目标知识库的现有数据进行整合，支持增量更新（按时间戳、版本号同步新增或修改的内容）或全量

融合，确保目标库知识体系的完整性与实时性。

5.1.2.5. 验证与评估模块

自动校验迁移后数据完整度、格式合规性，排查字段缺失、关联断裂等异常。

5.1.2.6. 版本控制与日志模块

留存全量迁移版本日志，可一键回滚至迁移前知识库版本，便于事后审计。

5.2. 知识处理

5.2.1. 文本切分工具

5.2.1.1. 字符切分

按固定字符数对文本进行切分。

5.2.1.2. 按符号分割

根据自定义的符号（如句号、问号、换行符或特定标记）进行分割。可保留分隔符，支持纯符号分割或与字符数限制结合的混合分割，比简单字符切分更能保持语义单元的完整性。

5.2.1.3. 按段落分割

识别文本中的自然段落进行分割。例如，按换行符识别段落，或利用 NLP 工具进行更精细的段落识别。特别适用于结构清晰的长文本文档，如文章、报告等。

5.2.1.4. 按标题/结构分割

针对具有明显结构标记的文档（如 Markdown、HTML），根据

标题层级（H1, H2 等）或其他结构标签进行切分。能将同一标题下的内容保持在一起，并将标题信息保留为元数据，非常适合知识库文档。

5.2.1.5. 语义切分

利用大语言模型理解文本内容并生成分割点，具备完整保留文本语义的能力。

5.2.2. 文档知识库自动归类打标工具

5.2.2.1. 文档/知识自动分类

能够基于大模型对文档形成摘要后，对存量文档、增量文档进行自动打标。

5.2.2.2. 基于提示词自定义打标

描述标签与知识内容匹配规则，模型理解规则对文档进行自动打标，主要以提示词形式实现。

5.2.2.2. 标签图谱化工具

以标签云图方式进行展示。背后关联对应文件。方便民警能快速看到已建的知识在标签维度的展示，和组织类型、编目类型形成内容快速筛选上的互补。

5.3. 知识管理

5.3.1. 知识目录构建/检索工具

5.3.1.1. 知识目录自动构建工具

依托大模型识别文档标签，并基于标签自动生成树形目录，

支持目录后续增删改。

5.3.1.2. 知识目录全视图工具

平台整体知识盘点。通过树状列表视图、图谱关系视图表示。可用于业务方快速进行知识构建。

5.3.1.3. 知识目录检索工具

全目录全文检索、元数据字段精准过滤、组合条件高级查询。

5.3.2. 知识间关系管理工具

5.3.2.1. 多知识关联关系管理工具

知识条目间关联关系定义、依赖关系可视化。

5.3.2.2. 相似问效果评估工具

通过向量相似性对相似问的生成效果进行评估。

5.3.3. 知识图谱工具（开源接入）

5.3.3.1. 工具集成

兼容接入开源图引擎，实现全栈私有化本地部署。

5.3.3.2. 多线程并行生成图谱

图谱支持多线程并行生成；按数据源、实体类型拆分任务，搭配负载均衡，充分利用多核算力。

5.3.3.3. 多图谱维护-版本控制

记录每次图谱更新的时间、操作人及变更内容，支持版本回滚至历史状态。

5.3.3.4. 多图谱维护-冲突检测

对多图谱间的重复实体 / 关系进行智能识别，避免冗余存储。

5.3.3.5. 增量图谱生成-增量数据识别

基于已有图谱的增量更新能力。通过捕获数据源的变更记录（如数据库的 binlog、文件的修改时间戳），识别需要更新的增量数据（新增实体、修改关系、删除节点）。

5.3.3.6. 增量图谱生成-增量合并算法

增量算法仅刷新变动内容，无需全量重生成图谱，附带数据校验保障图谱逻辑无误。

5.3.3.7. 增量图谱生成-增量触发模块

支持定时触发（如每日凌晨）或事件触发（如数据源更新后即时触发）两种模式。

5.3.3.8. 图谱检索

基于开源图谱工具定制图谱检索功能。该功能可用于增强推理效果。

5.3.4. 文档元数据管理工具

5.3.4.1. 元数据提取

核心元数据字段（标题、作者、日期等）、自定义元数据字段扩展、自动提取文档属性作为元数据。

5.3.4.2. 元数据变更管理

元数据的增删改查。

5.3.4.3. 元数据检索

可视化的元数据信息检索。

5.4. 知识服务

5.4.1. 知识检索服务

5.4.1.1. 自适应检索策略

按需组合多轮总结、意图识别、问句扩写、问题拆分等能力，根据用户意图自动匹配最优检索方案。

5.4.1.2. 检索策略支持

支持知识库的多种检索方式，包括：全文检索、语义检索、标签、知识图谱查询。

5.4.2. 知识共享工具

5.4.2.1. 开放授权接口

权限授权可追溯。

5.4.3. 知识质量评估工具

5.4.3.1. 知识淘汰归档工具

通过评估知识时效性、使用行为，对已经发布的知识进行淘汰、归档，降低存储开支和文本处理成本。

5.4.3.2. 冲突知识识别工具

检查知识实体间关系的合理性、发现矛盾或冲突的知识表述、

检测不同版本间的差异和冲突。

5.4.3.3. 重复知识识别工具

基于内容、语义或特征的相似性分析、区分名称相同但实际不同的实体、提供规则定义重复数据合并方式。

5.4.3.4. 知识溯源工具

知识溯源信息抽取工具。进行知识抽取时，会自动将知识点上游血缘关系嵌入的抽取知识内容中。

6. 评测中心

功能清单如下：

层级	二级功能	三级功能
评测中心	评测基础能力	模型效能分析
		算力资源评测
		多维评测指标矩阵
		评测能力自动化
	测评任务管理	任务创建与配置
		自动化调度与资源匹配
		实时监控与日志追踪
		智能分析与反馈优化
		任务版本与知识管理
		安全与权限管理
	模型对比测评	测评管理配置模块
		任务执行与监控

		数据分析与报告生成
		对比测评类型支持
	测试数据管理	多源数据采集与整合
		数据清洗与预处理
		领域增强型标注体系
		全生命周期版本控制
		数据存储优化
		数据质量智能监控

6.1. 评测基础能力

6.1.1. 模型效能分析

- ①效果评测：用准确率、召回率等指标量化模型输出质量；
- ②泛化测试：通过对抗样本、数据偏移验证模型适配能力；
- ③鲁棒测试：验证缺数据、脏数据等异常场景运行稳定性。

6.1.2. 算力资源评测

同一模型在不同算力卡上的性能、效率评测。

6.1.3. 多维评测指标矩阵

指标体系模块。构建覆盖功能完整性、性能效率、安全合规等维度的指标体系。

自动化评测。开发自动化评分工具与可视化看板。

建立上海市公安基准测试数据集，支持横向对比。

6.1.4. 评测能力自动化

测试用例构建模块。测试用例自动化生成与执行。

缺陷定位模块。缺陷定位与修复跟踪系统。

版本回归模块。版本回归测试自动化流水线。

6.2. 测评任务管理

6.2.1. 任务创建与配置

支持可视化任务模板设计，允许自定义评测指标（如准确率、响应时间）、数据集版本绑定、硬件资源配置（CPU/GPU 显存需求）等参数。提供任务参数校验机制，确保配置完整性。消除人工配置错误风险（如资源配置超限导致任务失败），缩短任务初始化周期。

6.2.2. 自动化调度与资源匹配

基于资源画像（CPU/GPU 利用率、网络带宽）实现智能负载均衡，支持抢占式调度（高优先级任务可中断低优先级任务）、分布式并行执行（多节点协同处理大规模评测）。提升资源利用率（降低任务排队等待时间）。

6.2.3. 实时监控与日志追踪

提供多维度监控看板（任务进度、资源消耗、异常事件），支持日志实时滚动查看与历史追溯。内置异常检测引擎（如评测指标偏离阈值自动告警）。实现缩短故障平均修复时间，提升关键任务执行成功率。

6.2.4. 智能分析与反馈优化

自动化生成评测报告（含可视化图表、指标对比分析），提供优化建议（如模型超参数调优方向）。减少人工分析时间，推动评测流程持续改进。

6.2.5. 任务版本与知识管理

①版本快照。支持任务版本快照（记录参数变更历史）。

②任务模板。提供模板库与最佳实践库。避免重复开发，降低新人学习成本。

6.2.6. 安全与权限管理

实现细粒度权限控制（任务创建/执行/删除分级授权），保障数据隔离（不同项目任务运行于独立沙箱），支持操作审计（记录完整行为日志）。降低数据泄露风险（审计覆盖率100%），满足数据安全合规要求。

6.3. 模型对比测评

6.3.1. 测评管理配置模块

待测模型的管理。支持添加、删除、启用/禁用待测试的模型。

模型对比测评数据集管理。支持基于测试数据管理模块，构建用于模型对比测评的数据集。

参数配置。支持基于任务进行模型对比评测的参数配置。

6.3.2. 任务执行与监控

支持多个模型同时执行评测任务，并进行实时监控。

6.3.3. 数据分析与报告生成

支持对选定模型进行数据分析和报告生成。能够直观比对不同模型在核心指标上的差异。

6.3.4. 对比测评类型支持

支持模型在基础能力、安全能力、性能、token 成本方面的对比评测。

6.4. 测试数据集管理

6.4.1. 多源数据采集与整合

支持跨平台数据接入（数据库/文件系统/API 接口），实现结构化与非结构化数据的统一归集。内置数据血缘追踪功能，记录数据来源与流转路径。突破数据孤岛，保障评测数据集的完整性与代表性。

6.4.2. 数据清洗与预处理

测试数据集清洗。自动化执行去重（基于哈希指纹）、去噪（时序数据平滑）、异常值检测（ 3σ 原则）等操作。

测试数据集标准化。支持数据标准化（JSON-Lines 格式统一）与格式转换（图像/文本编码适配）。

6.4.3. 领域增强型标注体系

标注规范。建立多层级标注规范（领域术语库+标注示例库）。

半自动标注（预标注+人工校验）。

标注质量评估。实现标注质量多维度评估（准确率/一致性/

召回率)。

6.4.4. 全生命周期版本控制

支持数据集快照(Git-LFS 管理)、增量更新(DeltaEncoding)、差异对比(Diff 算法)。记录版本变更日志(操作人/时间/内容)。

6.4.5. 数据存储优化

构建冷热分层存储(HOT/WARM/COLD 三级架构), 自动执行数据压缩(Zstandard 算法)与格式转换(Parquet 列存优化)。降低存储成本, 缩短查询响应时间, 支撑海量数据集管理。

6.4.6. 数据质量智能监控

部署多维度质量探针(完整性/一致性/时效性), 实时检测数据漂移。缩短质量问题发现时间, 提升数据可用性。

7. 通用知识库

功能清单如下:

层级	二级功能	三级功能
通用知识库	全警通用接处警规范与执法	通用案例知识库智能体
	安全防护案例知识库	通用案例知识库调优工作流
	全警通用办事指南知识库	通用办事指南知识库智能体
		通用办事指南知识库调优工作流
	全警通用公开政策/发文学习	通用政策发文知识库智能体
	/考核标准查询知识库	通用政策发文知识库调优工作流
	通用知识库工作台	通用问答应用窗口

		通用知识管理
		意图识别管理
		历史会话

7.1. 全警通用接处警规范与执法安全防护案例知识库

7.1.1. 通用案例知识库智能体

通过智能体平台和知识库工具，构建案例知识库。

需要基于案例知识特征，设计案例采集、案例去重、案例清洗、案例打标等多个环节。

7.1.2. 通用案例知识库调优 workflow

基于智能体平台通用工具中的应用调优工具，对案例检索进行调优。包括：处置流程检索调优；处置规范检索调优；案例主体/特征检索调优；调优节点和原有业务 workflow 和数据流进行融合。

7.2. 全警通用办事指南知识库

7.2.1. 通用办事指南知识库智能体

通过智能体平台和知识库工具，构建办事指南知识库。

需要基于窗口知识、办事流程、调解指南等知识特征，设计知识从采集、处理、入库、服务的完整 workflow 和数据流。

7.2.2. 通用办事指南知识库调优 workflow

基于智能体平台通用工具中的应用调优工具，对办事类知识检索进行调优。

调优节点和原有业务 workflows 和数据流进行融合。

7.3. 全警通用公开政策/发文学习/考核标准查询知识库

7.3.1. 通用政策发文知识库智能体

通过智能体平台和知识库工具，构建政策发文指南知识库。

需要基于政策发文/考核标准等知识。

7.3.2. 通用政策发文知识库调优 workflows

基于智能体平台通用工具中的应用调优工具，对公开政策发文类知识检索进行调优。

调优节点和原有业务 workflows 和数据流进行融合。

7.4. 通用知识库工作台

对接智能体平台，并基于平台能力开发，实现以下功能：

7.4.1. 通用问答应用窗口

提供交互窗口，依托智能体平台能力，响应用户各类常见问答需求，并提供个人中心的管理入口。

7.4.2. 通用知识管理

借助知识库平台平台能力，实现通用知识的存储、整理，支持便捷调用与管理。

7.4.3. 意图识别管理

智能识别用户需求意图，提供选项供选择，精准匹配服务。支持基于历史会话进行意图识别。

7.4.4. 历史会话

保存过往对话记录，方便用户随时查看、回溯历史交互内容。

8. 产品软件采购（智能体平台）

功能清单如下：

层级	二级功能
工具软件	智能体平台

8.1. 智能体快速构建

提供可视化拖拽式构建能力，支持应用流程编排、组件参数及关联关系灵活配置、组件配置及输出验证，以及发布为工具、发布至应用广场等多种发布形式，覆盖智能体从搭建到上线的完整流程。

8.2. 智能体版本控制

支持智能体各版本创建与变更记录，可追溯历史版本，实现版本切换、回滚与迭代管理，保障智能体持续演进过程中版本可控、可恢复。

8.3. 智能体引擎

提供智能体运行调度、长短记忆管理、任务管理与交互协议适配（A2A）、智能体应用网关、基于沙箱的智能体代码执行行为验证、提示词管理优化等核心引擎能力，支撑智能体编排平台内的工作流执行、智能体间协同及运行态资源管控，保障智能体稳定可靠运行与持续优化。

8.4. 智能体管理

提供智能体可发布为工具的方式实现智能体协同管理，并通过智能体应用网关保障平台资源安全有序流转。

8.5. 智能体监测

覆盖智能体从创建到下线的智能体生命周期管理，提供资源用量计量与流量控制能力，支持按角色、按用户、按组织限流，保障平台运行稳定可控。

9. 其他

功能清单如下：

层级	二级功能
其他	deepseek 模型接入
	商用密码应用建设

9.1. 商用密码应用建设

为实现本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用功能，需开发适配用户身份认证、用户访问控制信息签名验签、应用系统重要数据签名验签、应用系统重要数据数据加解密、服务器虚拟机设备日志/访问控制信息完整性、业务重要数据安全传输和重要可执行程序签名验签密码应用功能模块。

9.2. Deepseek 模型接入

将 Deepseek 模型作为基础模型接入大模型基础环境子系统。

四、技术性能指标及配置要求

（一）性能指标

项目指标涵盖智能体平台、扩展工具、知识库工具、评测中心、通用知识库 5 个维度：

1、智能体平台

并发用户数：系统支持 ≥ 100 用户同时在线进行智能体编排、管理等操作。

隔离：支持多租户资源隔离。

流控：支持指定租户通过大模型调用次数的限制来达成流量控制。

2、扩展工具

标准问题文本转 SQL：95%的 SQL 生成请求延迟不超过 25 秒。

文本知识转脑图生成响应时间：从处理文本到完成脑图可视化渲染,总耗时不超过 30 秒(输入文本不超过 3000 字)。

3. 数据生成图表工具：95%的图表渲染请求耗时不超过 5 秒。

4. 代码解释器：95%的代码执行请求耗时不超过 60 秒。

5. 跨站搜索结果响应时间：用户输入搜索关键词后，单次搜索平均响应时间不超过 2 秒。

6. 过程/临时数据处理工具：95%的单次数据处理任务请求耗时不超过 60 秒

7. 应用调优测试工具数据追踪覆盖率：问答全链路中每个处理节点的入参、出参及调用的底层能力信息（知识库、

大模型、提示词、重排算法等) 均被完整记录, 节点覆盖率 100%。

8. 业务工具-人员、车辆、人脸、驾照问数: 信息问数支持 20 并发, 且查询响应时间小于 80 秒

3、知识库工具

全文知识检索: 知识检索响应时间不超过 2 秒 (千万级向量规模)。

跨知识库知识迁移工具: 千条知识级跨库迁移任务, 总执行时间不超过 60 分钟。

文本切分工具: 文本切分处理速度不低于 10 篇/分钟, 单篇文档大小不超过 10000 字。

文档知识库自动归类打标工具: 基于大模型的文档自动分类与打标处理速度不低于 10 篇/分钟, 单篇文档大小不超过 100K B。

知识图谱工具: 1 万条切分结果全量图谱构建总时长不超过 2 小时, 10 万条切分结果不超过 24 小时; 1 万条切分结果规模下单次图检索平均响应时间不超过 1.5 秒, 10 万条规模下不超过 3 秒。

知识质量评估工具: 万条知识规模下, 单次知识质量评估任务执行时间不超过 60 分钟。

4、评测中心

单模型完整评测耗时: 1000 条标准测试数据集, 对单个模型完成涵盖准确率、召回率等指标的完整评测, 总耗时不超过 10 分钟。

多模型并发对比能力：系统支持不少于 10 个模型同时执行同一数据集的对比评测任务，各任务并行运行无排队等待。

5、通用知识库

案例检索命中率：接处警规范与执法安全防护案例知识库的场景化检索，Top5 命中率不低于 80%。

办事指南检索命中率：全警通用办事指南知识库的场景化检索，Top5 命中率不低于 80%。

政策发文检索命中率：公开政策、发文学习及考核标准查询知识库的场景化检索，Top5 命中率不低于 85%。

（二）配置及部署要求

1、本项目所需服务器资源由上海市公安局提供。本项目建设内容可适配并部署于新一代公安信息网环境的服务器或虚拟化平台，同时需要满足系统密码应用测评的需要。

2、在终端应用方面，对统信和麒麟等主流终端操作系统、浏览器进行适配，以满足不同终端均可访问本项目用户界面，并对相关适配情况纳入软件测试。

五、进度安排

本项目建设周期为合同签订后 6 个月，具体如下：

1、实施阶段。主要完成产品软件交付、系统设计、应用系统开部署实施等工作。本阶段周期约为 5 个月。

2、试运行阶段。主要完成项目整体试运行，修正项目各组成部分联调中出现的问题，修正软件 bug。试运行期约为 1 个月，试运行期无重大故障且解决所有发现的缺陷后开

展项目相关测评工作，并根据用户方或市相关要求开展验收。

六、实施要求和技术服务要求

（一）质量保证期

1、中标方在完成项目建设后应提供完整技术资料，包括应用软件清单及介质、用户手册、管理员手册、安装指南等用户文档资料。

2、本项目软件开发部分在验收一年内提供免费售后服务保障，包括：系统整体优化以及根据用户需求开展的功能更新，提供不少于 4 人的 5*8 驻场维护服务，7*24 小时的电话技术支持服务，如出现故障一般模块需 2 小时内响应，重要模块 1 小时内响应，2 小时内到现场服务；系统日常巡检服务（月度巡检），对于各开发功能提供技术支持。

3、本项目产品软件部分提供 3 年免费运维，要求开展免费的软件升级和故障维护服务，提供不少于 2 人的 5*8 驻场维护服务，7*24 小时的电话技术支持服务，如出现故障一般模块需 2 小时内响应，重要模块 1 小时内响应，2 小时内到现场服务；系统日常巡检服务（月度巡检）。

4、中标方在用户方指定的重大节点前对系统全面巡检，提供应急方案等，并根据用户方的要求在重大活动期间指派不少于 2 人，进行 7*24 小时的现场技术支持服务。

5、若用户在免费维护期内对软硬件环境进行调整，中标方需免费完成相关集成工作，包括但不限于将功能模块迁移至不同网域等。

（二）培训要求

1、对系统使用单位提供相关培训，培训内容包括不限于大模型相关知识培训、使用及管理培训和平台操作培训等，应提供详细培训方案。在 12 个月的质量保证期内，提供不少于 2 次与项目相关的必要培训。

2、中标方需要指派专人负责开展分层次的人员培训工作。培训应具有培训教材，使用说明书，培训环境和高水平的培训讲师。

3、中标方应提供一般用户的基础操作培训和部门管理员的日常应用维护的培训，确保用户对象能够掌握对应的操作技能。

（三）运维人员要求

1、派驻到项目方的运维人员需接受项目方的保密教育培训并通过项目方的背景审查,不通过则无条件更换。

2、运维人员应保证相对固定，如有变动，须至少提前两周征得用户方同意。

3、运维人员按规定签订有关工作保密协议。

4、运维人员能独立完成对系统的现场巡检、维护及故障快速响应处置工作。工作中能够按照市局要求在重大节日以及重要事件时间节点开展各项值班运维保障。

七、招标方案、投标单位资质要求及投标书应答要求

（一）项目团队及驻场人员要求

针对本项目提供不少于 40 人的项目服务团队，投标单位的相关服务人员需具备相应的服务能力，需提供相关证明（开标前三个月任意一月依法缴纳社保费的证明）。

角色	主要职责	人员数量	人员要求	驻场要求
项目负责人	项目实施期负责项目质量和进度控制	1 人	本科及以上学历, 有信息系统项目管理师证书者优先, 有 3 年以上人工智能、智能体相关项目管理经验优先	按需进场
软件研发工程师	项目实施期负责项目研发以及项目部署调试	30 人	本科及以上学历优先	按需进场
测试工程师	项目实施期开展项目功能、性能测试	5 人	本科及以上学历优先	按需进场
运维工程师	项目质保期内负责项目现场维护和支持	4 人	本科及以上学历, 有 2 年以上类似项目运维经验优先	驻场运维

（二）投标单位资质要求

（1）供应商提供的产品软件具有与本项目相关（智能体开发相关类别）的软件著作权。

（三）关于转让和分包的规定

本项目不得转让，不得分包。

（四）投标书应答要求

（1）供应商应针对招标需求中的每项条款逐条应答。

（2）供应商须提供内容详尽的投标方案，包括需求理解、总体设计方案、软件功能模块设计方案、安全保障方案、

实施方案、售后服务方案等。

（五）知识产权及保密要求

1、中标方保证其所提供的服务和交付的成果以及在履行本项目义务中使用到的所有数据、文件、信息不会引起任何第三方在专利权、著作权、商标权等知识产权方面向采购人或采购人的关联方及合作方（包括但不限于采购人的主管单位和采购人的合作单位等）发出侵权指控或提出索赔。若有，中标方应负责与第三方解决纠纷，若因此导致采购人损失的，采购人有权要求成交供应商赔偿采购人因此遭受的全部损失，包括但不限于直接损失、间接损失、诉讼费 / 仲裁费、律师费、公证费、鉴定费等。

2、中标方因履行本项目而产生的所有成果的知识产权等权利均归采购人所有，中标方应配合采购人进行相关权利登记或申请。未经采购人书面同意，中标方不得以任何形式使用或许可他人使用本项目成果的相关内容，不得擅自对外公开发表或向任何第三方透露。

3、在不影响上述条款规定的由采购人取得所有成果的知识产权的前提下，双方因履行本项目而被授权接触或使用对方之知识产权（包括但不限于商标、专利、著作权等），和/或任何其他相关资料、数据等涉及的任何权利，均不视为向另一方转让上述权利或在本项目范围外授权许可另一方使用上述权利，上述权利仍应属于提供方，并仅可适用于本项目，被授权接触或使用方未经提供方书面同意，不得擅自挪作他用。

4、中标方因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，中标方不得对外泄露采购人要求保密的信息，不得用于其他用途，否则成交供应商需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

5、中标方应采取必要的有效措施保证其参与本项目的人员（包括成交供应商聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及中标方的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标方人员或中标方合作单位违反保密规定，中标方应承担连带责任。

6、中标方（含成交供应商参与本项目的人员以及其合作方）未经采购方书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

7、中标方在提供本项目服务的全过程中，需严格遵循《企事业单位参与上海公安机关信息化建设安全管理实施细则》等各项安全管理规定，对存在严重安全隐患或者造成严重损害的，将追究中标单位违约责任和法律责任。

八、项目验收

1、中标方需配合完成软件测试、安全测评及密码测评。同时配合用户方开展信息系统安全等级保护定级及备案，相关费用由中标方承担。

2、本项目根据《上海市公安局信息化项目验收规范》执行，项目验收由市级信息化项目主管部门组织专项验收，中标方应配合完成项目各项验收准备工作。包括不限于提供《用户需求说明书》、《系统概要设计说明书》、《测试报告》、《用户使用手册》等）及可安装的程序运行文件。所交付的文档与文件应当是可供自然人阅读的书面和电子文档。