附件

科技处-上海公安信息系统应用日志智能

分析系统（2024年升级改造）

项目需求书

# 项目背景

2018年，上海市公安局开展上海公安信息系统应用日志智能分析系统的建设。从公安应用系统/资源库的应用日志入手，实现对用户操作行为（增、删、改、查询、登录等）的记录和分析，对数据盗取、越权访问等造成公安敏感信息泄露、侵犯公民隐私的行为进行监测预警和事后倒查追溯，提高公安数据应用的安全性。2019年各应用系统随着“智慧公安”建设推进，陆续迁移进视频传输网，2020年我局开展了“神经元”感知网安全审计智能分析系统建设，该系统的技术架构和应用功能充分借鉴了2018年应用日志智能分析系统。2018至2020年日志系统主要提供市局开展案事件反查信息支撑服务。自2020年起，根据市局工作“提前发现苗头问题、及时警示风险问题”等有关要求，我们与督察总队开始开展违规查询问题专项整治试点，并于2021年3月签订了《应用安全审计长效工作机制备忘录》。

当前，在从严管党、从严治警的形式下，市委市政府也对市局党委工作提出了更高要求，市局下发了《关于常态化整治“违规查询”问题的工作方案》，将违规专项整治工作基于日志审计平台常态化运作。故对于日志智能分析的需求产生了变化，平台定位上，该平台从原有的应用安全内部支撑服务，变成了为全警队伍风险隐患管理提供一个统一的平台，是一个基于内部人员和操作行为的搜索平台；服务对象上，从原有的为公安安全管理部门内部使用，向全局支撑综合性应用系统转变，让我局约3000个部门的政工领导，可基于平台日常进行常态化违规情况管控，看到所管人员的日常工作情况，及时获取到可能的队伍风险情况；界面展现上，需要建设相应的态势感知大屏，综合展现风险隐患点。

同时，随着原视频传输网应用系统的回迁、上海公安移动应用的繁荣，上海公安信息系统应用日志智能分析系统视频传输网、移动应用也需及时跟进进行应用日志采集。因此，需要对上海公安信息系统应用日志智能分析系统进行升级改造。

# 建设目标

基于2018年所建设的上海公安信息系统应用日志智能分析系统进行升级改造，完成对原“神经元”感知网安全审计智能分析系统中，视频传输网日志采集功能的构建，在视频传输网部署一套安全审计专用日志采集设备；迁移原“神经元”感知网安全审计智能分析系统中数据，统一汇聚至公安信息网；从终端、应用、资源服务接口等维度的日志入手，综合利用多源异构数据接入、数据识别处理、特征工程、模型训练、专家系统、全文检索、集群并行计算等技术构建一套智能化的日志分析与管理系统，实现日志的高效检索、行为的精准回溯、异常行为的实时预警以及快速响应处置等核心功能，为打击和威慑危害公安大数据安全的违法违规行为提供强有力抓手。解决公安信息化应用安全领域中的“发现难、查证难”问题，通过智能化的技术手段，提高安全事件的发现率和查证效率，提高公安信息化应用安全的管理水平，防范信息泄漏，保护公安数据的安全。

# 建设需求

## 日志采集

日志数据是公安信息系统应用日志智能分析系统的基础。本项目要求能够、实时、高效地采集和接入来自公安视频传输网和公安信息网中的应用、资源服务接口等多类日志数据，确保数据的完整性、准确性和时效性，以满足后续的数据分析、安全审计等多元化需求。

### 视频专网日志采集模块

对接原阿里云专有存储相应接口，获取原视频专网日志数据，并转存到NAS/DAS存储系统；通过主动采集和被动接收方式，获取视频专网视频图像信息系应用日志。

### 移动信息网日志接入模块

通过主动采集和被动接收方式，获取三类区移动警务应用日志。日志采集方式包括web服务接口方式、数据库接口方式、Kafka消息订阅方式和文件同步方式。

## 日志基础服务

### 查询服务模块

基于平台的数据仓库，提供查询检索服务接口，以供内部系统、分析工具、第三方应用或用户进行便捷查询和数据分析。

### 订阅服务模块

基于平台的数据仓库和分析计算能力，将日志数据和分析结果发布为相应主题的订阅服务，提供订阅服务接口，支持预警数据通知功能。

### 推送服务模块

基于WebSocket协议或数据库同步技术，实现数据的即时推送和分发，确保信息的时效性。

### 访问服务模块

基于REST API技术访问数据库，实现数据创建、读取和删除接口，可以更方便、安全地实现对平台数据库的访问和操作。

### 分析服务模块

平台支持模型分析、模型关联分析、统计分析等能力，并封装为API服务。日志分析服务模块支持对采集的应用系统日志进行数据分析服务，支持利用自然语言识别与处理技术、敏感数据分析技术，对日志内操作内容进行提取，包含个人隐私数据如身份证、手机号、姓名、银行卡号码、车牌号等敏感字段。

## 数据分析计算引擎调取

针对部署于公安网的存算一体设备，开发调用离线批处理计算、实时内存计算、OLAP关联计算、机器学习计算等能力，对海量日志数据进行深入的分析和挖掘。

## 日志应用

对现有智能分析系统进行功能增强、性能优化、技术升级和界面改进。

架构设计：设计新的技术架构，确保系统的可扩展性、稳定性、安全性，并考虑未来技术升级的可能性。

接口设计：定义清晰的API接口规范，确保与其他系统的无缝集成。

功能开发：根据需求说明书，开发或升级智能分析应用的核心功能，包括数据采集、处理、分析、可视化等。

用户界面改进：设计更加直观、易用的用户界面，提升用户体验。提供界面设计的原型图或示例图。

安全设计：确保系统的数据安全性，包括密码应用改造、访问控制、审计日志等。

### 态势大屏展现

以可视化态势大屏形式提供审计分析平台的整体信息概览，包括接入应用数、用户数、接入数据总量、组织机构数、模型数、活跃应用、活跃用户、活跃单位部门等信息，并可视化展现每个接入单位当前综合风险情况；并提供应用入口功能。

如：根据用户历史操作行为分析用户画像，包括但不限于信息查询时间分布、最长访问系统、最常用使用IP、查询银行卡号、查询电话号码、查询车牌号、查询邮箱、查询身份证、查询住宿记录、固定时间内告警趋势、告警类型占比、作息规律、常用功能等信息，并以图表形式展示。支持画像数据二次下钻分析，并可查看详情。

### 日志查询

提供基于时间、应用、用户、关键字等条件的日志搜索；以及基于终端、机构、应用系统等过滤功能。

全文模糊查询：用户可以通过输入关键词，对日志全文内容进行模糊查询。多条件组合查询：支持多种条件的组合查询，如时间范围、用户名、日志来源等。

### 日志下载输出

为使用人在页面上进行使用情况的翻译服务输出；提供用户对所查询日志的批量下载功能。

可以通过系统的用户界面，通过指定时间范围、用户名等条件，下载符合条件的日志文件。

### 日志分析

提供多种日志分析底层功能建设；支持实时接入案件、车辆、高风险人员其他业务数据，进行碰撞比对，为预警服务进行产出，提升预警准确性。

支持建立红名单人员库、白名单人员库、特定人员库，作为系统基础数据，提供作为日志分析补充能力。支持模版导入功能、支持批量导出、新增、修改、删除等功能；

### 模型建设

提供模型图形化配置界面或编程接口，支持自定义模型搭建，允许用户根据需求构建自定义的算法模型。提供不活跃账号异常启用模型、非执法办案部门查询模型、异常查询公安内部人员信息模型、反复查询同一信息模型、非案件承办人查询案件信息模型、超业务范围查询案件模型、查询交通事故涉及轨迹模型、异常查询接报警事件模型等模型模版。

### 模型配置

通过前端页面对系统内的所有告警模型进行参数设置，包括触发阈值、触发时间、启用/停用、模型名称、模型描述、告警级别等参数设置。

### 模型碰撞比对

满足用户自主进行多个模型碰撞分析需求，可以在模型目录选择多个模型，对于模型数据结果的交集、差集、并集进行分析。

### 告警中心

支持告警类型筛选、告警时间查询，展示告警事件总数、告警用户数、告警应用数、告警终端数、告警趋势（时间分布）、告警类型分布、TOP告警用户、TOP告警应用等信息。

### 用户画像

基于用户的行为日志和基础属性信息对用户进行刻画。包括但不限于姓名、编号、岗位、身份证号、性别、单位部门、常访问应用、常用IP、访问时间分布、告警数等信息。

### 应用画像

基于应用日志和基础属性信息对应用系统进行刻画。包括但不限于应用名称、负责人、应用类型、敏感等级、所属机构、用户数、告警数、日志量、跨区域访问数、访问用户TOP10等信息。

### 终端画像

基于终端行为日志和基础属性信息对终端进行刻画。包括但不限于IP地址、单位部门、告警数量、告警类型、使用用户、访问应用排行等信息。

### 组织机构画像

基于用户行为日志进行聚类分析，对组织机构进行刻画。包括但不限于机构详情、机构告警类型占比、机构人员预警、机构活跃用户、机构人员访问系统排名、机构终端日志top排行、机构时间日志数分布等信息。

## 平台维护功能

### 统计报表生成

基于预置规则生成各种报表，如日报、周报、月报等，并支持多种形式的展示方式，如表格、图表等，方便管理者快速了解用户异常行为情况、系统运行情况。

### 重点关注对象

用户可以设置重点关注对象，用于监控和预警特定对象（如用户、终端）的访问行为活动，一旦其行为出现异常或符合预设的预警条件，系统立即触发预警。管理员能够在关注对象列表中，查询关注对象的日志记录、告警等信息，方便管理员对被关注对象（用户和终端）进行快速便捷的日志审计和分析。

### 系统配置管理

提供平台的基本配置设置功能，包括参数配置、网络连接配置、运行状态监控管理等。

### 用户管理

负责管理系统的用户及其相关信息。包括用户的注册、登录、密码找回、账户禁用/启用、分配初始密码、组织结构管理等。用户与组织机构进行映射，提供树状层级结构目录，可以更加清晰地反映用户与组织机构的关系，并支持用户查找，支持用户信息导入导出。

### 权限管理

支持为不同用户分配不同的权限，控制他们对系统资源的访问和操作。支持角色管理，管理员可以定义不同的角色，并为每个角色分配一组权限。基于树状层级结构进行权限控制，可以提供更高的安全性，也便于权限和角色的继承，可以大大减少管理员的工作量。支持分层分级管理，分为多层级管理员、多层级使用员，且为分局、市局业务单位所有政工干部根据不同需求，开通相应的角色权限。

支持1、2、3级管理员权限管理，上级管理员可查看下级管理员的使用情况，如登录天数、登录次数、登录时间分布等信息。3级管理员可查看下级用户列表信息，以及下级的日志数据概况（访问量、告警数等），能够从用户列表点击人员，跳转查看人员档案。

权限管理功能够随着人员调动和人员组织机构变更，实现自动回收权限。

## 密码改造

为了确保关键信息基础设施和重要信息系统的密码应用符合国家密码管理的相关法规要求，对智能分析系统的密码算法进行评估，选择符合国家密码管理要求的算法进行升级，将密码应用集成到身份鉴别、数据传输、数据加密等模块中。

## 其他需求

### 关键性能参数

用户规模：支持55000个用户；

机构规模：支持1500个机构；

并发量：支持用户并发150以上；

日志记录数：支持日志数据存储1年以上。

### 适配需求

需针对该项目申请的市局服务器、数据库、中间件等资源做好软件适配。

## 需求清单

### 软件开发需求清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类别** | **功能模块** | **功能描述** |
| 1 | 日志采集 | 视频专网日志采集模块 | 对接原阿里云专有存储相应接口，获取原视频专网日志数据，均需并转存到NAS/DAS存储系统；通过主动采集和被动接收方式，获取视频专网视频图像信息系应用日志 |
| 2 | 移动信息网日志采集模块 | 通过主动采集和被动接收方式，获取移动信息网三类区移动警务应用日志。日志采集方式包括web服务接口方式、数据库接口方式、Kafka消息订阅方式和文件同步方式。 |
| 3 | 日志基础服务 | 查询服务模块 | 基于平台的数据仓库，提供查询检索服务接口 |
| 4 | 订阅服务模块 | 基于平台的数据仓库和分析计算能力，将日志数据和分析结果发布为相应主题的订阅服务，提供订阅服务接口 |
| 5 | 推送服务模块 | 基于WebSocket协议或数据库同步技术，实现数据的即时推送和分发，确保信息的时效性。 |
| 6 | 访问服务模块 | 基于REST API技术访问数据库，实现数据创建、读取和删除接口，可以更方便、安全地实现对平台数据库的访问和操作 |
| 7 | 分析服务模块 | 将平台的模型分析、关联分析、统计分析等能力封装为API服务 |
| 8 | 数据分析计算引擎调取 | 数据分析计算引擎 | 针对部署于公安网的存算一体设备，开发调用离线批处理计算、实时内存计算、OLAP关联计算、机器学习计算等能力 |
| 9 | 日志应用 | 态势大屏展现 | 以可视化态势大屏形式提供审计分析平台的整体信息概览，包括接入应用数、用户数、接入数据总量、组织机构数、模型数、活跃应用、活跃用户、活跃单位部门等信息，并可视化展现每个接入单位当前综合风险情况；并提供应用入口功能 |
| 10 | 日志查询 | 提供基于时间、应用、用户、关键字等条件的日志搜索；以及基于终端、机构、应用系统等过滤功能 |
| 11 | 日志下载输出 | 为使用人在页面上进行使用情况的翻译服务输出；提供用户对所查询日志的批量下载功能 |
| 12 | 日志分析 | 提供多种日志分析底层功能建设；支持实时接入案件、车辆、高风险人员其他业务数据，进行碰撞比对，为预警服务进行产出 |
| 13 | 模型建设 | 提供图形化界面或编程接口，允许用户根据需求构建自定义的算法模型。提供不活跃账号异常启用模型、非执法办案部门查询模型、异常查询公安内部人员信息模型、反复查询同一信息模型、非案件承办人查询案件信息模型、超业务范围查询案件模型、查询交通事故涉及轨迹模型、异常查询接报警事件模型等模型模版 |
| 14 | 模型配置 | 通过前端页面对系统内的所有告警模型进行参数设置，包括触发阈值、触发时间、启用/停用、模型名称、模型描述、告警级别等参数设置。 |
| 15 | 模型碰撞比对 | 满足用户自主进行多个模型碰撞分析需求，可以在模型目录选择多个模型，对于模型数据结果的交集、差集、并集进行分析 |
| 16 | 告警中心 | 支持告警类型筛选、告警时间查询，展示告警事件总数、告警用户数、告警应用数、告警终端数、告警趋势（时间分布）、告警类型分布、TOP告警用户、TOP告警应用等信息 |
| 17 | 用户画像 | 基于用户的行为日志和基础属性信息对用户进行刻画。包括但不限于姓名、编号、岗位、身份证号、性别、单位部门、常访问应用、常用IP、访问时间分布、告警数等信息 |
| 18 | 应用画像 | 基于应用日志和基础属性信息对应用系统进行刻画。包括但不限于应用名称、负责人、应用类型、敏感等级、所属机构、用户数、告警数、日志量、跨区域访问数、访问用户TOP10等信息 |
| 19 | 终端画像 | 基于终端行为日志和基础属性信息对终端进行刻画。包括但不限于IP地址、单位部门、告警数量、告警类型、使用用户、访问应用排行等信息 |
| 20 | 组织机构画像 | 基于用户行为日志进行聚类分析，对组织机构进行刻画。包括但不限于机构详情、机构告警类型占比、机构人员预警、机构活跃用户、机构人员访问系统排名、机构终端日志top排行、机构时间日志数分布等信息 |
| 21 | 平台维护功能 | 统计报表生成 | 基于预置规则生成各种报表，如日报、周报、月报等，并支持多种形式的展示方式，如表格、图表等，方便管理者快速了解用户异常行为情况、系统运行情况 |
| 22 | 重点关注对象 | 方便管理员对被关注对象（用户和终端）进行快速便捷的日志审计和分析。管理员能够在关注对象列表中，查询关注对象的日志记录、告警等信息 |
| 23 | 系统配置管理 | 提供平台的基本配置设置功能，包括参数配置、网络连接配置、运行状态监控管理等 |
| 24 | 用户管理 | 负责管理系统的用户及其相关信息。包括用户的注册、登录、密码找回、账户禁用/启用、分配初始密码、组织结构管理等。用户与组织机构进行映射，提供树状层级结构目录，可以更加清晰地反映用户与组织机构的关系，并支持用户查找，支持用户信息导入导出； |
| 25 | 权限管理 | 支持为不同用户分配不同的权限，控制他们对系统资源的访问和操作。支持角色管理，管理员可以定义不同的角色，并为每个角色分配一组权限。基于树状层级结构进行权限控制，可以提供更高的安全性，也便于权限和角色的继承，可以大大减少管理员的工作量。支持分层分级管理，分为多层级管理员、多层级使用员，且为分局、市局业务单位所有政工干部根据不同需求，开通相应的角色权限。 |
| 26 | 密码改造 | 身份鉴别 | 身份鉴别 |
| 27 | 远程管理通道安全 | 远程管理通道安全 |
| 28 | 访问控制信息完整性 | 访问控制信息完整性 |
| 29 | 数据加密存储 | 数据加密存储 |

### 硬件设备性能指标

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目** | **序号** | **名称** | **技术规格** | **数量** | **单位** |
| 硬件设备 | 1 | 安全审计产品1 | 机架设备；CPU≥2颗4核，内存≥32GB，数据硬盘≥4TB；冗余电源；千兆网络接口≥4个；万兆网络接口≥2个；吞吐量≥8Gbps。  系统功能：  1、具有知识产权。  2、日志采集：具备多种方式的日志采集功能，包括WEB服务接口采集、数据库采集、Kafka消息采集、文件共享服务采集等方式。  3、支持对视频图像信息系统、集成指挥应用等业务应用日志数据进行深度解析，提取出关键信息字段，如时间戳、源IP、目的IP、事件类型、事件描述等。  4、具备日志数据的映射功能，将源数据结构中的字段与目标数据结构中的字段进行对应和转换。  5、具备日志数据进行格转功能，以格式化文件通过边界接入平台同步进公安信息网。  6、具备数据校验功能，具备日志数据质量校验功能，包括格式校验、值域范围检查、字段齐全检查、空值检查、哈希值校验等。；  7、具备视频图像应用审计功能，支持查看视图库日志，审计内容包括操作时间、源IP、目标IP、用户名、流量大小、检索输入条件、操作详情等信息。  ▲8、具备日志数据校验、加密存储，存储总量>1050 万。同时具备统计分析结果列表展示，内容包括操作日志数、操作类型数等，可查看详情支持列表数据导出。提供CMA认证的检测报告以证明。 | 1 | 台 |
| 2 | 安全审计产品2 | 机架设备；CPU≥2颗4核，内存≥32GB，数据硬盘≥4TB；冗余电源；千兆网络接口≥4个；万兆网络接口≥2个；吞吐量≥8Gbps。  系统功能：  1、具有知识产权。  2、日志采集：具备多种方式的日志采集功能，包括WEB服务接口采集、数据库采集、Kafka消息采集、文件共享服务采集等方式。  3、支持对移动警务应用、移动服务总线日志数据进行深度解析，提取出关键信息字段，如时间戳、源IP、目的IP、事件类型、事件描述等。  4、具备日志数据的映射功能，将源数据结构中的字段与目标数据结构中的字段进行对应和转换。  5、具备日志数据进行格转功能，以格式化文件通过边界接入平台同步进公安信息网。  6、具备数据校验功能，具备日志数据质量校验功能，包括格式校验、值域范围检查、字段齐全检查、空值检查、哈希值校验等。。  7、具备服务总线引擎，对接移动服务总线获取移动警务应用日志。  ▲8、具备根据当前 IP、当前日志原文内容，解析出此IP 最近 7天是否存在与当前日志原文相似或者相同的日志发生，分析相同告警模型和内容中的同一性，相同资产告警的差异性，发现潜在的系统瓶颈、异常行为和安全威胁。提供CMA认证的检测报告证明。 | 1 | 台 |
| 3 | 应用安全审计一体机 | 2U机架式设备；配置国产CPU和国产操作系统；CPU≥16C（核），内存≥256GB，数据硬盘空间≥24TB；冗余电源；千兆网络接口≥4个。  系统功能：内置应用安全审计基础套件，包括日志采集、日志清洗、日志组织、日志管理、日志服务、分析服务等组件。  1、具备日志采集引擎，支持多种方式的日志采集功能，包括WEB服务接口采集、数据库采集、Kafka消息采集、文件共享服务采集等方式。  2、具备分布式SQL执行引擎，将SQL查询转换为分布式计算任务，能够在多个节点上并行执行查询，加速数据处理速度。  3、具备分布式数据映射搜索处理组件，提供索引创建、索引管理、全文搜索、范围查询、模糊匹配等多种搜索能力。  ▲4、具备自定义模型配置，包括模型名称、模型 Cron、是否草稿、模型描述、SQL 来源、参数化。提供CMA认证的检测报告证明。  ▲5、具备日志高级检索，可以根据操作人单位、业务线、系统名称、终端 IP、操作人地区、操作类型、日志类型进行对日志进行高级筛选。提供CMA认证的检测报告证明。  ▲6、具备用户行为大数据分析组件，提供异地登录、离退休人员、访问量突增、非工作时间访问、异常账号、频繁操作、高频查询、同人不同IP等20多种告警模型。提供CMA认证的检测报告证明。  ▲7、具备日志大数据分析系统，提供10多种研判分析模式，包括智能分析、反向追溯、交叉访问、同机构比对、数据泄露可疑名单、用户轨迹分析、操作量 TOP10 分析、热词反查分析、工作时间访问对比、越权访问、离职退岗人员查询等功能。提供CMA认证的检测报告证明。  8、具备日志清洗组件，对各类日志数据进行解析、映射、转换、清洗、标识和质量校验等处理，将其转化为满足《公安信息系统应用日志安全审计平台日志采集规范》要求的数据。  9、具备日志组织组件，满足大规模日志数据进行持久化存储，支持高可扩展性、高可用性。  10、具备日志管理组件，包括数据目录管理、数据质量管理、元数据管理、数据标签管理、数据统计、数据加密管理等功能，为数据分析提供高质量、高可靠的数据支撑。  11、具备日志服务组件，支持日志数据封装为查询服务接口、订阅服务接口、推送服务接口、访问服务接口、分析服务接口，对外部用户和系统提供数据支持。  12、提供数据分析计算组件，支持离线批处理计算、实时内存计算、OLAP关联计算、机器学习等能力。 | 5 | 台 |

**注：标记▲项目为关键技术指标，需要按要求提供证明文件。**

## 应用安全能力

（1）应用系统初步拟定为国家应用等级保护二级应用，配合按照国家应用等级保护相关要求开展定级、测评。

（2）配合开展商密改造；配合开展第三方软件检测；配合开展第三方应用安全检测，并修复安全漏洞。

（3）满足公安大量敏感性数据展示与查询脱敏显示的需要。

（4）能够满足我单位其他的网络、数据和应用安全管理要求。

# 运行环境

系统在上海公安信息网用户域运行并提供服务，视频传输网日志采集设备部署于视频传输网。

# 运维及服务要求

（1）项目完成后，中标方应向用户提供完整的技术资料。

（2）项目完成后，对项目涉及的软件开发功能提供1年免费维护、硬件部分提供3年的免费维护，包括：整体优化与根据用户需求开展的功能更新，提供不少于1人的驻场维护服务，7\*24小时的电话技术支持服务，如出现故障需一般各模块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，4小时内解决问题；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以及相关系统对接的技术支持；支持与市局应用开展对接联调调试。

（3）中标方在用户方指定的重大节点期间加强保障，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1人进行7×24小时的现场技术支持服务。

（4）投标方需要提供企业综合实力证明文件，如ISO27001信息安全管理体系、ISO20000信息技术服务管理体系认证、CCRC信息安全服务资质认证证书等。

# 实施要求

（1）中标方负责项目性能的优化指导、故障诊断等工作，根据实际运行情况，定期调整软件硬件配置策略。

（2）中标方应该保证所提供的所有产品皆不侵犯任何第三方的版权、知识产权和其他合法权利。

（3）项目经理需具备信息系统项目管理师证书，实施团队在实施期间需提供不少于8人（含项目经理）的专业服务。从业经验需得到用户方认可。并需提供相关证书扫描件、个人履历等，以及投标人为以上人员缴纳社保的证明。

（4）中标方应协助用户制定运行相关规范，并提供相关咨询、建议服务。

（5）中标方应在项目合同签订后4个月内完成建设工作（包含1个月试运行期）。

# 验收

在中标方完成项目系统和设备安装部署并通过按相关测评后进行验收，若存在双方无法达成共识的项目功能问题，用户有权委托第三方检查机构进行测试及验收。