监控联网子系统建设项目(2026 年升级改造)采购需求

一、项目概况

以网络传输、安全系统、视频存储等成熟技术为基础，融入监管场所检察业务，辅助监所检察办案，创新、优化驻监所检察机制，提升检察效能。收集、存储和管理所在场所监控视频数据，实现上海市派驻检察室所在场所监控数据收集，结合刑执业务开展检察监督，实时监看重要区域监控视频。同时，助推派驻检察部门对监管场所进行无盲区、无时空缝隙的检察监督，为检察工作和领导决策提供一线数据，提升检察监督职能，规范监管执法，促进公正执法，维护监管场所秩序，保障服刑人员合法权益。

本项目建设须符合信创要求。

二、建设目标

2.1、项目目标

本次项目总体建设目标主要如下，完善相关检察室监控联网系统，接入视频智能分析平台，建设一套刑罚执行视频监督管理，对接视频分析平台，提高监督效能。解决人工监督不能全覆盖、等问题，助力驻监监督业务从被动监督向主动监督转变。

2.2、考核目标

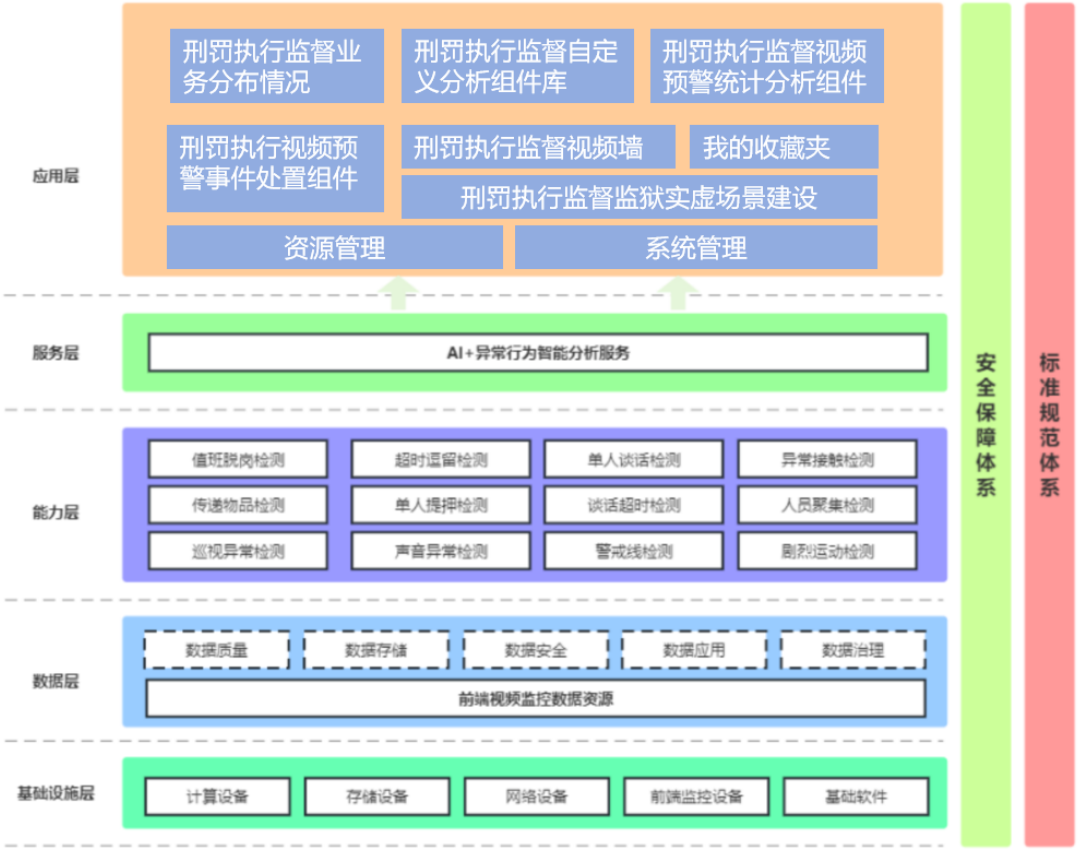
序号	一级指标	二级指标	三级指标	四级指标	目标值
1	通用指标	产出指标	产出数量	软件开发完成率	=100%
2	通用指标	产出指标	产出数量	硬件设备购置完成率	=100%
3	通用指标	产出指标	产出数量	软件产品购置完成率	=100%
4	通用指标	产出指标	产出时效	项目建设周期	≤24 月
5	通用指标	产出指标	产出质量	软件测试达标	通过
6	通用指标	产出指标	产出质量	密码测试达标	通过

7	通用指标	产出指标	产出质量	系统可靠性	≥99.9%
8	通用指标	产出指标	产出质量	网络安全等级保护	三级
9	通用指标	产出指标	产出质量	安全测试达标	通过
10	通用指标	产出指标	产出质量	一次性验收合格率	=100%
11	通用指标	产出指标	产出质量	安全事件发生次数	0 次
12	通用指标	应用系统	视频监控系统水平	视频数据可回放时间	≥15 天
13	通用指标	安全体系	安全建设水平	安全产品购置完成率	=100%
14	通用指标	安全体系	安全建设水平	数据安全措施	有
15	通用指标	安全体系	安全建设水平	网络安全措施	有
16	通用指标	安全体系	安全建设水平	系统安全措施	有
17	业务指标	产出指标	产出质量	一般操作网页响应时间	≤3 秒
18	业务指标	产出指标	产出质量	复杂查询或统计的网页响应时间	≤8 秒
19	业务指标	产出指标	产出质量	中等复杂度页面响应时间	≤5 秒
20	业务指标	产出指标	产出质量	建模是否可动态扩展	支持
21	业务指标	产出指标	产出质量	建模数量	≥11 个
22	业务指标	产出指标	产出质量	智能分析接入率	=100%
23	业务指标	产出指标	产出质量	数据对接（接口）成功率	≥99%
24	业务指标	产出指标	产出质量	数据采集频率	1 次/天
25	业务指标	产出指标	产出质量	数据恢复时效	≤1 小时
26	业务指标	效益指标	社会效益	提供监控联网安全保障的驻监检察室数量	≥11 个
27	业务指标	效益指标	社会效益	预警数据复核率	=100%

三、项目建设内容

3.1、总体架构

本项目总体架构如下图，从上往下分别为应用层、服务层、能力层、数据层、基础设施层，总体架构如下图：



3.2、建设原则

充分适应上海检察信息化发展的需要，遵循长远规划、基础规范、充分论证、可靠实用的理念，确保系统高效智能、操作简单、安全稳定、维护方便、升级灵活。需遵循以下原则：

1）开放性和标准性原则

软件系统应具备良好的开放性，可以根据检察业务的需要，进行多种系统或多种设备的集成和拓展。系统设计要遵循开放性标准，符合上海检察机关信息化建设基础规范的要求，实现业务信息的输入、输出标准化，便于与其他系统之间的互联互通。

2）先进性和实用性原则

采用基于三层体系结构的系统构架和面向对象设计的应用软件；选用稳定可靠且通用的系统软件、数据库软件、中间件软件、工具软件等开发平台；选用技术领先、设备先进、质量可靠、性能价格比合理的设备。

3）扩展性和维护性原则

系统采用的技术架构应具有较强的可扩展性与维护性，可根据业务需求变化进行灵活的功能调整和扩展，便于系统维护和故障排查。

4）安全性和可靠性原则

必须保证系统与各相关系统之间数据传输的准确性、可靠性，不能出现数据丢失和错误的现象；充分考虑系统的备份与恢复。保证数据通信的安全，所有用户的操作应在授权下执行，不能越权操作数据。系统建立日志记录、运行监控等机制，保证系统安全可靠。

3.3、建设规范

本项目建设遵循等级保护相关要求，《2025 年上海市检察机关检务保障工作要点》;《数字检察建设规划》;《2023—2027 年检察改革工作规划》;《关于加强派驻监管场所检察工作的意见》;《关于进一步规范看守所与驻所检察室信息联网工作的通知》等。

3.4、建设内容

本次项目主要包含刑罚执行视频监督应用系统开发、市检监控联网子系统安全加固、驻强疗所检察室监控联网建设、对驻监所检查室工作网进行安全加固。具体建设内容主要如下。

一.应用系统开发

刑罚执行视频监督管理系统主要功能包括监督管理分析、摄像头管理、收藏管理、地图管理、数据管理等功能。可将接入展示平台内的摄像头按层级展示，也可根据自定播放设置具体监控播放方式。同时包含相关业务统计数据分析，以直观、易懂的方式展示数据。为派驻检察官提供高效监督、快速处置的系统性软件。

系统需提供三维地理信息和三维室内布控能力，通过对监所的建模，派驻

检察官可以根据自己的需要选择监控点位和数据信息进行综合分析。提供预警信息统计分析、预警事件处置、自定义分析组件、视频墙、我的收藏夹和资源管理等核心功能。

系统应具有扩展性，应能与市院“智能图像分析系统”以及现有“监控联网子系统”对接，可根据预警信息进行趋势统计、分类统计等，辅助驻监检察人员了解整体情况，缩小监督范围，提高监督效率。

二.市检监控联网子系统安全加固

参照信息安全等级保护（三级）的相关要求，对市检察院监控联网子系统进行安全加固建设。在中心机房以及驻监检察室机房新增防火墙、安全感知平台、威胁探针、全网行为管理、违规外联检测等产品，提升驻监狱总医院检察室、驻强疗所检察室及驻南汇监狱检察室等地的网络边界安全防护能力。

依托于市检察院驻监狱检察室监控联网子系统，在国家检察官学院上海分院（中心机房）及各驻监检察室部署 VPN 加密设备，实现对国家检察官学院上海分院（中心机房）与 11 个驻监检察室机房之间建立安全、稳定的传输通道，实现检务数据的安全交互与高效业务处理。

三.驻强疗所检察室监控联网建设

根据高检院、公安部《关于进一步规范看守所与驻所检察室信息联网工作的通知》等相关文件要求，建设驻强疗所检察室监控联网子系统，部署视频监控管理系统、存储系统、支持 200 路视频接入，确保录像保存时间不少于 15 天。

根据公安接入要求，配置安全设备、网络设备，并对驻强疗所检察室机房基础设施进行改造，增加机房监控系统、UPS 系统等配套基础设施。其中机房环控系统应与市检现有环控系统进行对接，实现统一管理。

四.驻监驻所工作网安全加固

根据《信息安全技术网络安全等级保护基本要求》等相关标准，对驻监所检察室工作网出口边界进行安全加固，在边界处新增部署防火墙设备，保护内部网络免受外部威胁。

本项目主要建设内容的清单如下：

1、软件开发清单

序号	模块	功能	功能描述
1	刑罚执行监督业务分布情况	刑罚执行监督业务分布情况	在上海行政区域鸟瞰图显示各监狱位置信息，驻监检察人员可以选择某监狱标识后将立刻呈现该监狱的虚拟监控点位布控信息，对响应的统计分析数据也为当前监狱的
2	刑罚执行监督监控自定义分析组件库	数据分析组件库	提供数据分析组件库功能，制定统一组件标准，可以根据不同业务数据信息构建多个可视化组件存放在组件库中。检察官可以根据自己的工作需要在组件库中选择自己需要的可视化组件在主页面上展示
3		自定义界面布局	根据检察监督业务需求，业务人员可以根据自己需求从数据分析组件库中选择自己想要的组件并在主页上展示；展示的位置可以灵活调整。
4	刑罚执行监督视频预警统计分析组件	预警数量趋势统计	根据预警信息数量按发展趋势进行统计分析，通过预警数量的变化观测预警种类的发展变化，辅助驻监检察人员了解整体情况
5		预警数量分类统计	按监狱、预警分类等维度进行统计分析，通过对各监狱的预警类型进行统计分析，辅助驻监检察人员发现监管问题
6	刑罚执行监督视频预警事件处置组件	预警信息提醒	实时获取预警信息，通过事件描述的形式分批展示预警类型、预警信息和预警视频，并按“未处理”和“已经处理”分类展示
7		预警信息处置	业务人员根据预警信息情况，判断该预警信息是否为虚警，如果是虚警则忽略，否则正式纳入预警库长期保存
8		预警抓拍	驻监检察人员根据回放视频，提供视频抓拍功能，可以抓拍视频中的关键帧作为证据保存
9		联动录像	驻监检察人员根据回放视频，选着事件发生起止事件将事件完整视频录像保存
10	刑罚执	轮播管理	支持进行轮播管理设置，可以将播放列表里的视频源

序号	模块	功能	功能描述
	行监督监控视频墙		按要求进行轮播。包括轮播切换频率、轮播源设置等。
11		多屏播放管理	多屏播放管理-多屏类型选择：支持针对已接入的多路摄像头实现多屏展示，可选择 4 路、9 路及 16 路三种展示类型。
12		播放组件	提供视频回放和实时查看的视频播放组件，可以支持视频日常拖拽、快进等播放操作。
13	我的收藏夹	收藏分类	对收藏夹里的视频信息进行分类，业务人员可以根据分类进行快速定位需要查看的视频信息，并对该视频源进行相关的操作（添加视频墙或移动收藏夹）
14		自定义排序	自定义排序功能支持用户对收藏夹中的摄像头自行排列顺序
15		收藏检索	收藏搜索功能支持用户输入搜索条件，快捷搜索用户个人收藏夹内摄像头
16	资源管理	监控设备管理-监控视频源同步管理	从视频监控平台同步获取视频监控的视频源信息，将所有同步到的视频源 URL 信息保存。支持批量导入，在监狱监控设备发生线路调整或其他变动时，可快速完成展示平台内设备信息同步。
17		监控设备管理-监控设备维护	1、为驻监检察人员提供监控设备快速检索、异常状态查看和添加收藏夹等操作，发现有异常的监控设备也可以在该设备上标注“异常” 2、监控摄像头基本信息维护，可以增加、删除、修改监控摄像头的基本型，包括摄像头所属监狱、唯一标识，以及绑定监控视频源信息；
18		监狱楼宇信息管理-楼宇模型管理	配置各监狱楼宇模型信息，包括所属监狱、楼宇唯一标识，楼宇每层的点击触发事件信息设置，方便驻监检察人员点击楼宇的楼层时可以展开该楼层的平面视图以及该楼层的监控点位信息
19		监狱楼宇信	基于监狱室外监狱坐标系进行监控点位信息设置，支

序号	模块	功能	功能描述
		息管理-室外监控点位设置	持直接拖放设置设备位置。驻监检察人员可以根据监狱的实际情况放置监控设备至三维虚拟环境中，如果发现位置不正确可以调整
20		监狱楼层信息管理-楼层模型管理	配置各楼层模型信息，包括该楼层所属楼宇、楼层信息，驻监检察人员可以根据该楼层虚拟模型中的监控布局，直观查看监控视频信息。
21		监狱楼层信息管理-楼层室内监控点位设置	基于监狱室内楼层坐标系，拖放监控设备到楼层虚拟环境中，驻监检察人员可以根据监狱的实际情况放置监控设备至三维虚拟环境中，如果发现位置不正确可以调整
22	刑罚执行监督监狱实虚监控场景建设	五角场监狱刑罚执行监督虚实场景建设-五角场监狱楼宇建模及数据接入	根据五角场监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
23		五角场监狱刑罚执行监督虚实场景建设-五角场监狱楼层建模及数据接入	根据五角场监每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
24		周浦监狱刑罚执行监督虚实场景建设-周浦监狱	根据周浦监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位

序号	模块	功能	功能描述
		楼宇建模及数据接入	
25		周浦监狱刑罚执行监督虚实场景建设-周浦监狱楼层建模及数据接入	根据周浦监狱每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
26		南汇监狱刑罚执行监督虚实场景建设-南汇监狱楼宇建模及数据接入	根据南汇监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
27		南汇监狱刑罚执行监督虚实场景建设-南汇监狱楼层建模及数据接入	根据南汇监狱每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
28		监狱总医院刑罚执行监督虚实场景建设-监狱总医院楼宇建模及数据接入	根据监狱总医院外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位

序号	模块	功能	功能描述
29		监狱总医院刑罚执行监督虚实场景建设-监狱总医院楼层建模及数据接入	根据监狱总医院每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
30		新收犯监狱刑罚执行监督虚实场景建设-新收犯监狱楼宇建模及数据接入	根据新收犯监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
31		新收犯监狱刑罚执行监督虚实场景建设-新收犯监狱楼层建模及数据接入	根据新收犯监狱每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
32		青浦监狱刑罚执行监督虚实场景建设-青浦监狱楼宇建模及数据接入	根据青浦监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
33		青浦监狱刑	根据青浦监狱每个楼层室内布局结构进行三维建模，

序号	模块	功能	功能描述
		罚执行监督虚实场景建设-青浦监狱楼层建模及数据接入	构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
34		北新泾监狱刑罚执行监督虚实场景建设-北新泾监狱楼宇建模及数据接入	根据北新泾监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
35		北新泾监狱刑罚执行监督虚实场景建设-北新泾监狱楼层建模及数据接入	根据北新泾监狱每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
36		女子监狱刑罚执行监督虚实场景建设-女子监狱楼宇建模及数据接入	根据女子监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
37		女子监狱刑罚执行监督虚实场景建	根据女子监狱每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三

序号	模块	功能	功能描述
		设-女子监狱楼层建模及数据接入	维监控上快速找到需要查看的监控点位
38		未管所刑罚执行监督虚实场景建设-未管所楼宇建模及数据接入	根据未管所外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
39		未管所刑罚执行监督虚实场景建设-未管所楼层建模及数据接入	根据未管所每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
40		宝山监狱刑罚执行监督虚实场景建设-宝山监狱楼宇建模及数据接入	根据宝山监狱外景实际布局进行监狱外景的三维建模，包括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
41		宝山监狱刑罚执行监督虚实场景建设-宝山监狱楼层建模及数据接入	根据宝山监狱每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
42		提篮桥刑罚	根据提篮桥景实际布局进行监狱外景的三维建模，包

序号	模块	功能	功能描述
		执行监督虚实场景建设-提篮桥楼宇建模及数据接入	括各监狱的楼宇信息，为派驻检察官提供监狱外景三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
43		提篮桥刑罚执行监督虚实场景建设-提篮桥楼层建模及数据接入	根据提篮桥每个楼层室内布局结构进行三维建模，构建各楼层监狱房间、走廊、楼梯等虚拟场景；为派驻检察官提供监狱室内三维视图巡视功能，可以在三维监控上快速找到需要查看的监控点位
44	密码应用改造		密码应用改造，主要包括用户身份认证机制模块、业务重要数据安全传输模块、服务器虚拟机设备日志/访问控制信息完整性模块、重要可执行程序签名验签模块、用户访问控制信息签名验签模块、应用系统重要数据加解密模块、应用系统重要数据签名验签模块

2、产品软件清单

序号	软件名称	用途	功能说明／配置要求	数量	单位
1	操作系统	服务器操作系统	1.国产服务器操作系统，具备自主知识产权，需通过中国信息安全测评中心或国家保密科技测评中心的测评； 2.兼容国内主流的数据库、中间件产品，如金仓、达梦、南大通用、瀚高、东方通、金蝶、中创、华宇等； 3.一年质保。	3	套
2	中间件	服务器中间件	1.国产中间件 2.支持多种主流国产操作系统，如麒麟 OS、统信 UOS 等； 3.支持多种主流国产数据库系统，如达梦、金仓、神通、南大通用等； 3.一年质保。	1	套

序号	软件名称	用途	功能说明/配置要求	数量	单位
3	数据库	服务器数据库	1.国产数据库，具备完全自主知识产权，应通过中国信息安全测评中心集中式数据库安全可靠测评； 2.支持飞腾、龙芯、鲲鹏、申威、兆芯、海光主流国产芯片； 3.支持UOS、麒麟、中科方德等主流国产操作系统； 3.一年质保。	1	套

3、硬件设备清单

序号	名称	类别	配置要求	数量	单位
1	服务器	主机	1.国产CPU：≥2颗64核CPU； 2.内存：≥256GB； 3.硬盘：≥2块480GB SSD SATA，数据盘不少于3*8T企业级硬盘，不低于7200rpm，iops不低于140，支持热插拔； 4.网口：≥4个千兆电口，4个万兆光口（含光模块）； 5.RAID卡，支持raid0，1，5，10等，配置冗余电源； 6.配置标准滑轨，整机三年质保，三年介质保留服务，提供原厂针对本项目的授权及售后服务承诺函，符合国家有关安全可信要求。	2	台
2	服务器	主机	1. 国产CPU：≥2颗64核CPU； 2.内存：≥64GB； 3.硬盘：≥2块480GB SSD SATA，数据盘不少于3*8T企业级硬盘，不低于7200rpm，iops不低于140，支持热插拔； 4.网口：≥4个千兆电口，4个万兆光口（含光模块）； 5.RAID卡，支持raid0，1，5，10等，配置冗	1	台

序号	名称	类别	配置要求	数量	单位
			余电源； 6.三年质保，三年介质保留服务，提供原厂针对本项目的授权及售后服务承诺函，符合国家有关安全可信要求。		
3	核心交换机	网络设备	1.≥24 个万兆光口，≥24 个千兆电口，双电源，≥4 个万兆光模块； 2.三年质保，提供原厂针对本项目的授权及售后服务承诺函。	1	台
4	接入交换机	网络设备	1.≥24 个千兆电口，≥4 个万兆光口，≥4 个万兆光模块； 2.三年质保，提供原厂针对本项目的授权及售后服务承诺函。	1	台
5	视频监控平台	音视频监控设备	1．嵌入式一体化设计，应支持组件模块化插板； 2．单台设备可支持≥1000 个监控点接入； 3．支持平台级联扩展组网，至少可支持≥7 级级联； 4．单台设备支持单纯录像能力≥250Mbps,单纯转发能力≥580Mbps； 5．支持码流自适应功能，针对同时浏览的窗口数，可自动切换主流或辅流（提供彩页、功能截图或检测报告等有效证明材料）； 6．支持将监控点的录像绑定到指定磁盘分区； 7．▲为确保系统稳定性，需支持智能丢包恢复，支持重传缓冲和精确重传功能（提供彩页、功能截图第三方检测报告等。）； 8.支持跨平台的可视化应用，支持在 windows/	1	台

序号	名称	类别	配置要求	数量	单位
			国产操作系统的 PC 终端上进行视频监控； 9．▲支持图像增强，支持去雾、低照度、去模糊等图像增强功能。（提供彩页、功能截图或第三方检测报告等相关证明材料）； 10．支持 WebRTC/RTSP/RTMP/HLS/HTTP-FLV 协议调用音视频媒体流，支持基于 HTTP 协议传输 MP4 文件格式的视频。（提供彩页、功能截图或检测报告等有效证明材料）； 11．符合 GB/T 28181 相关要求； 12.三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
6	存储	存储设备	1．应采用国产化芯片，模块化可插拔； 2．具备≥2 个 SFP+万兆以太网光口； 3．▲支持视频流协议直接写入存储，具备录像机转发能力；写入能力≥960Mbits/s、转发能力≥380Mbits/s（提供彩页、功能截图第三方检测报告）； 4．支持创建/修改/删除/查看虚拟磁盘组,虚拟磁盘类型 ISCSI、NRU、NAS。支持磁盘在线修复功能； 5．在异常断电恢复后，设备可自动重启恢复正常； 6．支持 RAID0、1、5、6、10、RAIDX 模式；支持热备盘，针对坏扇区磁盘的热顶替； 7．支持 RAID 快速创建，可以根据写入码流带宽需求，动态调整 RAID 重建的速度； 8．支持 RAID 重建断点续建技术，设备重启之	1	台

序号	名称	类别	配置要求	数量	单位
			后，RAID 可以继续重建； 9．支持磁盘漫游功能，磁盘更换盘位后，不影响 RAID 正常使用，当存储池处于降级、重建状态，不影响数据写入； 10．在 RAID 组内丢失 2 块（含）以上磁盘但至少有 1 块正常磁盘时，不影响设备正常工作（提供彩页、功能截图或检测报告等有效证明材料）； 11．在 RAID 组内有磁盘失效且正常磁盘数量满足要求是，系统自动重构； 12．支持音视频、图片、智能结构化、文件等数据同时混合直接存入到一套存储中,系统可自动分配或指定存储空间池； 13．▲支持基本视频功能，可以与应用平台互联、接受平台的业务调度，实现视频录像、回放、检索以及录像文件的锁定，解锁等功能。支持视频录像以文件方式被第三方应用从存储中直接读取。（提供彩页、功能截图第三方检测报告等证明材料。）； 14.产品≥36 盘位，实配硬盘空间≥288T（36 个 8T 的企业级硬盘）； 15.三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
7	视频接入网关	音视频监控设备	1．应采用工业级嵌入式架构； 2．支持国标 GB/T28181 协议接入平台，支持≥100 路网络视频接入； 3.支持同时解码显示输出 16 路分辨率为 1920	3	台

序号	名称	类别	配置要求	数量	单位
			×1080、帧率为 30fps、码率不低于 6Mbps 的视频图像。最大解码显示输出 3840×2160 分辨率（提供彩页、功能截图或检测报告等有效证明材料）； 4.≥16 个 SATA 接口，硬盘热插拔，最大支持 10T 硬盘； 5. 支持将硬盘划分不同的存储空间，可进行 RAID0、RAID1、RAID5、RAID6、RAID10 设置管理，支持硬盘热插拔； 6. 支持按事件间类型查询录像并回放，可对指定录像设置标签，并可通过该标签对此录像进行检索，最大支持设置 64 个标签； 7.设备不少于 2×HDMI、≥1×VGA、≥3×RJ45、≥1×音频输入/输出、≥2×告警输入/输出接口； 8.三年质保，提供原厂针对本项目的授权及售后服务承诺函。；		
8	集中式综合业务平台	音视频监控设备	1.19 英寸标准机架式结构，模块化设计； 2.≥2 个千兆网口，配置 8 个解码板卡。； 3.单块板卡应支持不少于 2 路显示输出，不少于 2 路 HDMI、1 路 VGA 输出接口，支持 HDMI 与 VGA 双屏同时显示，HDMI 最高分辨率支持 4K（3840×2160）@30fps； 4.支持装配编码模块、解码模块、网关模块、控制键盘模块等，支持混合装配； 5.三年质保，提供原厂针对本项目的授权及售后服务承诺函。	1	台

序号	名称	类别	配置要求	数量	单位
9	双路高清解码模块	音视频监控设备	1. 单块板卡应支持≥2 路显示输出，≥2 路 HDMI、1 路 VGA 输出接口，HDMI 最高分辨率支持 4K（3840×2160）； 2. 板卡视频解码格式应支持 H.264、H.265； 3.板卡解码显示性能，4×4K、8×400 万（2592×1520）、16×1080P、32×D1；支持 GB 协议对接平台； 4. 解码显示画面风格，应支持 4/9/16 等分画面格显示； 5. 音频解码格式，应支持 G.711a，G.711u，ADPCM，G.722； 6.三年质保，提供原厂针对本项目的授权及售后服务承诺函。	8	台
10	机柜	机房建设	42U 标准机柜，含不少于 8 位 10A、2 位 16A PDU 两个	1	台
11	UPS	动力设备	1.在线式UPS主机支持额定容量不小于10kVA； 2.输入功率因数不小于 0.99，整机输出效率不小于 90%；输出电压、频率波动需符合国家\行业有关要求。 3.具备 ECO 运行模式； 4.支持开机自诊断功能； 5.支持系统过载、市电异常、系统故障、电池欠压等想象的告警功能； 6.符合 GB/T7260 相关标准，三年质保，提供原厂针对本项目的授权及售后服务承诺函。	1	台
12	蓄电池	动力设备	ups12V 蓄电池，三年质保。支持满载工况下持续稳定供电 2 小时以上	32	个

序号	名称	类别	配置要求	数量	单位
13	电池柜	动力设备	可容纳 16 节蓄电池，三年质保。	2	项
14	UPS 配套辅材	动力设备	包含配电箱、UPS 所需线材等，三年质保。	1	项
15	硬盘录像机	音视频监控设备	1.存储接口：≥2 个 SATA 接口； 2.视频接口：1×HDMI，1×VGA； 3.网络接口：1×RJ45 10/100/1000Mbps 自适应以太网口； 4.PoE 接口：8×RJ45 10/100Mbps 自适应以太网口； 5.存储容量不少于半年，三年质保。	1	台
16	摄像头	音视频监控设备	1.≥200 万半球网络摄像机，全彩； 2.最高分辨率可达 1920×1080 @25fps； 3.支持 Smart 侦测：越界侦测，区域入侵侦测； 4.支持背光补偿，强光抑制，3D 数字降噪，120dB 宽动态，适应不同环境； 5.支持 1 路报警输入，1 路报警输出，1 路音频输入，1 路音频输出； 6.支持 PoE 供电，符合 IP67，IK10； 8.实现机房场所全覆盖，无死角，三年质保。	2	台
17	硬盘	存储设备	硬盘空间≥6T，SATA 硬盘，三年质保	2	个
18	空调	机房建设	1.≥1.5 匹空调，含空调室内机及室外机； 2.最大制冷量不小于 3500W； 3.最大制热量不小于 5000W； 4.能效等级：1 级； 5.三年质保。	1	台

序号	名称	类别	配置要求	数量	单位
19	防火门	机房建设	1.防火门需满足国家相关标准，耐火极限达到甲级要求。 2.尺寸：定制 3.三年质保	1	扇
20	综合布线	综合布线	机房室内室外光纤敷设，含相关配套辅材，三年质保	1	项
21	静电地板	机房建设	600*600 全钢防静电地板，三年质保	16	平方米

4、安全产品清单

序号	名称	类别	配置要求	数量	单位
1	安全感知管理平台	安全管理与支持	1.支持信创 CPU 和操作系统,设备配置总核心≥32 核，内存：≥256GB，系统盘：≥2*240GB SSD，数据盘：≥48T，配置冗余电源； 2.整机处理能力≥9000EPS，端口≥4 千兆电口，≥2 万兆光口； 3.支持对网络设备、安全设备、主机系统的日志、网络流量等多种数据源的采集； 4.支持对日志采集器进行采集配置并下发；提供 Syslog、SNMP Trap、文本格式日志、数据库、WMI、Netflow、HTTP、Script 等采集方式；支持数据源信息导入、导出、数据源迁移操作； 5.▲支持对资产风险值的自定义计算，计算范围包括威胁告警及脆弱性的危害等级、时间范围、处置状态等纬度；支持对风险计算周期进行配置。（提供彩页、功	1	台

			能截图或检测报告等有效证明材料）； 6.支持主流厂商漏扫报告的解析识别和导入管理，支持人工漏洞报告导入，使用模板进行漏洞信息的导入；可通过网络数据传感器同步资产信息，通过平台的威胁告警模块同步漏洞，弱口令、网站漏洞信息； 7.支持自定义关联规则，支持日志关联规则建模，在指定的时间范围内，能够对来自不同数据源的日志进行关联分析； 8.▲支持在分析溯源时通过高级模式、Lucene、QAL 等多种模式进行日志检索；（提供彩页、功能截图或检测报告等有效证明材料）； 9.支持预置关联分析场景，包括攻击利用、恶意软件、拒绝服务、异常事件、内容安全、信息收集、威胁活动等场景分析； 10.支持事件调查管理，支持查看事件详情信息及事件调查处置的时间轴信息；支持事件调查管理，支持查看事件详情信息； 11.支持统计报表功能，支持对威胁告警和安全事件新增自动化响应策略； 12.▲支持以 IP 地址作为实体的多数据快速关联及分析展示能力。支持集中展示 IP 地址相关的威胁趋势、攻击阶段、威胁分类、威胁关联情况等数据以及该 IP 对资产的登录分析等信息（提供彩页、功能截图或检测报告等有效证明材料）；		

			13.含三年安全感知平台规则库更新，三年质保服务，提供原厂针对本项目的授权及售后服务承诺函。		
2	潜伏威胁探针	安全管理与支持	1.为保证产品兼容性，潜伏威胁探针需和安全感知管理平台同一品牌； 2.网络层吞吐量：≥20Gbps； 3.国产 CPU：≥32 核，内存：≥128GB 4.配置冗余电源； 5.接口≥4 千兆电口+4 万兆光口； 6.▲支持记录 TCP，UDP，HTTP 协议流量日志中的负载信息：TCP、UDP 的上下行负载支持可配;HTTP 协议的请求头、请求体、响应头、响应体支持长度可配；（提供彩页、功能截图或检测报告等有效证明材料）； 7.支持对 HTTP、FTP_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、NFS 等类型协议流量中出现文件传输行为进行发现和还原,并记录文件 MD5 发送至分析设备； 8.新增规则，在规则列表进行标签标记展示，新增规则产生的告警进行单独展示和标注；（提供彩页、功能截图或检测报告等有效证明材料） 9.支持远控/远程工具检测；支持对使用 base64、unicode、url 编码等混淆手段攻击检测；支持针对 shiro 反序列化，自定义添加密钥展示解密内容； 10.支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访	2	台

			问行为、传输文件行为； 6.含三年潜伏威胁探针规则库更新、三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
3	防火墙 1	边界安全	1.国产 cpu，符合安全可靠测评结果； 2.防火墙吞吐量 IPv4：≥15G；最大并发≥400 万；支持≥4 个千兆电口+2 个万兆光口 ,双电源，含 2 个万兆多模光模块； 3.支持路由模式、交换模式、旁路模式等； 4.支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由； 5.支持一体化安全策略：支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制功能； 6.系统预定义主流攻击规则，支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood 攻击，并支持警告、丢弃、增强防护等多种防护措施； 7.▲支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向的引流策略；（提供彩页、功能截图或检测报告等有效证明材料并）； 8.支持灵活的服务链编排功能（服务量管理），支持串接链和旁路链，支持网元组	1	台

			方向和目的位置设置；（提供彩页、功能截图或检测报告等有效证明材料）； 9.含三年 IPS 及 AV 特征库授权，三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
4	防火墙 2	边界安全	1.国产 cpu，符合安全可靠测评结果； 2.网络层吞吐量≥12G，并发连接≥350 万，每秒新建连接数≥9 万； 3.配置双电源；≥4 个千兆电口，≥4 个千兆光口，≥1 个 Console 口，板载≥4 个千兆电口，≥1 个扩展插槽； 4.支持路由模式、交换模式、旁路模式等； 5.支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由； 6.支持一体化安全策略：支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制功能； 7.系统预定义主流攻击规则，支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood 攻击，并支持警告、丢弃、增强防护等多种防护措施； 8.支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向的引流策略；	2	台

			9.三年 IPS 及 AV 特征库授权，三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
5	防火墙 3	边界安全	1.国产 cpu，符合安全可靠测评结果； 2.网络层吞吐量≥2G，并发连接≥250 万，每秒新建连接数≥5 万； 3..板载≥4 个千兆电口，≥1 个扩展插槽，≥1 个 Console 口； 4.支持路由模式、交换模式、旁路模式等； 5.支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由； 6.支持一体化安全策略：支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制功能； 7.系统预定义主流攻击规则，支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood 攻击，并支持警告、丢弃、增强防护等多种防护措施； 8.支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向的引流策略；（提供彩页、功能截图或检测报告等有效证明材料）； 9.三年质保，提供原厂针对本项目的授权及售后服务承诺函。	2	台

6	上网行为管理	主机及计算机环境安全	1. 支持信创 CPU 和操作系统，符合国家有关安全可靠测评要求； 2.性能参数：网络层吞吐量：≥2Gb，应用层吞吐量：≥150Mb，支持准入终端数：≥250，每秒新建连接数≥1000，最大并发连接数：≥50000； 3.支持外发内容过滤，支持支持基于关键字、正则过滤；支持对身份证号、电话等敏感信息过滤；（提供彩页、功能截图或检测报告等有效证明材料） 4.持实时提供在线用户趋势、用户流量排名、应用流量排名、用户实时流量和应用实时流量等信息； 5.支持对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等； 6.支持共享接入行为检测与审计；支持应用审计，可对应用进行分类识别及流量统计； 7.支持应用审计，可对应用进行分类识别及流量统计；可对网页的浏览、搜索、发帖、webmail 邮件进行审计；对用户传文件的行为进行审计； 8.支持邮件审计、FTP 审计以及 DNS 审计，支持业务审计监控，支持业务系统访问及 API 接口进行双向扫描，通过敏感信息、安全漏洞、行为接口等识别并标识数据及传输风险； 9.支持审计、控制国产主流、Oracle、MySql、SqlServer、PostgreSQL 等数据库	1	台

			的访问与操作；（提供彩页、功能截图或检测报告等有效证明材料） 10.三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
7	违规外联检测软件	主机及计算机环境安全	1.包含主机层违规外联检测，系统漏洞扫描，补丁修复管理、资产盘点，资产主动发现，轻补丁漏洞免疫，文件实时监控、勒索诱饵防护、恶意文件检测、进程阻断； 2.包含：≥10 套服务器，≥20 套 PC 软件授权； 3.国产化支持:统信 UOS、银河麒麟、中标麒麟、麒麟 v10、中科方德、欧拉、龙蜥、bclinux、深度、凝思、磐石、红旗等； 4.三年软件升级，提供原厂针对本项目的授权及售后服务承诺函。	1	台
8	防病毒	防病毒产品	1.服务器端防病毒授权； 2.兼容现有天融信品牌防病毒产品。	3	套
9	VPN 设备 1	数据安全	1.符合国密局制定的 GM/T 0022-2014《IPSEC VPN 技术规范》、GM/T 0023-2014《IPSEC VPN 网关产品规范》、GM/T 0024-2014《SSL VPN 技术规范》及 GM/T 0025-2014《SSL VPN 网关产品规范》等有关要求；整机与密码芯片由同一厂商生产制造；（提供相关证明材料。）； 2. 标准机架式设备，冗余电源，≥6 个千兆电口，≥4 个千兆光接口，≥2 个 40G 万兆光接口； 3. ▲IPSec:大包（1428 字节）加密吞吐能力≥19Gbps；小包（64 字节）加密吞吐	2	台

			能力≥900Mbps；支持隧道数≥40000；SSL 加密性能≥2.5Gbps,SSL 最大并发连接≥50000；SSL 最大新建≥20000；（提供彩页、功能截图第三方检测报告等有效证明材料。）； 4. 支持内置 CA，可为其他设备签发国密双证书；可由第三方 CA 进行证书签发； 5. 支持双机热备(Active-Standby),支持系统故障自动切换和抢占功能； 6. 支持管理员分权管理，不同管理员管理不同的功能模块；支持管理员的三权分立； 7. 提供基于标准 SSL 的加密通道，支持应用代理、VPN 隧道多种代理方式，能有效地支持 IP 层及以上应用协议数据保护； 8. ▲支持接口模式的应用系统单点登录，在 SSLVPN 客户端认证通过后，应用系统调用客户端 SDK 接口获取经过签名计算后的用户身份令牌，再通过 SSL VPN 的 WebService 接口验证身份令牌的合法性，并获取用户身份详细信息；（提供彩页、功能截图、第三方检测报告等有效证明材料。）； 9. 客户端支持国产化操作系统。 10. 支持证书、用户名口令、机器码、短信等多种认证因子，同时支持上述认证因子的组合捆绑认证； 11. 客户端支持多种工作模式:1）传统 VPN 客户端，建立安全虚拟通道；2）成功		

			建立安全虚拟通道道后，断开与互联网的连接，只允许本地终端访问安全网关授权的内网资源 3）客户端在安装到终端设备后，断开外设接口、禁止其它网络功能。只保留与安全网关通信的能力。在认证成功后，允许本地终端访问安全网关授权的内网资源； 12. ▲支持 VPN 设备统一管理中心，可被统一纳管，管理通道采用国密算法构建安全通道。（提供彩页、功能截图第三方检测报告等有效证明材料）； 13. 三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
10	VPN 设备 2	数据安全	▲1. 符合国密局制定的 GM/T 0022-2014《IPSEC VPN 技术规范》、GM/T 0023-2014《IPSEC VPN 网关产品规范》、GM/T 0024-2014《SSL VPN 技术规范》及 GM/T 0025-2014《SSL VPN 网关产品规范》等有关要求；整机与密码芯片由同一厂商生产制造； 2. 标准 2U 机架式设备，冗余电源，≥6 个千兆电口，≥4 个千兆光接口，≥4 个万兆光接口； 3. ▲IPSec:大包加密吞吐（1428 字节）：吞吐能力≥16Gbps；小包加密吞吐(64 字节)：吞吐能力≥900Mbps；支持隧道数≥40000；SSL 加密性能≥2.5Gbps,SSL 最大并发连接≥50000；SSL 最大新建≥4000；(提供彩页、功能截图第三方检测报告等	5	台

			有效证明材料。)； 4. 客户端支持国产化操作系统。 5. 支持证书、用户名口令、机器码、短信等多种认证因子，同时支持上述认证因子的组合捆绑认证； 6. 客户端支持多种工作模式:1)传统 VPN 客户端，建立安全虚拟通道；2）成功建立安全虚拟通道道后，断开与互联网的连接，只允许本地终端访问安全网关授权的内网资源 3)客户端在安装到终端设备后，断开外设接口、禁止其它网络功能。只保留与安全网关通信的能力。在认证成功后，允许本地终端访问安全网关授权的内网资源。 7. 支持 VPN 设备统一管理中心，可被统一纳管，管理通道采用国密算法构建安全通道； 8. 三年质保，提供原厂针对本项目的授权及售后服务承诺函。		
11	VPN 设备 3	数据安全	1. 符合国密局制定的 GM/T 0022-2014《IPSEC VPN 技术规范》、GM/T 0023-2014《IPSEC VPN 网关产品规范》、GM/T 0024-2014《SSL VPN 技术规范》及 GM/T 0025-2014《SSL VPN 网关产品规范》等有关要求；整机与密码芯片由同一厂商生产制造； 2. 标准机架式设备，冗余电源，不小于 6 个千兆电口，不小于 4 个千兆光接口，不小于 2 个万兆光接口；	6	台

			3. ▲IPSec:大包加密吞吐（1428 字节）：吞吐能力≥5Gbps；小包加密吞吐(64 字节)：吞吐能力≥600Mbps；支持隧道数≥20000；SSL 最大并发≥50000；SSL 最大新建≥600；SSL 加密性能≥400Mbps(提供彩页、截图、第三方检测报告等有效证明材料。） 4. 客户端支持国产化操作系统。 5. 支持证书、用户名口令、机器码、短信等多种认证因子，同时支持上述认证因子的组合捆绑认证； 6. 客户端支持多种工作模式:1）传统 VPN 客户端，建立安全虚拟通道；2）成功建立安全虚拟通道道后，断开与互联网的连接，只允许本地终端访问安全网关授权的内网资源 3）客户端在安装到终端设备后，断开外设接口、禁止其它网络功能。只保留与安全网关通信的能力。在认证成功后，允许本地终端访问安全网关授权的内网资源。(提供彩页、功能截图第三方检测报告等有效证明材料)； 7. 支持 VPN 设备统一管理中心，可被统一纳管，管理通道采用国密算法构建安全通道； 8. 三年质保，提供原厂针对本项目的授权及售后服务承诺函。		

四、电子政务云资源需求

本项目为本地部署，不涉及电子政务云资源，配置了 3 台服务器以及操作

性、中间件、数据库，供应商需按照机房环境以及应用建设完成相关服务器的部署。

五、其他工作要求

5.1、总体要求

供应商需充分考虑满足采购项目的建设要求，根据采购人的详细需求，提出完整的项目管理、培训、项目验收、售后服务方案。

供应商应本着认真负责态度，组织技术队伍，认真做好项目的实施工作。在签订合同前，提出具体实施、服务、维护以及今后技术支持的措施计划。

供应商应具备数据安全管控能力，具备数据管理能力等级证书优先考虑。

供应商在中标并签署合同后，应通过谈话、现场考察、资料学习、座谈会等形式深度了解用户需求，进一步细化明确建设内容，优化技术方案，并组织邀请社会专家参加的方案论证会，系统开发或硬件、软件产品等采购前须制作需求规格说明书或硬件、软件产品采购清单，由用户方书面确认后实施。咨询论证等费用由成交单位承担。

5.2、技术和性能要求

1）本项目建设须符合信创要求，系统支持信创环境。

2）系统具备良好的开放性，充分考虑今后功能扩展和应用系统集成。

3）软件性能指标：

✧ 标准软硬件配置环境下，一般操作网页响应时间不大于 3 秒；

✧ 复杂查询或统计的网页响应时间不大于 8 秒；

✧ 中等复杂度网页响应时间不大于 5 秒。

4）硬件性能指标：

✧ 清单中各产品的详细技术参数要求如下（标▲项为重要技术参数），偏离表中如实填写，签订合同前根据需要进行参数复核（包括性能参数）。

✧ 为确保真实性，指标要求所需的截图、彩页、测试报告、证书等证明材料，以及产品厂商针对本项目的授权函和服务承诺函，须加盖产品厂商公章。

5）本次市检监控联网子系统安全加固部分，应参照信息安全等级保护要求进行建设，满足等级保护（三级）的相关要求。

6）系统产生的电子文件符合电子归档的相关要求。

7）本系统需要在特定场所实施，采集的信息具有敏感性要求，对承建单位及人员具有安全性要求。

8）本次项目不得出现安全事件。

5.3、售后服务要求

本项目验收通过后，提供项目整体免费维护期 1 年；软件产品（包括，刑罚执行视频监督管理系统、工具软件），其免费质量保证期为 1 年；硬件产品的免费质量保证期则为 3 年，具体产品参照采购参数要求。承诺为系统提供终身技术支服务。服务对象为全市检察机关与项目相关的单位、部门和用户。为确保系统的正常运行，及时解决发生的各类问题，需结合项目实际，制定有效的运维保障方案和安全应急措施。并按约定，提供以下方式服务：

1）驻场技术服务

运维期间，根据系统运行的实际需求派驻现场工作人员，面向全市检察机关，对系统发生的事件、用户的要求进行及时响应；通过应用指导、运维保障和软件开发等多种方式提供高效和优质的综合技术服务。

2）重大活动伴随服务

用户若有跟系统相关的重大活动，项目组需提供活动所需专人进行事前调试和始终伴随服务，以确保系统的正常运行，最终实现用户活动的顺利完成。

3）巡检服务

每月进行一次巡检服务，由专业的技术支持人员上门通过专业的方式对系统运行状况进行全面检查测试，及时发现和排除隐患，确保数据备份的可靠性，保证系统可持续正常运行，并提交巡检报告。

4）远程支持服务

- 热线电话服务

提供项目组技术人员的 7*24 小时服务热线；针对检察院提出的问题，通过电话解答咨询、指导应用和故障排除。对于无法解决的问题，及时受理登记，安排运维任务。

➢ 电子邮件服务

提供项目组负责人邮箱地址，若遇到疑难的问题，用户可将问题通过 E-mail 的方式发给项目组相关负责人，项目组每天至少接收一次邮件，并在 2 个工作日内及时予以回复。

5）其它

将各项运维服务纳入上海检察机关统一运维平台，实现问题统一受理、解决、反馈和汇总，所有运维工作均应在运维管理平台中全程详细记录，并不断丰富应用系统常见问题知识库。

5.4、应急响应要求

供应商对系统故障应能够实时响应，若系统发生故障，接到通知后 30 分钟之内响应，专业工程师 2 小时内到达现场。特殊故障与客户沟通协商后，按照协商的方式制定解决方案并进行处理。

具体故障级别及对应的应急响应要求如下：

一级故障：在 1 小时内确诊，总故障解决时间不超过 4 小时。

二级故障：在 2 小时内确诊，并在 4 小时内由专家到达现场确诊并解决，总故障解决时间不超过 8 小时；

三、四级故障：在 4 小时内确诊故障，总故障解决时间不超过 16 小时。

5.5、培训要求

根据用户的要求，针对系统用户，应该组织技术交流和培训，内容包括系统的功能升级、常见问题、配置说明、操作技巧等。

培训对象包括系统管理员、业务操作人员，其中系统管理员不少于 2 天培训，业务操作人员不少于 3 天培训。系统管理员，经培训后能够完成系统的日常管理维护工作；业务操作人员，经培训后能够熟练掌握使用本系统进行相关业务操作。

5.6、进度要求

本项目要求合同签订后，供应商应根据用户方要求，及时整体或分批启动项目，在需求规格说明书确认后，按双方约定的时间节点完成项目。

自合同签订之日起至 2027 年 9 月前完成系统建设并通过验收。

5.7、项目团队及驻场人员要求

1）投标人须具有稳定的在职技术保障力量，能够提供及时的技术支援或服务，应针对本项目提供不少于 9 人的项目服务团队（包括项目负责人、实施工程师等），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。

角色	主要职责	人员数量	人员要求	驻场要求
项目负责人	负责项目质量和进度控制	1 人	具有全日制硕士及以上学历；具有信息系统项目管理师（高级）证书；具有信息安全专业人员 CISP 证书；具有弱电工程师证书的，8 年（含）以上类似经历	不驻场
技术负责人	技术负责人	1 人	技术负责人具有信息系统项目管理师（高级）证书；具有系统集成中级及以上职称；具有信息安全专业人员 CISP 证书；	不驻场
软件开发工程师	负责项目应用软件的需求调研、功能开发及测试	4 人	项目配备人员具有信息安全专业人员 CISP 证书、软件设计师或系统架构设计师（高级）证书、具有系统集成项目管理工程师。持证人员在记分中不重复。	不驻场
实施工程师	负责项目的实施部署与技术支撑	4 人		不驻场

2)投标人应针对本项目提供不少于 2 人的质保期间(不少于 1 年)支撑团队（运维人员 2 人），投标人的相关服务人员需具备相应的服务能力，需提供相关证明。

角色	主要职责	人员数量	人员要求	驻场要求
运维人员	负责项目具体运维	2 人	可与实施团队中实施工程师人员为同一人	其中一人驻场

3）投标人具有与本项目相关的检索相关功能的软件著作权登记证书的，为优。

5.8、等级保护要求

本项目按照等保 2.0 第三级进行建设。

5.9、商业密码应用需求

本项目依据 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》第三级指标要求进行建设，建设完成后供应商需配合相关的密码测评工作，通过第三方密码应用测评。

5.10、技术文件要求

项目验收以用户书面确认的细化需求为依据，完成所有建设要求并通过不少于一个月试运行，期间产生的所有问题都已解决且用户满意。须提交与本项目开发相关的所有纸质文档和电子文档，包括最终版本需求规格说明书、源代码、数据字典、概要设计文档、详细设计文档、数据库设计文档、安装部署文档、用户手册、维护手册、测试报告等。

5.11、验收要求

1、完成应用系统开发部署；

2、完成硬件的购置与安装调试；

3、试运行时出现的问题已解决；

4、通过第三方软件测试、安全测评、密码应用测评；

5、系统稳定运行后，乙方申请后由用户方组织项目验收；

6、供应商需提供详细的相关技术文档、使用说明书、维护手册等文档资料（纸质、电子各一份）。

5.12、其它要求

1、供应商需根据上海市人民检察院设计规划要求进行功能细化等工作。

2、系统建设过程中需要配合监理方监督检查。

3、系统交付符合考核要求。