

# 常州市公安局交警支队车驾管业务综合监管音视频联网共享项目采购合同

甲方： 常州市公安局 签订地点： \_\_\_\_\_

乙方： 常州市同济科技有限公司 签订时间： 2023年    月    日

采购代理机构： 常州市政府采购中心

根据常州市政府采购中心 2023年3月13日进行的常采公[2023]0027号招标,甲、乙双方就乙方中标的 常州市公安局交警支队车驾管业务综合监管音视频联网共享项目,本着平等互利的原则,通过共同协商,根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及有关法律法规,就相关事宜达成如下合同。

## 一、总则

乙方按甲方要求,为甲方提供的常州市公安局交警支队车驾管业务综合监管音视频联网共享项目具体服务内容见下表(单位:元):

序号	项目		品牌	规格型号	配置参数	数量	单位	人民币价格(元)	
								单价	合价
1	准入控制系统	准入控制主机	奇安信	NAC-V3600-PA	标准机架式 2U 设备, 冗余电源; 本次配置 6 个千兆电口, 2 个万兆光接口; 整机吞吐量: 10Gbps; 主机支持 5000 客户端接入 部署方式: 支持设备集中管理, 可在同一管理平台集中管理所有设备, 支持设备分组, 权限管理, 实现分布式部署、集中管理, 满足大型网络环境下的部署要求。	1	套	145800	145800
		客户端授权(1000个)	奇安信	NAC-CLT	本次配置 1000 个终端授权(同时支持视频准入和 PC 终端准入)	1	套	50000	50000
		网络安全准入控制中心	奇安信	NAC-MGR	支持海康威视、大华、宇视、科达、天地伟业、华为、安巡视、罗普特、索尼、菲力尔、英飞拓、云天励飞、英迪高、汉邦高科、乔安科技、易视云、华迈等市场主流视频设备厂商 支持双操作系统冷备, 当常用系统出现	1	套	32800	32800

					<p>故障，可以使用备用系统恢复；</p> <p>支持 VLAN 隔离准入技术，实现无客户端下端口级准入控制；</p> <p>支持多种准入技术的复用，至少三种以上；</p> <p>支持基于 IP/MAC 地址黑 / 白名单准入；</p> <p>支持实时监测哑终端指纹信息的变化，当哑终端指纹信息变化时，可及时对其进行告警或阻断；</p> <p>支持数字证书认证方式，必须支持证书的本地管理和发放，实现证书签发、管理和操作；</p> <p>支持终端安装软件의 检查和软件运行情况的检查，提供白名单、黑名单、红名单管理方式；</p> <p>支持对终端访问/终端被访问的地址、服务及访问的进程进行管理，允许的进程、服务、地址才能进行访问支持终端安装软件의 检查和软件运行情况的检查，提供白名单、黑名单、红名单管理方式。</p>				
2	视频安全交换接入系统	接入认证服务器	天行网安	Topwalk-MTP9049	<p>2U；10/100/1000Mbps（电口）×4；万兆SFP+（光纤口）×2；2个USB；1个CONSOLE；2颗Intel Xeon E5-2667 v4；单颗核数：8核；单颗主频：3.2GHz，内存64G，硬盘空间2T；</p> <p>应用层数据传输率：7.2Gbps；</p> <p>图像传输性能线性：线性7500Mbps,1250路1080p图像传输能力（单路码流6Mbps）；</p> <p>图像码率支持20Mbps（单路）；</p> <p>并发数&gt;2000；</p> <p>功能1.支持海康、大华、宇视科技、科达、东方网力、华为等国内外视频监控厂商的信令控制协议；</p> <p>2.支持海能达、承联、普天、万格等指挥系统厂商的信令控制协议；</p> <p>3.支持协议扩展，通过修改协议模板即可实现新厂商接入；支持简单二次API</p>	1	台	186880	186880

				<p>接口函数的开发,实现新视频厂商平台的安全接入;</p> <p>4. 支持对网络摄像机、网络硬盘录像机、流媒体服务器等音视频设备基于IP、MAC和证书的接入认证;</p> <p>5. 支持对视频访问终端、用户基于用户名、口令和数字证书的接入认证;</p> <p>6. 不需要第三方负载均衡服务器,系统即可实现负载均衡功能;</p> <p>7. 支持标准 SIP 信令控制协议,支持GB/T28181-2011《安全防范视频监控联网系统信息传输、交换、控制技术要求》;</p> <p>8. 支持对信令流进行网络协议、内容关键字等进行安全过滤,防止数据夹带;</p> <p>9. 支持对视频源和访问终端进行主动管理控制,可按照访问时间、流量和优先级等分配访问策略;</p> <p>10. 支持对用户行为进行审计,包括正常登录,非法登录,非法请求,退出等。</p> <p>11. 能够在 IPV4 和 IPV6 协议环境下,对视频流进行丢帧、插帧处理;可对信令协议做 register、play 等关键字过滤</p>					
		用户认证服务器	天行网安	Topwalk-MTP9049	<p>2U标准机架式机箱,提供1颗处理器,单颗主频3.0GHz,单颗6核,4个千兆光口,2个万兆光口(含配置相关模块),双电源供电,专用安全加固Linux操作系统,内存64G,硬盘空间2T;</p> <p>应用层数据传输率:7.2Gbps;</p> <p>图像传输性能线性:线性7500Mbps,1250路1080p图像传输能力(单路码流6Mbps);</p> <p>图像码率支持20Mbps(单路);</p> <p>并发数&gt;2000;</p> <p>功能1.支持海康、大华、宇视科技、科达、东方网力、华为等国内外视频监控厂商的信令控制协议;</p> <p>2.支持海能达、承联、普天、万格等指挥系统厂商的信令控制协议;</p>	1	台	186880	186880

				<p>3. 支持协议扩展,通过修改协议模板即可实现新厂商接入;支持简单二次 API 接口函数的开发,实现新视频厂商平台的安全接入;</p> <p>4. 支持对网络摄像机、网络硬盘录像机、流媒体服务器等音视频设备基于 IP、MAC 和证书的接入认证;</p> <p>5. 支持对视频访问终端、用户基于用户名、口令和数字证书的接入认证;</p> <p>6. 不需要第三方负载均衡服务器,系统即可实现负载均衡功能;</p> <p>7. 支持标准 SIP 信令控制协议,支持 GB/T28181-2011 《安全防范视频监控联网系统信息传输、交换、控制技术要求》;</p> <p>8. 支持对信令流进行网络协议、内容关键字等进行安全过滤,防止数据夹带;</p> <p>9. 支持对视频源和访问终端进行主动管理控制,可按照访问时间、流量和优先级等分配访问策略;</p> <p>10. 支持对用户行为进行审计,包括正常登录,非法登录,非法请求,退出等。</p> <p>11. 能够在 IPV4 和 IPV6 协议环境下,对视频流进行丢帧、插帧处理;可对信令协议做 register、play 等关键字过滤</p>					
		视频隔离网闸	天行网安	Topwalk-TG9049	<p>2U 标准机架式设备,双电源供电,提供 1 颗处理器,单颗主频 3.0GHz,单颗核数 6 核,6 个 10/100/1000Mbps 电口,4 个万兆光口(含配置相关模块);</p> <p>内存 64G,硬盘空间 2T;</p> <p>应用吞吐量: 6Gbps</p> <p>系统并发连接数: 50000</p> <p>内部系统交换带宽: 10Gbps</p> <p>功能产品通过硬件实现安全隔离,彻底阻断 TCP/IP 协议以及其他网络协议,通过自定义的通讯机制进行数据的读写,实现可控的信息交换,隔离部件不可从外部编程控制</p> <p>不允许外部网络与内部网络的主机建</p>	1	台	199800	199800

					立会话; 支持 Web 方式或客户端的管理界面, 可以对设别进行集中管理, 管理数据的传输可进行加密保护。				
3	视频共享平台	视频综合管理平台	宇视	VS-VM9500	<p>2U标准架式CPU: 10核, 内存: 64GB, 硬盘: 500G, 网口: GE*1</p> <p>兼容性 支持国标、ONVIF标准前端的接入, 本项目支持3000路视频接入许可。视频监控管理平台需支持第三方告警设备的接入和联动功能。</p> <p>支持 1080P/720P/D1/4CIF/2CIF/CIF 等解码上墙, 支持 TCP/UDP 解码上墙, 支持 onvif/GB28181 解码上墙, 支持 H. 265/H. 264 格式解码。</p> <p>扩展性 支持 1 个电源扩展槽位, 可实现 1+1 冗余</p> <p>支持 1 个 RS232 口, 支持 1 个 RS232/RS485 复用口</p> <p>支持 4 个 USB 接口</p> <p>支持 1 个 HDMI 视频输出接口</p> <p>支持 1 个 VGA 视频输出接口</p> <p>管理维护功能 1. 支持可视域管理及动态可视域, 地图上标定摄像机后, 摄像机的监控范围可在地图上展示, 云台摄像机的摄像场景可随云台转动与地图上可视域的方向同步</p> <p>2. 可视域反向控制: 可以通过地图上可视域方位反向控制云台摄像机转动并定位到目标监控区域。</p> <p>3. 支持对摄像机进行快捷回放; 支持录像分段回放, 把某监控点视频录像自动平均分成若干段, 同时播放; 需支持录像分段下载, 可实时显示下载进度, 可暂停或取消下载; 需支持录像下载权限控制管理</p> <p>4. 可定制手动 workflow 预案动作, 需要实现该动作时, 在 workflow 预案列表中点击该预案的执行按钮, 即可实现。</p> <p>5. 可设置向指定用户发送文字、图片、摄像机实况链接的预案动作, 该动作可</p>	1	台	175000	175000

					<p>设置为按计划时间定时执行,也可设置为手动点击执行按钮来执行或报警联动执行。</p> <p>6. 可根据需要将客户端中所有的数据表导出,数据表的数据项目可按客户需求任意定制。</p> <p>7. 回放上墙功能:需支持回放上墙,可以快进、快退、暂停、拖动、播放进度条跳转、快放慢放等操作。</p> <p>8. 为了实现快速定位录像关键节点,可以将录像文件进行切分成多片,通过切片点的图像差异,迅速启动回放关键录像时段。</p>				
		流媒体转发服务器	宇视	VS-MS9500	<p>2U 标准机架式 CPU: 10 核, 内存: 32GB, 硬盘: 500G, 网口: GE*1</p> <p>转发能力 单台媒体服务器支持 1024 路或 1Gbps 输入,单台媒体服务器支持 2048 路或 2Gbps 输出</p> <p>兼容性 支持多种网络协议: TCP/IP、RTSP、UDP、HTTP、IGMP、Telnet、ICMP、ARP, SIP、SNMP、FTP、TFTP</p> <p>支持 GB28181、DB33 等联网标准</p> <p>扩展性 支持 1 个电源扩展槽位,可实现 1+1 冗余</p> <p>支持 1 个 RS232 口,支持 1 个 RS232/RS485 复用口</p> <p>支持 4 个 USB 接口</p> <p>支持 1 个 HDMI 视频输出接口</p> <p>支持 1 个 VGA 视频输出接口</p> <p>管理维护功能 支持音视频单播流的复制分发。</p> <p>支持音视频组播流转单播复制分发。</p> <p>支持对跨域媒体流进行复制分发。</p> <p>支持负载均衡和动态互备。</p> <p>单/组播抗丢包功能: UDP 网络下单播和组播支持抗 5%的丢包。</p> <p>支持 VPN 的部署方式。</p>	1	台	105830	105830
4	视频服务网关	视频服务网关	锐菲网络	YLIT-IASTW-2N256	<p>2U 机架式; 处理器: 10核CPU*2; 内存: 64G;</p> <p>硬盘: 480GB/SSD*2; 网络: 千兆网口</p>	2	台	143860	287720

				<p>*4;</p> <p>功能 支持“公安交通管理综合应用平台”的并行接入和监测；</p> <p>支持接入设备状态检测,设备基本信息查询,支持设备实时视频浏览、录像查询可以支持接入设备按平台编号、设备编号、设备名称、设备 IP、通道号、设备状态和接入方式等条件查询；</p> <p>支持浏览器无插件实时视频的浏览,包括多画面浏览实现选择 1、4、9、16 多种画面分割模式以及全屏显示,同时能提供多种分辨率的选择；</p> <p>支持多通道接入配置类型,提供跨边界和无边界接入方式以及稽查布控上传协议方式,具备集群负载均衡,能实现多台堆叠扩容,提供 UDP、TCP、KCP 等多种级联协议模式,支持公安网和专网级联配置；</p> <p>支持多级平台级联管理,实现新增下级网关管理,提供 UDP、TCP、KCP 等多种级联协议模式,支持公安网和专网级联配置,可以查看下级平台推送设备目录,并支持推送设备查询及目录检索；</p> <p>支持界面化动态配置网关接入及分发,对网关服务接口状态可视化展示。分布式子系统微服务运行状态可视化展示；</p> <p>支持国标增强协议,提供视频通信 QoS 服务；支持视频防抖动、视频画面恢复稳定视频通信、视频风暴抑制等,保障视频在边界网络通信中的稳定性；</p> <p>支持 CBR/VBR 两种码率控制方式,并支持高并发的视频访问能力,并且根据客户端的不同处理能力,自动探测网络状况和动态调整编码策略的机制和功能,瞬时动态调整视频的分辨率,满足用户需求的同时降低网络带宽的消耗；</p> <p>支持系统基本信息配置和服务配置,基于“双网双平台”架构,支持单网架构或双网架构模式,包括支持视频专网、公安网独立部署和同时部署,以适配不</p>				
--	--	--	--	--	--	--	--	--

					<p>同网络架构下的应用场景。支持时间同步及系统服务授权；</p> <p>系统联网 支持 GB/T 28181-2016 并兼容 GB/T 28181-2011 国标的视频接入、联网和转发，支持行业内所有监控厂商视频平台国标接入；</p> <p>支持符合 GB/T28181-2016 协议标准的视频共享联网平台直接级联接入；</p> <p>支持开放接口支持 SDK、OCX、JSX 多种模式视频播放控制服务，支持 RTSP、RTMP、RTP/RTCP 等格式；</p> <p>支持 H.264、H.265、SVAC 编码协议的视频解码播放；</p> <p>通信并发数：256 路；</p> <p>接入数量：监控联网平台：支持同时接入 20 个</p> <p>节点数量：双网双平台架构，两台视频服务网关组成 2 个节点</p> <p>媒体转发量：400Mbps*4；</p> <p>监控点位：90000 个；</p> <p>兼容性 支持接入“公安交通管理综合应用平台”和“公安交通集成指挥平台”，实现视频联网、状态监测、设备管理及网络管理等功能。</p>				
5	三层交换机	交换机	华为	S5736-S24T4XC	<p>交换容量12.8Tbps</p> <p>支持24个10/100/1000BASE-T以太网端口，4个万兆接口（满配光模块），支持可插拔双电源模块</p> <p>三层功能 支持静态路由、RIP v1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+；</p>	1	台	27890	27890
6	零信任接入控制系统	零信任接入控制系统	合众	HTAP-SDP-A10SHFWZW	<p>控制器、安全网关二合一设备，标准机架式机箱，冗余电源；千兆电口12；千兆光口（SFP插槽）4；万兆光口（SFP+插槽）4。内置2张国家密码局检测通过的国家商用密码卡。</p> <p>性能指标 最大SSL国密吞吐（Mbps）300；</p> <p>标准吞吐量(bps)1518字节4G；</p> <p>最大并发连接数180万；</p> <p>最大每秒新建连接数1.8万；</p> <p>最大并发用户数1000。</p>	1	套	308900	308900



				<p>1000 个终端授权</p> <p>功能：</p> <p>1、使用 SPA 单包认证机制，用户在未经 SDP 控制器 SPA 认证前完全隐身，对外无服务端口暴露，无法通过扫描工具探测。</p> <p>2、基于黑白名单构建地址围栏，为白名单用户提供在线分发种子接口，将黑名单用户自动封禁。</p> <p>3、支持本地创建账户体系或与第三方认证系统联动实现用户接入设备信任基线的安全认证，确保接入主体身份可信。</p> <p>4、支持自建 CA，支持用户使用国际/国密算法 USBKey 认证接入；</p> <p>5、支持自带本地动态令牌服务端，对于通过动态令牌登录的用户，无需额外采购令牌服务器。</p> <p>6、支持 SPA 预认证种子配置，支持自动生成或手动配置的方式单个或批量生成 SPA 预认证种子信息，并支持批量导出。</p> <p>7、支持加密算法套件选择 RSA_DES_CBC_SHA, RSA_RC4_MD5, RSA_RC4_SHA, RSA_WITH_AES_SHA；支持 SM2 (ECC)_SM4_SM3 , SM2 (ECDHE)_SM4_SM3；支持安全密钥更新周期设置；</p> <p>8、支持对访问行为持续、动态的检测，一旦发现不符合访问控制策略的行为变化，可动态回收访问授权、阻断访问等。</p> <p>9、支持针对不同 B/S 应用开启屏幕水印，支持隐式水印和显示水印两种技术，支持点阵式水印，水印内容包括：用户名+当前日期，有效预防数据泄露；</p> <p>10、支持双系统引导，可在管理员界面直接配置启动顺序，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且分别支持加密导入导出。</p>			
--	--	--	--	--	--	--	--

					兼容性 支持对接公安交通管理综合应用平台、社会化服务系统终端电脑用户安管管控设备。				
7	应用服务器	服务器	超聚变	2288H V5	外观2U标准机架式 配置2颗，每颗CPU核心数24核；256GB DDR4内存，2*1.2T SAS硬盘；2*GE+2*10GE网卡，1块16G双口HBA卡； 配置独立 RAID卡，2G Cache，配置RAID卡超级电容，支持 Raid0/1/5/6/10/50/60；配置2个2000W标准电源，支持1+1冗余 可管理性 服务器管理软件支持国产自研管理芯片	4	台	77500	310000
总价			2017500.00 元						

本合同金额为人民币大写：贰佰零壹万柒仟伍佰元整，小写： 2017500.00 元。

项目的具体服务要求见采购代理机构的招标文件。

## 二、合同文件

下列文件是构成合同不可分割的部分，并与本合同具有同等法律效力，这些文件包括但不限于：

- 1、常采公[2023]0027号招标文件。
- 2、乙方提交的投标文件。
- 3、乙方投标的其他资料及承诺。
- 4、评标记录。

## 三、质量保证

1、乙方所提供的服务必须符合国家有关标准和常采公[2023]0027号招标文件(含技术说明)和投标文件的要求。

2、乙方应提供所投软硬件产品五年原厂质保服务、硬盘不返还服务(自终验合格之日起)。于合同签订之日起10个日历日内提供五年原厂质保函。

3、乙方应保证货物是全新、未使用过的原厂商、原产地、原包装合格正品(含配件)，进口产品应保证通过正规合法渠道，需提供相关手续供验证。若甲方发现乙方所供产品为OEM(非原厂)产品或非全新产品，乙方向甲方予以该产品合同价双倍赔偿。

4、乙方应保证提供的所有软件产品为最新正式版本，承诺所有软件产品都具有在中国境内正式合法使用权，不得侵犯第三方专利权、商标权和工业设计权、版权等。否则，乙方应负全部责任，并承担由此引起的一切后果。

5、乙方提供的货物必须符合国家有关质量技术标准及相关法律、法规规定的要求，具有完整的技术资料、配件和介质。

6、乙方应保证其货物在正确安装、正常使用和保养条件下，在其使用寿命期内应具有满意的性能。货物最终验收后，乙方应对由于设计、工艺或材料的缺陷而发生的任何不足或故障负责，并承担由此引起的一切后果。

#### 四、服务时间

1、乙方须在不迟于合同签订后的 60 个日历日内完成所有招标设备到指定地点的供货。到货完成后 90 个日历日内完成软硬件部署、调试，并投入使用。

2、设备质保 5 年，质保期内按照合同要求进行设备维护。

#### 五、付款方式

序号	阶段	付款条件	付款期限	付款比例	备注
1	预付款	签订正式合同后	收到发票 15 日内	30%	
2	中间款	初验合格后	收到发票 15 日内	30%	
3	中间款	终验合格后	收到发票 15 日内	30%	
4	尾款	终验合格后每满一年，每年支付	收到发票 15 日内	2%	

#### 六、服务要求

乙方应根据甲方的需要，在规定的时间内，保证质量完成投标所提供设备的使用规划、安装、调试及投入运行。项目建设完成，包括软硬件环境搭建、安装部署、调试并验收合格。包括但不限于以下工作：

##### 1、音视频资源联网与共享服务要求

将检验、查验专网和科目二、科目三考试专网内的视频数据进行互联整合，通过视频边界交换平台系统对甲方车驾管业务视频资源统一接入整合，为部署在公安信息网的公安交通管理业务综合监管系统提供实时视频服务。基于公安部发布的《公共安

全视频监控联网系统信息传输、交换、控制技术要求》(GB/T28181-2016)标准,实现音视频资源联网与共享,在数据存储安全和网络安全方面加强专网安全防护建设。

乙方需要在项目实施前对现有公安网、查验检验专网和科目二、科目三考试专网等网络安全及边界平台现状进行充分调研,以满足部署和实施要求。

乙方应配合甲方梳理现有查验检验专网和科目二、科目三考试专网至公安网边界平台数据及视频业务,对现有及计划接入的前端种类、数量和采集数据量进行充分测算,科学配置边界设备各项策略和参数,对相关业务进行整体规划设计,做好边界平台的策略配置及业务迁移等相关工作,最大化发挥通道使用效能。

在市局机房专网与公安网边界部署1套万兆安全视频交换系统,包括视频接入认证服务器、视频用户认证服务器、视频安全隔离网闸、三层交换机和下一代防火墙(利旧)。

在车管所机房,在查验检验专网和科目二、科目三考试专网之间部署下一代防火墙(利旧),联通两个专网组成新的社会化服务专网;

在车管所机房,在查验检验专网部署视频共享平台和视频服务网关;

在车管所机房,在查验检验专网部署1台网络安全准入控制系统。

## **2、社会化服务专网安全防护服务要求**

加强社会化服务专网安全防护建设。

社会化服务专网部署零信任安全接入系统,对社会化服务专网接入的前端应用进行认证,确保社会化服务网络安全。

统一版社会化服务系统采用微服务架构设计研发,采用现有的软硬件平台进行部署,对于性能达不到要求的,应当根据实际情况,扩容软硬件支撑平台。数据库设计采用分库分表原则,分别创建系统管理、机动车登记和查验、机动车检验、驾驶证管理、驾驶人考试5个数据库实例或用户,数据库安装 Oracle 10g 及以上可以利旧使用现有数据库资源。微服务应用发布按照社会化服务系统要求利旧与扩容应用服务器资源,应用服务器为 Windows 操作系统的,应先将操作系统调整为 Linux 内核操作系统,划分虚拟机并提供足额的 CPU 及内存资源。本次项目在车管所机房,在查验检验专

网部署 4 台社会化服务专网专用服务器，扩容应用服务器，并按部里统一版社会化服务系统要求完成软件步骤。

### **3、供货要求**

(1) 乙方在不迟于合同签订后的 60 个日历日内完成所有招标设备到指定地点的供货。

(2) 乙方保证所提供产品的技术指标必须满足或优于招投标文件技术要求。项目进场后，中标设备的品牌、型号及技术参数须得到甲方确认后方可实施，安装施工安全、质量全面负责，并承担成品保护，如因乙方原因造成安全、质量事故或成品损坏，由乙方承担一切经济法律责任。

### **4、安装调试要求**

(1) 乙方在到货完成后 90 个日历日内完成软硬件部署、调试，并投入使用。

(2) 环境搭建及安装调试时所用的工具、设备由乙方负责，并保证不影响现有业务系统的正常运行。

### **5、售后服务及日常维护要求**

(1) 本项目产品质保期为 5 年，自项目验收合格之日起计算，在质保期内乙方包维修、保养、安检、调换等；对于甲方人为原因造成的故障，乙方只收取成本费用。

(2) 乙方每月对系统平台进行预防性检查维护，保障系统的稳定运行。

(3) 乙方进行技术交流和反馈，填写维护记录，并定期提供客户服务维护技术档案，以提高客户技术人员的日常维护水平和对问题的解决能力。

(4) 乙方提供系统升级和补丁程序安装支持服务。

(5) 乙方结合应用软件，每季度实施一次系统健康状况检查和优化调整。

(6) 乙方每季度提供一次技术交流和评估。

(7) 乙方提供 7\*24 小时电话、远程响应，在系统发生故障时 20 分钟内作出响应，远程支持难以满足要求时，相关技术人员能够在 1 小时内赶到现场，一般问题 2 小时内解决，疑难问题 24 小时内处理完毕，重大疑难问题 3 日内完全解决，保证及时恢复系统运行。

(8) 乙方针对本项目所投产品应提供完整的运维方案。定期对所投设备进行巡检并提供巡检报告，发现故障或接到甲方保障通知后，应按照故障处理要求迅速进行处置。

## 6、自动化网络监控运维方案

根据甲方的生产环境实际要求，乙方部署自动化监控平台，提供全面、及时、高质量的信息化业务保障服务，通过该项目形成自动化、平台化的一体化运维服务管理。乙方按要求提供网络运行自动监控系统功能，其具体技术要求如下：

- (1) 实时显示甲方真实网络拓扑图；
- (2) 实时显示网络及安全设备的运行状态；
- (3) 实时显示设备间链路流量信息；
- (4) 实时显示甲方内部网络专线的链路状态及流量信息；
- (5) 实时显示监控的网络及安全设备告警信息，告警信息在网络拓扑图上实际位置突出显示；
- (6) 实时显示链路流量超过规定阈值时，告警信息在网络拓扑图上实际位置突出显示；
- (7) 实时监控 ping 不通的告警信息，告警信息在网络拓扑图上实际位置突出显示。

## 7、人员配备

(1) 乙方须成立项目实施团队，实施团队成员必须专职此项目服务，未经许可不得兼职或与其它项目复用。在项目启动后，如果需要更换实施团队人员，需征得甲方同意。乙方提供的项目实施团队中应安排原厂工程师进场进行所有软硬件设备部署工作，乙方必须积极主动与本项目的相关单位合作，并服从甲方的协调。

(2) 本项目需拟派项目团队成员不低于 5 名，包括项目负责人 1 名，项目成员不低于 4 名。本项目对信息安全有相应的要求，项目团队中的成员需要在服务实施过程中具备信息安全意识，并具备一定的信息安全能力水平。

项目经理 1 名：掌握项目管理理论，熟悉大型建设工程项目的流程、项目管理方法等；具有系统集成数据中心项目管理经验，至少具有独立完成 2 个以上综合性工程

项目工作经历；对项目整体的进度、质量负责；了解项目范围及需求，负责项目交付计划和技术方案的制定，管理和监控计划和技术方案的实施交付；

服务器实施工程师 1 名：具有 2 年以上相关工作经验；熟悉服务器操作系统（windows、liunx）安装部署，熟悉服务器多网卡网络配置，熟悉服务器多路径挂载存储配置，熟悉 KVM、vmware 等虚拟化系统部署，具有服务器操作系统、数据库及虚拟化系统运维及故障排查能力。

网络实施工程师 1 名：2 年以上网络构架工程交付经验，熟悉网络技术原理、精通 IP 网络，负责车管所社会化服务专网网络解决规划、设计及部署工作；

网络安全实施工程师 2 名：2 年以上网络安全工程交付经验，了解工程项目交付流程和技术管理方法等；熟悉车管所社会化服务专网安全整体架构及设计，负责网络安全设备解决规划、设计及部署工作。

## 8、培训要求

乙方提供不低于 2 次科学合理的培训计划及课程安排。2 次培训分别安排在项目交付完毕后和项目整体验收完成后，以保证车管所负责本次项目的相关人员能够对综合监管系统的技术实现原理和业务数据流向熟悉了解，并且能够独立完成综合监管系统的日常业务操作。

## 9、安全保密要求

(1) 乙方须与甲方签订安全保密协议，落实公安网络安全及信息保密的各项规定。

(2) 乙方应做好文档资料（含电子文档资料）的管理工作，不得向第三方透露涉及本项目线路、机房、点位、业务等内容。

(3) 未经甲方允许，乙方向第三方提供（直接、间接、口头或书面等形式）涉及保密内容的行为均属泄密，将追究乙方责任。

(4) 乙方不得有其他任何危害公安信息安全的行为。

(5) 公安业务系统数据属于公安秘密，乙方应当严格遵守相关规定，严禁泄漏公安秘密，未经甲方确认，乙方公司人员不得对甲方业务系统作任何操作，参与本项目人员必须做到以下几点：

只在规定的区域实行规定的工作，不得进入与之无关的工作区域；

不得在机房设备上建立与工作无关的网站、网页和服务；不得在设备中传输、粘贴有害信息或与工作无关的信息；

不得擅自对设备进行扫描、探测和入侵信息系统；

不得对工作信息和资源越权访问、违规使用；

不得私自允许他人接触和使用机房设备；

严禁将工作用设备和文件带离机房；

未经机房管理部门同意，严禁以任何方式和介质拷贝服务器上的任何信息及项目中涉及的信息；

对工作中接触到的信息做到保密。

其他须遵守的相关规定。

#### **10、网络安全责任**

合同有效期内，由乙方服务不到位造成的安全事件由乙方承担安全责任。

合同履行期间，乙方应为其产品和服务提供网络安全和数据安全服务保障，并根据国家相关法律、法规和行业标准规范履行相应的网络安全和数据安全保护义务，因乙方原因造成的网络、数据安全风险（含发生安全案事件），乙方须立即无条件整改并承担相应的法律责任。

合同履行期满后，乙方应配合甲方做好排除网络、数据安全隐患工作，如因乙方原因或未尽合理义务造成网络、数据安全风险（含发生安全案事件），不免除乙方相应的法律责任。国家法律、法规对甲、乙双方应承担的法律责任另有规定的，从其规定。

#### **七、违约责任**

1、如果甲方延期付款或者未尽配合义务，乙方不承担由此引起的项目建设工作的损失与责任，工期顺延；

2、乙方逾期交货，应向甲方支付违约金，迟延履行违约金以合同总额每日万分之八计算。逾期履行超过十天，应当以合同总额5%向甲方支付违约金，甲方有权解除合同的约定内容。违约方支付违约金后，甲方仍有权要求继续履行合同。



3、因乙方原因延误工期，乙方每延误 1 天按照合同总价的万分之八向甲方补偿延误费；

4、提供的部件不符合招标文件的技术要求，必须按要求进行修复、拆除或重新采购；若乙方拒不按要求更正的，将对乙方处以不低于 5 倍的罚款（按不合格部件价值计算），且乙方应承担由此发生的一切费用，延误的工期不予顺延。

5、保修期内乙方如果不能在合同规定的时间内作出反应和修复故障，每超出 1 天最高按合同总价的万分之五计算违约金。

## **八、不可抗力**

1、在执行合同期限内，任何一方因不可抗力事件造成不能履行合同时，应在不可抗力影响消失后 10 个工作日内通知对方，并寄送有关权威机构出具的证明，则合同履行期可延长，延长期与不可抗力影响期相同。出现上述情况甲乙双方不承担合同有关逾期违约责任。

2、不可抗力影响时间持续 30 日以上时，甲乙双方均可以单方面解除合同，并书面通知对方。

3、本条所述“不可抗力”是指不可预见、不能克服及不能避免的事件，包括战争、严重火灾、洪水、地震等。

## **九、合同纠纷处理**

1、凡涉及本合同或因执行本合同而发生的一切争执，应通过协商解决。

2、如果协商不能解决，则双方均应提交常州仲裁委员会进行仲裁。该仲裁是终局的，对双方均有约束力。

3、争议在处理过程中，除正在进行仲裁或诉讼的部分外，合同的其他部分将继续执行。

## **十、其他**

1、如需修改或补充合同内容，应经甲、乙和集中采购机构三方协商一致，共同签署书面修改或补充协议。该协议将作为本合同不可分割的一部分。

2、除甲方、集中采购机构事先书面同意外，乙方不得转让任何其应履行的合同义务。

3、乙方应遵守甲方有关保密规定，并签订保密协议，不得在未经甲方同意的前提下，透露技术图纸资料等相关信息。

4、本合同未尽事宜，按中华人民共和国现行有关法律法规执行。

#### **十一、合同生效**

本合同经双方盖章签字后生效，如有变动，必须经双方协商一致后，方可更改。  
本合同一式肆份，甲方贰份，乙方壹份，采购代理机构壹份。

其他未尽事宜，参照相关法律，双方协商解决。

(以下无正文 为签字盖章页)

甲方:

单位名称 (章): 常州市公安局

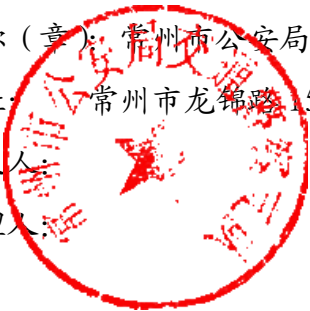
单位地址: 常州市龙锦路1588号

法定代表人:

委托代理人:

经办人:

日期:



乙方:

单位名称 (章): 常州市同济科技有限公司

单位地址: 常州市天宁区劳动西路11号3幢201室

法定代表人:

委托代理人:

经办人: 电话: 0519-86697390

开户银行: 华夏银行股份有限公司常州分行营业部

银行帐号: 1315 0000 0006 50120

日期:



# 常州市公安局交警支队车驾管业务综合监管音视频联网共享项目

## 安全保密协议

为确保信息安全保密，坚决杜绝失、泄密和安全隐患，切实执行《中华人民共和国国家安全法》和公安相关规定，我公司就参加“常州市公安局交警支队车驾管业务综合监管音视频联网共享项目”涉及的安全保密事项承诺如下：

1、在本次招投标过程中获得的相关信息坚决不向第三方传播，本项目招标文件仅用于本次招投标使用，不会用作本项目以外的任何用途；

2、加强对所有参与投标人员进行安全保密教育，开展必要的安全管理和技术管控，确保参与投标人员遵守安全保密纪律和工作纪律；

3、对本次招投标过程中涉及的文档、方案、存储介质等，我公司将落实专人负责统一保管，不向任何无关人员和单位泄漏；

4、凡属于我公司引起的失泄密事件，我公司将承担一切法律责任，接受相关规定和经济的处罚。

特具此承诺书，以资严格遵守。

乙方法人代表或负责人签名：



乙方（加盖公章）：



日期： 年 月 日