合同编号：JSCZE2502679CGN00

交警支队交通管理综合应用平台社会化服务系统升级改造建设项目采购合同

甲方：常州市公安局　　签订地点：常州

乙方：中电鸿信信息科技有限公司　　签订时间：2025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2025年3月27日进行的JSZC-320400-JZCG-G2024-0551号招标，甲、乙双方就乙方中标的交警支队交通管理综合应用平台社会化服务系统升级改造建设项目，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，为甲方提供的交警支队交通管理综合应用平台社会化服务系统升级改造建设项目具体服务内容见下表（单位：元）：

序号	产品名称			品牌	规格型号	技术参数	产地	单位	数量	单价	总价
1	国产化云平台	9节点国产化超融合系统	超融合系统软件平台	H3C	UIS Manager标准版	配置国产化超融合平台软件，同时配置本次项目建设所需授权：包含18颗CPU管理平台标准版授权、18颗CPU计算虚拟化软件授权、18颗CPU存储虚拟化软件授权，同时配置18颗物理CPU云主机深度安全防护系统功能授权（包含主机防病毒、防火墙、虚拟补丁功能）。 软件功能-管理平台(UIS Manager标准版)： 1.超融合管理平台即可实现对计算、存储、网络等资源进行统一管理，所有功能无需界面跳转即可实现全部操作，真正融合、简化管理。 2.支持一键切换展示大屏功能，直观展示虚拟化资源池的	杭州	套	1	250799	250799

						健康度、告警、资源使用情况等。 3.支持一键健康巡检功能，用于快速查看超融合管理平台健康情况。 4.支持一键分析后端存储上的无效镜像和文件，并提供一键清理和释放存储空间能力，提升资源利用率。要求提供 CNAS 认可的检测机构出具的检测报告作为证明材料。 5.支持一键快速查看、启动、删除、批量启动和批量删除长时间未使用且处于关闭状态的虚拟机，进行资源利用率统计，降低运维工作量与难度，保障投资。要求提供 CNAS 认可的检测机构出具的检测报告作为证明材料。 6.管理平台支持纳管 VMware。 7.支持对硬件平台进行监控，包括电源，风扇，温感，CPU、内存、硬盘等。 8.支持对整个平台虚拟设备实现统一的管理，虚拟化 WEB 管理平台可以完成网络拓扑的构建，完成各类虚拟设备的自助逻辑编排，支持在管理平台上连接、开启、关闭各类虚拟设备，拓扑呈现业务流量信息，方便运维管理。 9.超融合管理平台内置在线 p2v、v2v 迁移工具，支持业界主流的操作系统、公有云平台、虚拟化平台。包括但不限于 VMware、华为、Hyper-V 等平台的迁移功能。 软件功能-计算虚拟化(UIS CAS)： 1.在管理平台管理界面上提供虚拟机启动、暂停、恢复、重启、关闭、迁移、删除、快照等功能的批量操作.具有合理的内存调度机制，能够实现内					

						存的复用，保证内存资源的充分利用。 2.支持集群动态资源调度功能，可基于主机的CPU利用率、内存利用率、磁盘I/O、存储利用率、磁盘请求、网络流量等资源对虚拟机进行动态资源调度，实现自动化的存储资源分配和负载均衡功能，主动确保云环境的服务水平 3.支持批量修改虚拟机的配置参数，包括：I/O优先级、启动优先级、是否自动迁移、CPU调度优先级、CPU个数、内存大小、自动启动、VM启动设备、tools自动升级等；支持虚拟机桌面预览功能，降低配置工作量及运维难度。 4.虚拟化软件内置备份模块，可实现虚拟机全量、增量、差异备份功能，备份时对业务运行无影响，支持按时间（按分钟、按天、按周、按月）设置自动化备份策略。 软件功能-存储虚拟化(UIS ONEStor)： 1.采用分布式的软件定义存储架构，将所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点，使用超融合管理平台统一管理。 2.同一节点同时支持虚拟化和3种存储功能，最少只需3个节点集群即可同时提供虚拟化、分布式块、对象、文件存储服务。 3.支持纠删码特性，通过数据校验方式实现数据的高可靠性。支持多副本保护机制，支持依据业务数据重要性进行灵活设置副本数量机制。 4.为保障在数据重构过程中不造成对业务的影响，软件需支					

						持数据重构 QOS 设置，可以根据业务压力自动调整重构速率。 软件功能-虚拟化安全（DeepSecurity AV+DPI，包含主机防病毒、防火墙、虚拟补丁功能）： 1.支持主流 Windows、Linux、国产操作系统虚拟机无代理底层防病毒能力，包括 Windows、RedHat、CentOS、SUSE、Ubuntu、统信、银河麒麟等，不需要在虚拟机或虚拟桌面中部署安全防护代理，对虚拟机数量无限制。 2.支持无代理底层网络数据包检测，可以同时保护虚拟机操作系统以及服务应用，提供虚拟补丁功能，在已知漏洞修复之前，提供对漏洞攻击的防护能力，屏蔽漏洞以免遭受无限制的入侵。 3.支持虚拟化内核集成安全防护功能，功能模块为虚拟机提供防火墙防护能力，安全防护功能模块只需在虚拟化环境底层安装，不需要在每台虚拟机上安装。					
			重载业务超融合服务器	H3C	UIS 3060 G5	1.CPU：2 颗国产化 X86 架构(HYGON 7390)，每颗 CPU 核数 32 核，主频 2.7GHz，CPU 三级缓存 64MB，线程数 64 线程。 2.主板：32 个内存插槽，至少支持 SATA、SAS、M.2、NVME 等存储接口中的 1 种，PCIe 插槽或接口 6 个,符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe 的接口速率与位宽需保证向下兼容。 3.内存：1024G 3200MHz DDR4，支持多个内存接口通道。 4.硬盘：支持 16 个热插拔硬盘槽位,2*480GB SSD，12*960GB SSD。	杭州	台	3	136739	410217

						5.RAID 卡：2 端口 SAS RAID 卡（2G 缓存），RAID 卡支持的 SAS 接口数 8。 6.网卡：万兆光接口 6 个、GE 接口 4 个，满配光模块。 7.显示接口：显示接口类型应不少于 1 种，如： VGA、DP、HDMI 等。 8.USB 接口：配备 USB 接口，如 USB2.0、USB3.0 等。 9.电源：电源模块数 2，功率 1600W，电源冗余配置，电源能耗符合 GB/T 9813.3 的有关规定。 10.服务器支持智能温度监控，具备支持以图形化形式展示各组件温度传感器的分布图，可直观体现服务器整体温感状态，如发生温度告警可快速定位到具体区域。					
			普通业务超融合服务器	H3C	UIS 3060 G5	1.CPU： 2 颗国产化 X86 架构(HYGON 7390)，每颗 CPU 核数 32 核，主频 2.7GHz，CPU 三级缓存 64MB，线程数 64 线程。 2.主板： 32 个内存插槽，至少支持 SATA、SAS、M.2、NVME 等存储接口中的 1 种，PCIe 插槽或接口 6 个,符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe 的接口速率与位宽需保证向下兼容。 3.内存：256G 3200MHz DDR4，支持多个内存接口通道。 4.硬盘：支持 16 个热插拔硬盘槽位,2*480GB SSD，1*1.92TB NVMe SSD，6*8T SATA HDD。 5.RAID 卡：2 端口 SAS RAID 卡（2G 缓存），RAID 卡支持的 SAS 接口数 8。 6.网卡：万兆光接口 6 个、GE 接口 4 个，满配光模块。 7.显示接口：显示接口类型应不少于 1 种，如： VGA、DP、HDMI 等。	杭州	台	6	125660	753960

						8.USB 接口：配备 USB 接口，如 USB2.0、USB3.0 等。 9.电源：电源模块数 2，功率 1600W，电源冗余配置，电源能耗符合 GB/T 9813.3 的有关规定。 10.服务器支持智能温度监控，具备支持以图形化形式展示各组件温度传感器的分布图，可直观体现服务器整体温感状态，如发生温度告警可快速定位到具体区域。					
			24 口万兆交换机	H3C	S6520X-30QC-EI	交换容量 2.56Tbps，包转发率 720Mpps，24 个万兆光口，2 个 40G 光口，扩展插槽 2，双电源，双风扇（包含 10 个万兆多模光模块，一根 40G 3m 堆叠线缆）	杭州	台	6	33628	201768
			24 口千兆电口交换机	H3C	S5130S-28S-EI	交换容量 672Gbps，包转发率 171Mpps； 24 个千兆电口，4 个万兆光口（包含 1 根万兆 3m 堆叠线缆）。	杭州	台	2	7628	15256
2		文件存储服务器	文件、备份存储	H3C	R4930G5	硬件配置要求： 1.CPU：2 颗国产化 X86 架构(HYGON 7360)，每颗 CPU 核数 24 核，主频 2.2GHz。 2.内存：256G 3200MHz DDR4。 3.硬盘：2*960G SSD，4*8T SATA HDD 7200 转。 4.RAID 卡:2GB 缓存 RAID 卡 配置超级电容保护 支持 RAID0/1/5/6。 5.网卡：万兆光接口 2 个、GE 接口 4 个，满配光模块。 6.电源：1600W 电源冗余配置。	杭州	台	2	81430	162860
3		网络改造	核心交换机	华为	CloudEngine S8700-4	硬件配置要求： 1.交换容量 68.2Tbps，包转发率 51200Mpps；双主控； 2.48 个万兆 SFP+（满配光模块）； 3.48 个 10/100/1000BASE-T 以太网端口；	深圳	台	2	102000	204000

						4.电源槽位6、双电源1+1冗余备份，满配风扇； 5.业务板槽位4； 功能要求：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					
			万兆汇聚接入交换机	华为	CloudEngine S6730-S24X6Q	硬件配置要求： 1.交换容量2.56Tbps，包转发率1260Mpps， 2.24个万兆网络光口（满配光模块） 3.双电源 功能要求： 1.支持静态路由、RIP v1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+； 2. 其中两台设备用于切片云存储服务器组网。	深圳	台	4	34000	136000
			千兆接入交换机	华为	CloudEngine S5735-S24T8J4XEZ-V2	硬件配置要求： 1.交换容量672Gbps,包转发率321Mpps； 2.24个10/100/1000BASE-T以太网端口， 3.4个万兆接口（满配光模块）， 4.双电源 功能要求：支持RIP、RIPng、OSPF、OSPFv3路由协议	深圳	台	2	7650	15300
			汇聚交换机	华为	CloudEngine S5731-S32ST4X	硬件配置要求： 1.交换容量1.36Tbps，包转发率420Mpps， 2.8个10/100/1000BASE-T以太网端口， 3.24个千兆SFP(满配光模块)， 4.4个万兆SFP+(满配光模块)， 5.双电源 功能要求：支持静态路由、RIP v1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+；	深圳	台	2	16065	32130
4	自	音	音视频	华	音	（一）软件：	无	套	1	221000	221000

	建系统	视频切片存储管理系统	切片系统	通	视频联网管理模块&音视频切片模块	建设部署音视频切片系统，依托已建的车驾管音视频共享管理平台、机动车检验和驾驶人考试等业务平台，通过对机动车检验项目和驾驶人考试视频进行切片指令发送与管理，实现对切片视频与业务流水的精准关联，支撑业务抽查/回放、异常处置等环节。 （二）功能模块： 1.服务器状态预警 可图形化展示服务器状态信息，包括CPU、内存、网络等信息。 2.音视频切片模块 1）提供音视频切片管理接口，对接社会化服务系统，接收社会化服务系统的切片指令后，自动拉取音视频共享平台视频流进行切片，按业务流水主键存储，开展切片视频统一存储管理，并将视频切片结果地址信息上传至社会化服务系统。 3.切片视频统一存储 1）支持切片视频实时存储，对音视频共享平台的视频流实时转化成视频切片文件存储，提供切片存储的周期性管理，支持对不同场景业务类型的视频自定义配置存储时长和切片视频是否压缩。 2）支持切片视频配置冷热存储策略，冷热数据可配置不同的存储位置、压缩策略，可配置冷热数据转换条件。 3）支持切片视频防篡改，对电子数据完整性校验，当人为篡改数据库信息时，实现业务数据的锁定。 4.切片视频质量检测 1）支持对切片视频质量检测，及时发现丢帧卡顿、视频无法播放、播放无画面、视频无法解析、录像未完成、黑屏花屏	锡				

						等问题。 2）支持配置视频抽检策略，形成统计报表，并提供异常视频查看功能。 5.切片视频调阅 1）支持切片视频文件的在线播放和下载，可根据业务流水号、摄像机编号、业务办理时间等条件查询对应视频并播放，同时支持查看切片视频的参数和关联的业务信息。 2）支持对任意视频切片抓拍并保存，实现将任一帧抓拍的图像保存成 JPEG 或 BMP 的格式。 6.加密认证 1）提供安全的加密认证服务，支持对切片文件点播 URL 进行权限认证和时效认证。 2）提供安全传输服务，加密信息里包含切片的基本点位信息和业务流水信息等，防止电子图片、视频片段在传输、存储和校对过程中被非法篡改。 音视频共享平台服务对接 与现有音视频共享平台进行开发对接，按照摄像机国标编码进行统一管理，接收到社会化服务系统切片指令后，对业务音视频进行切片存储管理，支撑社会化服务系统通过摄像机编号、业务时间及业务属性等进行视频检索和下载。 社会化专网系统对接 对接社会化服务系统，实现切片视频与业务流水的精准关联，提供视频点播/回放、摄像机状态监测、视频切片管理等服务支持，并将视频切片结果按照规范化要求上传至社会化服务系统。支持社会化服务系统的实现切片视频调阅、视频监控资源运行监测等管理功能，满足音业务抽查、业务回访、预警信息调查处理、异常					

						业务分析等监管需求。					
5			视频切片云存储	新希望	XXWKI-FBSCC-36	硬件配置要求： 1.机箱：4U机架式，36盘位高密度配置； 2.CPU：国产化CPU 2颗，每颗CPU核数 24核，主频2.6GHz； 3.内存：128GB； 4.硬盘：系统盘 2*480G/SSD，数据盘裸容量576TB 5.电源：1+1冗余电源； 6.网络：4个万兆网口（含光模块）； 7.音视频处理卡：算力32TFLOPS@FP16；32路1920*1080 30fps的H.264/H.265解码；16路1920*1080 30fps的H.264/H.265编码。 功能要求： 1.FastDFS对接：支持对接公安交通管理综合应用平台社会化服务系统专用存储FastDFS接口F协议； 2.安全认证：提供身份验证的安全认证模式，如用户名、密钥、终端访问IP等； 3.存储租户：管理存储租户，可以自定义设置租户存储空间容量、访问IP地址，未授权IP地址范围内的文件无法上传至对应租户；可以在线扩大和缩小租户存储空间； 4.接入协议：选择存储协议类型，包括Amazon S3简单对象存储协议、POSIX可移植操作系统接口协议、HTTP超文本传输协议等	苏州	台	3	195500	586500
6		时钟同步系统	时钟同步服务器	北斗时源	S2000-1U-GBK	硬件配置要求：1U机架式，时间来源：北斗卫星，单北斗模式，NTP请求量25000次/秒，千兆网口7。 功能要求：授时服务器支持接收准确的北斗卫星数据，提供基于NTP/SNTP协议的网络授时	北京	台	2	30090	60180

						服务；通过授时服务器组成的时间同步系统可以为网络内的所有设备和系统提供精确、稳定且安全的时钟基准。					
7	统一版社会化服务系统运行安全	数据存储安全	数据库加固系统	合众	BOS-H3000-TCS-H-6401	硬件配置要求： 1.2U 标准机架式机箱，冗余电源，采用通过信息安全测评中心安全可靠测评的国产 CPU 和国产操作系统；接口 8 个 10M/100M/1000M 自适应电口、4 个 SFP 插槽、2 个 SFP+插槽、1 个万兆扩展卡插槽、1 个 Console 口和 2 个 USB 口。含 mSata64G，含机械硬盘 2T 性能要求：1.应用检控通量≥4Gbps； 2.应用检控并发连接数≥30000RPS； 3.数据检控通量≥4Gbps； 4.时延<10ms； 5.稳定性运行时间(MTBF)：>50000 小时； 6.SM4 算法加解密速度≥350Mbps； 功能要求：1.具备应用访问流量加密功能，内置 PCIE 国密卡支持通过 SSL 协议对业务流量加密传输，能兼容支持国密算法和国际算法； 2.具备基础的证书颁发与双向证书认证功能，支持颁发基于 PEM 编码的 SSL 公钥客户端与服务端证书； 3.具备用户令牌、应用令牌检查能力，支持与零信任控制设备服务联动验证用户令牌与应用令牌； 4.具备应用访问内容检控能力，支持对应用请求头、请求方式以及请求有效期做多维度检查与访问控制；支持基于请求方式、请求内容大小、请求速度、请求连接数和访问时段等做流量控制；	杭州	套	1	185300	185300

						5.要求具备基于敏感信息库的应用请求内容安全检控能力，可根据需要配置报警或阻断，内置敏感信息库并支持自定义敏感库关键字； 6.要求具备数据库协议检控能力,可兼容Oracle、SQL Server、MySQL 等主流数据库同步协议；要求具备数据库同步内容检控能力，可针对 Oracle、SQL Server、MySQL 等主流数据库同步内容安全检控； 7.要求具备详细的应用访问检控审计机制，可详细记录应用访问操作时间、服务名、访问用户、访问 IP、上下行流量、访问URI 以及与请求响应状态； 8.要求具备详细数据交换检控审计机制，可以详细的记录服务名、客户端 IP、数据大小、操作行为、SQL 执行结果等信息； 9.要求具备应用与数据检控态势展示功能，能够以可视化图表等方式直观展示当前检控对象的资源数量、服务数量、当日数据流量、策略拦截数量、数据流量、服务排名、最近告警事件以及系统负载情况； 10.要求产品满足高可用性支持双机热备和负载均衡功能； 11.支持数据监控功能，支持信息库管理、自定义敏感信息，对敏感数据进行检查，根据策略配置进行阻断或者放行并产生报警日志。 12.产品能够无缝对接“公安交通管理综合应用平台社会化服务系统”，开展数据库安全管理。					
8			备份软件（40T授权）	鼎甲	DBackup V8.	授权要求：备份软件提供 40 TB 容量授权 功能要求：1.支持文件合成备份。	广州	台	1	168300	168300

					0	2.支持国产主流的数据备份恢复，包括但不限于达梦（DM）、人大金仓（Kingbase）、南大通用（GBase）、Vastbase（海量）等国产数据库。 3.支持Oracle、DB2、MySQL等主流数据库的逻辑备份和物理备份，其中物理备份可以实现完全备份、增量备份、日志备份、连续日志备份，实现任意时间点的恢复，实现数据库变化数据秒级以内的备份保护。 4.支持VMware、Hyper-V、Xenserver、Xen、KVM、FusionSphere、H3C CAS、OpenStack、Cware、HCS等虚拟机的无代理备份恢复。 5.重复数据删除：支持固定块、变长块的数据重删技术。 6.提供智能报表功能。 7.投标产品支持IPv6的网络配置，支持对IPv6网络中的客户端资源进行备份和恢复。 8.提供对生产系统数据资源的保护设置。资源标记为受保护对象后，不可对受保护资源进行恢复操作。					
9		服务器安全	交换通道防火墙	天融信	NGFW4000-UF(FT-A200)(万兆)V3	硬件配置要求：1.CPU：国产化CPU(主频2.6GHz，每颗CPU核心数4核) 2.操作系统：国产化操作系统 3.内存64GB， 4.硬盘256G SSD固态盘 5.2U机架式，1个管理口、1个HA口、8个千兆电口、8个千兆光口（满配千兆多模模块）、8个万兆光口（满配万兆多模模块），冗余电源 6.整机性能不低于以下要求： 整机网络层吞吐量（双向）：IPv4：197399.219Mbps，IPv6：197399.200Mbps 整机应用层吞吐量（单向）：IPv4：23151.667 Mbps，IPv6：	北京	台	1	172550	172550

						23077.000 Mbps。 功能要求：1.提供包括但不限于入侵防御等功能模块。 2.支持路由、交换、虚拟线、Listening、混合工作模式； 3.支持 IP/MAC 绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作； 4.支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由； 5.访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址 6.支持多种地址转换，支持源/目的 NAT、双向 NAT、NoNAT 转换方式;支持源 IP 转换同一性；支持端口块地址转换和 EIM 地址转换。 7.整机 TCP 新建： IPv4：269.989 万/秒，IPv6：269.994 万/秒。 8.支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP REQUEST FLOOD、NTP REPLY FLOOD 攻击防护。					
10			数据域防火墙	天融信	NGFW4000-UF(FT-A200)(万兆)V3	硬件配置要求：1.CPU：国产化 CPU(主频 2.6GHz，每颗 CPU 核心数 4 核) 2.操作系统：国产化操作系统 3.内存 64GB， 4.硬盘 256G SSD 固态盘 5.2U 机架式，1 个管理口、1 个 HA 口、8 个千兆电口、8 个千兆光口（满配千兆多模模块）、8 个万兆光口（满配万兆多模模块），冗余电源 6.整机性能不低于以下要求：	北京	台	2	172550	345100

						整机网络层吞吐量（双向）：IPv4：197399.219Mbps，IPv6：197399.200Mbps 整机应用层吞吐量（单向）：IPv4：23151.667 Mbps，IPv6：23077.000 Mbps。 功能要求：1.提供包括但不限于入侵防御等功能模块。 2.支持路由、交换、虚拟线、Listening、混合工作模式； 3.支持 IP/MAC 绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作； 4.支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由； 5.访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址 6.支持多种地址转换，支持源/目的 NAT、双向 NAT、NoNAT 转换方式;支持源 IP 转换同一性;支持端口块地址转换和 EIM 地址转换。 7.支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP REQUEST FLOOD、NTP REPLY FLOOD 攻击防护。					
11			堡垒机	天融信	Top SAG（FT-B20）	硬件配置要求：1.CPU：国产化 CPU（主频 1.5GHz，每颗 CPU 核心数 4 核） 2.操作系统：国产化操作系统 3.内存 64GB 4.硬盘 1TB 5.1 个 console 口、2 个 USB 口、6 个千兆电口、4 个千兆光口、2 个扩展槽位，冗余电源 6.授权数：150 个主机/设备许	北京	台	1	83300	83300

						可，用户数不限制（5年保） 功能要求：1.支持中标麒麟、银河麒麟、Windows等操作系统基于B/S的访问与管理，支持网络设备、安全设备、数据库等的资产管理； 2.支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出； 3.支持数字证书等方式进行双因子认证。支持国产化操作系统的客户端采用数字证书双因子认证； 4.支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权。 5.支持权限审批功能，运维人员可根据工作需求临时申请设备运维工单，由管理员审批后可直接运维，过期失效。					
12		网络安全	边界防火墙	天融信	NGFW4000-UF(FT-A200)(万兆)V3	硬件配置要求：1.CPU：国产化CPU(主频2.6GHz，每颗CPU核心数4核) 2.操作系统：国产化操作系统 3.内存64GB， 4.硬盘256G SSD固态盘 5.2U机架式，1个管理口、1个HA口、8个千兆电口、8个千兆光口（满配千兆多模模块）、8个万兆光口（满配万兆多模模块），冗余电源 6.整机性能不低于以下要求： 整机网络层吞吐量（双向）：IPv4：197399.219Mbps，IPv6：197399.200Mbps； 整机应用层吞吐量（单向）：IPv4：23151.667 Mbps，IPv6：23077.000 Mbps。 功能要求：1.提供包括但不限于入侵防御等功能模块。 2.支持路由、交换、虚拟线、Listening、混合工作模式； 3.支持IP/MAC绑定，支持跨三	北京	台	2	172550	345100

						层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作； 4.支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由； 5.访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址 6.支持多种地址转换，支持源/目的 NAT、双向 NAT、NoNAT 转换方式;支持源 IP 转换同一性;支持端口块地址转换和 EIM 地址转换。 7.整机 TCP 新建：IPv4：269.989 万/秒，IPv6：269.994 万/秒。 8.支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP REQUEST FLOOD、NTP REPLY FLOOD 攻击防护。					
13			动态（WEB）应用防护系统	瑞数	RS-SP-DWAF	1.支持支持 IPv4 和 IPv6 双协议栈流量过滤 2.支持对 HTTP、HTTPS 协议的代理网关功能，支持透明代理、反向代理、负载均衡等模式 3.支持协议合规检测，可根据实际网络状况自定义协议参数合规标准，过滤非法数据 4.支持针对主流 Web 服务器及插件的已知漏洞防护。Web 服务器应覆盖主流服务器：apache、tomcat、lighttpd、NGINX、IIS 等；插件应覆盖：dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress 等。 5.支持对注入、XSS、Webshell 防护、支持 PHP 注入防护，路	上海	套	1	101150	101150

						径穿越及远程文件包含的攻击防护。 6.支持误报分析功能，以站点、路径、规则 ID 为聚合条件，根据命中次数进行排序，帮助管理人员分析和排查 WAF 误报的情况。 7.撞库防护：可有效防止通过自动化程序，发起撞库或暴力破解； 8.恶意爬虫防护，搜刮爬取网站上的页面、数据或敏感信息； 9.浏览器真实性检测：能识别用户是否使用真实客户端浏览器，包括但不限于扫描器及其他高级自动化工具； 10.灵活对抗策略：当请求触发防护规则时，可以设定多种拦截策略，如：阻挡，延时等；且可配置上述拦截策略按百分比随机响应，支持自定义响应状态码。 11.高级日志查询：支持高级查询，可基于字段（如源 IP、访问路径、攻击类型、请求方法、规则 ID 等）、AND/OR 等逻辑运算条件组合进行攻击事件查询，快速定位攻击事件。 12.支持标准 SNMP trap 和 Syslog 接口。 13.能对账户进行安全策略配置，包括口令复杂度和口令生存期。 防扫描：可有效防止各类自动化扫描工具发起的漏洞扫描与探测，防护后无法扫描出高危漏洞；0day 漏洞防御能力：系统应支持 0day 漏洞防御能力，不需要特征、规则即可有效封堵应用层未知漏洞攻击（Struts2、Weblogic 反序列等），0day 工具无法入侵系统，发起的勒索等攻击;追踪溯源：以便定位追踪，需支持全日志					

						记录，包括异常日志和正常日志，且支持除了 IP 以外的客户端定位技术，如指纹、客户端环境信息、客户端行为信息等。					
14			准入系统客户端（扩容）	奇安信	NAC-FL-IOT-CLT	终端授权（同时支持视频准入和 PC 终端准入） 1.要求能够接入交警已有的网络安全准入系统。 2.支持 VLAN 隔离准入技术，实现无客户端下端口级准入控制； 3.支持多种准入技术的复用，至少三种以上； 4.支持基于 IP/MAC 地址黑/白名单准入； 5.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； 6.支持终端安装软件的检查和软件运行情况的检查，提供白名单、黑名单管理方式； 7.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。 8.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。	北京	个	500	132.6	66300
15		应用安全	交通管理外挂软件智能安全卫士	华通	/	无缝对接公安交通管理综合应用平台社会化服务系统。	无锡	个	10	416.5	4165
16			Ukey 硬件	华通	/	无缝对接公安交通管理综合应用平台社会化服务系统。	无锡	个	100	102	10200
17			终端防病毒软	奇安	WS-ESM	1.接入交警已有的网络安全准入系统。	北京	项	10	83.3	83300

			件	信	-CLT	2.支持防病毒、补丁管理、主机防火墙功能； 3.病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本 4.支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。 5.支持对 Windows 操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复 6.支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标IP,支持输入IP范围。			00		
18		审计安全	日志审计软件	天融信	TA-L-SE	日志源授权 50 日志源,授权可扩展。 1.日志采集处理均值≥3000 EPS; 2.日志审计软件支持：日志收集、存储、查询、统计分析、告警响应等功能； 3.支持单级部署，只需在服务器上部署审计中心系统，审计中心可以直接采集管理对象的日志信息； 4.支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据； 5.支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格	北京	套	1	84575	84575

						式化处理，提炼出有用信息清晰、明确的展示给管理者； 6.支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计； 7.支持根据设备重要程度独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数； 8.支持对日志流量非常大但是日志重要程度低的syslog类型日志源限制接收速率，降低对系统资源的占用，保障重要日志的收集； 9.支持对重要日志源进行重点关注，可快速查看重点日志源的状态、当日日志量、采集日志总量等基础信息；					

19			数据库审计软件	美创	DAS_EE	软件性能要求：1.默认流量：200Mbps； 2.基础功能：双向审计，报表等； 3.支持国产化环境； 4.数据库实例 64； 5.峰值 SQL 吞吐 10000 条语句/秒。 功能要求：1.支持主流数据库的安全审计与审计配置功能，包括但不限于 Oracle、SQL Server、MySQL、DB2、达梦、Hive、Informix、Sybase、PostgreSQL、MariaDB、KingBase 等数据库。 2.支持对数据库审计的内容进行风险分析，保障整个数据库的安全可靠，以及安全事件整理。 3.提供综合性安全报表对数据库风险、客户端风险、规则风险及风险 SQL 进行统计，为数据库日常化运营提供依据。 4.支持日常运维中访问审计和返回结果集审计等需求，包括主机名、主机用户、IP、MAC、Port、请求的工具名称、访问时间、sql 语句、返回字段、执行状态、返回行数、执行时长等内容的审计。 5.支持对 Oracle、MySQL 等数据库本地审计，包括客户端 SSH 隧道代理访问数据库的操作，本地命令行访问数据库的操作等本地审计场景。	杭州	套	1	135150	135150
20	部署统一版社会化服		系统部署+业务迁移+割接+数据迁移+系统安全加固	定制	定制	深入摸排、全面掌握车驾管服务专网系统及网络现状，根据相关要求及本地实际情况，对系统部署迁移等工作，提供合理、可靠的解决方案。组建专职稳定的技术保障团队，保质保量完成系统部署、迁移、调试等工作，批次开展社会化服务机构接入联调，稳步推进系	/	项	1	853140	853140

	务系统				统切换，保障各项业务正常开展。					
投标总报价（人民币：元）										5687600

本合同金额为人民币大写：伍佰陆拾捌万柒仟陆佰元整，小写：5687600.00 元 。

项目的具体服务要求见集中采购机构的招标文件。

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、JSZC-320400-JZCG-G2024-0551 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 JSZC-320400-JZCG-G2024-0551 号招标文件（含技术说明）和投标文件的要求。

2、乙方应提供免费运维质保 5 年，自项目终验合格之日起算。

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。

7、乙方提供的所有设备须为全新未拆的产品，最终注册用户须为常州市公安局；乙方应提供所投软硬件产品 5 年原厂质保服务、硬盘不返还服务（自项目终验合格之

日起计算）；交换通道防火墙、数据域防火墙、边界防火墙需配套原厂 5 年入侵防御规则库、特征库免费升级服务。

8、本项目为交钥匙工程，乙方有义务保证甲方系统的完整性，如项目实施过程中因缺少设备、配件或软件授权导致无法满足甲方要求或者系统无法正常运行，乙方须承诺免费补齐相关设备、配件或软件授权；除甲方明确提出的变更外，本项目不再增加任何费用。

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 180 个日历日内完成软硬件部署、调试，并投入使用。

2、本项目软硬件质保 5 年，质保期内按照合同要求进行软硬件维护。

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	正式合同签订后15日内	收到发票 10 个工作日内	10%	
2	中间款	初验合格后 15 日内	收到发票 10 个工作日内	20%	
3	中间款	终验合格 15 日内	收到发票 10 个工作日内	40%	
4	尾款	终验合格满一年后15日内	收到发票 10 个工作日内	30%	

六、履约担保

履约保证金：合同金额的 5%，形式为银行保函；

履约担保期限：合同签订之日起至项目终验合格后满五年止。

七、服务要求

7.1 系统集成要求

乙方应根据甲方的的需要，排摸车驾管专网系统现状，包括社会化服务网点布点情况、业务办理范围、使用系统现状、网络环境等，形成详细的车驾管专网网络拓扑图和相关台账清单，为统一版社会化服务系统部署应用提供准确支撑。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。包括但不限于以下工作：

（一）统一版社会化服务系统软硬件运行环境建设服务要求

乙方根据甲方的要求，部署系统软硬件运行环境，完成国产化云平台建设、数据库建设、文件存储建设、软件中间件建设和网络改造等工作。

1. 网络环境方面，包括但不限于网络核心、服务器应用、数据库和用户访问等环境，采用重点核心交换机及汇聚交换机双机部署等可靠模式，保证网络环境平稳可靠。

2. 系统环境方面，采用云平台虚拟化等方式。

3. 数据库方面，部署数据库服务器双机容灾系统保证数据安全可靠。

4. 文件存储方面，搭建FastDFS文件分布式存储环境。

5. 软件中间件方面，搭建RabbitMq消息队列环境及Redis缓存环境等。

基于上述软硬件运行环境，支撑统一版社会化服务系统顺利部署、平稳运行。提供包括但不限于软硬件配置环境台账、系统架构图、网络拓扑图、部署方案等系统技术文档及实施方案。

（二）音视频切片存储管理系统建设服务要求

乙方利用服务器和存储资源，按照技术方案建设音视频切片存储管理系统，依托已建的车驾管音视频共享管理平台，对机动车查验、检验、驾驶人考试、业务窗口等场所的音视频开展切片存储管理，实现切片视频与业务流水的精准关联，提供视频点播/回放、摄像机状态监测、视频切片管理等服务支持，并将视频切片结果按照规范化要求上传至社会化服务系统。用于支持社会化服务系统的实现切片视频调阅、视频监控资源运行监测等管理功能，满足音业务抽查、业务回访、预警信息调查处理、异常业务分析等监管需求。

在社会化服务专网中部署统一的时钟同步服务器系统，针对需要确保时钟一致性的系统和设备，根据甲方要求，做好接入、调试等支撑保障工作,确保各系统及前端设备的时钟一致性。

（三）统一版社会化服务系统运行安全建设服务要求

1. 数据存储安全：部署数据库加固系统和备份软件；

2. 服务器安全：部署交换通道防火墙、数据域防火墙和堡垒机，针对堡垒机做好培训和运维管理等工作；

3. 网络安全：部署调试动态（WEB）应用防护系统和边界防火墙，做好客户端与准入系统对接调试工作；

4. 应用安全：部署调试交通管理外挂软件智能安全卫士，配合甲方做好社会化服

务机构的交通管理外挂软件智能安全卫士管理、调试工作。

5. 终端安全：根据甲方要求，做好Ukey、终端和零信任系统对接调试工作，开展终端防病毒软件安装调试工作，确保Ukey、终端正常开展业务工作；

6. 审计安全：部署日志审计软件和数据库审计软件，与相关系统进行对接调试，开展监测、审计、预警等工作。

乙方按照甲方要求，参照网络安全等级保护三级标准，整合应用上述安全设备，最大化发挥设备使用效能，提升车驾管服务专网整体安全防护水平。

（四）统一版社会化服务系统部署要求

乙方深入摸排、全面掌握车驾管服务专网系统及网络现状，根据相关要求及本地实际情况，对系统部署迁移等工作，提供合理、可靠的解决方案，包括但不限于设计方案、实施方案、实施进度安排等，并就实施过程中的难点及风险点进行重点阐述，经甲方审核确认后，按计划序时推进，及时保质保量完成部署、迁移、调试等工作。

开展部署迁移等相关工作时，组建专职稳定的技术保障团队，按照甲方及相关要求，做好社会化服务系统部署迁移调试等工作，包括但不限于网络规划、云平台部署、数据库安装调试、微服务应用发布配置、中间件部署调试、数据链路调优、系统安全加固、跨网交换服务系统部署调试等。提供系统部署迁移、业务迁移、割接、数据迁移治理、业务测试、功能测试、性能测试等服务。批次开展社会化服务机构接入联调，推进驾驶理论考试、考试监管、机动车查验/检验等系统切换，保障系统稳定运行，业务正常开展。

7.2 自动化监控运维要求

根据交警的生产环境实际要求，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。要求乙方提供自动化监控系统功能和网络运行自动监控系统功能。

（一）自动化监控系统功能具体技术要求如下：

实时监控服务器健康状况和性能指标，包括但不限于 CPU 使用率、内存使用量、硬盘 I/O 等信息；

服务器性能指标超过阈值时，实时告警。

（二）网络运行自动监控系统功能具体技术要求如下：

实时显示甲方真实网络拓扑图；

实时显示网络及安全设备的运行状态；

实时显示设备间链路流量信息；

实时显示甲方内部网络专线的链路状态及流量信息；

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；

实时显示链路流量超过规定阀值时，告警信息在网络拓扑图上实际位置突出显示；

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。

7.3 人员配备要求

乙方须成立项目实施团队和运维团队，实施团队负责前期准备和项目实施工作，运维团队负责日常软硬件及网络运维工作、保障系统平稳运行。项目一切接触人员，均需提前与甲方报备相关背景信息，经过甲方审核之后方可进场实施。

项目实施团队成员不低于 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。项目实施期间，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。

施团队成员具体要求如下：

职能	人数	要求
项目经理	1	1. 本科及以上学历，掌握项目管理理论，熟悉大型工程建设项目的流程、项目管理方法等。 2. 具有系统集成大型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。 3. 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。 4. 具备相应的专业资质认证。
云平台和服务器实施工程师	1	1. 本科及以上学历，具有 2 年以上相关工作经验。 2. 2 年以上服务器部署交付经验。 3. 熟悉 Windows\Linux 操作系统原理及运行机制，熟练

		掌握设备 RAID 配置、操作系统安装、网络配置、Linux 系统操作等技能，负责服务器部署、故障处理、性能优化等工作。 4.具备相应的专业资质认证。
数据库实施工程师 1	1	1.本科及以上学历，具有 2 年以上相关工作经验。 1.2 年以上数据库部署、迁移等相关工作实施经验。 3.具备相应的专业资质认证。
安全实施工程师	1	1.本科及以上学历，具有 2 年以上相关工作经验。 2.2 年以上网络安全工程交付经验。 2.熟悉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，且具备相应的专业资质认证。 3.具备相应的专业资质认证。
网络实施工程师	1	1.本科及以上学历，具有 2 年以上相关工作经验。 2.2 年以上构架工程工程交付经验。 3.熟悉社会化服务专网网络整体架构及设计，负责网络解决规划、设计、部署、故障处理、性能优化等工作。 4.具备相应的专业资质认证。

驻场人员要求运维：项目运维需有专门的运维团队，**且派驻 1 名成员驻场运维。驻场运维人员必须专职此项目服务，且必须全过程参与项目实施，提前熟悉本项目情况**，未经许可不得兼职或与其它项目复用，如需更换人员，需征得甲方同意且更换人员要求不得低于原运维人员，保证接替人员及时到位，不得存在运维空档期。

职能	**人数**	**要求**
驻场人员	1	1. 工作经验不得少于 2 年，学历不得低于本科。 善于沟通，熟悉 Java 开发语言以及相关框架，熟悉数据库搭建与操作,熟悉 Linux/Windows 等系统操作、原理、配置和使用，具备操作系统维护、软件工功能维护及测试、故障诊断排查、网络管理等相关能力。 2. 具备相应的专业资质认证。

7.4 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能进行日常维护运行工作，掌握软件、硬件的操作，熟悉硬件功能。能熟练地排除设备故障，

熟练地管理设备，分析软件、硬件故障等工作并能掌握组织、扩建网络/系统业务的能力。

7.5 安全保密要求

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。

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。

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。

乙方不得有其他任何危害公安信息安全的行为。

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：

（1）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；

（2）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；

（3）不得擅自对设备进行扫描、探测和入侵信息系统；

（4）不得对工作信息和资源越权访问、违规使用；

（5）不得私自允许他人接触和使用机房设备；

（6）严禁将工作用设备和文件带离机房；

（7）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；

（8）对工作中接触到的信息做到保密。

7.6 售后服务（质保期等）

1. 本项目提供免费运维质保 5 年，自项目终验合格之日起算。

2. 在质保期内乙方硬件方面提供包括但不限于设备运行巡检监测、维修保养、安装调换、调试对接等工作，确保硬件设备运行平稳可靠；软件方面提供但包括不限于系统环境搭建、系统开发改造、系统部署、系统对接、系统优化升级、漏洞修复、补丁程序安装、系统迁移、系统运维、数据备份还原、故障处置、安全检查等工作，保障系统平稳、高效地持续运转；对于甲方人为原因造成的故障，乙方提供免费的更换、

安装、对接、调试等服务，只收取硬件成本费用。

3. 项目中涉及的硬件设备、系统平台、网络环境有具体的台账清单、架构图、部署文档和维护文档，定期组织甲方、运维人员以及其他相关人员进行技术交流和反馈，并定期更新客户服务维护技术档案，以提高技术人员的日常维护水平和对问题的解决能力。每季度至少提供一次技术交流和服务评估。根据乙方需求，不定期提供培训服务。

4. 乙方需要根据甲方要求对系统相关软硬件做好安装调试工作，包括但不限于统一终端设备管理软件、考台桌面软件、安全管控设备（Ukey）、外挂软件智能安全卫士、跨网数据交换软件等，确保系统平稳运行、日常业务正常开展。

5. 乙方针对本项目涉及到的产品应提供完整的运维方案，针对机房断电、存储不足、数据库故障、病毒感染、网络故障等突发情况做好应急预案。

6. 驻场人员需要按照甲方工作要求和安排，做好系统管理、软硬件巡检运维、系统调优、技术文档完善、培训指导等工作。除日常巡检外，每月月初、重大节假日前或甲方要求的时间节点对系统平台等进行全面检查维护，每季度实施一次系统健康状况检查和优化调整。发生系统故障或其他问题时，驻场人员不能及时解决，乙方需及时提供技术保障团队现场处置，直至故障彻底解决，系统恢复正常稳定运行。

7. 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. 系统故障处置完毕后，3 日内对故障排查和处置过程进行复盘整理，详细列明故障表象、故障原因、处置方式以及调优建议等，形成故障分析报告，及时提交至甲方。

7.7 其他要求

项目实施过程中，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。

八、验收标准

乙方按照甲方要求准备验收材料，满足初验条件后，乙方可向甲方申请初验；经甲方组织初验合格后进入试运行阶段，乙方按照甲方要求准备验收材料，满足终验条件后，乙方可向甲方申请终验。

1. 初验条件：

完成所有建设内容；硬件安装部署、调试、培训并通过市局初验安全检测。

2. 终验条件：

稳定试运行三个月后，通过甲方组织的等保评估等。

3、项目所有产出成果的知识产权由常州市公安局和乙方共同拥有。

九、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会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(含发生安案事件)，不得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。

十、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。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。

十一、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。

十二、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，则提交常州仲裁委员会进行仲裁。

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。

十三、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。

十四、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。本合同一式伍份，甲方贰份，乙方贰份，集中采购机构壹份。

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）：常州市公安局交通警察支队

单位地址：常州市天宁区和平中路 330 号

法定代表人：

委托代理人：

经办人：

乙方：单位名称（章）：中电鸿信信息科技有限公司

单位地址：南京市玄武大道 699-1 号

法定代表人：

委托代理人：

经办人：　　电　话：

开户银行：中国建设银行股份有限公司南京湖北路支行

银行帐号：3200 1881 4360 5900 0588