常州市公安局2025年度公安基础设施建设项目合同

项目名称：常州市公安局2025年度公安基础设施建设项目

甲方：常州市公安局　　签订地点：常州市锦绣路2号1-1号

乙方：江苏移动信息系统集成有限公司　签订时间：_____

集中采购机构：常州市政府采购中心　合同编号：

根据常州市政府采购中心2026年1月27日进行的JSZC-320400-JZCG-G2025-0565招标，甲、乙双方就乙方中标的常州市公安局2025年度公安基础设施建设项目，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，为甲方提供的常州市公安局2025年度公安基础设施建设项目（JSZC-320400-JZCG-G2025-0565）具体服务清单和价格（单位：元）如下：

本合同金额为人民币大写：壹仟柒佰壹拾捌万零叁拾元整，小写：￥17180030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-G2025-0565 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 JSZC-320400-JZCG-G2025-0565 招标文件（含技术说明）和投标文件的要求。

2．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。

3．乙方应保证提供的所有软件产品为最新正式版本，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。

4．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。

5．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．合同有效期：项目合同签订之日起至项目质保期结束。

2．质保期：项目终验合格之日起五年。

五、付款方式

预付款支付时间：合同签订后15日内，预付款支付比例：合同金额的10%。满足合同约定支付条件的，自收到发票后10个工作日内支付。

验收款支付时间：项目终验合格后三年内，按照每次合同金额的30%为基础，根据合同履约情况，分三次支付合同款。

质保期内因乙方维护工作不到位导致考核扣款，在质保期结束十个工作日内，乙方须将扣款金额从已收到项目款中退还给甲方。

六、服务要求

要求本次所采购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。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）。

本项目为交钥匙工程，乙方有义务保证甲方系统的完整性，部分连接、运行配件未在招标书中明示的，乙方应在投标时予以补充，如项目实施过程中因缺少设备、配件、辅材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，乙方须免费补齐相关设备、配件、辅材或软件授权；除甲方明确提出的变更外，本项目不再增加任何费用。

1.供货要求

乙方须在不迟于合同签订后的60个工作日内完成所有招标设备到指定地点的供货；90个工作日内完成设备调试（包括但不限于设备上架、上电、网络连接及配置等工作），确保设备运行正常。接到甲方通知后，180天内完成零信任系统和安全访问通道与省厅级联对接、零信任系统与市局统一鉴权系统对接；1年内完成统一运营运维系统开发，数据迁移和应用适配工作。

乙方须保证所提供产品的技术指标必须满足或优于以上技术要求。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。

乙方须保证所提供硬件产品包括相关附件为相应硬件厂家原装正品，提供软件产品为软件厂商正版产品，符合国家有关规定。

乙方在网络管理系统中已提供的设备监控授权基础上,多提供 100 个授权。

设备到货后，甲方与乙方共同配合有关部门对所有设备进行开箱检查，出现损坏、数量不全或产品不对、软件版本不正确等问题时，由乙方负责解决。

2.现场实施人员要求

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。

乙方须根据甲方要求安排原厂工程师进场进行软硬件设备规划、部署工作，积极主动与本项目的相关单位合作，并服从甲方的协调。

乙方现场实施团队人员（不含原厂工程师）数量、人员资质、人员技能要求见下表。

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 3 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
网络实施工程师	2	1.本科及以上学历，具有 2 年以上相关工作经验； 2.2 年以上网络构架工程交付经验，了解工程项目交付流程和技术管理方法等； 3.熟悉网络技术原理、精通大型 IP 网络、云平台网络架

		构及设计，负责公安网络解决规划、设计及部署工作。
安全实施工程师	2	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，了解工程项目交付流程和技术管理方法等； 3.熟悉公安网络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。
软件开发工程师	2	1.本科及以上学历，具有 2 年以上相关工作经验； 2.2 年以上软件开发经验，熟悉软件开发流程，面向对象开发，代码规范，具有良好的分析和解决问题的能力。 3.终验合格前需常驻现场。
数据治理工程师	2	1.本科及以上学历，具有 2 年以上相关工作经验； 2.2 年以上数据治理、数据运维经验，熟悉公安大数据治理相关标准规范； 3.熟悉国产数据库、公安大数据环境。 4.终验合格前需常驻现场。

3.实施要求

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。包括但不限于以下工作：

3.1 方案制定

乙方需要在项目实施前对机房环境进行充分调研，根据甲方现场环境和总体规划，充分考虑机房供电、制冷，机房功能布局，业务部署、运维管理、网络连接等因素，合理规划设备部署位置。

3.1.1 新一代公安信息网

乙方需要在项目实施前对现有公安网络现状进行充分调研，并在合同签订后 15 个工作日内，针对出口防火墙、汇聚路由器、核心交换机、网络准入控制系统、准入控制网关、管理交换机，提供详细的规划和施工方案（包括网络架构需求和分析、网络架构设计、地址规划、设备安装部署

方案、应急回退方案、与省厅网络对接方案），针对统一运营运维系统提供详细的开发和部署方案，提交甲方。

3.1.2 零信任体系和安全访问通道

乙方需要在项目实施前对现有公安网络现状进行充分调研，并在合同签订后 15 个工作日内，提供详细的规划和施工方案（包括软件部署需求、设备部署安装方案、系统联动方案，应用对接方案、省厅对接方案、应急回退方案等），提交甲方。

3.1.3 数据域云平台

市局目前采用华为云平台，乙方需安排华为原厂工程师在项目实施前对市局云平台现状进行充分调研，并在合同签订后 15 个工作日内，提供详细的规划和施工方案（包括机柜位置规划、设备地址规划、云平台软件部署方案、应急回退方案等），提交甲方。

3.1.4 数据迁移及应用适配服务

乙方需要在项目实施前对市局数据中心数据资源及数据治理平台现状进行充分调研，并在合同签订后 20 个工作日内，针对数据域提供的服务器、数据库、中间件等基础环境，提供详细的适配改造和数据迁移规划方案，提交甲方。

3.2 项目实施

3.2.1 新一代公安信息网

网络部分：涉及设备为数据域出口防火墙、数据域汇聚路由器、数据域核心交换机，乙方需安排原厂工程师实施部署，2 台数据域汇聚路由器须分别部署在市局机房和市大数据中心机房，互为备份，向上与省厅下发的市级节点路由器互联，向下与数据域核心交换机互联。2 台数据域核心交换机与市级数据汇聚路由互联，部署在市大数据中心机房，同时作为数据域数据中心核心、云平台核心，2 台出口防火墙，部署在汇聚路由器和省厅下发的市级节点之间，实现纵向安全防护，数据域汇聚路由器、数据域核心交换机配置须满足《新一代公安信息网 网络设备配置基本要求》。

网络管理系统：乙方需完成网络管理系统部署，并实现对用户域、数据域、感知网、社会面网、移动警务专网的交换机、路由器、服务器等设备的进行监控。提供监控数据、告警信息等接口供统一运营运维系统调用。

统一运营运维系统：在系统建设中，乙方必须提供完整的文档，主要包括各类规范、标准、系统需求规格说明书、系统概要设计说明书、系统详细设计说明书、系统安装部署说明书、系统用户使用手册、系统测试用例及测试报告、系统运行与维护手册，系统验收合格前，乙方应维持一支不少于 2 名系统开发人员及实施人员组成的技术队伍常驻现场，人员须经采购方认可，开发设备由乙方提供，存储介质不返还。在本系统的开发过程中和交付使用后，各个阶段的所有成果（包括但不限于设计文档、开发文档、源代码等）需全部交付给常州市公安局，而且要提供明确的交付清单，成果和文档资料必须符合软件的相关要求。

网络准入系统，涉及软硬件设备为网络准入控制系统、准入控制网关、管理交换机，乙方需安排原厂工程师实施准入系统部署，并对接准入控制网关，同时部署准入网关 2 台，其中 1 台部署在大数据中心机房，另外 1 台部署在市局数据中心机房，通过对入网数据流量进行分析，进而实现准入管控。部署完成后须与市局一机两用系统对接，设备在进入公安网时，准入可以和“一机两用”联动，对未注册未保护设备进行阻断。

3.2.2 零信任体系和安全访问通道

本项目建设的零信任体系需满足《公安大数据安全 零信任体系与应用接口技术要求》，并实现与省厅零信任体系上下联动，具备与部、省进行数据同步的条件，既可以通过省市对接的接口获取省厅数据，也可以向省厅汇聚数据，同时需配合市局完成本次迁移的应用系统、统一用户鉴权系统与零信任体系的对接，且满足公安部测评要求。

3.2.3 数据域云平台

云平台：涉及设备为管理节点服务器、网络节点服务器、计算节点服务器、云平台防火墙、增强云专线交换机、云平台管理区交换机、计算节点接入交换机、存储节点接入交换机、存储节点后端交换机、大数据接入

交换机、大数据管理交换机，市局目前采用华为云平台，市局提供存储节点服务器和大数据节点服务器和相应的云平台软件授权，乙方需安排华为原厂工程师实施云平台部署（包括虚拟化和大数据部分），所需线缆等辅材有由乙方提供。

物理服务器：乙方需按照甲方要求，上架到机房指定位置，安装操作系统并入网。

图片存储：需完成设备上架，设备入网调试，纳入市局现有超融合平台存储集群统一进行管理、按需分配资源等。

国产数据库云平台：涉及软硬件设备为国产数据库服务器、国产数据库管理交换机、国产数据库云平台。乙方需完成设备上架，入网调试，并安排所投国产数据库云平台原厂工程师进行平台部署，实现所有平台组件，包括操作系统、集群、分布式存储、数据库等一站式集中统一管理，提供可视化运维管理和监控功能。

3.2.4 数据迁移及应用适配服务

应用适配：乙方需按照甲方要求，将数据中心数据治理、资产管理、数据可视化等模块，在国产化硬件、基础环境下，完成改造适配，实现在数据域中数据的标准化治理和共享应用

数据迁移：与数据域基础环境对接，在不影响公安网数据使用情况下，完成公安网数据中心建设有汇聚库、标准库、新标库中全量数据资源，MPP 数据库全量数据资源，ES、HIVE 等大数据环境中的增量数据资源迁移至数据域对应数据环境中，上述数据对接完成后，公安网和数据域同步正常运行，乙方做好相关运维工作。

统一用户鉴权对接：由统一用户鉴权模块同零信任体系进行对接改造，在即不改变原有智慧警务生态体系内（包括超融合）应用的认证、鉴权方式的前提下，同时满足零信任体系安全接入规范，最小化减少对原有应用模块中用户认证鉴权相关的改造工作。

3.3 联调测试

项目实施完成后，乙方应向甲方提交测试内容和方法。测试计划和技术内容由乙方拟定，经甲方确认，对软硬件设备在现网中运行所能达到的功能、性能等进行综合测试，并形成测试报告。

乙方需为本项目配不少于四台台式机用于软件开发，不少于四台笔记本用于设备部署调试，保证项目顺利开展，使用完归还，硬盘不返还。

3.4 注意事项

按照实施方案，在收到甲方通知后，规定时间内完成所有设备部署、系统割接、业务配置，保证部署、割接后系统功能完好。如有问题，按照回退方案及时回退，保证各类业务恢复割接前功能，各业务正常运行。部署完成后，应做好线缆整理、设备及线路标签粘贴，以及资料整理形成实施文档。

设备安装、调试所需的工具、仪表及安装材料（包括尾纤、网线、扎带、机柜层板等）由乙方自行解决。施工过程应严格执行相关的强弱电施工规范，并保证施工安全。

因乙方原因在项目实施过程中或者实施完成后，造成甲方系统不稳定，业务中断的或其他未达到甲方要求的，造成的损失应由乙方承担，严重的可解除合同，并要求乙方承担相应责任。

4.验收要求

初验条件：

硬件设备及成品软件系统。所有设备安装到位，系统部署到位，各项指标满足招标文件要求。乙方提供完整的系统技术文档，包括用户手册、常见故障分析和排除指南、配置文件等资料。零信任体系需通过公安部测评，并提供测评报告。防火墙配备 IPS 模块、AV 防病毒模块，并保证 IPS 特征库和 AV 病毒库更新至最新。

统一运营运维系统。完成所有开发内容，项目软件通过数据项标准检测，与数字证书系统、大数据应用安全审计等系统对接并通过安全检测，通过第三方软件测试。

数据及系统迁移。完成数据治理、布控服务、资产管理、数据可视化模块改造适配，完成统一用户鉴权模块对接改造，完成数据公安网数据迁移至数据域，通过数据项标准检测，与数字证书系统、大数据应用安全审计等系统对接并通过安全检测，通过第三方软件测试。

终验条件：项目通过初验后，交付试运行不少于3个月，所投产品运行正常，满足甲方需求，乙方提交全部报告材料，通过等保三级等安全测评、风险评估、商用密码应用安全性评估、国产化适配符合性测试和电子文件归档合规性检测。

如验收中出现不符合标书和合同要求的严重质量问题时，甲方保留索赔权利。

5.运维要求

5.1 质保期

乙方必须提供采购的软硬件设备及配件至少五年原厂维保服务，质保期自项目终验合格之日起计算。不得在系统中设置注册码等限制。

5.2 运维方案

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。乙方提供每季度至少一次原厂商上门巡检（包括设备、系统），并出具深度巡检报告。

5.3 日常巡检

乙方按照甲方规定的流程定期对采购的软硬件设备进行巡检，包括日巡检、月巡检、半年度巡检、年度巡检及甲方要求的巡检计划。

5.4 维护人员

质保期内，乙方须配备至少1名专业工程师负责整个项目维护，具体要求如下:

岗位职责：主要负责本项目中所有软硬件系统的的日常运维，包括巡检：查看设备的运行状态，设备日志分析、运行状态分析、链路状态分析、系统资源占用情况分析等；业务配置：网络设备、准入系统、零信任系统、

安全访问通道及云平台的业务配置，资源发放等；排障：对设备故障或异常情况及时排除解决、坏件及时更换等工作；协调：协调原厂商现场配合。

质保期内，乙方需为本项目配不少于四台台式机用于日常运维，不少于四台笔记本用于机房巡检、设备管理平面运维，保证运维人员正常的运维巡检需要，维护期满后归还，硬盘不返还）

5.5 服务响应及故障处理

（1）服务响应及维修。乙方提供 7*24 小时的技术支持和服务。5 分钟内对甲方所提出的需求做出响应，1 小时内到达现场，在规定的时间内完成维修。

（2）故障响应及恢复。

按故障严重程度从高到低分为四级：

重大故障：核心业务系统不可用或将导致其业务数据缺失的；

严重故障：核心业务系统性能受到严重影响的故障或可能导致核心业务系统不可用的，非核心业务系统不可用的或导致其业务数据缺失的；

较大故障：非核心业务系统性能受到严重影响的故障或可能发生严重以上故障风险的故障；

一般故障：其他隐患类故障。

（3）要求做到全天候 7*24 小时的技术服务，对于故障抢修涉及的响应时间和故障处置时间的要求如下：

1）故障响应。

a） 重大及严重故障：故障发生后，应在 5 分钟内人员响应，30 分钟内到达故障发生现场。

b）较大及一般故障：故障发生后，乙方维修人员到达故障服务现场的时间应不大于 1 小时，具体为：工作时间到达故障服务现场的时间应不大于 30 分钟，非工作时间到达故障服务现场的时间应不大于 1 小时。

2）故障恢复。

重大故障：恢复时间在工作时间内不超过 1 小时，非工作时间内不超过 2 小时；

严重故障：恢复时间在工作时间内不超过 2 小时，非工作时间内不超过 3 小时；

较大故障：恢复时间不超过 4 小时；

一般故障：其他隐患类故障，恢复时间由乙方与甲方协商决定，原则上不超过 1 工作日。

重大、严重故障连续发生一个月内两次以上的，除提交故障处置报告以外还应提交问题分析报告，深度分析故障产生的原因，并提出预防性改善建议。

（4）如因特殊原因无法在指定处置时间内修复故障的，乙方需将故障原因、过渡方案和恢复计划等在 2 小时内书面上报，并在此期间积极配合相关应用开发商实施过渡方案，全力保证应用的不间断，临时过渡方案产生的人力成本、时间成本、社会经济损失等由乙方承担。

（5）在重大、严重故障或者甲方要求提供故障报告的故障处理结束后 24 小时内应向甲方提出书面故障处理报告。

（6）乙方在本次所采购设备发生故障无法排除的情况下，乙方须协调原厂解决，所涉及的费用由乙方承担。

5.6 技术支持

质保期内，为提供全面的技术支持，帮助甲方及时解决网络、安全、云平台等软硬件设备运行中遇到的技术问题，配合甲方根据运行环境和要求调整性能参数；定期检查所有设备和系统的运行情况，并能根据甲方系统变化情况及时调整优化，包括漏洞补丁修复、操作系统兼容性支持、数据库兼容性支持、大数据组件兼容性支持等。甲方在重大网络割接时，乙方应及时提供支撑，必要时应安排原厂工程师免费到达现场提供帮助。乙方应及时对防火墙规则库、病毒库进行升级更新。

实施期及质保期间，如公安部的新一代公安信息网、零信任体系的相关对接标准进行更新，乙方及设备（系统）原厂商须按照最新标准进行统一运营运维系统、准入控制管理系统、零信任体系接口进行免费适配性改造，保证市局与部、省对接不受影响。业务系统在数据域部署或者迁移至

数据域过程中，需要与零信任体系和安全访问通道进行对接时，零信任系统原厂商及安全访问通道原厂商需配合本项目乙方，按照甲方要求，到甲方现场，在规定时间内免费完成系统配置和业务对接等工作，不得推诿。

5.7 安全服务

质保期内，围绕项目采购的网络、安全等设备，定期为甲方提供配套的安全服务，包括设备的基线核查、策略优化更新、软件版本的更新升级等。

5.8 其他

质保期内，设备发生故障后，在规定时间内无法解决技术问题和更新故障软硬件，直接影响甲方正常开展业务工作的，甲方有权选择第三方公司提供服务，所需费用由乙方承担。

6.文档要求

乙方必须在对其所提供的设备进行安装、测试、验收过程中提供和准备的技术文档。包括操作手册以及系统实施方案等开发过程中形成的一整套完整技术文档资料。

技术文件：乙方必须向甲方提供设备的安装、运行、使用、测试、诊断和维修维护的技术文件。

安装计划：安装日期是乙方执行合同的开始，最少包括：运输/交货、测试、调试、正常运行。

安装指南：乙方应当提供所购软硬件设备的安装指南。

维保资料：维保过程中，乙方因按照要求提供完成的设备巡检记录、故障处理报告和升级优化方案等资料。

7.培训要求

乙方应针对采购单位管理人员、技术人员提供培训，以便对工程实施进行有效的管理，保证工程验收移交后，甲方能够胜任系统的全部运行、操作、维护；故障分析处理；设备维修和保养等工作。

技术现场培训：乙方在产品安装调试时，对甲方的技术人员进行现场安装调试培训，讲解产品的结构、安装步骤、调试方法和系统配置等。一般技术培训应该不限制人数。

维护团队培训：乙方提供管理员培训，对甲方的系统维护技术团队开展培训，掌握设备的日常维护技能。包括提供教材、场地、人员等。

8.安全保密要求

8.1 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。

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。

8.2 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。

9.考核要求

9.1 考核办法

项目质保期内，服务质量实行按月定量考核制度，月考核按照每 1 分 3000 元为基准，按比例倒扣分（即月得分 98，扣款为 3000*2=6000 元）。考核打分办法如下：

（1）日常巡检服务(20 分-40 分)

完全按照甲方规定的流程进行巡检（包括日巡检、月巡检、半年度巡检、年度巡检及甲方要求的巡检计划）的不扣分，发生 1 次未遵循规定流程巡检或者不巡检的，扣 0.5 分，以次类推，直至本项分值扣为 0 分。

巡检及故障处理中违规操作，造成甲方设备损坏、数据丢失等严重后果的，有 1 次扣 10 分。

（2）服务响应时限。(20 分)

发生重大及严重故障在时，能够有效开展故障处理的技术人员在工作日内到达现场时间不超过 1 小时，在节假日内到达现场时间不超过 2 小时。（每迟 30 分钟扣 1 分，直至本项分值扣为 0 分）；

（3）故障解决时限（20 分）

重大及严重故障，业务恢复时间不超过 2 小时，每超过 30 分钟扣 1 分，直至本月得分为 0 分。

较大故障，业务恢复时间不超过 4 小时，每超过 1 小时扣 1 分，直至本月得分为 0 分。

一般故障，业务恢复时间不超过 24 小时，每超过 1 小时扣 1 分，直至本月得分为 0 分。

因乙方操作失误导致所采购设备或其他相关设备出现故障，正常运行的业务受影响或者不可用，按照影响情况扣 1-10 分/次，直至本月得分为 0 分。

遇到设备故障，故意拖延处理，导致更严重后果的，有 1 次扣 10 分。

（4）运维文档管理。(20 分)

每日巡检报告（上午 10:00 点前提交，发生 1 次未按时提交的扣 0.5 分，直到本月得 0 分）。

故障报告。(每次故障后 2 天内提交，每迟 1 天扣 0.5 分，直到本月得 0 分)

月度服务报告。(次月 3 号前提交，每迟 1 天扣 0.5 分，直到本月得 0 分)

年度服务报告。(服务结束前 10 天内提交，服务结束后每晚 1 天扣 0.5 分，直到得 0 分)

在巡检报告、故障处理报告等文件中弄虚作假，情节严重的；有 1 次扣 5 分。

(5)驻场人员管理（0 分-20 分）

驻场人员须按照甲方要求正常上下班，

每出现 1 人/次迟到、早退扣 0.1 分，

每出现 1 人/半天旷工扣 0.5 分，1 人/天旷工扣 1 分。

办公区域不整洁、着装不规范等发现 1 人/次扣 0.1 分，

未按时完成交办任务的每 1 人/次扣 0.1 分，

交办任务不执行或不完全执行扣每 1 人/次扣 0.1 分，

驻场人员参加甲方组织的技能考试，未通过的每 1 人/次扣 0.1 分，

被所在部门或上级部门检查发现或通报的批评的，每 1 人/次扣 0.5 分，

中途更换驻场人员，驻场人员交接过程中内断档 1 天，按旷工 1 天计算，以此类推。

9.2 得分计算办法

每月考核得分=日常巡检服务得分+服务响应时限得分+故障解决时限得分+文档提交时限得分+驻场人员管理得分（提供驻场人员则日常巡检服务总分 20 分，驻场人员管理总分 20 分，未提供驻场人员则日常巡检服务总分 40 分，驻场人员管理不赋分）。

9.3 考核月得分表格：

序号	日常巡检服务	服务响应时限	故障解决时限	文档提交时限	本月合计

维保期内，甲方有权根据实际情况对具体考核条款进行调整。

9.4 质量保证

乙方出现以下任意一种情况的，经查实涉及本项目的，扣除合同总价的 1%，出现两次的，扣除合同总价的 3%。

（1）乙方发生违反保密协议的，造成严重后果或被所在部门及上级部门检查通报的；

（2）乙方及运维人员违反《数据安全管理“十个严禁”》、《江苏省公安机关信息化合作企业安全管理十项管理规定》等管理规定的，造成严重后果或被所在部门及上级部门检查发现的；

（3）乙方在合同执行中有触犯法律法规的其他情形。

10.其它要求

甲方仅负责提供与本项目相关系统的原建设维护单位的联系方式，乙方负责协调机房环境、网络、安全、服务器、存储、云计算平台等系统的原建设维护单位完成对接和实施的工作。在实施过程中，如需要以上单位配合安装调试和实施的，相关联系协调工作以及由此所产生的费用（包括且不限于对接、实施费用等）均由乙方承担。

乙方协调项目所有有关单位，将新购设备融入用户现有的使用环境中，满足用户统一规划的要求。在配合实施过程中如果牵涉到相关费用由乙方承担。如果乙方不能按照用户统一规划的要求进行实施，从而影响信息系统管理，视为乙方违约，甲方有权依照法律程序解除合同，并追究乙方的违约责任，同时将有关违约情况通报政府采购管理部门。

本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，乙方须配合甲方完成软件著作权和专利申请，至少完成 1 项软件著作权和 2 项专利申请，涉及的费用由乙方承担。

本次招标，乙方的投标报价中应包括但不限于设备采购费用、安装调试费用、培训费用、售后服务费用、相关知识产权申请费用和所需缴纳的任何税费等所有的费用。

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。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、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。

九、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、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，则应向甲方所在地人民法院提起诉讼。

3．争议在处理过程中，除正在进行诉讼的部分外，合同的其他无争议部分将继续执行。

4．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。

5．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。

6．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。

7．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

本合同经双方盖章并签字后生效，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，乙方贰份。

其他未尽事宜，参照相关法律，双方协商解决。

甲方：单位名称（章）：常州市公安局

单位地址：常州市新北区龙锦路 1588 号

法定代表人：

委托代理人：

经办人：

乙方：单位名称（章）：江苏移动信息系统集成有限公司

单位地址：南京市虎踞路 59 号

法定代表人：

委托代理人：

经办人：

电　话：

开户银行：中国银行南京云锦路支行

银行帐号：479361758530