合同编号：_____

商丘市公安局交通警察支队公安交通管理综合应用平台社会化服务系统升级改造项目合同

项目名称：商丘市公安局交通警察支队公安交通管理综合应用平台社会化服务系统升级改造项目

甲　　方：商丘市公安局

乙　　方：中移系统集成有限公司

签 订 地：

签订日期：2026 年 1 月 5 日

2025 年 12 月 23 日，商丘市公安局 以 公开招标方式 对 商丘市公安局交通警察支队公安交通管理综合应用平台社会化服务系统升级改造项目 进行了采购。经评定，中移系统集成有限公司 为该项目成交供应商。现于成交通知书发出之日起三十日内，按照采购文件确定的事项签订本合同。

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平和诚实信用的原则，经 商丘市公安局 (以下简称：甲方)和 中移系统集成有限公司 (以下简称：乙方)协商一致，约定以下合同条款，以兹共同遵守、全面履行。

1.1 合同组成部分

下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定的事项的前提下，组成本合同的多份文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 成交通知书；

1.1.3 磋商文件（含澄清或者说明文件）；

1.2 标的

1.2.1 标的名称：服务器、存储设备、虚拟化系统、文件存储系统、网络设备、原有设备的利旧使用服务、音视频巡查切片等设备及配套软件服务（包括软件系统、硬件系统、驻场服务等）的全部集成建设及优化完善等服务工作。详见附件一《采购清单明细表》；

1.2.2 标的数量：详见附件一《采购清单明细表》；

1.2.3 标的质量： 合格，符合国家及相关行业标准 。

1.3 合同价款

本合同总价为：￥ 2653000.00 元（大写： 贰佰陆拾伍万叁仟元整 人民币）。

分项价格详见附件一《采购清单明细表》

1.4 付款方式、发票开具方式、结算方式、乙方收款账户

1.4.1 付款方式：_：合同签订后，甲方向乙方支付合同款的 40%预付款；采购人在中标单位完成监理服务、等级保护测评（三级）、密码应用安全性评估并经采购人验收小组验收合格后，自收到发票之日起 3 个工作日内，甲方向乙方支付合同款的 60%。

；

1.4.2 发票开具方式：付款前乙方应开具相应金额的增值税发票 ；

1.4.3 结算方式：甲乙双方之间通过银行转账方式进行结算 ；

1.4.4 乙方收款账户信息如下

开户名称：中移系统集成有限公司

开 户 行：招商银行股份有限公司北京分行营业部

帐　　号：8888015100002818

1.5 安装及调试期、质保期、交货地点

1.5.1 安装及调试期：合同签订后 30 日历天内；

1.5.2 质保期： 自安装及调试完成且验收通过之日起 4 年 ；

1.5.2 交货地点： 甲方指定地点（商丘市市区内）。；

1.6 技术服务

在本项目实施过程中，乙方承诺将为甲方提供完整的培训服务、网络安全咨询、技术咨询等融网通服务，助力项目管理人员尽快掌握相关设备之使用、应用、管理能力。

为此，乙方将为本项目制定出详细的用户培训方案及 1 人两年驻场服务，根据要求，不定期提供服务，服务内容 1.硬件日常维护：服务器、存储、网络、安全设备及巡检监控。应急响应、重大故障处理。2.基础软件系统：操作系统、数据库软件、中间件等基础支撑软硬件设施运行监测、定期检查、故障处理、系统备份。3.交管业务软件：社会化服务系统、分发库系统、音视频系统管理、自建系统维护（机动车登记、查验、检验、）。4.信息安全：网络安全运行监控，记录、监控相关安全事件；系统安全巡检服务，系统安全调优服务，应急响应、重大安全故障处理。防火墙策略调整。5.制度建设：制定运维技术管理、运行管理、备品备件管理、服务质量考核等相关制度，建立规范化标准化的运维体系。6、服务内容：售后服务及培训：提供软硬件 3 年运维服务，提供 7*24 小时技术支持服务，提供每月数据库巡检服务，提供每季度整体平台软、硬件设备巡检服务；提供不少于 10 人次的现场技术培训。在验收后为用户进行专业、系统化的技术培训。

1.7 项目验收

项目完工后，由乙方向甲方提出书面验收申请。甲方需在收到验收申请之日起 7 个工作日内组织验收，验收通过后 3 个工作日内应出具验收报告，验收报告中载明的日期视为验收合格之日。

如有验收不合格的需要进行返工或整改，由此产生的一切费用和给甲方造成的损失均由乙方承担，且交付期限不予顺延。

乙方交付标的不符合本合同约定、未通过甲方验收而返工或整改造成的工期延长，视

为乙方违约，按照迟延交付标的承担违约责任。

1.8 违约责任

1.8.1 除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式交付标的，那么甲方可要求乙方支付违约金，违约金按每迟延交付标的一日的应交付而未交付标的价格的万分之一计算，最高限额为本合同总价的 3 %；

1.8.2 除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的 万分之一 计算，最高限额为本合同总价的 1 %；

1.8.3 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，或者任何一方有腐败行为（即：提供或给予或接受或索取任何财物或其他好处或者采取其他不正当手段影响对方当事人在合同签订、履行过程中的行为）或者欺诈行为（即：以谎报事实或者隐瞒真相的方法来影响对方当事人在合同签订、履行过程中的行为）的，对方当事人可以书面通知违约方解除本合同；

1.8.4 任何一方按照前述约定要求违约方支付违约金的同时，仍有权要求违约方继续履行合同、采取补救措施，并有权按照己方实际损失情况要求违约方赔偿损失；任何一方按照前述约定要求解除本合同的同时，仍有权要求违约方支付违约金和按照己方实际损失情况要求违约方赔偿损失；且守约方行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

1.8.5 除前述约定外，除不可抗力外，任何一方未能履行本合同约定的义务，对方当事人均有权要求继续履行、采取补救措施或者赔偿损失等，且对方当事人行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

1.9 知识产权

乙方保证，对于其提供的软件系统拥有知识产权或已获得权利人的授权，本项目使用乙方提供的软件不会侵犯第三方的合法权益，否则乙方应当负责处理索赔或涉诉等各项事宜，造成甲方损失的，乙方还应当承担赔偿责任。

1.10 合同争议的解决

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，任何一方均可以向甲方所在地有管辖权的人民法院提起诉讼。

1.11 网络安全相关条款

(一)基本安全要求

1.11.1 乙方应针对本项目设置安全负责人岗位，全面负责和管理本项目的网络安全相关工作。

1.11.2 乙方应严格审核二级供应商安全资质，建立动态风险评估及替代方案，对二级供应商导致的安全风险承担连带责任，

1.11.3 集成系统设计、实施至废止的全流程，须嵌入安全管控节点，设计方案要遵守适用的法律法规和行业标准，系统上线前须完成安全检测，废止时确保数据不可恢复。

1.11.4 乙方应与甲方签订保密协议，明确系统集成过程中接触的敏感信息的保密责任。

1.11.5 乙方应对参与项目的服务人员进行安全保密教育,因乙方人员违规泄露信息导致的法律责任由乙方承担。

1.11.6 乙方应配合甲方对其开展远程检测和现场检查。

1.12 集成实施

1.12.1 乙方应制定详尽的故障恢复和灾难恢复计划，包括数据备份策略、备用系统配置等，并定期进行测试演练，确保能够及时响应突发事件。

1.12.2 乙方应定期对集成系统进行安全补丁更新和系统升级。

1.12.3 乙方应在实施阶段定期使用相关安全工具对集成系统进行安全漏洞扫描并记录存在的安全漏洞。

1.12.4 乙方应对实施阶段发现的漏洞和安全隐患制定修复计划，征得甲方同意后，按照计划进行修复。

1.12.5 乙方应充分熟悉集成系统中所使用的组件或者产品的知识产权，对知识产权进行规范管理，防止侵权。

1.12.6 乙方应及时提供交付环节变化的通报，以及相关的交付途径安全性分析报告，并对可能造成严重后果的变化快速采取补救措施。

1.12.7 乙方应在甲乙双方约定的质保期或者过渡期内对实施过程中引入的安全漏洞进行修复。

1.12.8 乙方应明确集成系统安全交付条件为满足法律法规、标准规范和甲方需求，禁止开启无关功能、捆绑无关软件等交付约定范围外的内容。

1.12.9 乙方应制定详细的部署计划和流程，包括但不限于完善的回滚机制和必要的初始化机制，并定期进行部署演练。

1.12.10 乙方在部暑完成后应协助甲方对集成系统的功能和稳定性进行测试和监控。

1.12.11 在集成系统上线前，乙方应使用安全检测工具进行扫描检测，确保所有高危及以上的漏洞和安全隐患均已被有效修复，并向甲方提供漏洞修复后的检测报告。

1.12.12 乙方应在部署新系统或者进行系统更新前为甲方提供必要的安全培训和演练。

1.12.13 涉及软件废止环节的，乙方应负责开展软件卸载、停用及数据备份、迁移以及销毁工作。

1.13 集成设计

1.13.1 乙方应确保集成系统的设计方案符合甲方的总体业务目标和项目目标。

1.13.2 乙方应在集成设计阶段进行安全风险评估工作，对集成系统中可能出现的安全威胁和漏洞进行评估，并向甲方提供评估材料。

1.13.3 乙方应确保集成设计方案在整个软件生命周期内都遵守适用的法律法规和行业标准。

1.13.4 乙方在设计过程中应考虑集成系统各单元模块的权限安全，确保每个模块只被授予满足其基本功能需求的最小权限。

1.13.5 乙方在设计过程中应考虑用户权限，合理限定每个应用和用户的权限范围和有效时间。

1.13.6 乙方在设计中应对集成系统的敏感数据加密传输和存储。

1.13.7 乙方应要求二级供应商在开发交付产品时明确说明并提供所有必要的接口和功能，包括但不限于 API 文档、数据格式、调用方式等。

1.13.8 乙方应设计接口访问控制规则，确保经过身份认证和权限认证的用户才能访问相应的接口。

1.13.9 乙方在设计过程中应考虑为集成系统配备威胁防护措施，以防止恶意软件和其他侵入威胁。

1.13.10 乙方设计中存在密钥相关功能的，应有完整的密钥管理模块，该模块包括密钥的生成、存储、分发、更新、吊销等环节。

1.13.11 乙方在设计过程中应考虑系统参数和配置信息的监控审计机制，及时发现并应对异常行为。

1.13.12 乙方在设计中应考虑日志和安全事件管理机制，收集系统和网络设备的日志并建立快速响应机制应对威胁。

1.13.13 乙方在设计中应考虑软件废止的相关管理机制，包括但不限于数据备份迁移策

略和数据清理方法等。

1.13.14 乙方应编制详细的安全需求文档，明确列出集成建设的核心安全目标和参与集成建设的二级供应商必须具备的安全能力和资质。

1.14 集成管理

1.14.1 乙方应定期同步集成建设过程中的信息，包括需求变更、实施进度、风险评估和后续计划等。

1.14.2 乙方应建立文档版本管理制度，整理所有集成项目相关的文档资料和记录系统历次的更新操作，保证所有操作可溯源。

1.14.3 乙方应确保集成管理中有完善的变更流程，并建立变更的申报和审批控制程序。经甲方同意后，确保服务变更以受控的方式得到评估、批准和实施。

1.14.4. 乙方应定期更新集成系统的应急响应计划，并建立安全监控机制，对安全事件进行实时监测和响应，包括安全漏洞和即将到期或者超过授权、维保期限的软件或者组件。

1.14.5 在发生突发事件时，乙方应在双方约定的时间范围内恢复服务。

1.14.6 乙方应明确运维人员的访问权限级别，对其访问范围和授权期限进行严格控制。

1.14.7 乙方应建立并执行离职离岗人员的制度，包括账号、权限、材料等交接、清理。

1.14.8 乙方应确保与其合作的所有分包商都承担相应的安全义务，并对分包商可能带来的安全风险承担连带责任。

1.14.9 乙方应对集成系统内的所有子系统和应用进行核查，确保二级供应商所采用的安全政策和程序符合集成系统的安全策略。

1.14.10 乙方应保证建设的集成系统通过权威的供应链安全检测机构的检测认证。

1.14.11 乙方应识别和评估与二级供应商相关的所有潜在风险，并针对供应链安全风险较高或者未整改风险的供应商采取额外的监控和审查措施。

1.14.12 发现乙方提供的产品或者服务存在安全漏洞的情况时，乙方应及时组织技术团队对安全漏洞进行修补，并在确认修补方案后，向甲方提供修补计划。乙方还应提供必要的技术支持，包括但不限于远程协助和现场服务等，确保甲方系统能够尽快恢复正常运行，且漏洞得到妥善解决。

1.14.13 乙方应定期对安全测试工具进行评估和更新，确保能够有效地识别到最新的安全威胁和漏洞。

1.14.14 在乙方无法履行其责任义务或者由于其他不可抗力无法继续履行责任义务的情况下，甲方有权直接与二级供应商沟通，在本项目中行使乙方与二级供应商约定的权利。

1.14.15 乙方应对集成建设系统进行周期性安全评估，确保符合现行法律、法规和行业标准，并记录合规性要求。

1.14.16 乙方应建立持续的风险监测机制，定期审查和评估集成系统的风险状态和现有风险处置应对措施的有效性。

1.14.17 乙方应定期评估二级供应商的安全事件应对能力和供应产品的安全性，确保供应产品符合安全政策。

1.14.18 乙方应定期审查和更新集成系统的安全架构，评估现有安全架构的健壮性，并采取必要的改进措施。

1.14.19 乙方应定期审查所需硬件在仓储和物流过程中安全措施的有效性，并根据需要进行调整。

1.15 人员操作

1.15.1 “人员操作”是指乙方服务人员在本服务中的现场及远程技术行为，包括但不限于上机操作、运行自动化脚本、应用安全测试、漏洞扫描测试、渗透测试以及接入测试设备等。

1.15.2 在本服务中，甲方应对服务人员实施最小权限原则，确保乙方服务人员仅拥有完成任务所需的访问权限。

1.15.3 本服务中所包含的运营、运维的信息系统、应用、数据库等，乙方开通相关账号、权限等必须经过甲方审批允许，不得私开账号、擅自更改权限等。

1.15.4 乙方应合理使用操作账号，本服务中严禁存在多名人员（2 人及以上）共用一个操作账号的情形，同时操作账号应采用高强度的口令，乙方应妥善保管口令并定期（每月至少一次）更新账号口令，不得在电脑终端桌面存放账号口令信息。

注：高强度口令应满足以下基本条件：

1）口令长度至少为 8 位；

2）包含大小写字母、数字和特殊符号的组合，例如@#$%^&*()_+；

3）避免使用连续的某个字符（如 AAAAAAAA）或者重复某些字符的组合（如 abcdabcd）；

4）避免使用姓名、手机号、生日等个人信息作为口令，包括父母、子女和配偶的姓名和出生日期、纪念日期等。

1.15.5 未经甲方允许，乙方不得对服务资源私开端口，不得利用服务资源进行与本服务无关的工作，不得将公安网络和互联网私自打通。

1.15.6 乙方派驻的服务人员应按照甲方要求办理入场、离场等手续，并且遵守甲方劳

动、工作纪律、安全管理制度和保密制度，并按照甲方要求的工作时间进行出勤。

1.15.7 在乙方服务人员进行上机操作时，须由甲方调取数据，服务人员读数据，操作结束后双方复核签字确认。

1.15.8 在本服务中需要在甲方真实网络及业务环境中运行自动化脚本前，须经甲方审核脚本对系统的影响，待审核通过后，乙方方可实施，且在操作结束后双方复核签字确认。

1.15.9 乙方在本服务中进行应用安全测试时如需分配高权限账户，甲方必须在场监督，操作结束后双方复核签字确认。

1.15.10 乙方在本服务中进行漏洞扫描测试时，须填写《漏洞扫描申请单》，不得进行拒绝服务和溢出等对系统影响的测试，并对应用状态进行监控，操作结束后复核签字确认。

1.15.11 乙方在本服务中进行渗透测试时，不得进行对系统正常运行有影响的测试，不得留后门和木马，并提前通知甲方进行相关数据备份和系统状态监控，操作结束后复核签字确认。

1.15.12 乙方在本服务中需接入测试工具时，须制定详细接入方案，由甲方审核，接入时由甲方指定人员监督，操作结束后复核签字确认。

1.16 其他

乙方应按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《网络数据安全管理条例》《关键信息基础设施安全保护条例》《商用密码管理条例》等法律法规及规章制度的要求，履行网络和数据安全保护义务。

1.17 送达条款

本合同联系方式和联系信息适用于双方往来联系、书面文件送达及争议解决时法律文书送达。因联系方式和联系信息错误而无法直接送达的自交邮后第 7 日视为送达。双方指定联系地址与联系方式如下：

甲方联系人：刘鹏，联系电话：13273822599，联系地址：睢阳区神火大道 128 号，邮编：476000，电子邮箱：/。

乙方联系人：吴童，联系电话：18856030056，联系地址：郑州市金水区文化路街道经三路 68 号 2 号楼招商银行大厦 6 楼，邮编：450000，电子邮箱：18856030056@139.com。

1.18 合同生效

1.18.1、本合同未尽事宜，双方另行补充。

1.18.2、本合同一式三份，甲方持两份，乙方持一份，甲、乙双方法定代表人或授权代

表签字并加盖单位公章或者合同章后生效。

甲方： 商丘市公安局（盖章）

法定代表人或授权代表（签字）：

日期：2026.1.5

乙方： 中移系统集成有限公司（盖章）

法定代表人或授权代表（签字）：

日期：2026.1.5

附件一《采购清单明细表》

序号	名称	品牌、型号和规格	数量	单位	产地	制造商名称	单价	总价
1	服务器（微服务集群）	华启智慧科、DH-RS2297、配置 2 颗处理器，单颗处理器主频 2.2GHz，单颗处理器核心数 24	3	台	浙江	浙江华启智慧科技有限公司	100000	300000
2	服务器（fastDFS 集群）	华启智慧科、DH-RS2297、配置 2 颗处理器，单颗处理器主频 2.5GHz，单颗处理器核心数 16	2	台	浙江	浙江华启智慧科技有限公司	65200	130400
3	服务器（跨网交换）	浪潮、CS5260H2、配置 2 颗处理器，单颗处理器主频 2.5GHz，单颗处理器核心数 16	4	台	山东	浪潮（山东）计算机科技有限公司	60500	242000
4	存储（虚拟化）	华为、OceanStor5210、2U 盘控一体架构	1	台	东莞	华为技术有限公司	199700	199700
5	服务器（数据库节点服务	H3C、UniServer R4930 G5、配置 2 颗处理器，单颗处理器主频 2.2GHz，单颗处理器核心数 32	2	台	杭州	新华三技术有限公司	120000	240000
6	存储（数据库存储）	华为、OceanStor5210、2U 盘控一体架构	1	台	东莞	华为技术有限公司	216000	216000
7	业务网交换机	华为、S6730-S24X6Q、交换容量	1	台	杭州	华为技术有限公司	30800	30800

序号	名称	品牌、型号和规格	数量	单位	产地	制造商名称	单价	总价
		2.5Tbps，包转发率 1200Mpps						
8	存储交换机	联想、DB610S、24端口激活数,24个32Gb多模光模块	1	台	北京	联想中国	120000	120000
9	车驾管音视频应用管理	无锡华通、车驾管音视频引用管理系统、支持接入支持GB/T28181 协议标准的所有视频共享平台或视频联	2	套	无锡	无锡华通智能交通技术开发有限公司	250000	500000
10	下一代防火墙	迪普、FW1000、千兆电口16个，万兆光口16个，100G光口2个，2个扩展槽，双交流电源，高度1U	1	台	杭州	杭州迪普科技股份有限公司	120600	120600
11	堡垒机	迪普、运维审计管理平台、千兆电口6个，扩展槽2个，硬盘4T，高度2U，USB接口2个，Console 口1个，1+1冗余电源，单电源350w；	1	台	杭州	杭州迪普科技股份有限公司	60000	60000
12	网络交换机	华为、S6730-S24X6Q、交换容量2.5Tbps，包转发率1200Mpps	4	台	杭州	华为技术有限公司	30800	123200
13	虚拟化软件	华为、FusionComputer、虚拟化支持双架构部署，可通过一套平台对	1	台	东莞	华为技术有限公司	110800	110800

序号	名称	品牌、型号和规格	数量	单位	产地	制造商名称	单价	总价
		x86、C86及ARM架构服务器进行统一管理						
14	终端 Ukey	无锡华通、智能密码钥匙（USB KEY）、采用国产安全芯片，内置SM1. SM2、SM3、 SM4等国密算法	30	个	无锡	无锡华通智能交通技术开发有限公司	150	4500
15	国产化应用程序适配管理服务平台	国产终端应用适配系统/怀讯、客户端支持国产终端电脑（ARM、AMD、Mips架构）；支持国产操作系统，包含300个客户端	1	套	河南	河南怀讯信息技术有限公司	145000	145000
16	系统集成（业务迁移服务、业务数据迁移服务、利旧设备的融入）	定制	1	项	河南	中移系统集成有限公司	50000	50000
17	运维驻场服务	定制	1	项	河南	中移系统集成有限公司	60000	60000
总计：							2653000.00	