政府采购合同

需方：延津县公安局

供方：中国移动通信集团河南有限公司新乡分公司

签署日期：2026 年 2 月 26 日

需方（采购人全称）：延津县公安局

供方（中标供应商全称）：中国移动通信集团河南有限公司新乡分公司

供方持中标/成交通知书，根据采购文件、供方的投标/报价等文件[项目编号：延交财谈判采购【2026】001 号（延津竞谈-2026-1）]，按照《政府采购法》、《民法典》等有关法律、法规，供需双方经协商一致，达成以下合同条款：

一、本合同名称：延津县公安局专线电路租用项目合同 。

二、本合同含税总价为人民币 1030440 元（大写：壹佰零叁万零肆佰肆拾元整），税率 6%。

服务范围、技术规格、及分项价格如下（单位：人民币元）：

序号	电路名称	电路类型	技术参数	合约期（月）	数量（条）	单价	小计	备注
1	[redacted]							
2								
3								
4								
5								
投标总价	大写：壹佰零叁万零肆佰肆拾元整 小写：1030440.00 元							

三、质量要求及供方对质量负责条件和期限：

所供服务必须首先符合有关国家强制性规定、国家（行业）标准或相关法律法规要求，同时符合采购文件规定的质量要求，供方保证全部按照合同规定的时间和方式向需方提供服务，并负责可能的弥补缺陷。需方对服务质量有异议的应在 15 日内以书面形式向供方提出，提出异议的期限为 180 日。

四、服务承诺：

1、成交供应商为每个线路接入点位提供网络接入设备。在合同期内，由成交供应商免费负责对所提供的网络接入设备进行维修和更换，确保通信网络畅通。

2、新装电路具备资源的1个工作日开通，不具备线路资源的，7个工作日开通。

3、所有网络故障7*24小时专人处理，确保做到30分钟内响应，6小时内解决完毕并恢复正常通信（中断原因为不可抗力的除外）。

4、每季度对453条数据专线进行抽检，抽检数量不低于总线路的10%，每季度形成总体运行情况（含抽检情况）报告提交延津县公安局。

5、本次租赁服务合同期限结束，如重新招标、服务模式调整等，本次中标服务方需免费免责留出下次招标、交接等延展期，免费免责提供30天的服务，确保系统在招标、交接等过渡期内持续稳定运行，避免因服务中断导致系统停摆，影响社会治安综合治理。延展期服务内容需与本次租赁服务合同保持一致。

6、服务机构名称、地址及联系方式：中国移动通信集团河南有限公司新乡分公司，新乡市新中大道中666号，联系人司晶宁，联系电话18837330377。

7、其他服务承诺：按采购文件及响应文件中相应条款执行。响应文件中项目实施方案与服务承诺理解有歧义的，以服务承诺为准。

五、合同履行地点及进度：

供方自本项目采购合同签订之日起7个工作日按需方要求在（需方指定的地点）完成本项目的安装、调试。履约服务期限2年：2026年3月1日至2028年2月28日。

六、供方在服务期间应向需方提供相关说明、合格证书及其它相关资料，否则按不能完成。

七、人员培训：

供方免费对需方人员进行技术培训，直到需方人员熟练操作或掌握为准。

培训地点：延津县公安局指定会议室（理论）及中心机房（实操）。

培训时间：本项目计划在合同签订后的30天内，分批次完成对所有相关人员的培训，确保不影响延津县公安局日常工作的正常开展，每期培训为期1天。

培训方式：按采购文件及响应文件相应条款执行；

培训时间、地点、方式需方有权根据工作需要进行调整。

八、验收要求。

1、供方履约完毕及时向需方提出验收申请。

2、需方在收到供方验收申请后5个工作日内组织验收。需方成立3人以上验收工作组（合同金额在50万以上的验收工作组不少于5人），按照采购文件规定、中标供应商响应文件承诺，及国家有关规定认真组织验收工作。大型或者复杂的政府采购项目以及需方认为必要的项目，应当邀请国家认可的质量检测机构参加验收工作。如本项目属国家规定的强制性检测项目，需方必须委托国家认可的专业检测机构验收，检测费由供方承担。

3、验收合格后10日内，需方出具《政府采购验收报告》，由质量检测机构负责验收的，还应出具合法的检测报告。

九、付款程序、方式及期限：

1、供方开具以需方单位名称为抬头的增值税普通发票，发票税率6%。

2、付款方式：合同期内按季度支付，每季度支付一次（按成交金额除以8即为每季度支付费用），共分8次支付完毕，经验收合格，每季度初支付中标方上季度专线线路租用服务费用。本条约定的付款期限为财政资金支付的一般期限，如因财政支付流程原因导致的付款迟延，甲方不承担违约责任，但甲方负有财政支付流程的发起义务。

十、违约责任：

供方所交付的网络线路服务不符合国家规定标准及合同要求的，或者供方不能提供服务的，供方应向需方支付合同金额总值0.1%的违约金，该违约金不足以弥补需方损失的，供方应另行赔偿。如供方拒不履行，需方有权解除合同。供方如逾期完成的，每逾期一日供方应向需方支付合同金额的0.1%的违约金。

需方在合同约定内无正当理由拒收服务，需方应向供方偿付部分款项总额0.1%的违约金，需方如逾期付款的，每逾期付款一日的需方应向供方偿付所欠合同金额0.1%的违约金。本条约定的付款期限为财政资金支付的一般期限，如因财政支付流程原因导致的付款迟延，甲方不承担违约责任，但甲方负有财政支付流程的发起义务。

供需双方履行合同期内,因租赁网络线路使用的特殊性,供方因其他原因需线路停摆的应书面通知需方,需方应采取应急措施,经双方书面同意的情况下方可线路停摆.非因自然灾害或线路故障供需双方不得单方面进行线路停摆或接受服务,违约方每次应向对方偿付合同额度总值0.1%的违约金.

十一、供需双方应严格遵守采购文件要求，如有违反，按采购文件的规定处理。

十二、因服务的质量问题发生争议，由新乡市法定的质量检测机构进行质量检测或鉴定。

十三、项目采购文件及其修改和澄清、及供方响应文件、供方在投标中的有关承诺及声明均为本合同的组成部分。

十四、本合同签订和履行适用中华人民共和国法律，因履行合同发生的争议，由供需双方友好协商解决，如协商不成的，任何一方均可向签订合同地延津县人民法院提起诉讼。

十五、本合同未尽事宜，供需双方可签订补充协议，与本合同具有同等法律效力，但不能违反采购文件及供方的投标或报价文件所规定的实质性条款。

十六、知识产权： 供方须保障需方在使用该项目或其任何一部分时不受到第三方关于侵犯专利权、商标权或工业设计权的指控。如果任何第三方提出侵权指控，供方须与第三方交涉并承担可能发生的一切费用。如需方因此而遭致损失的，供方应赔偿该损失。

十七、合同生效、备案及其它

1、本合同经双方代表签字并加盖公章或合同专用章后生效。

2、本合同一式陆份，供方持两份，需方持肆份。

十八、通知与送达

本合同履行过程中，一方向对方发出的通知、函件、法律文书等，应以书面形式送达以下地址。一方变更地址的，应在变更后 3 日内书面通知对方，否则对方按原地址寄送即视为有效送达。

需方地址：【延津县平安大道西段】，联系人：【左美菊】，电话：【13938767007】；

供方地址：【新乡市新中大道 666 号】，联系人：【司晶宁 】，电话：【18837330377】。

十九、合同变更

对本合同的任何修改、补充或变更，均须由双方协商一致并订立书面协议，经双方授权代表签字并加盖公章或合同专用章后方为有效。

二十、保密

双方应对在订立和履行合同过程中知悉的对方未公开的技术信息、经营信息等商业秘密以及其他未公开的信息承担保密义务。未经对方书面同意，任何一方不得向任何第三方泄露，但法律法规另有规定或监管机构另有要求的除外。本保密义务不因合同的变更、解除或终止而失效。

二十一、合同终止后义务

本合同终止或解除后，供方应在【 7】日内向需方移交与服务相关的全部技术资料、运行日志等文件。本合同中关于保密、知识产权、争议解决等具有延续效力的条款，不因合同终止而失效。

附件： 《网络安全相关要求》

需方（印章）：延津县公安局

地址：延津县平安大道西段地址：

法定代表人或授权委托人

（签字）：

电话：

联系人：

开户银行：

账号：

供方（印章）：中国移动通信集团河南有限公司新乡分公司

地址：新乡市红旗区新中大道666号

法定代表人或授权委托人

（签字）：

电话：18837330377

联系人：司晶宁

开户银行：工行新乡平原路支行

账号：1704020529021039568

签约时间：　年　月　日

签约地址：河南省延津县

附件2：网络安全相关要求

（一）基本安全要求

1.1 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。

1.2 乙方须承诺在本服务中所使用的服务工具满足以下供应链安全管理要求：

a）服务工具具备一定的安全性，有资质证明或者甲方认可，不存在已知安全问题；

b）服务工具应在《网络关键设备和网络安全专用产品目录》中并通过认证；

c）服务工具的版权合法且授权在有效期内，运行状态良好；

d）服务工具均有对应的详细使用方法，并已对工具使用人员进行技术培训；

e）定期检验服务工具的安全性，包括对工具进行杀毒、对工具产生的网络流量进行分析等，避免工具存在有害功能，以及隐蔽的链接、协议或者端口；

f）密切关注服务工具及其组件的安全漏洞公告和相关信息，在发现漏洞被披露时，第一时间评估漏洞的影响，采取更新补丁、下线工具等措施，以确保此类安全漏洞不影响服务涉及的系统或者平台。

1.3 乙方须承诺参与本服务中的相关人员满足以下供应链安全管理要求：

a）服务项目负责人须具备2年以上相关经验；

b）服务人员能够理解和应用相关的法律法规、政策和标准；

c）服务人员满足《信息安全技术 网络安全从业人员能力基本要求》（GB/T 42446）中关于网络安全运营类人员的要求；

d）服务人员已接受岗前培训并经考核评定合格后上岗；

e）已与服务人员签订保密协议，约定服务项目实施中的通用保密要求，并会定期进行安全保密教育。

1.4 在本服务中，乙方应持续关注安全领域的技术动态和威胁情报，保持服务技术的先进性。

1.5 在本服务中，甲方应定期对服务技术进行评估和升级，不断更新和优化服务工具和服务方案，以确保服务的安全性和有效性。

1.6 在本服务中，乙方应深入调研甲方现状和需求，提出可行性高的服务建议并提供定制化的安全服务方案。

1.7 乙方应配合甲方对其开展的远程检测和现场检查。

（二）信息防泄露

2.1 “信息防泄露”是指在本服务中防止与甲方相关的敏感信息、保密信息或者未公开的信息在未经授权的情况下被透露、传播或者获取，包括但不限于个人身份信息、网络拓扑、系统/软件信息、知识产权、技术方案等电子及纸质材料。

2.2 乙方须将涉及服务内容的U盘等存储设备进行加密处理。

2.3 禁止乙方在本服务中将涉及服务内容的纸质材料带出甲方指定服务场地，如需带出，须向甲方申请（材料类型、使用时间、使用目的、归还时间、责任人），批准后方可带出场地。

2.4 乙方应当采取技术措施和其他必要措施，确保其网络和数据安全，防止出现信息泄露、毁损、丢失等风险。在发生或者可能发生信息泄露、毁损、丢失等情况时，应当立即采取补救措施，并将相关情况及时告知甲方。

2.5 甲方有权利对乙方服务人员的身份背景进行安全审查，包括但不限于主合同要求具备的学历、学位、专业资质证书和过往工作经验要求以及安全保密协议签字等方面内容，乙方须配合提供与本服务相关的证明审查材料，存在泄密风险的乙方服务人员不得参与本服务。

2.6 本服务所涉及的乙方服务人员均须与甲方签订保密协议，乙方应做好人员安全保密教育工作，因服务人员违规恶意泄露敏感信息，所产生的相关法律责任由乙方承担。

2.7 乙方在本服务中处理或者存储甲方数据时，应采用国产加密算法对数据进行加密处理，并确保数据传输过程的安全性。

（三）人员操作

3.1 “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。

3.2 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。

3.3 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。

3.4 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。

3.5 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。

3.6 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。

3.7 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。

3.8 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。

3.9 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。

3.10 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。

3.11 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。

3.12 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。

（四）第三方安全

4.1 “第三方安全”是指独立于甲乙双方的公司或者组织提供的服务、产品或者评估的安全性。

4.2 当发现所使用的第三方服务或者软件存在安全漏洞时，乙方须立即评估漏洞影响，采取更新补丁、下线工具等措施，以确保此类安全漏洞不影响本服务涉及的系统或者平台。

4.3 乙方应与可靠的第三方供应商合作，并签订明确的安全责任协议，在服务过程中明确因第三方的问题导致发生信息泄露等安全事件，甲方有权对乙方进行追责。

4.4 乙方须对所使用的第三方服务或者软件进行安全审查和定期的安全评估，建立及时更新和补丁管理流程，保证所有组件保持最新状态，确保所使用的第三方服务和组件符合甲方的安全标准。

（五）服务方案变更

5.1 “服务方案变更”是指在主合同中甲乙双方约定的服务期限、服务内容和实施计划因外界因素发生变化和调整。

5.2 在本服务中，若甲方需要变更服务方案、服务范围或者增加服务内容，造成工作量增多，应提前与乙方充分协商、考虑进度因素，适当延迟工期或者增加人力，保证服务进度。

5.3 在本服务中，乙方应提供充足的人力资源、人员备份，以应对人员工作调动等因素造成减员的影响，保证服务进度。

5.4 乙方应建立健全本服务标准化交付的流程和模板，并在服务过程中严格按照标准流程实行，减少因方案变更、范围变更、人员变动、外部因素等导致的服务进度波动。

（六）服务商变更

6.1 “服务商变更”是指甲方因成本、服务质量、技术能力等原因决定更换服务提供商。

6.2 产生服务商变更时，原服务商与新服务商需进行工作内容的交接，具体交接内容包括但不限于以下内容：

a）服务终止时，原服务商需与甲方签订数据删除协议，确保所有遗留数据被安全删除；销毁存储介质时，乙方应当邀请甲方派员到现场全程监督，并制作销毁记录，由双方签字确认。

b）服务终止时，甲方应立即变更服务账号密码，同时撤销原服务商的所有访问权限；

c）服务终止时，原服务商应立即转交涉及甲方业务和敏感数据的所有材料，包括但不限于网络拓扑、系统软件信息、实施方案、应急处置方案、服务日志、巡检报告等，并禁止备份留存和外发；

d）服务终止时，原服务商须基于甲方现状，出具运维运营与安全服务报告，详细梳理服务现状以及现存的遗留性问题及风险，并与甲方、新服务商三方开会同步，达成一致后方可退出。

（七）业务连续性

7.1 “业务连续性”是指甲方在面对突发事件、灾难或者其他中断情况下，能够持续提供关键业务和服务的能力。

7.2 在本服务中，乙方须提前制定和实施业务连续性计划和灾难恢复计划，包括数据备份和系统冗余，并测试恢复流程，确保在突发事件发生后能快速恢复业务连续性。

7.3 乙方须在甲方参与下制定应急预案，并定期组织演练测试，确保在突发事件发生时能够迅速启动应急预案，减小影响面。

（八）不可抗力

8.1 “不可抗力”指在本协议签署后发生的、本协议签署时不能预见的、其发生与后果是无法避免或者克服的、妨碍任何一方全部或者部分履约的所有事件。上述事件包括地震、台风、水灾、火灾、战争、流行病、罢工，以及根据法律认作不可抗力的其他事件。

8.2 如果发生不可抗力事件，影响一方履行其在本协议和项目合同项下的义务，则在不可抗力造成的延误期内中止履行，该遭受不可抗力的一方不承担违约责任或赔偿对方因之而产生的经济损失。

8.3 宣称发生不可抗力的一方应迅速书面通知另一方，并在其后的十五天内提供证明不可抗力发生及其持续时间的足够证据。

8.4 如果发生不可抗力事件，各方应立即互相协商，以找到公平的解决办法，并且应尽一切合理努力将不可抗力的影响减少到最低限度。

（九）应急响应

9.1 “应急响应”是指甲方在面对安全事件或者危机情况时，乙方采取的一系列计划、策略和行动，以快速、有效地识别、评估、控制和解决安全事件，从而减轻事件对甲方的影响。

9.2 乙方应建立快速应急响应机制，并根据突发事件风险等级（一级至四级）设置不同层级的应急处置预案，确保在发生安全事件时能够及时监测发现、应急处置并向甲方报告。

9.3 乙方在服务过程中涉及甲方业务系统时，应提前与甲方协调，制定详细的维护计划和变更管理

流程，最小化对甲方业务的影响。

9.4 乙方在本服务中，应实施性能监控和优化措施，确保甲方的服务水平协议得到满足。

（十）其他

10.1 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。