政府采购合同

项目名称:洛阳市老城区行政审批和政务信息管理局老城区合署办公楼网络安全改造项目

政府采购管理部门备案编号：洛老磋商采购-2024-11

招标采购文件编号：老城政采磋商新(2024)0003号

甲方合同编号:

甲方：洛阳市老城区行政审批和政务信息管理局

乙方：中国联合网络通信有限公司洛阳市分公司

甲方合同法律审核部门：

签订时间：2024年12月

洛阳市老城区行政审批和政务信息管理局（甲方）所需洛阳市老城区行政审批和政务信息管理局老城区合署办公楼网络安全改造项目(项目名称)委托东虹建设工程招标代理有限公司以 老城政采磋商新(2024)0003 号 磋商文件以竞争性磋商方式进行采购。经**磋商小组(或甲方)确定**中国联合网络通信有限公司洛阳市分公司 （乙方）为成交供应商。甲、乙双方根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法律以及本项目磋商文件的规定，经平等协商达成合同如下：

第一条 合同文件

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

1. 本项目磋商文件

2. 成交供应商响应文件

3. 乙方在投标时的书面承诺

4. 中标通知书

5. 合同补充条款说明

6. 保密协议或条款

7. 相关附件、图纸及电子版资料

第二条 合同内容

服务名称：详见合同附件中《服务一览表》。

第三条 合同金额

人民币￥ 604000元（大写： 陆拾万零肆仟元整 ）。（含税价）为人民币604000元（大写： 陆拾万零肆仟元整），本合同适用增值税税率为 6% 、13% ，不含增值税的价款为人民币 541042.24 元（大写：人民币伍拾肆万壹仟零肆拾贰元贰角肆分），增值税税款为人民币 62957.76元（大写：人民币 陆万贰仟玖佰伍拾柒元柒角陆分 ）。（分项价格详见合同服务清单）。

其中：

技术服务（含税价）为人民币 60000元（大写： 陆万元整），本合同适用增值税税率为 6% ，不含增值税的价款为人民币56603.77 元（大写：人民

币 伍万陆仟陆佰零叁元柒角柒分 ），增值税税款为人民币 3396.23元（大写：人民币 叁仟叁佰玖拾陆元贰角叁分 ）；

设备融资租赁（含税价）为人民币 492280元（大写： 肆拾玖万贰仟贰佰捌拾元整），本合同适用增值税税率为 13% ，不含增值税的价款为人民币 435646.02 元（大写：人民币 肆拾叁万伍仟陆佰肆拾陆元零贰分），增值税税款为人民币 56633.98元（大写：人民币 伍万陆仟陆佰叁拾叁元玖角捌分 ）；

集成服务（含税价）为人民币 51720元（大写： 伍万壹仟柒佰贰拾元整），本合同适用增值税税率为 6% ，不含增值税的价款为人民币 48792.45元（大写：人民币肆万捌仟柒佰玖拾贰元肆角伍分 ），增值税税款为人民币 2927.55元（大写：人民币 贰仟玖佰贰拾柒元伍角伍分 ）。

第四条 权利义务和质量保证

1.甲方保证服务期间，对乙方工作给予支持，提供水、电、场地等必须的基础工作条件。如乙方有需要，还应提供履行合同所必需的有关图纸、数据、资料等。没有甲方事先同意，乙方不得将甲方资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围内。

2.乙方保证所提供的服务或其任何一部分均不会侵犯任何第二方的专利权商标权或著作权。一旦出现侵权，索赔或诉讼，乙方应承担全部责任。乙方保证服务不存在危及人身及财产安全的隐患，不存在违反国家法规、法令、法律以及行业规范所要求的有关安全条款否则应承担全部法律责任。

3、乙方负责在货物质保及技术运维支持服务期间的安全服务，对造成的网络安全事件承担全部责任。

4、乙方应积极配合甲方完成老城区合署办公大楼的网络安全等级保护二级的测评工作。

5、乙方应将施工中设计的图纸、数据、配置、资料等提供给甲方，以便甲方后续工作。

第五条 付款方式

1.本合同项下所有款项均以人民币支付。

2.乙方向甲方提供下列文件材料，经甲方审核无误后支付：

（1）经甲方确认的发票。

（2）其他材料。

3.款项的支付进度以招标采购文件的有关规定为准。如招标采购文件未作特别规定，则付款进度应符合如下约定：

（1）双方合同签订后硬件设备送达现场，安装、调试到位、验收合格后支付合同价款总额的 50%，即￥ 302000 元（大写： 叁拾万零贰仟元整 ）。（含税价）

（2）系统改造完成，运行正常后支付至合同总价的 100%。即付款至￥ 604000元（大写： 陆拾万零肆仟元整）。（含税价）

乙方收款账户如下：

合同乙方：中国联合网络通信有限公司洛阳市分公司

开户名称:中国联合网络通信有限公司洛阳市分公司

开 户 行:工行洛阳分行

帐号:1705020119021021996

第六条 履约保证金

按照洛阳市财政局洛财购〔2021〕10 号文件《关于进一步降低企业交易成本优化营商环境的通知》要求，本项目免收履约保证金。

第七条 项目管理服务

乙方要指定不少于 1 人全权全程负责本项目的商务服务，以及服务的落实、咨询、执行等后续工作。

项目负责人姓名： 周玉利 联系电话：15637901770

第八条 分包

除招标文件事先说明、且经甲方事先书面同意外，乙方不得分包、转包其应履行的合同义务。

第九条 合同的生效

1.本合同经甲乙双方授权代表签字并加盖公章或合同专用章后生效。

2. 生效后，除《政府采购法》第 49 条、第 50 条第二款规定的情形外，甲乙双方不得擅自变更、中止或终止合同。

3. 如遇政策调整或相关部门要求，导致不能按时或完全履行合同，双方免于承担责任。（注：本项目所涉及的硬件设备甲方以融资租赁方式获得使用权，设备融资租赁期限 为12 个月，租赁期间自本项目竣工验收之日起算。租赁期内，设备所有权归属乙方所有，甲方只有使用权，甲方不得在租赁期内对租赁设备进行销售、转让、转租、分租、抵押、投资或采取其他任何侵犯租赁设备所有权的行为。否则，甲方应赔偿由此给乙方造成的损失。租赁期满后，设备所有权归属甲方，租赁期起始日期以甲乙双方签订合同日期为准。租赁期满，设备所有权转移给甲方。）

第十二条 违约责任

1、除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式履行，甲方可要求乙方支付违约金，违约金按每迟延履行一日的应提供而未提供服务（或货物）本合同价格的 1‰计算，最高限额为本合同总价的 5‰；迟延履行的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

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，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 1‰计算，最高限额为本合同总价的 5‰；迟延付款的违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；

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来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；

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；

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；

6、 如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响中标结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

第十三条 不可抗力

甲、乙方中任何一方，因不可抗力不能按时或完全履行合同的，应及时通知对方，并在 15 个工作日内提供相应证明。未履行完合同部分是否继续履行、如何履行等问题，可由双方初步协商，并向主管部门和政府采购管理部门报告。确定为不可抗力原因造成的损失，免予承担责任。

第十四条 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，可以选择向 洛阳市老城区 人民法院起诉。

第十五条 合同生效

本合同经甲乙双方签字盖章之日起生效，合同有效期 38 个月。

第十六条 合同保存

本合同一式 四 份，甲方 二 份，乙方 二 份。

甲　　方：洛阳市老城区行政
审批和政务信息管理局

单位名称(公章)：

法定代表人/负责人
或授权代理人：（签字或盖章）

签订日期：2024 年 12 月 31 日

乙　　方：中国移动通信有
限公司洛阳市分公司

单位名称(公章)：

法定代表人/负责人
或授权代理人：（签字或盖章）

签订日期：2024 年 12 月 31 日

附件：项目清单（元）

序号	服务名称	服务内容	单位	数量	单价	总金额
1	防火墙	提供防火墙服务实现网络层安全访问控制防护，实现多区域的安全访问控制、入侵检测、病毒的扫描检测，防范非法访问行为和恶意攻击行为等安全威胁。 参考技术服务标准： 1.标准机架设备，冗余电源，CON口≥1个，USB3.0口≥1个，千兆电口≥10个，千兆光口≥6个，另具备不少于2个接口扩展板卡插槽； 2.防火墙吞吐量≥18Gbps，最大并发会话数≥700万，每秒新建会话≥13万； 3.防火墙要求采用下一代防火墙系统； 4.支持多操作系统，可在WEB界面上配置系统A/系统B/备份系统启动顺序； 5.支持虚拟路由器功能，可以划分出多个虚拟路由器，每个虚拟路由中拥有独立的路由表，实现不同区域的路由隔离；支持多路由系统，可以把其它路由系统中的路由条目引入到当前路由系统中进行使用； 6.支持主流ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD攻击防护，采用专业高效攻击防护算法，非采用简单的阈值进行攻击防护； 7.具有垃圾邮件过滤功能，能够通过黑白名单、关键字过滤、敏感参数限制等方式保护服务器的稳定运行； 系统支持Flood防护阈值学习功能，通过统计各种正常业务流量数据，进行检测阈值的智能学习，得到各种攻击流量类型对应的合理阈值，为攻击检测阈值提供合理参考。	套	2	41980	83960
2	日志审计系统	提供日志审计服务能够全面详实地记录网络内流经监听出口的各种网络行为，并根据国家有关法规规定保存至少180天，以便进行事后的审计和分析。 参考技术服务标准： 1.标准机架设备，有效存储容量≥2T，SSD系统盘≥32G，CON口≥1个，USB口≥1个，千兆电口≥6个，千兆光口≥2个，另具备不少于2个接口扩展板卡插槽； 2.事件处理性能≥3000EPS，配置接入≥30个； 3.通过SSL加密对数据传输等进行处理、采用B/S架构，HTTPS访问。支持集中、分布、集群部署。 4.日志审计对象操作系统支持：Linux、Windows、Window server、Uinx 等主流操作系统；数据库支持：Oracle、MySQL SQLServer 等主流数据库；应用系统支持：如	套	2	38590	77180

		Apache、Tomcat、IIS、weblogic 等。 5.内置标准化策略达到800种以上。支持通过标准化策略统一日志格式，标准化字段多达90个字段。 6.系统内置丰富关联/审计类告警策略，并灵活支持自定义策略。支持告警响应联动本次投标防火墙设备。 7.系统的标准化策略具备良好的可扩展性，可通过配置文件或界面实现管理功能。 8.系统需具有归并技术，安全事件收集代理会在一段时间内比较收到的安全事件，如果安全事件相同，则只需发送一条安全事件，该安全事件应包括安全事件详情及该安全事件发生的次数。 9.支持专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询。 10.支持全球地理位置库，支持外部威胁分布地图展示。系统的后端存储平台需采用高性能海量数据存储管理系统。				
3	网络安全审计系统	提供网络安全审计服务对全网经由核心交换区的信息数据进行检测，发现各种攻击企图、攻击行为或者攻击结果并进行报警。 参考技术服务标准： 1.硬件参数：标准机架设备，千兆电口≥14个（至少包含1对bypass），千兆光口≥4个，千兆管理口≥1个，硬盘≥1T。 2.性能参数：应用层吞吐≥2.8G，网络层吞吐≥9G，VPN吞吐≥1G；最大并发≥145万，每秒新建≥7万； 3.采用自主研发的多核多线程ASIC并行操作系统； 4.提供三年规则库升级服务。 5.接口实际配置支持second IP地址，每个接口要求支持至少200个second IP。 6.提供WEB防护功能，可对防盗链、CSRF攻击、CC等攻击行为进行防护。 7.支持端口扫描功能，用于直观的了解网内主机所存在的安全问题。 8.支持弱密码扫描功能，即时了解网内主机是否存在弱口令，内置弱口令库，并可自定义字典库。 9.提供威胁情报功能，支持全网威胁情报的搜索查询，可供攻击溯源，预知风险；支持威胁情报订阅，及时对突发威胁进行防护建议；支持不少于20种威胁分类，包括C&C、僵木蠕、勒索、钓鱼、垃圾邮件等。 10.提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并可在WEB界面显示检测结果；支持实时和周期性对所有安全策略进行分析。 11.支持基于邮件收件人、发件人的黑白名单自定义控制方式。	套	2	44720	89440

		支持内网资产监控，可对终端风险级别、操作系统、浏览器类型、应用、杀毒软件等方面进行监控。				
4	APT 攻击预警系统	提供网络安全审计服务对全网经由核心交换区的信息数据进行检测，发现各种攻击企图、攻击行为或者攻击结果并进行报警。 参考技术服务标准： 1.硬件参数：标准机架设备，千兆电口≥14个（至少包含1对bypass），千兆光口≥4个，千兆管理口≥1个，硬盘≥1T。 2.性能参数：应用层吞吐≥2.8G，网络层吞吐≥9G，VPN吞吐≥1G；最大并发≥145万，每秒新建≥7万； 3.采用自主研发的多核多线程ASIC并行操作系统； 4.提供三年规则库升级服务。 5.接口实际配置支持second IP地址，每个接口要求支持至少200个second IP。 6.提供WEB防护功能，可对防盗链、CSRF攻击、CC等攻击行为进行防护。 7.支持端口扫描功能，用于直观的了解网内主机所存在的安全问题。 8.支持弱密码扫描功能，即时了解网内主机是否存在弱口令，内置弱口令库，并可自定义字典库。 9.提供威胁情报功能，支持全网威胁情报的搜索查询，可供攻击溯源，预知风险；支持威胁情报订阅，及时对突发威胁进行防护建议；支持不少于20种威胁分类，包括C&C、僵木蠕、勒索、钓鱼、垃圾邮件等。 10.提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并可在WEB界面显示检测结果；支持实时和周期性对所有安全策略进行分析。 11.支持基于邮件收件人、发件人的黑白名单自定义控制方式。 支持内网资产监控，可对终端风险级别、操作系统、浏览器类型、应用、杀毒软件等方面进行监控。	套	2	34520	69040
5	柜式七氟丙烷灭火	七氟丙烷气体灭火服务主要适用于计算机房、通讯机房、配电房等场所，可用于扑救电气火灾、液体火灾或可熔化的固体火灾，它能够精确控制七氟丙烷的释放量和释放时间，从而保证灭火效果和系统的可靠性。 参考技术服务标准： 1.使用环境温度：0℃～40℃；相对湿度：≤95（40℃） 2.交流输入电压：220V ，50Hz1 3.交流输入功率：≤100W 4.直流备电：DC24V/5.0Ah,全密封免维护蓄电池 5.容量：4区（可选）；回路容量≤160点 6.DC24V电源最大输出电流：2A（瞬态输出可达3A）	套	1	6860	6860

		7.总线长度：≤1500米 8.外形尺寸：500mm×340mm×111mm				
6	钢瓶检测充装	钢瓶检测充装服务依据《气瓶安全技术监察规程》相关规定对钢瓶压力、药剂等参数进行检测，定期进行冲压、药剂补充，保障七氟丙烷灭火系统正常运行。 参考技术服务标准： 七氟丙烷灭火剂充装在气体灭火装置内提供，充装体积≥90L	套	2	5880	11760
7	等保测评服务	针对网络信息系统，按照等级保护2.0的标准开展等保测评工作，及时发现可能存在的问题，提出可行的整改方案，并协助采购人开展整改落实工作；出具公安部门认可的系统安全保护等级测评报告，依据测评报告编制整改建议方案，并协助完成整改工作；协助完成信息系统安全保护等级备案工作。	项	1	60000	60000
8	安全管理平台系统	提供安全管理平台服务对安全设备进行统一集中管理、实现全网安全态势分析、安全风险评估、集中管控。 参考技术服务标准： 1.标准机架式设备，千兆电口≥2个，千兆光口≥2个，千兆管理口≥1个，硬盘≥1T，整机性能≥20Gbps。 2.根据所辖IP设备资产与风险的重要程度关系，结合风险评估信息、脆弱性信息和资产详细信息，遵循ISO13335标准定义的资产CIA属性，按照不同种类的资产信息分类导入或登记入库，建立安全设备库，并为其他安全管理模块提供信息接口。 3.以层次分明的拓扑页面，呈现用户的网络部署情况。网络拓扑图上直观呈现管理对象的安全属性、运行状态、告警状态，可以让用户对安全设备的运行状况一目了然。支持对IP网络的设备搜索功能，自动收集网络的设备信息，支持自动设备发现功能和自动网络拓扑生成功能。 4.网络拓扑图功能支持快速定位、拓扑鸟瞰、拓扑图缩放、拓扑自动布局等功能，功能全面。 5.提供统一的策略配置下发功能。通过图形化界面配置管理网络安全设备的安全策略，系统会将策略批量下发到网络安全设备，既能保证安全策略的一致性，又可以大量减少管理员的工作强度。安全策略种类全面，涵盖入侵防护策略、病毒防护策略、安全资源定义等。支持策略模板功能，通过策略模板可以指导管理员快速完成安全策略定义，通过策略模板功能，规范了策略管理工作，使得策略管理工作变得更加流程化、规范化。 6.可以多维度呈现网络安全设备安全策略的防护是否科学合理、效果是否显著。审计分类至少包括：宽泛策略审计、冗余策略审计、乱序策略审计、交集冲突审计、策略变更审计等。	套	1	38560	38560

		7.提供设备的统一升级功能，允许用户在管理中心管理所有已发布的升级包和特征库，并自动进行统一下发。 8.系统可通过SNMP Get、Ping、Resful、远程登录等多种方式，周期性轮询安全设备的运行数据，并结合安全事件管理功能，实时监控各类管理对象的运行状态、网络流量、性能数据、告警状态。 9.用来展示全网的安全等级和安全趋势，安全等级通过仪表盘将当期时间的安全分为5级，在0-1级属于安全区，1-2级属于可控安全区，2-4级属于不安全区，在非安全区表明检测到了病毒和入侵攻击行为，管理员需要引起警惕。安全趋势以趋势图方式展示24小时的全网安全等级的上下波动情况，为管理员提供处理安全事件的效果。与此同时以柱图等图形输出网络安全设备升级与配置备份的统计信息，辅助管理员分析安全设备是否由于未升级导致出现防护漏洞。 10.按网络安全设备类型进行分类统计，使管理员可以全局掌控全网安全设备的使用情况，并统计输出各类安全设备的功能和特征库升级情况。为统筹安排网络安全设备的升级提供参考依据。 11.采用拓扑图或图表方式实时监控安全设备的实时运行情况，可即时监控设备的连通性及资源利用率，使管理员可以及时保障安全设备在全网的可用性，排除全网网络安全故障。 12.支持基于角色的分权配置管理。系统通过角色管理可将管理人员分为三类：配置管理员、安全管理员和安全审计员。				
9	网络安全应急工具箱	为常规应急响应工作提供技术支持；提供网络应急专业知识资料；辅助网络安全应急工作流程管理；提供网络安全时间处置方法和思路。建立安全管理与技术并重的长效机制，促进网络安全稳定保障。 参考技术服务标准： 1.处理器≥4核4线程，内存≥8G，硬盘容量≥450G。 2.内置的知识库体系至少包含：制度体系、基线检测、安全加固、应急指南、文档模板、标准规范、案例分析、法律法规等。 3.内置的应急工具库集合多种应急工具，至少包含WebShell查杀、专杀工具、日志采集工具、流量分析工具、主机应急分析工具等安全应急工具。 4.支持的应急全流程阶段处置至少包含处置阶段、临时处置、系统排查、日志排查、清除加固、提交阶段等。 5.能够详细记录应急处置过程中的每一个细节，至少包含检测阶段、抑制阶段、根除阶段、恢复阶段等不同阶段的内容。 6.支持病毒样本测试，至少包含gbot、lpk、murofet、	套	1	115480	115480

		ramnit、sality、sdbot、virut、zeus病毒样本。 7.内置的第三方威胁情报平台链接至少包含奇安信、360、VenusEye、绿盟、微步在线、安恒六大威胁情报平台。 8.支持对主流攻击类型进行记录、上传，至少包含勒索病毒、WebShell、挖矿木马、网页篡改、DDos攻击、数据泄露、流量劫持。 9.支持网络安全应急工具和应急知识库下载学习，满足日常应急学习培训需求。 10.具备不少于7种病毒的应急处置流程。 具备不少于7个种类的专杀工具。				
10	集成服务	确保老城区合署办公楼办公网络稳定运行，建立健全现有网络与信息安全管理体系，提升网络与信息安全防护总体水平，满足采购人业务需求。	项	1	51720	51720
合计						604000