老城区行政事业单位国有资产购入验收报告

单位章：

验收日期：2024年10月23日

项目名称	洛阳市老城区政务服务和大数据管理局 老城区电子政务外网2016升级改造项目
项目金额（元）	1320000元
验收意见	对该系统集成项目的技术服务、相关设备的安装、调试等工作，以及系统设备运行情况进行验收。 验收合格。 验收小组成员：原建梅 刘庭岐 任宇川 负责人：高燕川　　2024年10月23日
备注	

说明：此表一式两份，区国资办、单位财务各留存一份。

政府采购合同

项目名称:洛阳市老城区政务服务和大数据管理局老城区电子政务外网 IPV6 升级改造项目

政府采购管理部门备案编号：洛老磋商采购-2024-4

招标采购文件编号：老城政采磋商(2024)0014 号

甲方合同编号:

甲方：洛阳市老城区政务服务和大数据管理局

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：　　年　　月　　日

洛阳市老城区政务服务和大数据管理局（甲方）所需洛阳市老城区政务服务和大数据管理局老城区电子政务外网 IPV6 升级改造项目(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(2024)0014 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￥ 1320000 元（大写： 壹佰叁拾贰万元整 ）。（含税价）为人民币 1320000 元（大写： 壹佰叁拾贰万元整 ），本合同适用增值税税率为 6% ，不含增值税的价款为人民币 1245283.02 元（大写：人民币 壹佰贰拾肆万伍仟贰佰捌拾叁元零贰分 ），增值税税款为人民币 74716.98 元（大写：人民币 柒万肆仟柒佰壹拾陆元玖角捌分 ）。（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 1100000 元（大写： 壹佰壹拾万元整），本合同适用增值税税率为 6% ，不含增值税的价款为人民币1037735.85 元（大写：人民币 壹佰零叁万柒仟柒佰叁拾伍元捌角伍分 ），增值税税款为人民币 62264.15元（大写：人民币 陆万贰仟贰佰陆拾肆元壹角伍分 ）；

软件开发（含税价）为人民币 20000元（大写： 贰万元整），本合同适用增值税税率为 6% ，不含增值税的价款为人民币18867.92 元（大写：人民币壹万捌仟捌佰陆拾柒元玖角贰分 ），增值税税款为人民币 1132.08 元（大写：人民币 壹仟壹佰叁拾贰元零捌分 ）；

集成服务（含税价）为人民币 200000元（大写： 贰拾万元整），本合同适用增值税税率为 6% ，不含增值税的价款为人民币 188679.25 元（大写：人民币壹拾捌万捌仟陆佰柒拾玖元贰角伍分 ），增值税税款为人民币 11320.75 元（大写：人民币 壹万壹仟叁佰贰拾元柒角伍分 ）。

第四条 权利义务和质量保证

1.甲方保证服务期问，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电子政务外网 IPv6 升级改造后的二级等保测评工作。

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￥ 660000 元（大写： 陆拾陆万元整 ）。（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￥ 1320000 元（大写： 壹佰叁拾贰万元整 ）。（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：李小静 联系电话：15637902070

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。

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_ 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：洛阳市老城区政务服务和大数据管理局

单位名称(公章)：

法定代表人/负责人或授权代理人：（签字）

签订日期：

乙　　方：中国联合网络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）

签订日期：

附件：项目清单（元）

老城区电子政务外网IPV6升级改造项目清单							
序号	服务内容	数量	单价	总价	税率	不含税	税额
1	电子政务外网的规划服务:对电子政务外网进行统一的整合规划和顶层设计,规划IPv6地址在全区的应用，满足业务需求，符合国家、省、市大数据的统一规划标准，提供规划方案。	1	20000	20000	6%	18867.92	1132.08
2	边界安全防护服务:提供边界的安全防护功能。在不同的边界处部署安全边界网关设备，实现 IPv6 和IPv4 的双栈的多区域的安全访问控制、入侵检测、病毒的扫描检测。对工业互联网、智慧医疗、公共视频等业务的边界接入，达到实现三级防护标准。 参考技术服务标准： 1.标准机架式设备,提供≥4 个千兆电口，≥2 个千兆光口。 2.性能：防火墙吞吐率：≥20Gbps，并发连接数：≥500 万，达到隧道安全隔离、多区域安全隔离,达到多行业专网的专网安全隔离，符合电子政务业务要求。 3.满足全区IPv4、IPv6 双栈工作模式。满足数据隧道的加密传输,满足行业专网的隧道隔离，满足互联网、电子政务外网逻辑隔离。加密算法要求满足 SM1,SM2,SM4。 5.满足高级威胁防护能力，可对 DGA、隐蔽信道、恶意加密流量进行检测，并进行可视化展示。 6.提供策略变更信息管理功能,满足查看变更策略、变更动作、变更时间、修改人、登陆 IP,满足对变更前的策略进行直观对比，并能一键还原配置。 7.满足构建以防火墙为中心的动态防御体系，可与web 防火墙、入侵检测、EDR、防病毒网关、数据防泄漏、数据库审计、僵木蠕、漏洞扫描等产品实现协同联动。 8.满足多维度流量控制功能，满足基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。 9.满足按照攻击者视图、受害者视图和事件视图查看安全事件,获取事件原理和安全建	1	132500	132500	6%	125000.00	7500.00

	议，并能对选定安全事件进行一键处置。 10.满足基于IPv6 的应用层检测、病毒防御、入侵防御、URL 过滤、 ADS、WAF、流量控制、连接限制、文件过滤、数据过滤、邮件安全等安全控制功能。						
3	政务外网边界接入服务:广域网边界对政务外网终端访问流量进行安全检测,且满足对加密流量的安全检测，重点对僵木蠕、C&C异常、渗透攻击等异常或恶意行为进行告警，重大应急情况下可进行实时阻断。 参考技术服务标准: 1.标准机架式设备，设备满足内置CA，可为其他设备或移动用户签发证书，可生成、吊销、删除证书；满足证书链管理。 2.符合国密局制定的《SSL VPN 技术规范》，满足国家商用密码算法SM1、SM2、SM3、SM4;满足传统集群和分布式集群功能,集群能同时提供 SSL 和 IPSEC 客户端用户接入;传统集群满足状态和 Session 同步，对外提供同一接入IP;分布式集群能提供线路优选和线路备份两种接入策略。 3.满足接入主机的安全检查,包括安装的软件、进程、端口、服务、注册表、操作系统及补丁、文件、网卡等，满足接入前检查、接入后检查、定时检查等策略;满足可信接入分级授权。 4.满足GRE over IPsec 方式，满足组播穿越IPSec 隧道，满足IPv6 over IPv4，满足IPv6 地址穿越IPv4 隧道的特殊环境。 5.依照国家电子政务外网一机多用的标准的要求，做好电子政务外网和互联网、行业专网的安全隔离，提供数据加密传输服务，满足隧道解密对接,满足终端用户的透明隔离接入,满足全区电子政务外网用户的数据	1	150000	150000	6%	141509.43	8490.57

	安全透明隔离并加密传输。 6.满足静态用户名口令、数字证书、短信、硬件特征码绑定、图形码、人脸识别认证方式；满足两种或两种以上组合认证方式。 7.满足设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC 隧道状态、用户流量、安全事件、中国任意省市区县的接入用户数监控，并通过图表展示。 8.满足虚拟门户功能,满足虚拟门户中使用用户名口令、数字证书、人脸识别认证方式，满足虚拟门户双因子认证。 9.满足“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类。						
4	网络安全监测服务：提供流量检测服务，需采用专业的检测设备对电子政务外全网的网络流量进行检测，包含扫描探针攻击、缓冲区溢出攻击、拒绝服务攻击、漏洞扫描攻击、蠕虫病毒攻击、非授权访问攻击、后门木马攻击、文件漏洞攻击等常见攻击行为检测。对各种弱口令的攻击检测，对邮件件、ftp 等口令的暴力破解行为检测。 参考技术服务标准： 1.标准机架式设备，配置为≥4 个 10/100/1000BASE-T 接口,≥2个千兆光口。 2.IPS 吞吐率≥10Gbps，整机性能≥20Gbps，提供≥3 年的规则库升级服务。 3.满足多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择。 采用专业的检测探针对电子政务外全网的网络流量进行检测，包含扫描探针攻击、缓冲区溢出攻击、拒绝服务攻击、漏洞扫描攻击、蠕虫病毒攻击、非授权访问攻击、后门木马攻击、文件漏洞攻击等常见攻击行为检测。 5.对访问流量进行僵尸网络行为、木马控制行为、蠕虫活动行为、勒索病毒行为、移动端木马控制行为等多种行为检测。对被检测到的僵尸主机，进行异常行为报文取证、事件记录，包含攻击源信息、事件应用协议、事件具体行为等,在检测到僵木蠕行为的同时,会联动网络中的网关类安全设备进行联动阻断，防止病毒传播泛滥。同时对检测到	1	130000	130000	6%	122641.51	7358.49

	的安全事件进行记录并告警。 6.满足对 HTTP、FTP、SMTP、IMAP、POP3、TELNET 等服务的隐蔽通信检测，可设置相应警告、阻断动作,并可设置忽略知名应用。 7.满足IPv6、IPv6 over IPv4、IPv6 和IPv4混合网络,能够在该网络环境中检测出攻击事件。 8.满足卸载SSL，实现对HTTPS、IMAPS、SMTPS、POP3S、FTPS、RDP、 MQTT、SIP 等加密流量的分析检测。 9.系统能够根据数据内容而非端口智能识别包括 P2P、即时通讯、电子商务、股票交易、网络游戏、网络电视、移动应用等在内的20大类超过2000 种应用。 10.内置百兆、千兆、万兆的 Web 服务器、DNS 授权服务器DNS 缓存服务器、FTP 服务器等不同应用场景下的 DDoS 检测模板。满足对模板导入、导出等操作。 11.满足 DDoS 自学习模式检测，可设定学习时长，根据周期内流量状态自动学习，设置检测流量值。流量异常触发阈值系统自动进行告警。						
5	上网行为管理服务:提供终端用户的上网行为管理服务，要求实时对互联网、电子政务外网、行业专网、互联网的业务数据进行实时分析，提供数据分析报表。 参考技术服务标准： 提供≥2000 人上网的数据处理分析能力。提供≥4 个千兆电口，4 个光口，整体吞吐不小于2G。 2.要求满足直连、路由、VLAN、旁路监听、混合部署等多种接入模式,切换部署模式无需重启，不影响设备正常使用。要求和上下游设备可以建立≥2000 条加密隧道用于数据逻辑隔离。 3.系统能够根据数据内容而非端口智能识别包括 P2P、即时通讯、电子商务、股票交易、网络游戏、网络电视、移动应用等在内的23大类超过2400 种；应满足实时基于主机、区域的攻击与被攻击的统计显示，在监控信息中直观显示IP 地址所处国家。并满足自定义地址薄导入功能。 4.实配安全准入模块,准入类别包含但不限于管理员准入、进程准入、文件准入、注册	1	134000	134000	6%	126415.09	7584.91

	表准入、操作系统准入；实配L2TP、GRE、PPTP、 IPSEC 接入模块，实现数据的安全传输。 5.为满足IPv6 环境的使用要求，设备接口及部署模式均满足 ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都满足IPv6。 6.满足与威胁防御系统联动,建立终端准入基线,实现安装了终端检测防御系统的终端才能入网，没有安装的不允许入网。 7.满足将多个以太网物理端口捆绑成一条逻辑端口(即将多个端口捆绑成一个逻辑的端口以增加带宽,同时增加链路备份)满足基于轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等多种负载方式。 8.可通过 NetbIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等,然后可以将其加入某个用户组中，逐步完善组织结构的管理。 9.满足刷卡认证功能,实现通过磁卡识别用户身份并进行用户权限控制。						
6	核心网接入交换服务:需对整个网络设备进行升级服务，不满足IPv6 的设备需进行替换，以便整个网络满足IPv4、IPv6 双栈，可在IPv4 向IPv6 过渡的时候正常运行,以满足技术服务标准。核心交换机参考技术服务标准1： 1．机框式插卡设备，具有专用操作系统，稳定可靠，主控槽位≥2个，业务槽位≥6个，电源槽位≥4 个； 2.交换容量≥76Tbps,整机转发性能≥8600 Mpps，如有双重指标则以小指标为准； 3．IPv4 路由：满足静态路由、策略路由、等价路由、RIP v1/v2、OSPF、IS-IS 和BGP等； 4．IPv6 路由：满足静态路由、RIPng、OSPFv3、IS-IS v6、BGP4+等； 5．满足多个物理端口的流量镜像到一个端口；满足跨单板的端口镜像；满足跨设备的端口镜像；满足流镜像到端口； 6．单台配置≥48 个万兆接口。	1	100000	100000	6%	94339.62	5660.38

	汇聚交换机参考技术服务标准2： 1．汇聚交换机，交换容量≥336Gbps，包转发率≥50Mpps，（如官网有多个参数，以最小值为准）； 2.配置≥24个千兆电口,≥4 个千兆SFP 光口； 3．满足MAC地址≥16K，满足ARP 表项≥2K，满足IPv4 FIB表项≥4K ； 4．满足4K 个VLAN，满足Voice VLAN，基于端口的VLAN，基于MAC的VLAN，基于协议的VLAN； 5．满足端口聚合，每个聚合组至少 8 个端口；满足跨设备链路聚合； 6．满足防止DOS、ARP攻击功能、ICMP 防攻击，满足端口隔离、端口安全、Sticky MAC； 7．满足IP/Port/MAC 的绑定功能，满足CPU防攻击、CPCAR 限速； 8．满足纵向虚拟化，作为纵向子节点零配置即插即用； 9．满足对端口接收报文速率和发送报文速率进行限制，满足 SP、WRR、SP+WRR 等队列调度算法，满足基于端口的流量监管，满足基于队列限速和端口整形的功能； 10.满足SNMP v1/v2/v3、Telnet、RMON，满足通过命令行、Web、中文图形化配置软件等方式进行配置和管理； 11.为统一管理及方便运维，需要与核心交换机为同一品牌；	81	3500	283500	6%	267452.83	16047.17
7	运维检测服务:提供全区的网络线路监控服务,能够对电子政务外网提供实时线路状态检测、展示，需提供运维检测终端一台，满足移动检测的需求。	1	20000	20000	6%	18867.92	1132.08
8	日志审计服务:日志审计服务主要收集互联网、电子政务外网、行业专网的访问日志信息及安全事件的日志信息,并对收集到的日志信息进行统一处理，实现日志集中管理、统一分析。对出现的网络安全事件，可通过日志分析结果，及时进行追踪溯源。 参考技术服务标准： 1.硬件参数：标准机架式设备，具备≥4 个千兆电口，≥2 个万兆光口，冗余电源,满足≥50 日志源授权；≥4T 存储容量。 2.满足安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等≥26 类	1	90000	90000	6%	84905.66	5094.34

	300 种日志对象的日志数据采集;满足独立展示每个被采集源最近24 小时的日志数量趋势，便于掌握设备的安全事件情况，满足独立展示每个设备日志的最新采集时间,便于了解设备日志的采集状态。 3.满足IPv6/IPv4 双栈环境部署，对IPv6/IPv4 日志源的日志进行高速采集。 4.满足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。 5.满足对重点日志源的关注设置,并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息。 6.满足通过首页地图快速下钻查询指定区域的日志详细信息,并在查询结果页面上直接下钻二次查询，快速定位关键日志。 7.系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。 8.满足独立展示每个被采集源最近24 小时的日志数量趋势,便于掌握设备的安全事件情况,满足独立展示每个设备日志的最新采集 时间，便于了解设备日志的采集状态。						
9	终端安全防护服务:提供全体终端的病毒防护服务，包含不限于病毒查杀、广告拦截、桌面管理、补丁更新、软件下发等功能。 参考技术服务标准: 1.提供终端用户一体化的自适应威胁防御系统，系统满足Windows、 Linux、国产化、虚拟化等多种部署方式,威胁防御系统主要用于终端PC 的防护,目前包含1000 个终端电脑授权,满足现有电子政务外网接入电脑的全部部署。 2.实配勒索病毒诱捕模块,可设置诱饵文件并实时监控,当勒索病毒对该文件进行加密操作时进行拦截。 3.满足文档检测和文档跟踪功能,对含有指定关键字的文档进行发送、拷贝等行为进行管控。可按照不同文件、压缩包类型跟踪文档的流转方向，实现文档的拷贝、压缩、解压缩、修改、删除、重命名、移动等操作。 4.满足对系统关键位置进行防护,阻止无文	1	60000	60000	6%	56603.77	3396.23

	本攻击、流氓、广告程序对系统的恶意篡改等行为。从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。 5.内置动态分析引擎，利用虚拟沙盒技术，恶意代码行为分析技术,可深度解析恶意代码的本质特征，实时阻断未知病毒。 6.具备基因识别功能，采用基因特征技术，实现通过核心基因特征信息提取对病毒种族进行识别，可以对病毒变种进行查杀防护。 7.能够与防火墙联动，实现对终端资产进行管理，定位终端的物理位置、责任人、以及终端状态信息。同时对未安装威胁防御系统客户端的终端阻断连接,并且可重定向至威胁防御系统下载页面指引安装。 8. 满足对 webshell 后门进行扫描检测，webshell 后门规则数量大于 100000。 9.满足定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP 协议控制、恶意网站拦截、IP黑名单）；文档安全（文档检测、文档跟踪、USB 存储）；系统监控（设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置）。						
10	对整体IPv6 升级提供技术满足，提供改造工程的规划、实施、终端配置等工作，满足业务需求，符合国家、省、市大数据的统一规划标准，提供安全建设方案的规划、实施和维护以及终端的地址改造工程。提供所有产品的安装调试对接、解决IPv6 使用中的问题，提供3 年的技术运维满足服务。	1	200000	200000	6%	188679.25	11320.75
合计				1320000	/	1245283.02	74716.98