合同编号：

新乡市教育专网建设项目合同

甲方(采购人全称)：新乡市教育资源保障中心

乙方(中标人全称)：中国联合网络通信有限公司新乡市分公司

签署日期：2025年6月13日

根据新乡市教育专网建设项目（二次）的采购结果，按照《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法律法规的规定，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

一、合同金额

中标金额为(大写)：壹仟伍佰陆拾玖万柒仟肆佰捌拾柒元贰角贰分（￥15,697,487.22元)人民币。实际结算金额为(大写)：壹仟叁佰捌拾捌万（￥13,880,000.00元)人民币。

二、服务范围

甲方聘请乙方提供以下服务：

1．本合同项下的服务指和新乡市教育专网建设项目（二次）（以下称本项目）相关的服务。

2．项目概况：本项目目的是遴选新乡市教育专网建设与运维服务的服务商，全额投资建设新乡市教育专网，并承担三年的运营和维护服务。项目将采用“统一建设，一体化运营服务交付”模式。

教育专网建设项目采购主要有四方面内容。一是以太网络及链路服务；二是教育云托管服务；三是网络与信息安全保障服务；四是快捷高效运维与服务。包含市教育局机关、2 个独立办公直属机构的网关与核心交换，15 个县（市）区教育局的出口网关、市直属 40 个校区的出口网关和核心交换，还包括建设新乡市教育专享云及其满足等保三级的安全工具。

充分利用我市公共通信资源和原有教育网络资源，按照分级负责原则，建成由运维期间须提供新乡市市级、市直属单位（学校）、县（市）区教育局三级运维服务网络组成的全市教育专网，可以服务各级各类学校和其他教育机构，推动网址、域名和用户的统一管理。

通过教育专网和电子政务外网、互联网等公共网络的互联互通，优化教育专网网内互访质量，提供快速、稳定、绿色、安全的网络服务。并可以实现 IPv6 的规模部署，实现 IPv6 全覆盖。

3.服务要求：

乙方需根据实地调研每个学校及单位的人数确定服务工具档次，并满足后续3到5年的使用需求，提供更好的服务，不低于招标文件基本要求；本次项目服务过程中，需要乙方提供本项目所需软硬件服务工具，具体内容详见招标文件中的服务要求。

本项目包含的所有固定资产以及运维期间产生的各类服务日志、数字资源等无形资产归甲方所有。合同服务期满或服务供应商提前解除服务合同退出时，乙方须将所有为本项目已投入的服务工具及运维服务期间产生的无形资产无偿移交给甲方，移交期间须保持系统运行稳定，能够正常使用，且不附带任何债权债务,不存在法律、经济的异常状态或纠纷。

乙方需在中标后10个工作日内，使用本项目拟投入的服务工具，在甲方指定的一个单位（本次招标范围内的单位）组建样板网络，同时甲方有权要求乙方提供相关证书及检测报告原件备查，如最终结果无法达到招标文件要求，则按虚假应标处理，因此造成的一切损失由乙方承担，并将依据国家相关法律法规追究其法律责任。

3.1.专网链路租赁

根据《河南省加快教育新型基础设施建设专项行动的方案（2023-2025年）》（2023年10月，省教育厅、发改委、财政厅等八部门）。提出实施教育专网建设行动，充分利用国家和我省公共通信资源，按照分级负责原则，建成由省级主干网、市县教育网和学校校园网组成的全省教育专网，覆盖各级各类学校和其他教育机构，推动网址、域名和用户的统一管理。加强教育专网和电子政务外网、互联网等公共网络的互联互通，优化教育专网网内、网间互访质量，提供快速、稳定、绿色、安全的网络服务。全面推进IPv6的规模部署，加速设备和应用的IPv6改造，实现IPv6全覆盖。实现IPV6全覆盖，宽带网络万兆到县，千兆到校。包含市教育局机关、2个独立办公直属机构的网关与核心交换，15个县（市）区教育局的出口网关、市直属40个校区的出口网关和核心交换。各单位之间通过高品质专线以实现互联互通。

3.1.1.总体要求

骨干网要保障带宽的专用通道，采用网络保障手段，保障教育专网的用户体验和网络服务质量。学校师生的上网流量以及教学、办公所需要的各类业务流量，需要和非教育类客户进行区隔，保障教育网络的服务质量，实现专网专用；学校师生和所有网络信息点，需具备同时访问教育网络资源和可管可控互联网上网的条件，解决网络

孤岛问题。教育专网除了承载基础的教育业务，还承担教育绿色上网、网络审计、对教育资源安全访问等功能的引入和分发。

（1）可靠性

大带宽，低时延，从设备级、链路级、网络级等多个层次保证专网的可靠性、稳定性，保证实时性业务平稳运行。

（2）扩展性

教育专网划分为新乡市市级、市直属单位（学校）、县（市）区教育局三级，每层功能清晰，架构稳定，易于扩展和维护，所选服务工具接口具备多样性和兼容性，服务工具选型具备前瞻性，适应未来的发展。

（3）冗余性

关键服务工具采用双节点冗余设计，关键链路采用双备份或者负载分担，关键服务工具的电源、主控板等关键部件冗余备份,提高整个网络的可靠性。

（4）安全性

网络安全符合国家网络安全相关法律法规要求，教育专网安全达到网络安全等保三级，建设完成后需提供相关证书。各县（市）区教育局作为各区域网络安全责任主体，可实现对网络安全事件的事前预判，事后追踪。

（5）易维护性

网络应当具有良好的可管理性，便于维护，选取集成度高、模块可通用的产品，实现网络的便捷维护和快速故障定位。

（6）统一认证

接入用户统一认证，实现教育专网网内用户全网认证，执行灵活而精细的策略管控。

（7）管理维护

实现新乡市市级、市直属单位（学校）、县（市）区教育局三级通过服务工具WEB管理界面进行管理维护。

3.1.2.骨干网

本项目按照分级部署集中管理原则，需要配备1个市级数据中心，市直属40个校区及3个直属单位的数据汇聚中心，15个（或以上）县（市）区数据汇聚中心进行支

撑，市直属学校通过专线接入教育专网，实现万兆接入到县（市）区，千兆接入到校。网络服务工具全面支持IPV6，实现IPV6的规模部署及全覆盖。

乙方需根据实地调研每个学校及单位的人数确定服务工具档次，并满足后续3到5年的使用需求。

3.2.教育云托管服务

需提供：1.相应服务基本要求：提供1套教育云资源，提供托管服务，并含相应的云平台授权费用；

2.自定义大屏展示服务；

3.运维管理服务。

3.3.网络与信息安全保障服务

教育专网建设整体安全要符合《网络安全法》要求，包括但不局限于网络系统运营日志保存、上网行为分析、出口入侵防御、终端准入、主动安全态势感知等，网络安全防护能力达到网络安全三级等保要求。能对师生的上网行为进行监控和管理，保证学生只能访问白名单中的网站并且屏蔽游戏，色情，购物等和学习无关的网络访问业务。校内个人隐私信息采用加密存储方式存储。

全网设置信息安全管控中心，对敏感数据与信息安全相关网络出入口进行安全管控。提供黑白名单、上网访问时间段控制等基础的上网行为管理，可提供对访问特定网站、特定资源的主机实现溯源。

可实现本地认证、第三方认证服务器认证、微信认证、短信认证、Portal认证、APP认证和混合认证等多种用户识别手段,将各类用户上网行为定位到“人”。可实现主流入侵攻击和病毒的检测和防御并保证每周更新特征库。可实现网络私接行为识别和管理，可自定义设置PC终端和移动终端的接入数量阀值，有效保障网络安全接入。

具备攻击防范功能，可实现：Land、IP Spoofing、IP分片报文、ARP欺骗、ARP主动反向查询、TCP报文标志位不合法、超大ICMP报文、地址扫描、端口扫描等攻击防范，还应具备DDoS攻击的检测防御能力。

3.3.1 提供高级安全托管服务；

3.3.2 提供终端并发准入服务；

3.3.3 提供安全等保服务；

3.3.4 提供零信任接入服务；

3.3.5 提供流量采集服务；

3.3.6 提供入侵防御系统服务；

3.3.7 提供上网行为管理服务；

3.3.8 提供数据中心防火墙服务

3.4.运维与服务

乙方作为运维与服务主体保障全市教育专网平稳安全运行，保障日常教学网络的安全稳定。可视化网络管理平台，达到网络统一可视化管理、故障自愈、自动调优等，并结合管理需求建设相应的账号、权限分配机制。

运维人员配置和故障响应时间

故障级别	响应时间	解决时间
I级：属于紧急问题；其具体现象为：骨干网络出现故障链路不通或平台异常不能使用。	5分钟响应，20分钟以内提交故障处理方案	20分钟以内
II级：属于严重问题；其具体现象为：骨干网络出现故障，系统报错，部分学校网络异常；平台部分业务运行异常。	5分钟响应，30分钟内提交故障处理方案	30分钟以内
III级：属于较严重问题；其具体现象为：网络出现故障，系统报错，不影响业务使用；平台部分业务运行异常。	5分钟响应，40分钟内提交故障处理方案	40分钟以内
IV级：属于普通问题；其具体现象为：个别终端异常。	5分钟响应，50分钟内提交故障处理方案	50分钟以内

提供广域网SDN控制服务并纳管本项目中所有的出口网关；

3.4.1 提供网络健康报告服务；

3.4.2 提供可靠性服务；

3.4.3 提供报表服务；

3.4.4 提供智能分析服务；

3.4.5 提供备品备件库服务；

3.4.6 服务要求

项目提供驻场服务、运维服务3年（运维期间提供三级等保评测报告），自项目验收合格投入运行之日起计算。运维期间提供新乡市市级、市直属单位（学校）、县（市）区教育局三级运维服务，数据中心配备运维人员。运维期内为本项目软件提供免费升级及维护服务。服务期内，乙方主动参与甲方举办的信息化相关的赛事活动并积极提供服务。

4.其他

本合同所列上述服务范围的未尽事项，以招标文件的要求为准。

三、双方的权利和义务

（1）乙方应当按照招标文件的要求和投标文件的承诺提供服务和设备，确保服务质量符合招标文件的要求。

（2）乙方应当按照本合同及附件约定的内容进行交付，所交付的文档与文件应当包括纸质及电子版式并可供阅读。甲方应当负责交付过程中的整体协调等事项。

（2）乙方应当在每项交付2个工作日前以书面方式通知甲方，甲方应当在接到通知后及时安排交付事宜。

（3）因甲方原因导致交付不能按时进行的，乙方可相应顺延交付日期，造成乙方损失的，甲方应当承担赔偿责任。

（4）硬件设备交付后5个工作日内，甲乙双方应当共同对设备的规格、数量等状况进行检验，并记录检验情况。如交付的硬件设备与约定不符的，乙方应当及时予以更换或补足并重新提交检验。

四、服务期间(项目完成期限)

项目建设期限：30日历天；自甲方具备施工进场条件开始起算。运维周期：三年；自项目验收合格之日起开始计算。

五、付款方式

合同签订后，向乙方支付合同总金额的30%作为预付款，自验收合格并平稳运行满一年后支付至合同总金额的70%，满两年后运行正常支付剩余金额（不计利息）。

六、验收要求

1.中标人履约完毕及时向采购人提出验收申请。

2.采购人在收到中标人验收申请后5个工作日内组织验收。采购人成立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)，按照招标文件规定、中标

人投标文件承诺，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，中标人必须委托国家认可的专业检测机构验收。

3. 验收合格后10日内，采购人出具《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。

七、知识产权归属

1. 知识产权

乙方承诺对提供给甲方的任何产品及服务享有合法权利，不侵犯任何第三方的知识产权等权益(包括但不限于商标权、专利权、版权、著作权、对不便申请专利的技术秘密和商业秘密的权利等)。否则，乙方将赔偿由此给甲方造成的全部损失。

2. 甲方在使用乙方提供的属于第三方软件时，应当依照乙方与第三方对该软件使用的约定进行。乙方应将该约定的书面文件的复印件交甲方参阅。

3. 本合同项下双方的任何权利和义务不因合同双方发生收购、兼并、重组、分立而发生变化。如发生上述情形之一，则本合同项下的权利和义务随之转移至收购、兼并、重组或分立之单位。如甲、乙双方在本合同项下的各项权利和义务由甲、乙双方之分立单位分别承受的，则甲、乙双方与甲、乙双方之分立单位分别享有和承担相关权利和义务。

4. 甲方在领受本合同项下的服务后，应严格遵守相关的知识产权及软件版权保护的法律、法规，并在本合同所规定的范围内使用。甲方因非经授权而实施的商业性复制行为构成违约或侵权责任造成对方损失的，由其承担相关责任。

5. 本项目包含的所有固定资产以及运维期间产生的各类服务日志、数字资源等无形资产归甲方所有。合同服务期满或服务供应商提前解除服务合同退出时，服务供应商须将所有为本项目已投入的服务工具及运维服务期间产生的无形资产无偿移交给甲方，移交期间须保持系统运行稳定，能够正常使用，且不附带任何债权债务,不存在法律、经济的异常状态或纠纷。

八、保密

1. 未经对方书面许可，任何一方不得向任何第三方提供或与泄漏本协议有关的业务资料和信息。

2. 甲方对乙方所提供的技术应采取合理的保密措施，未经乙方同意不得向其他方泄漏。

九、违约责任与赔偿损失

1. 任何一方未履行本协议项下的任何一项条款均被视为违约。任何一方在收到对方的具体说明违约情况的书面通知后，如确认违约行为实际存在，则应在 7 日内对违约行为予以纠正并书面通知对方；如认为违约行为不存在，则应在 7 日内向对方提供书面异议或说明，在此情况下，甲乙双方可就此问题进行协商，协商不成的，按本协议争议条款解决。违约方应承担因自己的违约行为而给守约方造成的直接经济损失。

2. 甲方必须依照协议按时向乙方交纳业务使用费用，如不能按时交纳，甲方应在规定付款时间至少提前 7 天向乙方说明情况，延时付款时长不得超出合同期 7 天，否则按规定收取违约金。

3. 如遇乙方网络、系统、设备等调整，乙方应及时通知甲方，并明确调整时间以书面形式承诺。若因乙方原因影响甲方正常办公使用，并给甲方造成损失的，由乙方承担全部责任。

十、合同变更、解除或终止

1. 在采购合同履行中，甲方需要追加与合同服务范围相同的服务的，在不改变合同其他条款的前提下，可以与乙方签订补充合同，但所有补充合同的采购金额不得超过原合同金额的10%。

2. 双方当事人不得擅自变更、中止或终止合同。如确需修改或补充合同内容，应经甲乙双方协商一致，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。

3. 合同继续履行将损害国家和社会公共利益的，应当解除合同。

4. 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同：

(1) 如果乙方未能按合同规定的期限或甲方同意延长的限期内提供部分或全部服务；

(2) 乙方在收到甲方发出的违约通知后 7 天内，或经甲方书面认可延长的时间内未能纠正其过失；

(3)如果乙方未能履行合同规定的其他义务或其服务质量不能满足本合同约定的质量标准的；

5.因乙方破产或无清偿能力时，甲方在任何时候书面通知乙方中止合同而不给乙方补偿。该中止合同将不损害或影响甲方已经或将要采取的补救措施的权利。

十一、争端的解决

合同执行过程中发生的任何争议，如双方不能通过友好协商解决，按相关法律法规处理。

十二、不可抗力

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后1日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。不可抗力包括不能预见、不能避免并且不能防止其结果发生的自然或人为灾害，以及由于政府行政行为、非甲乙双方所能控制的行为。

十三、税费

在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

十四、其它

1.本合同附件包括：

①甲方发布的招标文件；

②乙方提供的投标响应文件

③《中标通知书》；

④甲方和乙方商定的其他必要文件。

2.合同附件与本合同具有同等效力。

3.合同文件应能相互解释、相互说明。若合同文件之间有矛盾，则以最新的文件为准。

4.如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

5.除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。

十五、合同生效

1. 本合同经双方代表签字并加盖公章之日起生效。

2. 需方应在本合同签订后1个工作日内将采购合同副本报财政局备案。

3. 本合同一式 陆 份，甲乙双方各持 叁 份。

4. 其他要求：采购需求及要求作为合同条款的一部分，中标单位应严格按照采购需求及要求的内容进行履约。

甲方(盖章)：新乡市教育资源保障中心

地址：新乡市人民东路780号

法定代表人或委托代理人(签字)：

电话：15903886369

开户银行：中国建设银行股份有限公司新乡新区支行

银行账号：41050163285508000063

签订地点：新乡市教育资源保障中心

日　　期：2025 年 6 月 13 日

乙方(盖章)：中国联合网络通信有限公司新乡市分公司

地址：新乡市平原路319号

法定代表人或委托代理人(签字)：

电话：16637330007

开户银行：中国工商银行新乡分行平原路支行

银行账号：1704020529021039320

签订地点：新乡市教育资源保障中心

日　　期：2025 年 6 月 13 日

附表一：项目清单

序号	服务内容	服务费用（万元）	备注
1	建设费用	523.805082	三年（包含附表三、四的服务内容）
2	云资源租赁	158.993640	三年服务费
3	链路租赁费	838.950000	三年服务费
4	安全等级保护测评费	24.000000	三年费用。按照豫财预〔2024〕105 号计取，等保三级。
5	商用密码应用安全性评估费	24.000000	三年费用。按照豫财预〔2024〕105 号计取，商密安全三级。
总价	1569.748722万元		

附表二：服务工具明细清单

序号	名称	品牌	规格型号	单位	数量
（一）网络系统					
1	核心交换机	H3C	S12508G-AF	台	2
2	出口综合网关C	H3C	F5000-AI-20	台	1
3	出口综合网关A	H3C	F1000-AI-60	台	8
4	出口综合网关B	H3C	F1000-AI-90	台	7
5	核心交换机1	H3C	S7503X-M-G	台	2
6	出口综合网关D	H3C	F1000-AI-05	台	2
7	核心交换机2	H3C	S5560X-30F-EI	台	1
8	出口综合网关E	H3C	F1000-AI-15	台	1
9	核心交换机2	H3C	S5560X-30F-EI	台	40
10	出口综合网关D	H3C	F1000-AI-05	台	40
11	安全管理交换机	H3C	S6520X-18C-SI	台	2
（二）安全系统					
1	下一代防火墙	H3C	F5000-AI160	套	2
2	上网行为管理	H3C	ACG1000-AI-180	台	2
3	入侵防御	H3C	T5000-S	套	2
4	零信任	H3C	ZTNA-AK8010	套	1
5	流量采集	H3C	CSAP-NTA-AK375	套	1
6	终端准入控制	H3C	EAD-EIA	套	1
7	SDN控制软件	H3C	AD-WAN	套	1
8	专网安全组件 (1).漏洞扫描组件	H3C	OMP	套	1
9	专网安全组件 (2).综合日志审计组件	H3C	OMP	套	1
10	专网安全组件 (3).运维审计组件	H3C	OMP	套	1
11	专网安全组件 (4).数据库审计组件	H3C	OMP	套	1
12	专网安全组件 (5).安全威胁发现与运营管理组件	H3C	OMP	套	1
13	专网安全组件 (6).终端安全管理	H3C	OMP	套	1
14	安全托管组件	H3C	威胁检测与响应专属版MDR服务	套	1

附表三：软硬件设备清单

序号	设备/软件名称	主要技术参数	数量	单位	单价（万元）	小计（万）
	硬软件合计					338.643
（一）	网络系统					
1	核心交换机	框式正交CLOS核心交换，交换容量1000T，包转发460000M；CPU、SW均为国产芯片，独立交换网板插槽数量6个，业务插槽数量8个，配置双主控，4块独立交换网板，冗余电源风扇模块，48个万兆光口，48个万兆多速率电口，36个40G端口，6个万兆光模块，6个40G光模块。	2	台	15.648750	31.2975
2	出口综合网关C	可插拔冗余电源模块。防火墙吞吐量60G，并发连接数3200万，每秒新建连接数100万。千兆电口8个，千兆combo口4个，万兆光口8个，4个万兆单模光模块；硬盘扩展槽2个，接口扩展槽6个。配套授权：入侵防御和防病毒特征库升级授权3年，15个SSL VPN用户授权，自带IPSec VPN、链路负载、流量控制功能，且不限制数量。	1	台	6.105000	6.1050
3	出口综合网关A	可插拔冗余电源模块。防火墙吞吐量16G，并发连接数1000万，每秒新建连接数16万。千兆电口16个，千兆光口12个，万兆光口4个；硬盘扩展槽2个，双硬盘支持Raid 0和Raid 1，接口扩展槽2个；2个万兆光模块，防火墙应用识别/IPS/AV/URL特征库升级授权3年，15个SSL VPN用户授权；自带IPSec VPN、链路负载、流量控制功能，且不限制数量。支持IPV6功能。	8	台	2.775000	22.2000
4	出口综合网关B	可插拔冗余电源模块，可插拔冗余风扇模块。防火墙吞吐量50G，并发连接数2000万，每秒新建连接数48万。千兆电口16个，千兆光口8个，万兆光口8个；硬盘扩展槽2个，接口扩展槽4个。2个万兆光模块；防火墙应用识别/IPS/AV/URL特征库升级授权3年，15个SSL VPN用户授权，自带IPSec VPN、链路负载、流量控制功能，且不限制数量。支持IPV6功能。	7	台	4.125000	28.8750
5	核心交换机1	主控槽位2个，业务槽位数3个，主控引擎自带业务端口，主控、电源、接口模块、风扇、网板等关键部件可热插拔。交换容量38Tbps，包转发率36000Mpps。	2	台	1.387500	2.77500

		配置主控2个，万兆光口24个，千兆电口32个，冗余风扇电源。				
6	出口综合网关D	防火墙吞吐量3G，并发连接数400万，每秒新建连接数3万。千兆电口10个，千兆combo口2个，硬盘扩展槽1个，2个千兆单模光模块；15个SSL VPN用户授权，自带IPSec VPN、链路负载、流量控制功能，防火墙应用识别/IPS/AV/URL特征库升级授权3年。	2	台	1.237500	2.475000
7	核心交换机2	交换容量750Gbps，包转发率220Mpps；千兆光端口24个（其中千兆combo口8个），万兆光口4个；扩展插槽1个，支持双电源，双风扇模块；配置2个万兆光模块。	1	台	0.562500	0.562500
8	出口综合网关E	24个千兆电口，8个Combo口，2个万兆光口；防火墙吞吐量4G，并发连接数400万，每秒新建连接数4万。2个千兆单模光模块，防火墙应用识别/IPS/AV/URL特征库升级授权3年。	1	台	0.885000	0.885000
9	核心交换机2	交换容量750Gbps，包转发率220Mpps；千兆光端口24个（其中千兆combo口8个），万兆光口4个；扩展插槽1个，支持双电源，双风扇模块；配置2个万兆光模块。	40	台	0.562500	22.500000
10	出口综合网关D	防火墙吞吐量3G，并发连接数400万，每秒新建连接数3万。千兆电口10个，千兆combo口2个，硬盘扩展槽1个，2个千兆单模光模块；15个SSL VPN用户授权，自带IPSec VPN、链路负载、流量控制功能，防火墙应用识别/IPS/AV/URL特征库升级授权3年。	40	台	1.237500	49.500000
11	安全管理交换机	交换容量2.56Tbps，包转发率360Mpps（官网最小值），支持2个电源插槽，1个接口扩展槽位；配置16个1/10G SFP Plus端口；配置8个万兆多模光模块；支持M-LAG跨设备链路聚合技术；支持10KV业务端口防雷；支持硬件层级双boot，实现硬件级boot冗余备份；支持内置智能图形化管理功能，能够实现通过图形化界面设备配置及命令一键下发和版本智能升级，全局配置及网管口配置，设备升级备份、监控及设备故障替换，组网拓扑可视及管理、设备列表展示等功能。	2	台	0.277500	0.555000
（二）	安全系统					
1	下一代防火墙	可插拔冗余电源模块，可插拔冗余风扇模块。吞吐量300G，并发连接数8000W；固化接口形态：6个100G（自适应40G），20个10G，8个25G，2万兆HA端口；2	2	套	15.093750	30.187500

		个100G光模块；4个万兆光模块；4个40G光模块；支持NAT44、NAT46、NAT64、NAT66，支持多种NATALG功能；支持一体化安全策略，能够统一界面进行安全策略配置；配置AV特征库一年升级授权。				
2	上网行为管理	应用特征库数量7100个，180G；新建连接数：130W；并发连接数：14000W，8个千兆电口，8个万兆口，6个扩展插槽，8个40G端口含光模块；具备共享接入管理、移动终端管理等功能。（1）用户行为轨迹及行为分析报表服务：支持用户虚拟身份画像，以时间轴的形式展示用户上网行为轨迹；支持单用户全天行为分析报表，支持对单用户进行网站访问质量检测；（2）行为审计对接服务：系统满足解决安全合规要求，支持集中和独立两种与当地网监对接方式，支持任子行、派博、虹旭、爱思、锐安、宽广智通、网博、云辰、携网、兆物、恒邦、中新、博网、美亚柏科、盛世光明、烽火科技、中科新业、新网程、网盾、海康、白虹、西软、兴容、佰安、珠海网盈以上厂商的非经对接，支持下一代防火墙IPS、AV、WAF、弱密码扫描、SSL VPN、负载均衡等一系列能力。	2	台	16.650000	33.3000
3	入侵防御	专业入侵防御工具，支持可插拔冗余电源模块，支持硬盘扩展槽位，且双硬盘时支持Raid，吞吐性能：网络层70G、全威胁25G，新建连接数60W，并发连接数4000W，固化接口形态及插槽4个Combo口，8个接口扩展槽位，6个40G端口含光模块；硬盘插槽2个，单插槽最高支持1.92T SSD硬盘。	2	套	11.100000	22.2000
4	零信任	吞吐性能8G，支持用户信息管理、用户组管理、用户机构管理、用户权限管理、在线用户管理、角色管理等管理模块，认证方式包括Radius、LDAP、AD、Oauth，第三方认证平台对接支持LDAP、Radius、HTTPS、CAS等第三方服务器；支持静态密码、动态令牌（RSA、软令牌等）、短信、USB Key、数字证书、LDAP服务器、Windows域管理器、WLAN等方式的认证；具备用户基于终端和用户风险动态权限管理等权限控制；具备服务隐藏、应用级访问控制、高敏用户强制下线、访问控制日志、默认访问规则等功能。提供500个零信任接入授权。	1	套	4.856250	4.85625
5	流量采集	应用层吞吐2G，3年流量分析探针特征库升级授权。攻击特征库数量8500个、病毒特征库数量600W、支持的协议识别数量5500个、WEB攻击特征库3500个；若通用攻击规则库无法完全满足安全防护的需求，可以	1	套	1.800000	1.80000

		根据自己网络实际环境情况，自定义去构建特征；为满足灵活适配应用变化的需求，支持自定义应用审计规则。				
6	终端准入控制	配置100000个终端准入功能，支持Portal认证，支持纯Web认证和客户端Portal认证；支持二次地址分配；Portal页面支持定制；支持IPV6纯Portal认证以及NAT环境下的Portal认证；基于不同的端口组、WLAN SSID、终端操作系统推出不同的认证页面；支持Web Portal页面可视化定制；支持无感知认证，可在多台认证服务工具间漫游；支持微信认证。	1	套	23.505000	23.505000
7	SDN控制软件	广域网SDN控制服务并纳管本项目中所有的出口网关；提供网络健康报告服务，该报告涵盖多个层面的分析。报告支持直观地展示网络的整体健康状态，并从多个角度进行深入分析，以帮助运维人员快速定位并解决问题，确保网络的稳定运行；提供可靠性服务，支持控制器集群部署，支持定期自动或手工方式备份控制器数据，支持站点双服务工具路由协议独立部署，支持链路故障时，在无控制器干预下，自动切换到其余可用链路转发，当控制器出现故障时，服务工具仍然可以按照已有策略（如质量策略、带宽策略等）进行选路。100台广域网设备管理授权。	1	套	12.487500	12.487500
8	专网安全组件	1.漏洞扫描组件，支持分布式、单机部署方式，支持IPV4、IPV6环境的漏洞扫描，支持系统漏洞扫描、WEB漏洞扫描、安全基线漏洞扫描、数据库漏洞扫描功能和口令猜解功能，60000条系统漏洞库，支持漏洞库涵盖标准6种，支持针对工控专用网络设备的漏洞扫描，支持多种漏洞验证方式，漏洞报表涵盖漏洞描述、漏洞参考链接和详尽的安全修补方案建议，支持多种告警方式。512个可扫描IP地址数，80个数据库&系统扫描并发，4个Web扫描并发，含首年漏洞库升级。	1	套	4.125000	4.125000
9		2.综合日志审计组件，支持单机、分部署多采集部署方式，支持市面主流安全设备、网络设备、中间件、服务器、数据库、操作系统等设备对象的日志数据采集，支持主动、被动相结合的数据采集方式，支持Syslog、SNMP、JDBC、WMI、FTP、文件等进行数据采集，支持通过Agent采集日志数据，支持绘制全网事件关联关系图谱，支持以告警页面、邮件、SYSLOG等方式告警，支持日志文件备份到外部存储设备，支持丰富的图表可视化分析功能。提供256个日志源授	1	套	4.305000	4.305000

		权；				
10		3.运维审计组件，支持单机、双机主备、多机集群等部署模式；兼容IPv4及IPv6网络协议；支持国产化主流浏览器，产品应用不依赖JAVA及Flash；运维协议支持Telnet、SSH、RDP、VNC、Xdmcp、SFTP等；支持通过应用发布方式实现对B/S、C/S协议的扩展；支持部门分级管理、用户账号管理、资产管理、权限管理、资源访问管理等管理功能；用户身份认证支持手机APP、动态令牌、USBkey等双因素认证方式；支持对图形、字符、文件传输、数据库等进行操作审计；支持密码自动改密、设备配置自动备份等自动化功能。500个可管理资产，500个字符并发，250个图形并发。	1	套	4.218750	4.2187
11		4.数据库审计组件，支持旁路、多路部署方式，支持在IPV4、IPV6环境、虚拟云环境、VXLAN环境下的数据库审计，支持对国外国内超过12种数据库协议进行审计，还支持对HTTP、Telnet、FTP、RDP、VNC、Ssh等协议进行审计，数据库审计支持双向审计、返回结果审计、因子监测、内容审计等，支持对医院防统方审计，支持审计结果进行钻取分析、数据对比和趋势分析，支持邮件和短信多种告警方式，支持对审计数据结果进行多条件组合查询。支持2个数据库实例，无限个数据审计授权；	1	套	5.212500	5.2125
12		5.安全威胁发现与运营管理组件，支持综合态势、外网攻击态势、整网威胁态势及脆弱性态势展示；支持资产安全评估，可展示风险资产明细，展示风险资产遭受的安全事件的攻击阶段分布，并且能够进行溯源取证；支持用户安全评估，可展示风险用户明细及安全事件趋势；支持安全事件分析，包含漏洞利用类、恶意文件类、数据泄露类、Web安全类等；支持攻击阶段的还原和攻击取证溯源；支持手动/自动联动同品牌FW设备或者IPS设备；支持分区分域划分展示态势威胁。安全威胁发现与运营管理平台威胁情报1年更新升级授权；	1	套	12.510000	12.5100
13		6.终端安全管理，采用B/S架构，支持通过HTTPS方式登录管理控制台，管理控制台访问进行加密访问；支持一个管理控制台同时管理Windows,Linux，国产操作系统，同时支持这些操作系统的服务器版和客户端版；产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意	1	套	4.987500	4.9875

		威胁；支持对压缩文件扫描，并可设定压缩层数16；对于恶意文件处理措施支持三种，同时不同病毒/恶意软件类型5种分类；处置措施支持提供两项措施；同时支持扫描例外目录和扫描例外文件；具有病毒日志查询与统计功能，可以随时对网络中病毒发生的情况进行查询统计；50节点1年升级授权。				
14	安全托管组件	依托安全运营中心和安全专家团队，围绕资产、威胁、漏洞、事件四要素，为客户提供7*24小时响应安全服务，风险及时告警，专家快速响应，定期安全巡检，过程全程可视。资产管理，对服务资产进行识别和梳理，并在后续的服务过程中对资产的变更进行持续跟踪，确保资产信息的准确性和完整性；安全现状评估服务：首次对客户现有网络做安全现状评估，输出安全巡检分析报告，并对发现的问题协助客户处置及跟踪（首次巡检报告）；安全服务工具策略优化，根据安全分析结果定期对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到有效的防护效果；漏洞管理：漏洞扫描与验证、漏洞优先级排序、漏洞协助处置、漏洞复测与状态跟踪；威胁情报预警，实时抓取互联网热点事件及最新漏洞（0day或漏洞预警）；威胁分析，7*24小时安全事件分析研判，通过威胁分析对安全事件进行研判；事件协助处置，针对需人工处置的一般安全事件提供处置建议，协助进行处置闭环；重大保障值守：重大时刻保障期间，云端工程师提供每天24小时的值守服务，值守工作内容包括态势感知等安全流量服务工具日志分析与研判，每天输出值守报告。日常安全运营输出日报、月报、阶段性进行汇报总结。	1	套	7.218751	7.218751

备注：1.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 36 个月，租赁期间自 本项目竣工验收 （本合同生效/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。

2.融资租赁费用：318.325126万元，税率为13%；集成服务费用20.318625万元，税率为6%。

附表四：软硬件设备运维费

序号	租赁设备名称	数量	单位	运维标准	运维价格（万元/3年）	备注
	合计				185.161331	
（一）	网络系统					
1	核心交换机	2	台	3.5%	7.667888	定期巡检、调整优化、维修更换、网络接入、备品备件等
2	出口综合网关C	1	台	8.5%	3.632475	
3	出口综合网关A	8	台	8.5%	13.209000	
4	出口综合网关B	7	台	8.5%	17.180625	
5	核心交换机1	2	台	3.5%	0.679875	
6	出口综合网关D	2	台	8.5%	1.472625	
7	核心交换机2	1	台	3.5%	0.137813	
8	出口综合网关E	1	台	8.5%	0.526575	
9	核心交换机2	40	台	3.5%	5.512500	
10	出口综合网关D	40	台	8.5%	29.452500	
11	安全管理交换机	2	台	3.0%	0.116550	
（二）	安全系统					
1	下一代防火墙	2	套	8.5%	17.961562	定期巡检、调整优化、维修更换、网络接入、备品备件等
2	上网行为管理	2	台	8.5%	19.813500	
3	入侵防御	2	套	8.5%	13.209000	
4	零信任	1	套	8.5%	2.889468	
5	流量采集	1	套	8.5%	1.071000	
6	终端准入控制	1	套	10.0%	16.453500	运行监控、定期巡检、专家巡检、专家优化、故障排除、补丁升级、安全加固、数据备份和恢复、资产管理、配置管理等
7	SDN控制软件	1	套	5.0%	4.370625	
8	专网安全组件(1).漏洞扫描组件	1	套	10.0%	2.887500	
	专网安全组件(2).综合日志审计组件	1	套	10.0%	3.013500	
	专网安全组件(3).运维审计组件	1	套	10.0%	2.953125	
	专网安全组件(4).数据库审计组件	1	套	10.0%	3.648750	
	专网安全组件(5).安全威胁发现与运营管理组件	1	套	10.0%	8.757000	
	专网安全组件(6).终端安全管理	1	套	10.0%	3.491250	
9	专网安全组件安全托	1	套	10.0%	5.053125	购买的厂家的

	管组件					安全服务，不计取运维费
备注：						
1.核算服务费时，按1年免费质保计算。8年运维费=(8-1)*每年运维费						
2.运行维护费按照豫财预〔2020〕67号计算。						

附表五：云资源租赁费

序号	服务类别	规格	单位	数量	单价（万元/年）	总价（万元）	备注
1	基础云服务	包括云主机、数据库一体机、存储与备份、操作系统、数据库、中间件、负载均衡和容器等服务	核	380	0.086100	98.154000	依据豫财预〔2024〕106号，三年服务
2	云安全服务	符合等保三级要求	项	费率	2.50%	3.749850	依据豫财预〔2024〕106号，三年服务
3	云密码服务	符合密码应用三级要求	项	费率	3.50%	5.249790	依据豫财预〔2024〕106号，三年服务
4	单机柜租赁服务	4kW	台	4	4.320000	51.840000	依据豫财预〔2024〕106号，三年服务，用于承载教育专网设备
	合计					158.993640	

附表六：专网链路租赁费

序号	链路名称	服务规格	单位	数量	单价（万元）	总价（万元）/3年	备注
	合计					838.950000	
1	VPN专线1	VPN专线，带宽1Gbps，建立私有数据传输通道，3年服务。	条	43	1.190000	153.510000	市教育局、直属学校、直属机构合计43条
2	VPN专线2	VPN专线，带宽10Gbps，建立私有数据传输通道，3年服务。	条	15	11.900000	535.500000	区、县（市）教育局15条
3	VPN专线3	VPN专线，带宽1Gbps，建立私有数据传输通道，3年服务。	条	2	1.190000	7.140000	市教育专网至省教育专网专线2条
4	互联网出口	互联网独享链路，带宽40Gbps，3年服务。	条	1	47.600000	142.800000	市教育网络中心统一互联网出口
备注：							
1.对全市教育专网IP地址进行规划，并按每个学校至少提供5个私有网络IP地址（可按实际需求增减），提供地址转换、IPv4/IPv6双栈服务能力，相关服务设备均满足IPv6要求，在省级层面有新的建设标准后，提供更换相应IP地址工作服务，满足省级教育城域网接入要求。							
2.保证网络的畅通，负责专网主干光缆及配套的所有网络设备的免费运行维护，如光端机、转换器等设备；免费培训传输知识，指导技术人员做好日常维护。							
3.提供传输设备要求具有全网网管监控服务，并实行7*24小时实时监控，可有效地检测并定位网络故障，确保对网络性能的监控。							
4.提供校园接入网关，预留接入端口，实现市级学校数字校园接入全覆盖，并协同有条件的学校接入市教育专网，实现与省、市教育专网无缝对接。							