项目编号：管招采（2025）24 号

中共郑州市管城回族区委智慧城市运行办公室视频监控联网安全系统建设项目

合同协议书

甲方：中共郑州市管城回族区委智慧城市运行办公室

乙方：中国联合网络通信有限公司郑州市分公司

签订地点：河南省郑州市

根据《中华人民共和国民法典》及相关法律规定，甲乙双方在平等、自愿、公平、协商一致的基础上，就甲方委托乙方提供中共郑州市管城回族区委智慧城市运行办公室视频监控联网安全系统建设项目的有关事宜协议如下：

第一条 服务内容

1.甲方委托乙方承接中共郑州市管城回族区委智慧城市运行办公室视频监控联网安全系统建设项目（以下简称“本项目”）。本项目的整体功能应当符合本合同附件中规定的各项技术指标和技术参数要求。

2.项目内容：

本项目所涉及的服务对应的采购规格、数量、价格相关约定见附件。

3.服务期：自合同签订之日起 45 日历天内完成系统交付，系统验收合格使用之日起提供三年运维服务。

4.服务标准及要求：合格，符合国家及行业标准。

5.软件系统升级服务：提供三年软件系统升级服务。

第二条 合同价款及付款方式

1.固定价款总额

合同价款总额为：人民币（含税价）4850000元（大写：人民币肆佰捌拾伍万元整），不含增值税的价款为人民币4575471.70元（大写：人民币肆佰伍拾柒万伍仟肆佰柒拾壹元柒角），增值税税款为人民币274528.30元（大写：人民币贰拾柒万肆仟伍佰贰拾捌元叁角）。

2.付款方式：合同签订后预付合同价款的 10%；系统验收合格后，甲方向乙方支付至合同价款的 70%，剩余 30%作为 3 年传输系统链路和运维保障评价费用，每年根据评价结果按比例进行支付。

3.支付方式

（1）甲方与乙方之间通过 银行转账 方式进行结算。

（2）银行信息：

合同甲方：中共郑州市管城回族区委智慧城市运行办公室 开户名称：中共郑州市管城回族区委智慧城市运行办公室 开户行：郑州银行股份有限公司管城支行 帐号：999156010300000086	合同乙方：中国联合网络通信有限公司郑州市分公司 开户名称：中国联合网络通信有限公司郑州市分公司 开户行：中国工商银行股份有限公司郑州市五里堡支行 帐号：1702022829200004203

4、发票种类：

（1）乙方提供发票种类为增值税普通发票。

（2）本项目提供的发票应按照本合同约定内容，乙方根据服务的不同区别开具。

5、甲乙双方账户信息：____/____。

6、本项目实施过程中，若甲方中途变更方案或发生设备及其他服务的调整变化，相应费用的变化由双方另行协商解决。

第三条 项目实施管理

（一）项目团队组建

甲乙双方应当指定人员对接联系，联系方式如下：

甲方地址： 郑州市商城路2号院7号楼 联系人： 马雅洁 联系电话： 15936249235	乙方地址：郑州市中原东路98号 联系人：孙莉莉 联系电话： 15637119911

（二）项目信息与资料提供

1.乙方有权向甲方有关职能人员调查、了解现有的相关信息和资料，包括而不限于与项目有关的可研报告、背景资料等，甲方应当予以配合。

2.乙方认为甲方提供的信息和资料不符合本项目要求的，有权要求甲方补齐、补正。甲方未按照约定补齐、补正，也未作出合理解释的，相应产生的工程质量、工期延误等法律责任由甲方自行承担。

（三）项目技术文件

1.甲方应当对乙方提交的技术文件进行审核，并在2个工作日内签字确认或提出书面修改意见。根据甲方的书面修改意见，乙方应当及时予以修改并再次提交审核。甲方无正当理由怠于审核的视为无异议，延误的工期相应顺延。

2.技术文件经甲方签字确认后，作为本合同的附件。但甲方对技术文件的确认，并不代表免除乙方对技术问题所应承担的相应责任。

（四）项目实施及变更

1.因甲方未提供场地、资料等原因，导致乙方无法组织项目实施的，乙方有权要求顺延工期，并请求赔偿停工、窝工损失等。

2.因乙方原因造成自身或任何第三人人身损害或财产损失的，乙方应该承担损害赔偿责任。

3.因乙方原因致使项目质量不符合约定的，甲方有权请求在合理期限内修理/修复。

4.甲乙双方均有权在本合同履行过程中提出变更、扩展、替换或修改本项目内容的建议，包括但不限于增加或减少系统的相应功能、提高有关技术参数、变更产品交付或系统安装的时间与地点等。

5.本合同履行过程中的重大变更（包括但不限于信息系统性能、项目实施计划、合同价款、交付日期等的更改以及材料换用等），甲乙双方应当以书面形式予以确定。

6.项目实施过程中，如甲方需要对项目设计等内容进行变更，应该提前7日通知乙方，并签署《需求变更确认单》；如因甲方提出变更导致合同价款的增减，双方应另行签署补充协议，并顺延合理工期，给乙方带来其他损失的，由双方根据具体损失情况另行协商处理。

7.如乙方基于甲方利益、社会公共利益或项目安全考虑，可以就变更技术方案、换用材料设备等提出合理化建议，甲方于2日内给出决策意见，紧急情况下，乙方在未经批准情形下自行组织实施后，应及时报备。

第四条 履约保证金

1.本项目不收取履约保证金

第五条 项目验收和交付

（一）项目验收

1.本项目整体功能符合招标文件的技术部分以及本合同附件中规定的各项技术指标和技术参数要求，具备验收条件时,乙方应当书面通知甲方组织验收。

2.甲方应当自收到验收通知后5个工作日内组织验收，并在验收后2个工作日内出具验收报告或提出整改意见。甲方提出整改意见的，乙方应当及时整改并承担由自身原因造成整改的费用。

3.验收通过后甲方应向乙方出具《验收报告》，甲方无正当理由未在约定期限内组织验收或提出书面修改意见的，自期限届满之日起视为本项目验收合格。

（二）项目交付

1.乙方应当按照本合同及附件约定的内容进行交付，交付内容涉及文档与文件的应当包括纸质及电子版式并可供阅读。

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，由双方根据具体损失情况另行协商处理。

第六条 项目培训

1.乙方应当根据项目实施计划、进度和系统实际运行的需要，及时培训甲方技术人员。培训目标为甲方技术人员能够熟练掌握系统的操作技能和日常的维护技能。

2.乙方培训时应当提供设备、系统操作说明和日常维护说明等技术资料。如未能达到培训目标的，乙方应当按照甲方的要求提供1次再培训。

第七条 知识产权和保密义务

（一）知识产权

1.甲乙双方应当对本合同所涉及的各种软件的知识产权进行约定，以保证本项目使用的软件不会侵犯对方或第三方的知识产权。

2.甲方保证，对本项目中选用的甲方原有软件拥有相应的使用、修改、升级的权利，严格遵守知识产权及软件版权保护的法律、法规，并在本合同所约定的范围内使用本信息系统，否则应当承担相应的法律责任。

3.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，造成甲方实际经济损失的，乙方应当承担赔偿责任。

4.本合同项下全部成果的所有权和知识产权归乙方所有。

5.对于乙方许可甲方使用的软件，甲方拥有使用权、修改权、升级权的具体内容。甲方应当依约定使用，不得超出约定范围。除本合同另有约定外，甲方不得将被许可使用的软件再许可第三方使用。

（二）保密义务

1.保密期限为本合同履行期间及本合同终止后_3_年。甲乙双方可另行约定保密范围，作为附件。

2.在保密期限内，甲乙双方均有为对方保密的义务。甲乙双方保证，因履行本合同所获得的对方商业秘密，仅用于履行本合同项下的义务，并只为履行本合同的相关人员所知悉。任何一方的相关人员违反保密义务的，由该人员所属一方承担全部法律责任；但法律另有规定的除外。

3.本合同履行完毕后，甲乙双方均应当按照对方要求，处理所获得的对方有关资料信息或电子文档。

第八条 违约责任

本合同生效后，甲乙双方均应当全面履行合同义务。任何一方违约，均应当按照约定

承担违约责任，并赔偿对方由此受到的损失。其中：

（一）乙方逾期履约或不履约责任

1.乙方无正当理由逾期交付，每逾期一日，乙方应当向甲方支付合同总价款0.5‰的违约金。

2.乙方不履行合同或交付的信息系统存在重大缺陷以致无法实现合同目的的，甲方有权要求乙方继续履行或解除合同。

（二）甲方逾期付款责任

1.甲方无正当理由逾期付款，每逾期一日，甲方应当向乙方支付合同总价款的0.5‰的违约金。

2.合同签订后，如需解除合同，须经合同双方协商一致。单方面终止合同，终止方应支付合同总金额5%的违约金。

（三）双方违反知识产权义务责任

任何一方违反本合同所约定的知识产权义务，未经对方书面同意，将对方享有知识产权的有关技术成果、计算机软件、源代码、数据信息、技术资料和文档擅自向第三方披露、转让或许可使用的，违约方除应当立即停止违约行为外，还应当赔偿由此给对方所造成的损失，如损失无法准确计算的，违约方应当支付相应违约金。

（四）双方违反保密义务责任

任何一方违反本合同所约定的保密义务，违约方应当支付相应违约金。

第九条 合同的解除和终止

1.本合同生效后，除法律法规和本合同另有规定外，任何一方不得随意单方变更或解除合同，否则应当承担违约责任。

2.甲乙双方各自履行完毕本合同的全部义务后，本合同终止。

第十条 通知与送达

1.合同各方一致确认以下通讯地址和联系方式为各方履行合同、解决合同争议时向接受其他方商业文件信函或司法机关文书的送达地址和联系方式。

2.合同各方均承诺：双方确认的通讯地址和联系方式真实有效，如有错误，导致的信函和诉讼文书送达不能的法律后果由己方承担。

3.本合同项下任何一方向对方发出的通知、信件、数据电文等，应当发送至本合同下列约定的地址、联系人和联系方式。一方当事人变更名称、地址、联系人或联系方式的，应当在变更后五日内及时书面通知对方当事人，对方当事人实际收到变更通知前的送达仍为有效

送达，电子送达与书面送达具有同等法律效力。

4.合同各方均明知：因载明的地址有误、或未及时告知变更后的地址、或者当事人和指定接收人拒绝接收等原因，导致相关文书及诉讼文书未能实际被接收的、邮寄送达的，以文书退回之日即视为送达之日。一方当事人向对方所发出的书面函件，应以挂号信或特快专递的方式邮寄，函件签收的，以函件签收为送达，函件未签收的，以邮件寄出（以邮戳为准）后的第二日视为送达；发出的短信/传真/微信/电子邮件，自前述电子文件内容在发送方正确填写地址且未被系统退回的情况下，视为进入对方数据电文接收系统，即视为送达；被系统退回且非发件方原因的，则以前述电子文件退回之日视为进入对方数据电子接收系统，即视为送达。若送达日为非工作日,则视为在下一工作日送达。

5.本合同约定的合同各方的联系地址、联系人、联系方式为各方工作联系往来、法律文书及争议解决时人民法院/仲裁机构的法律文书送达地址，人民法院/仲裁机构的诉讼文书（含裁判文书）向任何合同任何一方当事人的上述地址送达的，视为有效送达；当事人对电子通信终端的送达适用于争议解决时的送达。

6.通知与送达条款的适用范围包括合同各签约方非诉时各类通知、协议等文件以及就合同发生纠纷时相关文件和法律文书的送达，同时包括在争议进入仲裁、民事诉讼程序后的一审、二审、再审和执行程序。

7.本合同中的通知送达、结算、违约责任等解决争议条款为独立条款，即使本合同变更、撤销、解除、终止或认定无效的，该条款约定依然有效。

第十一条 不可抗力

1.本条所述的“不可抗力”指的是下列不能预见、不能控制的事件，但不包括乙方的违约或疏忽，这些事件主要包括重大自然灾害（洪水、台风、地震、泥石流等）、政府行为、重大社会非正常事件（比如疫情、战争等）。

2.一方当事人因不可抗力不能按照约定履行本合同的，根据不可抗力的影响，可部分或全部免除责任，但是法律另有规定的除外。但应当及时告知对方，以减轻可能给对方造成的损失，并自不可抗力结束之日起15日内向对方当事人提供证明。

3.当事人迟延履行后发生不可抗力的，不免除其违约责任。

第十二条 争议解决方式

本合同项下所发生的争议，由双方协商解决，协商不成的，任意一方均可向甲方住所地有管辖权的人民法院提起诉讼。

第十三条 其他条款

1.本合同自双方签字盖章之日起生效。

2.本合同一式肆份，其中甲方贰份，乙方贰份，具同等法律效力。

3.本项目招标文件（包括投标文件、中标通知书）、本合同附件以及合同履行过程中形成的各种书面文件，经双方签署确认后为本合同的组成部分，与本合同具有同等法律效力，解释的顺序除有特别说明外，以文件生成时间在后的为准。

4.如遇国家税收政策调整，则按照调整后内容执行。

5.本合同未尽事宜，双方可协商签订补充协议，补充协议与本合同具有同等法律效力。

（以下无正文）

甲方（盖章）：

中共郑州市管城回族区委智慧城市运行办公室

授权代表人（签章）：

日期：2025年12月22日

乙方（盖章）：

中国联合网络通信有限公司郑州市分公司

授权代表人（签章）：

日期：2025年12月22日

附件一：评价办法

《评价统计表》

评价统计表(____月)						
序号	项目	评价项	达标率（%）	单项得分	小计	备注
1	安全管理平台	工单完成率（10 分）				
		设备完好率（10 分）				
2	安全系统设备	工单完成率（10 分）				
		设备完好率（10 分）				
3	互联网边界设施（含线路 1 条）	工单完成率（10 分）				
		设备完好率（6 分）				
		线路正常率（4 分）				
4	部门专网边界设施（含线路 1 条）	工单完成率（10 分）				
		设备完好率（6 分）				
		线路正常率（4 分）				
5	单位社区线路（129 条）	工单完成率（10 分）				
		线路正常率（8 分）				
		设备完好率（2 分）				
运维工作扣分情况						
合计						

填表人：　　复核人：

审核单位（盖章）：　　年　　月　　日

注：

一、计分方法：

1、工单完成率：按照月达标率*相应分值计算得分，月达标率按照每日工单完成率平均计算

后得出。

2、设备完好率：按照月达标率*相应分值计算得分，月达标率按照每日设备完好率平均计算后得出。设备包括：各类服务器、路由器、交换机、供电电源、配电架（柜）、电表、支架等。

3、线路正常率：按照月达标率*相应分值计算得分，月达标率按照每日线路正常率平均计算后得出。

4、运维工作扣分：

4.1、视频安全运维管理平台中断影响各政府单位使用，超过 48 小时的一次扣 5 分，超过 24 小时的一次扣 3 分，超过 12 小时的一次扣 1 分。认定以平台日志系统记录为准；

4.2、因互联网或部门专网边界设施运维措施不当导致中断服务超过 48 小时的一次扣 5 分、超过 24 小时的一次扣 3 分、超过 12 小时的一次扣 1 分。认定以平台日志系统记录为准；

4.3、因维护不及时导致设备发生火灾、高温、水淹等灾害情况的一次扣除扣 20 分；

4.4、因维护人员巡检不及时不到位，未能发现故障隐患和预警，导致平台硬件设备损坏的一次扣除 10 分；

4.5、驻场人员未按运维合约要求履行运维职责的一次扣 2 分；

4.6、其他违反运维合约，造成重大影响的一次扣 2 分

（月评分采用百分制，满分 100，如有扣分，相应减除，以最后得分为准）

二、评价结算金额

每月按上述计分方法对中标方进行打分，采用百分制，按年度综合评价分值（取月平均得分）核算支付每年费用，具体标准如下：

1、综合评分 95 分以上（含 95 分），结算金额为合同总价×10%×100%。

2、综合评分 85--95 分（含 85 分），结算金额为合同总价×10%×85%。

3、综合评分 75--85 分（含 75 分），结算金额为合同总价×10%×70%。

4、综合评分 75 分以下，合同总价的 10%将不予结算，并依法追究违约责任。

注：每年传输系统链路和运维保障评价费用根据评价结果于次年年初进行支付。

附件二：项目清单　　单位：元

序号	产品类别	名称	数量	单位	技术参数	税率	单价（含税）	合计（含税）
一	互联网边界系统、其他专网边界系统、安全管理区系统							
1.1	软件服务	互联网边界系统	1	项	1、原有防火墙系统特征库升级服务： 1.1、提供3年入侵防御特征库升级服务。 2、异常流量管理系统能力： 2.1、提供混合共计处理能力为1Gbps的异常流量管理能力，用以防御流量型flood攻击 ：SYN Flood 、SYN-ACK Flood、 ACK Flood、FIN/RST Flood、ICMP Flood、UDP Flood、IP Fragment Flood、Stream flood等； 2.2、防御HTTP get /post Flood攻击、CC应用层攻击，必须能够自定义web防护端口，同时要求有如下set-cookie、javaScript、mouse click、flash、encrypt javaScript、encrypt set-cookie 6种验证方式； 2.3、针对HTTP 攻击、CC应用层攻击提供如下防护能力：连接缓存、屏蔽HTTP代理、屏蔽搜索引擎、源IP连接数限制、源IP新建连接速率限制、源IP GET请求速率限制、源IP POST请求速率限制、源IP OTHER请求速率限制。 3、数据安全交换系统能力： 3.1、提供吞吐量为400Mbps的数据安全交换系统能力，包含数据库交换、文件交换、消息总线交换、请求服务交换、内容安全等模块； 3.2、能力需符合GA/T 1788.3-2021针对互联网边界的建设要求； 3.3、支持在数据库同步过程中把交互数据落地为私有格式文件进行落地交换；	6%	390500	390500

					3.4、支持对数据库内格式化数据基于安全策略进行内容过滤，对含有敏感信息的数据库数据进行拦截丢弃，并进行日志报警； 3.5、支持通过鉴权方式对服务调用方进行身份认证，认证凭证包括数字证书、口令密码、动态令牌、Token 等； 3.6、支持 JWT 认证，API 接口可通过 JWT 进行认证和鉴权。 4、安全隔离与单向传输系统能力： 4.1、提供吞吐量为 400Mbps 的安全隔离与单向传输系统能力，包含通道管理、数据库导入、文件导入、邮件导入、断网恢复、日志管理等模块； 4.2、支持交叉热备功能，能在双机热备功能下提供一端的故障切换（如主设备发送端故障，切换至备用设备发送端，主设备接收端正常工作）； 4.3、支持报表管理功能，支持文件、数据库同步数据流量和恶意代码软件发现次数的报表展示（包括饼状图、柱状图和线形图）； 4.4、支持抗脆弱性扫描能力。 5、准入控制网关系统能力： 5.1、提供吞吐量为 400Mbps 的准入控制网关系统能力，包含设备注册、设备认证、设备审核、视频协议识别、设备环境感知、设备监控、日志审计等模块； 5.2、具备视频边界准入的能力支持对符合 GB/T 28181、GA/T 1400、GB 35114 的设备进行准入控制；支持 IP/MAC、设备 ID 认证；支持接入平台数 2 个、设备点位 1W 个； 5.3、具备数据边界准入的能力提供安装客户端方式；支持 IP/MAC、口令密码、设备指纹、数字证书认证； 5.4、支持采集设备 IP/MAC、BIOS 序列号、CPU 序列号、硬盘序列号、操作系统、设备进程、注册表信息			

					等设备环境感知数据向设备准入控制系统报送； 5.5、支持采集实例名称、实例大小、实例路径、实例文件时间戳、实例文件摘要等关键信息进行注册登记，防止接入设备篡改用于交换的实例； 5.6、支持通过对 IP/MAC 地址、数字证书 KEY、MD5 值校验进行设备准入控制，仅有认证通过的设备才能访问指定资源； 5.7、支持对具有唯一性标识的设备（支持 GB 35114 协议）进行认证；支持设备注册，注册信息包括设备 IP/MAC、设备 ID、设备属性等。 6、探针系统能力： 6.1、提供吞吐量为 800Mbps 的探针系统能力； 6.2、支持 SNMP v2/v3、telnet、ICMP 协议采集内网侧网络安全设备、网络交换设备的运行状态信息； 6.3、支持 Syslog、Flume 等方式采集网络安全设备、网络交换设备的告警日志等数据； 6.4、支持以 syslog、JDBC、FTP、API 接口等方式采集业务日志数据。 7、交换系统能力： 7.1、提供相应匹配的路由交换及业务前置服务能力。			
1.2		其他专网边界系统	1	项	1、防火墙系统能力： 1.1、提供吞吐量为 40G 且具有万兆接口能力的防火墙系统； 1.2、支持透明、路由、混合三种工作模式；支持各种策略路由； 1.3、支持多系统引导及具备恢复系统；支持策略命中数显示； 1.4、支持静态路由，动态路由（OSPF、RIP、BGP、ISIS 等），VLAN 间路由，单臂路由，组播路由等； 1.5、可支持多出口路由情况下的	6%	1220000	1220000

					默认路由备份、负载均衡； 1.6、支持 PPPoE 接入，并具备自动断线重连技术，一个物理接口至少支持 4 路 ADSL 拨号，能够针对每条 ADSL 链路单独设置保证带宽，并能够设置按需拨号。 2、视频安全接入系统能力： 2.1、提供吞吐量为 8G 的视频安全接入系统能力，三主机架构； 2.2、能力需符合 GA/T 1788.3-2021 针对其他专网边界的建设要求； 2.3、兼容 GB/T 28181 标准规范； 2.4、支持 GB 35114 标准规范，支持数字身份证书认证、支持信令 2.5、签名验证，支持 SM3、SHA、MD5、HMAC 摘要认证算法； 2.6、支持视频服务可信域管理，可自定义可信域 IP 及端口； 2.7、支持用户登录超时锁定次数、超时时间设置，WEB 界面设置； 2.8、具备外网视频服务器探测功能，能通过 telnet 等方式检查与外网视频服务器是否能正常通讯。 3、视频安全交换系统能力： 3.1、提供吞吐量为 8G 的视频安全交换系统能力，包含监控中心、资源管理、任务管理、信令行为分析、视频设备监控、日志管理、系统管理模块； 3.2、支持对集群媒体流提供负载均衡，在集群媒体流情况下，媒体流会进行分流； 3.3、支持对集群媒体流提供动态容灾，在集群媒体流其中一台关闭服务器的情况下，会动态容灾跳转到另一台服务器上； 3.4、支持对持有平台公钥对平台发送的信令中的信息做校验，校验不通过则拒绝平台的注册行为； 3.5、支持对视频播放时间的管控，在设置时间段内的视频能够正常播放，在设置时间外的视频无法播放；			

					3.6、支持对视频规定时间范围内点播次数的管控，在设置的规定时间范围内点播次数视频能够正常播放，超出规定时间范围内点播次数视频无法播放。 4、安全隔离与信息交换系统能力： 4.1、提供针对视频安全交换系统吞吐量为 8G 的安全隔离与信息交换系统能力、针对数据安全交换系统吞吐量为 400Mbps 的安全隔离与信息交换系统能力，包含通道管理、数据库/文件/消息总线的同步传输、各种协议代理访问、内容安全、日志管理等模块； 4.2、支持 PostgreSQL、OceanBase、OpenGauss 等同类型数据库 之间同步表单信息，配置完成后表单数据同步交换响应正常，数据库清单列表包含 Oracle、MySQL、PostgreSQL、 SQL Server、达梦、南大通用、 人大金仓、OceanBase 、 OpenGauss、TIDB、神舟通用、 巨杉、GaussDWS、HUAWEI Hive、ODPS、DataHub 等； 4.3、支持 Kafka 、RabbitMQ 、RocketMQ 等消息总线进行消息队列数据信息同步，支持人工设置消息同步的起始位置和起始时间，支持指定时间戳同步、消息队列顺序同步，支持指定消费位置进行分区分配； 4.4、支持 ftp、Sftp、CIFS/samba、NFS、hdfs、阿里 oss 等文件显性和隐性水印，显性水印支持设置水印大小、水印颜色、水印位置等，隐性水印无法直接阅览仅通过标签识别， 系统支持上传水印文件、输入水印标签的 2 种形式进行水印记录溯源； 4.5、支持对数据库表中的姓名、身份证号码、手机号码、详细地址等敏感数据字段加插数据水印，系统支持上传水印数据库表、输入水印标签的 2 种形式进行水印记录			

					溯源。 5、数据安全交换系统能力： 5.1、提供吞吐量为400Mbps的数据安全交换系统能力，包含数据库交换、文件交换、消息总线交换、请求服务交换、内容安全等模块； 5.2、能力需符合GA/T 1788.3-2021针对互联网边界的建设要求； 5.3、支持在数据库同步过程中把交互数据落地为私有格式文件进行落地交换； 5.4、支持对数据库内格式化数据基于安全策略进行内容过滤，对含有敏感信息的数据库数据进行拦截丢弃，并进行日志报警； 5.5、支持通过鉴权方式对服务调用方进行身份认证，认证凭证包括数字证书、口令密码、动态令牌、Token等； 5.6、支持JWT认证，API接口可通过JWT进行认证和鉴权。 6、探针系统能力： 6.1、提供吞吐量为800Mbps的探针系统能力； 6.2、支持SNMP v2/v3、telnet、ICMP协议采集内网侧网络安全设备、网络交换设备的运行状态信息； 6.3、支持Syslog、Flume等方式采集网络安全设备、网络交换设备的告警日志等数据； 6.4、支持以syslog、JDBC、FTP、API接口等方式采集业务日志数据。 7、准入控制网关系统能力： 7.1、提供吞吐量为400Mbps的准入控制网关系统能力，包含设备注册、设备认证、设备审核、视频协议识别、设备环境感知、设备监控、日志审计等模块； 7.2、具备视频边界准入的能力支持对符合GB/T 28181、GA/T 1400、GB 35114的设备进行准入控制；			

					支持 IP/MAC、设备 ID 认证；支持接入平台数 2 个、设备点位 1W 个； 7.3、具备数据边界准入的能力提供安装客户端方式；支持 IP/MAC、口令密码、设备指纹、数字证书认证； 7.4、支持采集设备 IP/MAC、BIOS 序列号、CPU 序列号、硬盘序列号、操作系统、设备进程、注册表信息等设备环境感知数据向设备准入控制系统报送； 7.5、支持采集实例名称、实例大小、实例路径、实例文件时间戳、实例文件摘要等关键信息进行注册登记，防止接入设备篡改用于交换的实例； 7.6、支持通过对 IP/MAC 地址、数字证书 KEY、MD5 值校验进行设备准入控制，仅有认证通过的设备才能访问指定资源； 7.7、支持对具有唯一性标识的设备（支持 GB 35114 协议）进行认证；支持设备注册，注册信息包括设备 IP/MAC、设备 ID、设备属性等。 8、交换系统能力： 8.1、提供相应匹配的路由交换及业务前置服务能力。			
1.3		安全管理区系统	1	项	1、入侵检测系统能力： 1.1、提供吞吐量为 10G 的万兆入侵检测系统能力； 1.2、具有对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解、拒绝服务、缓冲区溢出、欺骗劫持、僵尸网络、SQL 注入、XSS、Xpath、网页木马、钓鱼网站、Webshell、数据库攻击、网络设备攻击、可疑行为等常见攻击具有高精度的检测能力； 1.3、具备全面的 Web 应用类攻击检测能力，能够检测各种 SQL 注入攻击、XSS 跨站攻击、Webshell 上传、命令注入、目录遍历、命令执行等攻击行为；	6%	341600	341600

					1.4、具备对 Web 类攻击行为双向数据提取的功能，能够详细展示攻击者的请求和返回数据，可以帮助分析者快速研判攻击。 2、日志审计系统能力： 2.1、提供 25 个授权的日志审计系统能力，含日志分析驾驶舱，主机操作系统、网络设备、安全设备、应用系统等日志收集，查询，告警，审计，报表，上报等模块； 2.2、支持对 Agent 代理策略进行配置与多服务器一键分发功能，包括但不限于 Input 输入、Processor 处理、Output 输出、Route 路由配置等信息； 2.3、支持对 Agent 输入应用日志名称、文件路径、抽取间隔进行自定义设置，同时支持多行解析能力； 2.4、支持资产拓扑测绘能力，对已注册资产进行拓扑图关系绑定，建立资产拓扑，显示资产关系。同时支持拓扑图导出为图片； 2.5、建立资产日志的全量库，记录资产单位、资产类型、设备类别、源 ip 地址、目标 ip 地址、资产级别、采集时间、入库时间、冗余信息、日志内容、文件路径等详细信息； 2.6、系统提供数据库高危操作、主机高危操作、日志采集量异常、日志断流监测、接口鉴权信息泄露分析、入侵行为分析、日志存储超量、存储空间不足、堡垒机异常、非正常时间访问、潜在危害在内的十几种告警模型。 3、运维审计系统能力： 3.1、提供 50 个授权的运维审计系统能力； 3.2、支持扩展属性自定义，根据自定义的扩展属性的类型、字段 ID、字段名称、最大长度添加资源相关属性。以便基于扩展属性进行资源管理及新建；			

					3.3、运维人员输入账号密码成功单点登录后，系统将自动上收账号到对应资源的账号列表。系统可以对账号进行鉴别；便于借助拥有资源登录权限的运维人员将资源账户进行接管。 4、漏洞扫描系统能力： 4.1、提供系统漏洞检测、web 漏洞检测、数据库漏洞检测、配置合规检测、弱口令检测在内的五合一脆弱性检测能力。包含以上规则库升级能力及服务； 4.2、支持部署在 IPV4、IPV6 环境下，且系统扫描、Web 扫描、数据库扫描、弱口令扫描、基线配置核查等各类型任务均支持添加 IPv6 扫描目标； 4.3、支持主流数据库漏洞的检测，应包括但不限于：Oralce、Sybase、SQLServer、DB2、MySQL、Postgres、Informix、达梦、南大通用、人大金仓、神通等； 4.4、支持数据库弱口令检测，包含 Oracle、REDIS、MySQL、Postgres、MsSQL、DB2、MongoDB、Sybase、Informix ； 4.5、支持导出针对相同扫描目标的同时包含系统扫描、Web 扫描、弱口令扫描结果的综合脆弱性分析报表。 5、数据库审计系统能力： 5.1、提供实例数无限制的数据库审计系统能力，包含数据库自发现、数据库告警、数据库画像、双向审计、可视化大屏功能模块； 5.2、IP 地址的 DML 数据操作报表功能，统计 SELECT、UPDATE、DELETE、INSERT 数量，并可对字段进行升降序筛选及数据下钻分析详情； 5.3、支持提供数据库近 24 小时整体流量分析、整体最常访问 IP 分析、整体最常访问账号分析、最常访问 DBA IP 分析、最常访问 DBA			

					账号分析、DBA 增删改查分析，统计相应 IP/账号及次数； 5.4、系统通过数据库协议特征分析识别出网络环境中可能存在的所有数据库，识别出数据库地址、端口、数据库类型、首次出现时间，可一键转注册； 5.5、支持以省市为单位，对所属 IP 地址段及范围进行维护。可新增、编辑、删除、修改 ip 值，支持开启或关闭。			
二	视频监控运维管理平台							
2.1	软件服务	视频监控运维管理平台系统	1	项	1、数据采集与绩效考核评价系统能力 1.1、提供数据采集子系统支持对前端设备信息采集、网络设备采集、平台软件信息采集、平台设备信息采集能力。系统同时支持本地采控能力、远程采集能力，也支持分布式采集方式，以支持大规模多区域管理场景； 考核管理子系统可根据全域平台系统的特点，对稳定性（离线时长）、联网考核（联网基础、目录完整、联网超标）、图像质量、坐标采集、建档率（“一机一档”）、档案数据准确性、国标规范性（ID 规范与国标码流规范）、重点图像在线率、高清率、录像完整、录像完好、联网率、二类点、三类点的联网率等制定管理考核方案。 2、综合运行态势与运行监测系统能力 2.1、提供对视频专网前端设备、平台软件设备和存储设备进行综合分析能力；实现对监测运维对象的运行状态进行时间、区域、单位和人员、设备和故障类型等多维度展现。提供数据精确统计和质量评估，依据综合数据研判不同品牌、型号设备性能与运行质量，为产品选型、运维服务商选择、设备更换等业务提供数据支持。对严重故障的时间和区域进行分析，季度末和	6%	663700	663700

					年终生成综合运维态势报告，预测系统未来一段时间内的运行趋势并对薄弱环节提前预警等功能； 2.2、运行监测子系统包括视频运维管理模块、录像检测管理模块、NTP 校时检测模块、字幕标注检测模块；同时支持统计分析状态数据，判断识别运行状态，生成运行监测报告。 3、视频流数据治理系统能力 3.1、视频流数据治理能力包括：重点实时视频可调阅率治理、重点历史视频可调阅率治理、重点字幕标注合规率治理、重点时钟准确率治理、二三类点联网数理提升治理、二三类点可调阅率提升治理、二三类点字幕合规率提升治理及二三类点时钟准确率提升治理。 4、视频运维级联管理系统与系统检测分析能力 4.1、视频运维级联管理子系统能力提供上级运行监测平台级联管理、级联任务巡检比对、分级考核任务管理、异常级联推送复核、重点指挥级联管理、一机一档级联管理、级联结果分析模块组成，实现上下级运维数据的级联交互，并分析定位多级之间运维质量与层级间的故障分析比对； 4.2、系统授权管理采用“集中管理，分散授权”的方式进行管理，由各子系统版本提供者分别创建相应子系统的授权文件，集中打包后，由平台门户统一导入授权文件，由各子系统通过授权管理接口从平台门户获取子系统授权文件，进行授权验证，并向平台门户返回授权控制信息，由平台门户统一显示各子系统授权状态，授权有效性由各子系统独立控制； 4.3、提供按照部、省、市的考核巡检办法升级服务。以图形化的形式向用户展现了资源统计概览、资源运行情况、主题资源运行情况、			

					故障总览、离线时长、图像异常统计、频繁维修点位等信息，帮助各类用户快速了解视频专网内资源整体运行情况。系统支持运维资源统计分析，并能以表格、柱状图、饼状图等进行展现，支持 WORD、EXCEL、PDF 等多种方式的导出形成周报、月报，向用户展现资源统计概况及设备运行态势。			
三	智能安全系统管理平台							
3.1	软件服务	智能集中监控与审计系统	1	项	提供针对安全及边界系统的相关管理能力，包含视频安全接入、数据单向导入、数据安全交换管理模块： 1、支持边界安全交互系统资产管理，实现信息注册、资产维护、知识管理、漏洞管理功能； 2、支持对边界安全交互系统内核心关键设备运行状态进行检测和展现；支持对业务运行状态进行统计；支持依据业务审批信息设置业务监控报警阈值；支持流量和流速异常告警、违规业务告警和应用访问异常告警等业务监控报警功能； 3、支持边界安全交互系统策略管理，实现安全策略配置下发、策略变更、策略删除、策略查询等功能； 4、支持将采集到的所有安全组件日志向相关系统进行报送； 5、支持对采集到的日志数据进行范式化、标准化处理； 6、支持边界安全交互系统的服务配置管理，支持使用通用数据交换、接口服务、指定协议等交换服务接口申请服务对象，并审核申请合规性；支持通过审核服务的发布、变更和注销等功能； 7、应支持边界安全交互系统级联管理，实现数据报送、审批、通报等功能； 8、具备边界僵尸设备、儒尸业务、隐蔽通道、未注册协议、未注册资产、未注册应用服务的监控； 9、事件处置功能模块中可以对告	6%	195200	195200

					警事件进行处置动作，并支持填报告警事件处理意见； 10、支持后期可扩展为智算环境下模型分析边界安全状态、异常信息提醒功能。			
四	安全系统							
4.1	软件服务	安全加密系统	1	项	1、提供36个部门共36路各自独立的安全加密系统能力，完成与视频平台安全加密联网。支持ONVIF、GB/T28181、私有协议等多种视频协议接入； 2、提供不低于50路的视频接入能力； 3、支持车辆道闸、出入门禁等设备接入； 4、视频图片输出协议：GB 35114-C级，GA/T 1400.4（数据国密签名加密）； 5、提供不低于8路的视频转发能力； 6、支持数字证书登陆、IP/MAC绑定管理、白名单策略； 7、支持视频准入、网络访问控制、应用协议控制等入侵防御技术。	6%	244000	244000
五	传输系统链路							
5.1	互联网	主干网	36	月	1、2条千兆VPN专线。	6%	4400	158400
5.2		其他干线	36	月	1、129条干线，每条200兆带宽。		21930	789480
六	运维保障							
6.1	运维服务	运维	3	年	1、专职人员7*24小时驻场提供运维服务。	6%	200000	600000
七	集成服务							
7.1	集成服务	集成服务	1	项	1、提供平台虚拟化集成、调试部署、技术支持、培训服务等。	6%	247120	247120
合计								4850000

附件三：

政府采购合同融资意向征求函

为减轻中小企业资金成本运行压力，缓解中小微企业融资难、融资贵问题，促进中小微企业健康发展，省、市、区积极研究出台了《深入推进政府采购合同融资工作实施方案》（豫财办（2020）33号）、《河南省政府采购合同融资工作实施方案》（豫财购〔2017〕10号）等一系列支持中小微企业政府采购合同融资政策。

请问是否了解或者知晓相关政策？

已了解

请问您是否有合同融资意向？

否

中标供应商名称（签字及盖章）：

供应商联系方式：

中标供应商地址：

2025年12月22日