

合同编号: _____

郑州市区域中医药信息系统升级项目 ——中医药传承创新项目合同

甲 方: 郑州市中医院

乙 方: 数字郑州科技有限公司

签订地点: 河南郑州

签订时间: 2024年 11 月 20 日



甲方（全称）： 郑州市中医院

乙方（全称）： 数字郑州科技有限公司

根据《中华人民共和国民法典》以及相关法规的规定，遵循平等自愿和诚实守信的原则，经甲乙双方达成一致，签订本合同，并共同遵守。

第一条 项目基本情况

1.1 项目名称：郑州市区域中医药信息系统升级项目—中医药传承创新项目

1.2 项目概况：郑州市区域中医药信息系统升级项目—中医药传承创新项目属于《郑州市中医药传承创新发展示范试点项目建设方案》的一部分，主要依据《郑州市卫生健康委员会关于开展区域中医药信息系统升级行动的通知》（郑卫办〔2024〕34号）开展项目建设。项目以“构建中医数智化生态标杆，引领中医药现代化转型”为战略定位，深度融合 AI、大数据等技术，将传统中医药理论与现代信息技术进行创新性重构，该体系以数智中医药服务平台为核心，三大支撑体系为运行基座，构建起覆盖中医诊疗全链条、传承全周期、监管全维度的数智化服务体系。

第二条 采购内容和供货要求

2.1 下列与本次招标活动有关的文件及附件是本合同不可分割的组成部分，与本合同具有同等法律效力，这些文件包括但不限于：本合同、中标通知书、协议书、招标文件或采购文件（含招标补充通知）、乙方在投标时的书面承诺（包括但不限于技术标准、参数、售后维护等方面的承诺）、投标文件（含澄清文件）、合同补充条款或说明、保密协议或条款及其他相关附件。

2.2 产品和技术支持服务的名称、规格、型号、计量单位、数量、单价详见附件《分项报价表》。

2.3 合同项下服务地点为：甲方指定地点。

2.4 合同项下的质量标准为：符合国家现行验收规范和标准，满足甲方要求。

2.5 合同实际价款按甲方实际接收产品和技术支持服务内容进行结算。

第三条 项目工期

总工期 300 日历天，计划开工日期：2025 年 11 月 12 日，计划竣工日期：2026 年 9 月 11 日。实际工期总日历天数与根据前述计划开、竣工日期计算的工期总日历天数不一致的，以本条约定的工期总日历天数为准，实际开工日期以甲方通知为准，本合同履行期间，如遇洪涝等不可抗力因素，经甲方和监理签字认可后，工期可相应顺延。



第四条 技术资料

4.1 乙方应按本合同规定向甲方提供本项目有关技术资料。

4.2 没有甲方事先书面同意,乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划或资料提供给与履行本合同无关的任何其他人。即使向乙方履行本合同有关的人员提供,也应事先获得甲方书面同意并同时注意保密并限于履行合同的必需范围,该类人员需签署书面保密协议。

4.3 乙方需在项目竣工完成后 30 日内将甲方提供的技术资料等以及与该项目有关的所有信息全部退回甲方,乙方在使用甲方提供的资料期间及使用后,将资料归还甲方,同时应对相关资料严格保密,不得用于非合同目的。因乙方原因导致技术资料、信息泄露的,其责任由乙方承担。

4.4 乙方需在合同执行过程中按阶段提供过程技术文档,技术文档需按国家相关规范提交,主要文档要求如下(具体以监理单位要求文档为准):

- (1) 调研阶段:《调研报告》《安装部署计划》;
- (2) 准备阶段:《项目实施方案》《项目开发计划》《软件配置方案》;
- (3) 需求分析阶段:《需求分析报告》《需求规格说明书》(含软件功能需求与数据要求);
- (4) 实施阶段:《系统概要设计说明书》《系统详细设计方案》《数据库设计说明书》《系统编码规范》《数据接口设计规范》;
- (5) 测试阶段:《测试记录》《测试报告》;测试报告包括:测试计划、测试方案、测试用例、单元测试、接口测试、功能测试、性能测试、压力测试等;
- (6) 上线阶段:《系统实施方案》《试运行报告》《试运行记录》;
- (7) 过程文档:《培训计划》《培训记录》《项目周报》;
- (8) 交付使用:《业务操作手册》《系统安装维护手册》《系统功能说明书》《程序维护手册》《应急服务响应方案》《签收单》;
- (9) 程序安装包、安装步骤说明手册;
- (10) 与项目相关的其他文档。

第五条 合同价款及支付方式

5.1 本合同价款含税总额为人民币 75,000,000.00 元(大写:人民币 柒仟伍佰万元整),具体税率和分项价款详见附《分项报价表》,如因本合同税率、税金与国家税收政策不一致,以国家税收政策为准,合同含税总额不变,



5.2 本项目为交钥匙项目，本合同总价款包括但不限于完成所有系统部署、数据对接、业务流程开发、上线、培训、初验、终验、质保、运维、专家论证费、税费等全部费用，乙方不得要求甲方再支付其他任何费用。

5.3 甲乙双方确认，本项目采用进度付款方式支付：

第一次付款：本合同签订后，甲方向乙方支付合同总金额 60 %，即人民币 45,000.00 0.00 元（大写：肆仟伍佰万元整）；甲方付款前，乙方向甲方提交一份由金融机构开具的、不可撤销的、见索即付的保函，保函金额等同于第一次付款金额，保函有效期至少 6 个月，若乙方未能在约定时间内提交符合本合同约定的保函，甲方有权相应顺延支付合同款项，且不承担任何违约责任。

第二次付款：本合同约定的系统上线完成后，经甲方、设计单位、监理单位初步验收通过，甲方向乙方支付本合同价款总额的 30 %；即人民币 22,500,000.00 元（大写：贰仟贰佰伍拾万元整）。

第三次付款：项目最终验收（即竣工验收）合格后，甲方向乙方支付本合同价款总额的 10 %；即人民币 7,500,000.00 元（大写：柒佰伍拾万元整）。

甲方付款前，乙方需出具对应金额的增值税普通发票，否则甲方有权暂缓支付且不承担违约责任。

5.4 甲方通过银行转账方式向乙方以下指定账户支付本合同约定价款：

公司名称：数字郑州科技有限公司

纳税人识别号：91410100MA47CLJP9W

地址电话：地址：河南自贸试验区郑州片区（郑东）中兴南路与商鼎路交汇处新发展
科创大厦 24、25 层、联系电话：037163371661

开户行：中国建设银行郑州金水支行营业部

账 号：41050167860800001502

甲方将合同款项付至前述账号，即视为甲方已履行付款义务，由于乙方原因造成延迟付款等问题的，一切后果由乙方承担。

5.5 甲方开票信息

单位名称：郑州市中医院

统一社会信用代码：12410100416046299C

地址电话：河南省郑州市中原区文化宫路 65 号、0371-67447674

开户行：郑州银行建设支行



账号: 9050020109007585

第六条 履约保证金

乙方以转账或见索即付银行保函的方式提供合同总额5%的履约保证金。履约保证金在项目最终验收结束后无息退还,如乙方提供见索即付保函的,乙方应保证保函持续有效,并应在保函有效期届满前10日内重新提供新的等额保函,否则甲方有权直接予以全额兑付,由此造成的全部损失由乙方承担。

第七条 双方权利、义务

7.1 甲方的权利和义务

7.1.1 合同签订后甲方对乙方提交的所有文档内容进行审核;

7.1.2 甲方有对本合同的项目进度、服务质量等情况进行监督、检查的权利,并要求乙方按照监督检查情况制定相应措施并加以整改,甲方不因行使该监督和检查权而承担任何责任,也不因此减轻或免除乙方根据本合同约定或相关法律法规规定应承担的任何义务或责任;

7.1.3 甲方有组织项目验收的权利,甲方、甲方委托的监理单位与乙方共同对项目结果进行验收,出具结论性验收报告;

7.1.4 甲方负责支持、协助、配合乙方做好项目的相关工作;

7.1.5 甲方为乙方的驻场人员和现场实施人员提供办公场地,办公所需用品和办公场所改造由乙方负责,相关费用由乙方自行承担;

7.1.6 在项目达到相关要求后,甲方应按照本合同约定的时间、金额向乙方支付费用;

7.1.7 甲方对乙方委派到现场的人员不能达到项目实施、售后等要求的,可以提出更换要求,乙方应当在收到甲方书面通知后 日内更换完毕,更换期间不能影响项目的整体进度。

7.1.8 甲方有义务对乙方提交的《阶段性工作量确认报告》进行确认。《阶段性工作量确认报告》以项目实际交付进度为准,其中硬件设备以设备到货上电测试确认为节点,软件产品以安装调试完成为节点,软件定制化开发以实际投入产出情况与项目交付清单比例情况进行确认,项目实施服务以实际完成工作量占比情况确认。非基于乙方原因导致合同解除或终止履行,甲乙双方应依据本合同约定,对乙方已完成工作内容据实结算。阶段性工作量确认节点清单详见附件。

7.2 乙方的权利和义务

7.2.1 乙方应按照国家及行业相关标准完成本项目的实施,并向甲方提供合同中约定的所需产品及服务,定期向甲方汇报项目的进展情况;

7.2.2 乙方保证甲方使用其服务及成果时不受第三方关于侵犯专利权、著作权等知识产



权或其他合法权益的指控；如因使用乙方提供的服务及成果而使甲方遭受任何第三方提出诉讼、索赔、指控等，乙方负责与第三方交涉，并承担赔偿责任；在甲方与第三方争议解决之前，乙方应作出必要的安排，保证甲方不会因此中断使用乙方的服务及其服务成果，否则甲方有权单方解除本合同，乙方除应赔偿甲方全部直接损失外（包括但不限于甲方为实施本合同所支出的费用、遭受第三方的索赔、罚款以及为合理主张权利而产生的律师费、诉讼费、差旅费等相关费用），还应向甲方支付采购合同价款总额0.02%的违约金；如果第三方的侵权指控成立，乙方除按照前述标准向甲方支付违约金、赔偿损失之外，甲方还有权选择单方解除本合同；

7.2.3 乙方应严格按照本合同的约定及时完成项目工作的实施，提交建设成果；在甲方委托的项目范围内，对服务中出现的问题应及时调优或完善；

7.2.4 乙方应保守本合同履行过程中获得的与甲方相关的所有秘密信息（包括但不限于技术信息、商业信息、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法和其他专有信息，本合同的条款和与本合同有关的其他信息，本合同履行过程中形成的所有信息、数据、资料、意见、建议、阶段性工作成果和最终工作成果等），在任何情形下，本合同约定的保密义务应永久持续有效；

7.2.5 乙方应接受并配合甲方或甲方组织的对本合同履行情况的监督与检查，对于甲方指出的问题，应在7个工作日内作出合理解释、予以纠正；乙方应接受监理单位对本项目的全过程进行监管，无条件配合监理单位工作，不扯皮推诿；

7.2.6 乙方指派柳周为项目经理（移动电话13027617891，邮箱liu.z@digitalcnzz.com），负责合同整体履行；指派柳周为乙方驻场代表（移动电话13027617891，邮箱liu.z@digitalcnzz.com），负责现场实施。按合同要求完成交付任务，解决由乙方负责的各项事宜；乙方项目经理和驻场代表的行为视为乙方行为，乙方对此予以认可且自愿承担全部法律责任；乙方不得擅自更换项目经理及驻场代表，如需更换需提前一个月以书面形式向甲方发起更换申请，征得甲方同意后方可更换；无故擅自更换一次项目经理，乙方需承担2万元/次的违约金；无故擅自更换一次项目团队人员，乙方需承担1万元/次的违约金。

7.2.7 乙方在完成本合同项下之子系统的部署、硬件安装等工作，初步具备运行状态，可申请阶段性工作量确认，确认工作量以《阶段性工作量确认报告》为准。

第八条 数据对接和功能扩展

8.1 本期项目对接不仅包含与政策性要求的系统对接，还包含与现有系统之间的数据融合和数据的互联互通，凡涉及系统对接的，由乙方自行解决对接环境、接口等，并承担由此



产生的全部费用；乙方应当在接到甲方书面通知后，在限定时间内完成。

8.2 项目实施阶段, 甲方已有的系统牵涉到与本期合同内容数据对接或评级数据改造等, 对接接口和数据改造等费用包含在本合同价款总额里; 项目实施和免费质保期内, 本期合同内容牵涉到的系统对接, 对接的工作量和费用包含在本合同价款总额里, 不再单独计取费用; 乙方应当在接到甲方书面通知后, 在限定时间内完成。

8.3 项目实施期内, 乙方为完成系统对接服务, 在对接过程中的接口开发、产品替换、安装调试、软件授权等, 包含在本合同价款总额里。

8.4 项目实施和免费质保期内, 本项目包含的软件产品在现有功能的基础上进行的流程优化、调整等(不牵涉功能增加), 均需免费, 乙方应当在接到甲方书面通知后, 在限定时间内完成。

8.6 乙方保证向甲方提供清晰、正确、完整的技术资料。

8.7 免费运维和质保期后的后续服务为有偿服务, 相关费用由甲乙双方另行协商。

第九条 项目变更

9.1 以兼顾各方的利益和信息系统的最优化为原则, 在本项目的基本范围内, 甲乙双方均有权在履行本合同的过程中适时地提出变更、扩展、替换或修改本项目的某些部分, 包括但不限于增加或减少系统的相应功能、提高或提升系统的技术参数、改变交付的时间与地点。

9.2 若甲方提出项目的部分变更, 甲方应以书面形式提交给乙方。乙方应在 5 个工作日内对此做出书面回应, 其内容包括详细的该变更对合同价格、项目交付日期、系统性能、项目技术参数的影响和变化以及对合同条款的影响等。乙方逾期未回应的, 视为对甲方提出变更要求予以默认。

9.3 甲方收到乙方的上述回应后, 应在 3 个工作日内以书面方式通知乙方是否同意和接受乙方的上述回应。如果甲方接受乙方的上述回应, 则双方另行对此变更签署补充协议予以确认, 甲乙双方则按变更后的约定履行本合同。

9.4 如乙方提出项目的部分变更建议, 乙方应以书面方式向甲方详细阐明该变更对合同价格、项目交付日期、系统性能、项目技术参数的影响和变化以及对合同条款的影响等, 甲方应在 10 个工作日内对此做出书面回应。双方另行对此变更签署补充协议予以确认, 甲乙双方则按变更后的约定履行本合同。

9.5 变更内容在合同清单内, 按照合同清单的单价进行调整; 变更内容在合同清单外, 由甲乙双方针对变更内容的价款另行协商。

9.6 变更内容牵涉到本合同价款调整, 在第 2 次付款时进行结算。



9.7 甲乙双方就合同变更事宜未达成一致的，双方仍按原合同执行。

第十条 验收要求

10.1 乙方完成本合同约定的项目建设内容并完成文档整理工作，系统上线运行稳定由乙方向甲方提出初验申请，经甲方同意后，甲方组织评审专家对项目初步验收论证，论证通过后完成初步验收工作，且期间未出现影响甲方运营的问题。

10.2 软硬件设备安装、调试完成，并已提供了合同的全部系统软件、硬件和相关资料，解决了软件使用过程中及初步验收提出需要整改的问题，完成软件功能和性能测试，完成了项目初步验收并稳定运行3个月后，乙方书面提出最终验收申请（即竣工验收），由甲乙双方、项目的设计方、监理方按本合同所列项目的内容和国家相关行业标准共同组织验收，出具项目最终验收报告签字盖章确认。

10.3 在两个验收阶段中，若项目验收不合格的，乙方应在3日内完成整改，并自行承担因乙方原因导致验收不合格的整改费用，若整改后仍不合格，甲方有权解除合同并要求乙方按照合同约定承担违约责任。

第十一条 质量保证及售后服务

11.1 免费运维和质保期为五年，免费运维和质保期均从甲方对合同项下项目最终验收合格之日起开始计算，如需分项验收的，应当自本合同采购清单全部产品和服务均最终验收合格后开始计算运维和质保期；质保期内采用本合同 11.1.2 款要求的方式提供运维服务，在免费运维和质保期内乙方对货物的硬件故障、软件升级提供免费原厂保修服务。

11.1.1 免费运维和质保期内提供1人免费驻场服务，按照医院工作时间提供本地化售后服务并按照医院的人员排班要求提供值班服务；驻场人员具备一定的行业工作经验，指导各科室使用系统，保障系统稳定、有序的为甲方服务，包括但不限于功能增强性维护等应用软件系统扩充升级（其中包括系统维护、跟踪检测、数据迁移等）、系统维护等。

11.1.2 免费运维和质保期内每月不少于1次的现场服务，包括：

各类使用问题进行及时排查处理；对甲方各科室工作人员进行应用系统使用操作指导；信息系统使用过程中的问题受理、事务处理、故障排除；信息系统的流程改造；新增需求，新增内部、外部接口。通过定期巡检和排查工作，对维护性问题及时处理，对涉及系统BUG问题进行处理，做到尽早发现问题、尽快消除安全隐患、提前预防重大事故发生，从而保障甲方信息系统安全稳定运行。定期到各院区各科室走访，了解实际使用中的问题，提出合理的流程优化及改进建议等。

重大时间节点保障：在国家法定节假日、医院院庆日、重要接待活动日等重大时间节点



期间，乙方须按医院统一时间安排提供现场技术保障服务，派驻不少于 1 名具备相关经验的技术人员提供现场保障服务；驻场技术人员须携带必要的工具及备件，确保具备现场故障处理能力，其联系方式须 24 小时保持畅通。

并在服务完成后，到医院的信息科填写现场服务单。

11.2 免费运维和质保期内售后服务时间：乙方免费提供 7*24 小时服务，实时解决常见问题，系统故障后 30 分钟内做出明确的响应和安排，如需现场支持的，将立即派常驻维护人员在 2 小时内到达故障现场；4 小时内做出故障诊断报告，常规故障 8 小时内解决。疑难问题，应当在 24 小时内向甲方提供解决方案，48 小时内解决。若超出前述要求的时间仍未解决的，甲方有权另行委托任何第三方维修，由此产生的费用由乙方承担。

11.3 乙方保证本合同中所供应的产品是符合国家相关标准规范的合格产品，如发生所供产品与合同不符，甲方有权拒收，由此产生的一切责任和后果由乙方承担。

11.4 乙方提供的产品在免费运维和质保期内发生故障的，乙方应负责免费更新。对达不到本合同约定的技术要求的，甲方有权根据实际情况要求乙方按以下办法处理：

11.4.1 开发更新：由乙方承担所发生的全部费用。

11.4.2 贬值处理：由甲乙双方协议定价。

11.4.3 拒收处理：乙方应全额退还甲方支付的合同款，同时应承担该产品的直接费用（保险、检验、款项利息及银行手续费等）。

甲方选择上述办法之一的，有权同时要求乙方支付不超过合同总价款 0.1 % 的违约金作为补偿，该违约金不足以弥补甲方损失的，甲方有权要求乙方承担全部损失赔偿责任。

11.5 在免费运维和质保期内，乙方应对产品出现的质量及安全问题负责免费处理解决。

11.6 对于因甲方从第三方采购的本合同范围以外的设备或软件造成的故障，不在乙方维护范围内，需要时乙方应提供相应的配合。

11.7 免费运维和质保期满后，乙方收取维护费，具体甲乙双方另行协商签订维护协议。

第十二条 保密约定

12.1 甲乙双方明确承诺严格对对方的任何保密信息或独有信息保守秘密，不将此等保密信息或独有信息用作本协议以外的任何目的，也不将此等保密信息或独有信息透露给本协议以外的任何人，除非经对方明确书面授权。

12.2 乙方对本合同的内容及执行本合同过程中知悉的甲方商业信息、技术信息、客户信息等负有保密责任，未经甲方书面同意，乙方不得公开或向第三人透露上述甲方资料，否则，造成甲方损失的，乙方应向甲方承担损失赔偿责任。



12.3 乙方应遵守《中华人民共和国保守国家秘密法》实施条例及甲方相关客户保密管理规章制度，对本项目中涉及到的平台敏感数据及项目相关信息履行保密义务。

12.4 保密条款具有独立性，长期有效，不受本合同终止、中止、解除的影响。

12.5 乙方提供的软件程序对用户信息的搜集以及用户设备权限的索取（如有）应坚持最少够用原则，不违反《中华人民共和国个人信息保护法》等相关法律法规的规定。本合同软件免费运维和质保期内，如甲方要求对软件信息数据搜集、用户设备权限索取调整进行调整的，乙方应免费予以调整。

第十三条 知识产权约定

13.1 本项目所有定制开发软件，知识产权均归郑州市中医院所有，且乙方应提供定制开发部分的全部源代码。乙方应保证所提供的全部软件产品、服务或其任何一部分均不会侵犯任何第三方的知识产权等合法权益，如发生第三人指控甲方实施的技术侵权，乙方应当承担由此而产生的全部责任，包括但不限于甲方支付的诉讼费、律师费、对外赔偿等。

13.2 乙方应并保证所提供的任何第三方的（若有）、应用于本合同的所有系统软件等知识产权，具有合法的所有权或使用权或许可权，并不会侵犯第三人的合法权益。

13.3 本合同签订实施之前已产生的技术资料等知识产权仍归双方各自所有，不因本合同的签订、履行发生转移。在此合同基础上开发的软件知识产权，归甲方所有。

13.4 根据本合同产生的全部技术成果（包括但不限于定制化开发软件、项目交付作品和以此为基础研发出的其他技术成果）的知识产权归甲方所有。上述知识产权及相关权利主要包括但不限于专利申请权、版权、著作权、研究成果署名权、奖项申报申请权、获得报酬权、非专利技术所有权、商誉等，产生的全部技术成果按以下条款处理：

13.4.1 甲方拥有本项目开发成果的知识产权，但仅限于本项目且甲方不得进行其他版本的复制，不得披露乙方技术，按照项目管理、验收、测评、测试需要向第三方检验检测机构提供，或依法向政府及监管部门提供除外。

13.4.2 在本项目实施过程中，甲方利用乙方提交的技术服务工作成果所完成的新的定制技术开发成果，归甲方所有。

13.4.3 乙方参与本合同项目的开发人员不可以以本项目申请任何相关的技术成果和专利。

第十四条 技术指导及培训约定

乙方应在向甲方交付合同内容后，根据甲方的请求，为甲方指定的人员提供技术指导和培训，或提供与使用合同相关的技术服务。乙方提供的技术指导和培训已包含在合同总价款



中。

第十五条 违约责任

15.1 合同项下，甲方未能按照约定的时间提供技术材料、信息的，乙方同意给予相应的宽限期，且不视为甲方违约。乙方交付的工作成果亦顺延相应的天数。

15.2 甲方无正当理由逾期向乙方支付合同款项的，每逾期1日，甲方应按照应付未付款项为基数以全国银行间同业拆借中心公布的一年期 LPR 为标准承担违约金，违约金最高不超过本合同总价款的1%。若因此给乙方造成的直接损失超过约定违约金的，甲方还应当赔偿超出违约金部分的损失。

15.3 乙方未在合同约定的日期完成工作成果交付的，应按合同总价款的0.01%向甲方支付违约金。乙方逾期交付超过90日以上或者验收不合格且整改后仍不合格的，甲方有权解除合同；甲方解除合同的，乙方除应退还甲方已支付的全部款项并向甲方支付合同金额1%的违约金及赔偿甲方的损失。

15.4 乙方交付的受托项目成果未能通过甲方验收的，甲方有权要求乙方整改（更换、修改或者重做）或者减少相应价款后接受乙方所提交的受托项目交付成果，并有权要求乙方按照合同总价款的1%的标准向甲方支付违约金，因此给甲方造成的损失大于前述违约金的，甲方有权要求乙方按照实际损失向甲方承担赔偿责任。乙方交付的受托项目交付成果累计经叁次整改仍无法通过甲方验收的，甲方有权解除本合同协议。乙方应在甲方解除合同的书面通知送达之日起60日内全额退还甲方已支付的合同款项，并向甲方支付合同总额的1%作为违约金，因此给甲方造成的损失大于前述违约金的，甲方有权要求乙方按照实际损失向甲方承担赔偿责任。

15.5 除前文约定的违约责任之外，乙方违反本协议约定的其他义务的，应当按照每次2000元的标准向甲方支付违约金，由此给甲方造成的损失大于前述违约金的，乙方应当向甲方赔偿损失。

15.6 乙方向甲方提供的软硬件设备质量不符合合同及招标文件要求的，乙方应在7日内更换全新的设备。乙方因更换设备造成合同逾期的，按照本条15.3的约定向甲方承担违约责任。若拒不更换或更换后仍不能满足合同及招标文件要求的，甲方有权解除合同，乙方应归还甲方已支付的全部款项并按合同总标的0.01%向甲方支付违约金及赔偿甲方的损失。

15.7 在法律允许的范围内，乙方在本合同项下所累计承担的违约、赔偿责任总额最高不超过合同总价款的 2%。乙方应付的违约金或应赔偿的损失，甲方有权从任一笔款项中直接扣除。乙方因违约给甲方造成的损失，包括但不限于甲方为履行本合同所支出的费用、可得



利益损失、因合理主张权利所产生的律师费、差旅费、鉴定费、公证费、保全费等全部相关费用。

第十六条 通知与送达

16.1 乙方应提供确保通知可以送达的通讯地址和联系方式

地 址: 郑州市郑东新区中兴南路与商鼎路交汇处新发展科创大厦 24 层

邮 编: 450008

电子邮箱: liu.z@digitalcnzz.com

联系人: 柳周

固定电话: 037163371661

移动电话: 13027617891

甲方向乙方发出的任何通知、送达行为, 应以专人送递、EMS 等特快专递或电子邮件方式发出。

如以专人送递的, 以乙方法定代表人、联系人或其他工作人员签收之日为送达之日;

如以特快专递发出的, 则以实际签收时间为送达时间; 拒收或者退回的, 则拒收或者退回之日视为已经送达;

如使用电子邮件方式送达的, 电子邮件在发信通知服务器上所记录的发出时间视为送达时间。

除此之外, 甲方还可采用电话、短信等方式向乙方发出通知。

上述送达地址、联系人、联系电话等若有变动, 乙方应在变更前三天内以书面形式通知甲方。若因本合同上注明的乙方地址及联系方式等不准确或变更前未通知甲方而导致不能通知或不能送达的, 视为甲方已送达, 乙方承担因此产生的一切后果和责任, 同时视为甲方已履行通知或送达义务。

16.2 以上通知和送达方式可直接适用于因履行本合同所引发争议的仲裁、一审、二审、再审、执行等全部司法程序。

第十七条 不可抗力

17.1 “不可抗力”, 是指不能预见、不能避免并不能克服的客观情况。在合同有效期内, 任何一方因不可抗力事件导致不能履行合同, 则合同履行期可经双方协商后延长, 其延长期与不可抗力影响期相同。

17.2 受不可抗力影响不能按时、全部履行合同的一方, 在不可抗力发生后应立即通知另一方, 并且在不可抗力发生后的 10 日内向另一方提供有关该不可抗力的权威证明文件和书



面说明,该书面说明中应包括对迟延或部分履行本合同的原因的说明。另一方接到通知后有权选择待不可抗力事件结束后继续履行本合同或解除本合同,并将结果书面通知对方。另一方同意待不可抗力事件结束后继续履行的,不可抗力终止后,受阻方应继续履行本合同并尽快通知另一方、受阻方应相应顺延履行本合同,延长的时间应相当于不可抗力实际造成延误的时间。

17.3 不可抗力或其影响持续达 90 日或以上的,双方应根据该不可抗力对履行本协议的影响程度,协商变更或解除本合同。

第十八条 争议解决

因本合同履行过程中引起的或与本合同相关的任何争议,双方应争取以友好协商的方式迅速解决;若经协商仍未能解决,任何一方均可将有关争议提交甲方所在地有管辖权的法院。

第十九条 其他

19.1 本合同自双方签字并加盖公章或合同专用章之日起生效。

19.2 合同如有未尽事宜,须经双方共同协商,作出补充协议。

19.3 本合同所涉及的正文、附件均为本合同不可分割的部分,与本合同具有同等法律效力。

19.4 本合同未尽事宜,遵照《中华人民共和国民法典》有关条文执行。

19.5 本合同一式捌份,甲方持肆份,乙方持肆份,具有同等法律效力。

19.6 本合同自双方签字并盖章之日起生效。

附件

- 1.项目清单及技术参数
- 2.分项报价表
- 3.阶段性工作量确认报告

甲方(盖章): 郑州市中医院

法定代表人/负责人: 
日期: 2025年11月10日

乙方(盖章): 数字郑州科技有限公司

法定代表人/负责人: 
日期: 2025年11月10日



附件 1：项目清单及技术参数

序号	标的名称	招标参数要求
一	硬件部分	
(一)	服务器	
1	大数据服务器	1、规格：≥12 个 3.5 英寸硬盘盘位； 2、CPU：配置≥2 颗国产化处理器，主频≥2.6GHz，≥64core 处理器，支持超线程； 3、内存：配置≥16*32GBDDR5 内存条； 4、系统盘：配置≥2*960GBSSD； 5、数据盘：配置≥6*4TB SATA； 6、缓存盘：配置≥2*3.2TB NVMeSSD； 7、网口：配置≥4 个 GE，≥2 个 10GE 光口（含光模块），≥2 个 25GE 光口（含光模块）； 8、RAID 卡：配置独立 RAID 卡； 9、配置冗余电源，冗余风扇； 10、为保证项目正常交付，须提供服务器厂家的质保函；
2	应用服务器	1、规格：≥12 个 3.5 英寸硬盘盘位； 2、CPU：配置≥2 颗国产化处理器，主频≥2.6GHz，≥64core 处理器，支持超线程； 3、内存：配置≥16*32GBDDR5 内存条； 4、系统盘：配置≥2*960GBSSD； 5、网口：配置≥4 个 GE，≥2 个 10GE 光口（含光模块），≥2 个 25GE 光口（含光模块）； 6、RAID 卡：配置独立 RAID 卡； 7、配置冗余电源，冗余风扇； 8、为保证项目正常交付，须提供服务器厂家的质保函；
3	边缘超融合节点	1、通过服务器节点构建，同一节点内实现计算存储融合，可配置副本(2 副本或 3 副本)或 EC（纠删码），可满足不同可靠性要求的业务场景。 2、支持图形化界面划分存储资源池，每个存储资源池即为一个故障域，保证可靠性。 3、配置超融合管理授权及分布式存储授权，共配置≥3 个节点，单节点配置如下： 1) 规格：≥12 个 3.5 英寸硬盘盘位； 2) CPU：配置≥2 颗国产化处理器，主频≥2.6GHz，≥64core 处理器，或支持超线程； 3) 内存：配置≥16*32GBDDR4 内存条或 DDR5 内存条； 4) 系统盘：配置≥2*960GBSASSD； 5) 数据盘：配置≥5*4TB SATA； 6) 缓存盘：配置≥1*3.2TB NVMeSSD； 7) 网口：配置≥4 个 GE，≥4 个 10GE 光口（含光模块）； 8) RAID 卡：配置独立 RAID 卡； 9) 配置冗余电源，冗余风扇； 10) 为保证项目正常交付，须提供服务器厂家的质保函；
4	高性能存储节点	1、控制器规格：≤5U 机架式双控制器存储； 2、缓存：≥768GB 缓存，交流电源； 3、处理器：国产化处理器，总核数≥128 核；



		4、端口：≥4*100GbRDMA； 5、端口：≥2*4 端口 25GbETH(含模块)； 6、端口：≥2*4 端口 1GbETH； 7、硬盘：配置≥16 块 7.68TB NVMeSSD，≥77 块 16TB 7.2KRPM NL SAS，RAID6 后 可得容量不低于 1PB； 8、线缆：配置≥8 根多模光跳线； 9、线缆：配置≥4*高速电缆-48G Mini SAS-3m； 9、配置 SAN 许可(含存储管理软件,瘦分配,数据迁移,快照,远程复制,克隆,服务质量 管理,智能运维软件,主机多路径,异构虚拟化,双活,CDP)； 10、配置 NAS 许可(含 CIFS,NFS,NDMP,瘦分配,快照,远程复制,克隆,服务质量管理, 双活,CDP,智能运维软件,NAS 备份)； 11、存储系统为对称 AA 架构，LUN 无控制器归属，在多控配置下，能够负载到所 有控制器，CPU 利用率差异小于 5%，提供 CNAS 检测证明，并加盖厂商公章。
5	中心智算 节点	1、单节点国产化 AI 算力：≥2.2PFLOPS FP16，单节点≥512GB HBM 高带宽显存。 单个 AI 处理器/加速卡支持≥280TFLOPS@FP16 算力,单卡≥64GB HBM 高带宽内存。 2、单节点 CPU：≥4 颗国产化处理器，单颗物理核心数≥48，主频≥ 2.6GHz。 3、单节点内存：容量≥512GB DDR4，内存频率≥3200MHZ。 4、单节点硬盘：≥2*960GB SSD，≥2*3.2TB SSD；。 5、单节点网络：≥2 个 10GE 光口（含光模块），≥4*25Gbps 端口(含光模块)，≥ 8*200G 光口（含光模块）。 6、根据网络信息安全要求，主板管理控制器为国产管理芯片，该芯片能提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能，支持 IPMI2.0 标准，提供 iKVM 功能，实现远程 KVM 功能。 7、为保证项目正常交付，须提供服务器厂家的质保函；
6	边缘智算 节点	1、规格：≥12 个 3.5 英寸硬盘盘位； 2、CPU：配置≥2 颗国产化处理器，主频≥2.6GHz，≥64core 处理器，或支持超线 程； 3、内存：配置≥8*32GB DDR4 内存条； 4、系统盘：配置≥2*960GB SAS SSD； 5、网口：配置≥4 个 GE，≥4 个 10GE 光口（含光模块）； 6、RAID 卡：配置独立 RAID 卡； 7、加速卡：≥4*AI 加速卡；单卡≥140TFP16，≥96GB； 8、配置冗余电源，冗余风扇； 9、为保证项目正常交付，须提供服务器厂家的质保函；
7	备份一体 机	1、支持对 Oracle、MySQL、SQLServer、GaussDB OLTP、OpenGauss、PostgreSQL、 达梦、KingBase、DB2、SAPHANA、GoldenDB、HCS GaussDB 数据库进行在线备份保护。 2、支持 Oracle、MySQL 数据库的永久增量备份功能，合成副本支持数据重复删除、 备份副本异地复制，备份副本长期保留到对象和带库功能，支持备份副本即时挂载 和恢复。 3、支持 HDFS、HBase、Hive、ElasticSearch、Redis、ClickHouse 等大数据组件的数 据备份功能。备份任务配置过程全部图形化操作，无需编写脚本，且支持 HDFS 单 文件、HDFS 目录、HBase 单表、HBase NameSpace 级、Hive 表级、ElasticSearch 索



		引级、ClickHouse 表级细粒度备份和恢复能力。 4、提供按备份任务细粒度复制，支持设置立即复制和周期性复制，支持设置复制副本保留时长（支持永久保留、按年/月/周/天保留）； 5、双控,SSD&HDD,≥256GB 缓存,采用国产化处理器，主频≥2.6GHz，总核心数≥40core；实配≥4*960GBSSDSAS 硬盘；≥8*8TB7.2KRPMNLSAS 硬盘；配置≥32T 备份许可；提供≥8 个 GE，≥4 个 10GE 光口（含光模块）；
8	云平台	1、平台云软件支持对存储、交换机、服务器、超融合、虚拟化资源的统一管理，无需多个软件界面分散管理，管理能力包括设备基本信息查询、配置信息查询、历史性能信息、资源利用率查询、设备告警信息查询等； 2、支持在同一界面配置交换机设置，块存储、文件存储快速发放，实现虚拟机端到端的发放。 3、提供了虚拟机视角的 IO 路径全链路故障诊断：一个界面展示虚拟盘、虚拟机、主机、交换机、存储设备的 IO 路径级的拓扑信息。 4、基于应用视角，提供了包含虚拟机、主机、LUN、存储等对象实例的多维度的关联对象分析，快速定位问题。 5、支持通过设置快照策略任务对虚拟机进行定时快照，满足日常运维管理诉求。运维人员可设置不同的虚拟机快照策略，可按天、周、月设置执行计划。 6、提供预见式运维，支持管理员可自定义检查条件，对存储、计算、网络的配置、容量、性能、可用性、低负载、可回收资源进行检查，在匹配到违规条件时，产生事件，帮助管理员实现风险提前识别与闭环。 7、支持用户针对指定的虚拟机配置检查策略，达到策略定义的阈值后自动扩容虚拟机的 CPU 或者内存。过程中虚拟机正常运行不需要重启。 8、支持批量对多个虚拟机的 CPU、内存、磁盘硬件参数做变更配置，提升运维效率。 9、支持大屏展示，预置超过 3 种大屏；预置超过 20 种图表控件，可支持用户自定义大屏内容。 10、支持租户管理，提供资源配额管理。 11、支持报表统计，支持周期性自动生成报表，预置容量、资源性能，告警等 30 多种典型业务场景的报表。支持用户自定义报表统计内容。 12、配置≥42 颗 CPU 计算虚拟化高级版/企业版授权、≥1800 核容器授权及≥110 颗 CPU 云平台授权；
(二)	网络设备	
9	互联网核心交换机	1.交换容量≥170Tbps，包转发率≥128000Mpps； 2.主控槽位≥2 个；整机业务板槽位数≥8 个，主控槽位与业务线卡槽位宽度相同，为全宽槽位，电源槽位≥4 个； 3.要求设备采用国产化 CPU 芯片和转发芯片； 4.支持 VxLAN 分布式网关、集中式网关，BGP-EVPN，通过 Netconf 配置 VxLAN； 5.支持整机 MAC 地址≥380K；MAC 学习速率≥16000/s;整机 ARP 表项≥140000，整机 ND 表项≥80000，IPv4 路由表以及 FIB 表≥256000，IPv6 路由表以及 FIB 表≥80000； 6.支持 Telemetry 技术，实时采集设备数据并上送至网络分析组件平台,通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态,及时定界故障以及故障发生原因，精准保障用户体验； 7.配置要求:双主控引擎，≥2 个独立风扇框，≥2 个交流电源，≥2 个 100G 光口，



		≥24 个万兆光口, ≥32 个千兆光口, ≥48 个千兆电口, ≥24 个万兆多模模块, ≥1 根 5 米万兆集群线缆。为满足后期扩容需求, 满足上述配置后空余业务槽位≥4 个;
10	互联网接入交换机	1.交换容量≥2.5Tbps, 转发性能≥1500Mpps; 2.万兆光接口≥24 个, 100G 光接口≥2 个, 交流电源≥2 个, ≥24 个万兆多模模块, 40G 堆叠线缆≥1 根; 3.支持 VXLAN 分布式网关, 集中式网关, 支持 BGP-EVPN, 支持 VXLAN 路由交换; 4.支持 RIP、RIPng、OSPF、OSPFV3、ISIS、ISISV6、BGP、BGP4+; 5.设备关键芯片(CPU、转发芯片)均为国产化芯片; 6.MAC 地址表容量≥128K, ARP 地址容量≥64K, FIBv4 表容量≥128K,FIBv6 表容量≥64K; 7.为了方便后期维护, 要求设备支持外置复位按钮, 可在忘记密码或清空配置时使用, 使设备快速恢复出厂配置;
11	核心交换机	1.交换容量≥800Tbps, 包转发率≥230000Mpps; 2.整机主控槽位≥2 个, 业务槽位数≥4 个, 交换网板与业务槽位垂直正交 CLOS 架构; 3.设备关键芯片(CPU、转发芯片)均为国产化芯片; 4.支持 Vxlan 协议, 且支持 BGPEVPN 协议; 5.MAC 地址表容量≥250K, ARP 地址容量≥250K, FIBv4 表容量≥250K, FIBv6 表容量≥80K; 6.配置要求: 冗余主控, 交换网板≥6 个, 电源≥2 个, 40G 光接口≥36 个,10G 光接口≥48 个, 万兆多模模块≥48 个, 5 米 40G 高速线缆≥2 根;
12	接入交换机	1.交换容量≥4.8Tbps, 包转发率≥2000Mpps; 2.固定接口交换机, 独立风扇模块≥3 个, 电源槽位≥2 个; 3.设备 CPU 芯片和转发芯片均采用国产自研芯片; 4.支持配置回滚, 在系统运行过程中发现配置错误、业务运行不正常, 可以通过该命令将系统回退到指定的历史配置状态; 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维 ID 指示灯,现场定位用指示灯, 运维人员可远程控制 ID 灯开启和关闭; 6.配置: 10GE 光接口≥48 个, 100GE 光接口≥8 个, 万兆多模模块≥48 个,40G 多模模块≥4 个, 配置冗余电源;
13	存储互联交换机	1.交换容量≥8Tbps, 包转发率≥2300Mpps; 2.固定接口交换机, 独立风扇模块≥5 个, 电源槽位≥2 个; 3.支持智能无损网络特性, 支持 PFC 死锁预防, 支持识别流量模型动态调节 ECN 门限功能即 AIECN 功能; 4.设备 CPU 芯片和转发芯片均采用国产自研芯片; 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维 ID 指示灯,现场定位用指示灯, 运维人员可远程控制 ID 灯开启和关闭; 6.配置: 25GE 光接口≥48 个 (不可通过接口拆分提供), 100GE 光接口≥8 个, ≥48 个 25G 多模模块, ≥4 个 40G 多模模块, 配置冗余电源;
14	超融合接入交换机	1.交换容量≥4.8Tbps, 包转发率≥2000Mpps; 2.固定接口交换机, 独立风扇模块≥3 个, 电源槽位≥2 个; 3.设备 CPU 芯片和转发芯片均采用国产自研芯片; 4.支持配置回滚, 在系统运行过程中发现配置错误、业务运行不正常, 可以通过该



		命令将系统回退到指定的历史配置状态; 5.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维 ID 指示灯,现场定位用指示灯, 运维人员可远程控制 ID 灯开启和关闭; 6.配置: 10GE 光接口≥ 48 个, 100GE 光接口≥ 8 个, 万兆多模模块≥ 48 个,40G 多模模块≥ 4 个, 配置冗余电源;
15	高速互联交换机	1.交换容量≥ 25.6Tbps, 包转发率≥ 8000Mpps; 2.固定接口交换机, 电源模块槽位≥ 2 个, 支持电源 1+1 备份, 风扇模块槽位≥ 6 个; 3.400GEQSFP-DD 光接口≥ 32 个, 10GESFP+光接口≥ 2 个, 配置≥ 24 个 400G 光模块以及配套 400G 一分二线缆; 4.设备 CPU 芯片、转发芯片均为国产自研芯片, 满足自主可控; 5.支持 AIECN, 可以根据现网流量模型智能调整无损队列的 ECN 门限, 可以保障零丢包下的低时延和高吞吐, 让无损业务达到最优性能; 6.支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术; 7.支持 RDMA,RoCEv2,可提供“无丢包、低时延、高吞吐”的网络环境; 8.支持 Vxlan, 且支持 EVPNVxLAN, 支持 VxLAN 网络与 VLAN 网络互通;
16	管理交换机	1.交换容量≥ 660Gbps, 包转发率≥ 200Mpps; 2.固定接口交换机, 电源槽位≥ 2 个; 3.设备支持复位按钮, 忘记密码可以通过按钮恢复出厂设置; 4.设备 CPU 芯片和转发芯片均采用国产自研芯片; 5.支持配置回滚不重启, 在系统运行过程中发现配置错误、业务运行不正常, 可以通过该命令将系统回退到指定的历史配置状态; 6.设备支持 ID 指示灯, 便于快速定位设备位置; 7.配置: 千兆电接口≥ 48 个, 10GE 光接口≥ 4 个, 支持≥ 2 个专用堆叠口,≥ 4 个万兆多模模块, 配置冗余电源;
17	应用负载均衡器	1、千兆电口≥ 8 个, 万兆光口≥ 8 个, 万兆多模光模块≥ 4 个, 冗余电源,含国密和商密芯片加速卡; 采用国产化 CPU 和操作系统; 2、吞吐量≥ 40G; 并发连接数大于等于 2500 万, 新建连接数≥ 20 万; 支持多存储介质, 可同时支持 EMMC 卡≥ 4GB, SSD 硬盘≥ 512GB; 3、支持 TCP、HTTP、ICMP、DNS、SNMP、UDP、SMTP、POP3、SSL、Oracle、FTP、SIP、RADIUS、自定义等健康监测方式; 支持源 IP、目的 IP、SIP、HASH、httpcookie、httpheader、URL、Radius、DHCP、SSLID、自定义等多种会话保持方式; 4、单一设备可同时支持包括链路负载均衡、服务器负载均衡、全局负载均衡的功能: (需提供设备功能界面截图证明) 5、支持 TCP、HTTP、HTTPS、ICMP、DNS、SNMP、UDP、SMTP、POP3、SSL、Oracle、FTP、SIP、RADIUS、自定义健康监测脚本等健康监测方式; 6、支持轮询、加权轮询、最小流量、最小连接、加权最小连接、加权最佳性能、每源 IP 轮询、源地址源端口哈希散列等服务器负载均衡调度算法; 7、支持主备真实服务组功能, 在缺省实服务组内的成员均不可用时, 启用备份实服务组对外提供服务, 无需单独配置真实服务的优先级; 8、支持手动方式的双机配置一致性检查功能, 在日常运维中, 可以通过手动的方式检查双机之间的配置是否保持一致, 并且显示上次检查时间以及检查结果是否为一, 在不一致的情况下, 可以详细展示出双机在地址池、NAT、真实服务、真实服务组、虚拟服务、健康检查、会话保持、HTTP 内容调度、SSL 策略等模块的配置差异化对比; (提供设备功能界面截图并加盖原厂商公章)



		9、支持一键跳转至命令行 CLI 功能，支持通过设备 WEBUI 页面，一键跳转至命令行 CLI 界面，无需通过远程管理工具登录命令行 CLI 界面；
(三)	安全设备	
18	万兆防火墙 (专网区)	1、机框式插卡设备，主控≥2，支持 N+1 冗余备份，业务槽位数≥3，具有良好的扩展性；支持扩容业务功能板卡数量，实现整机业务性能叠加，满配整机业务吞吐量≥1080Gbps，最大并发连接数≥2 亿，每秒新建连接数≥1440 万，支持扩展万兆接口≥96 个，100G 接口≥8 或 40G 接口≥16； 2、本次实配国产化主控，电源模块≥2 块，主控≥2，风扇模块≥2 个，千兆电口≥4 个，万兆光口接口≥16 个，万兆多模光模块≥16 个，业务吞吐量≥80Gbps； 3、支持丰富的 VPN 特性，如 IPSecVPN、SSLVPN、L2TPVPN、MPLSVPN、GRE 等；支持国用商用密码对数据进行加密。 4、支持 L2~L7 的全面安全防御，包括防火墙、NAT、LB、IPS、AV、ACG、VPN 等； 5、支持 Land、Smurf、Fraggle、WinNuke、PingofDeath、TearDrop、IPspoofing 攻击防护；支持 SYNflood、ICMPflood、UDPFlood、ARPFlood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 6、支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作； 7、支持主机和业务模块统一 IP 管理和统一的配置界面，支持统一网管功能，支持紧耦合部署； 8、支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的 CPU 和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙； 9、支持同一块板卡、跨板卡的链路聚合，支持多台物理设备完成虚拟化之后，不同物理设备的物理端口进行聚合； 10、支持自动生成安全策略，统一运维管理平台可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率（提供和统一管理平台对接的承诺函）； 11、支持 802.1Qbg、DCB 等；支持 VXLAN 等 Overlay 主流标准技术；支持 Openflow1.3 协议标准；具备 SDN 及专网区特性； 12、支持设备在线状态监测机制，实现对包括主控引擎，背板，芯片和存储等关键元器件进行检测；
19	万兆防火墙 (互联网区)	1、具备千兆电口≥8 个，千兆光口≥2 个，万兆光口≥4 个，千兆多模光模块≥2 个，万兆多模光模块≥4 个，支持扩展槽≥1 个，冗余交流电源； 2、整机吞吐量≥10Gbps，每秒新建连接数≥23 万，最大并发连接数≥500 万，含 5 年病毒、IPS、应用识别、URL 特征库及升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持一体化安全策略配置，可以通过一条策略实现五元组、应用、服务、时间、长连接、IP 限速、IPS、AV、URL 过滤、行为审计等功能配置,简化用户管理； 5、具备防火墙、应用识别、链路负载均衡、IPV6、VPN 等功能，支持扩展 URL 过滤、IPS、AV、IP 信誉库、区域特征库、威胁情报等功能； 6、支持 IPv4 / IPv6NAT 地址转换，支持源地址转换 SNAT，目的地址转换 DNAT 和



		双向地址转换双向 NAT, 支持 NAT66 地址转换; 支持多种应用协议, 如 FTP、H.323、RAS、RTSP、SIP、ICMP、DNS、PPTP、NBT 的 NATALG 功能; 7、支持通过命令查询数据流在设备上的处理流程, 可以看到报文经过设备的处理流程, 包含不限于入接口、会话创建、NAT 匹配结果、路由查询结果、安全策略匹配、出接口等以及数据包在设备中最终的处理结果等信息, 便于进行故障排查; 8、支持在一台物理设备上划分出 ≥ 30 个并发相互独立的虚拟系统, 并可以查看虚拟系统的 CPU 和内存利用率、新建、并发和吞吐等信息, 并支持单独重启一个虚拟系统, 其他虚拟系统以及公共系统的业务不受影响。 ;
20	千兆防火墙	1、具备千兆电口 ≥ 8 个, 千兆光口 ≥ 4 个, 千兆多模光模块 ≥ 4 个, 支持扩展槽 ≥ 2 个, 冗余交流电源; 2、整机吞吐量 $\geq 4\text{Gbps}$, 每秒新建连接数 ≥ 9 万, 最大并发连接数 ≥ 390 万, 含 5 年病毒、IPS、应用识别、URL 特征库及升级服务; 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成; 4、支持一体化安全策略配置, 可以通过一条策略实现五元组、应用、服务、时间、长连接、IP 限速、IPS、AV、URL 过滤、行为审计等功能配置, 简化用户管理; 5、具备防火墙、应用识别、链路负载均衡、IPV6、VPN 等功能, 支持扩展 URL 过滤、IPS、AV、IP 信誉库、区域特征库、威胁情报等功能; 6、支持 IPv4 / IPv6 NAT 地址转换, 支持源地址转换 SNAT, 目的地址转换 DNAT 和双向地址转换双向 NAT, 支持 NAT66 地址转换; 支持多种应用协议, 如 FTP、H.323、RAS、RTSP、SIP、ICMP、DNS、PPTP、NBT 的 NATALG 功能; 7、支持通过命令查询数据流在设备上的处理流程, 可以看到报文经过设备的处理流程, 包含不限于入接口、会话创建、NAT 匹配结果、路由查询结果、安全策略匹配、出接口等以及数据包在设备中最终的处理结果等信息, 便于进行故障排查; 8、支持在一台物理设备上划分出 ≥ 30 个并发相互独立的虚拟系统, 并可以查看虚拟系统的 CPU 和内存利用率、新建、并发和吞吐等信息, 并支持单独重启一个虚拟系统, 其他虚拟系统以及公共系统的业务不受影响;
21	WEB 应用防火墙	1、具备千兆电口 ≥ 8 个, 千兆光口 ≥ 2 个, 千兆多模光模块 ≥ 2 个, 支持扩展槽 ≥ 2 个, 冗余交流电源; 2、整机吞吐 $\geq 9\text{Gbps}$, HTTP 吞吐 $\geq 1\text{Gbps}$, 最大并发连接数 ≥ 300 万, 每秒新建连接数 ≥ 3 万, 含 5 年特征库升级服务; 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成; 4、支持透明模式、代理模式、网关模式和旁路模式, 且模式之间切换不需要重启设备或者检测引擎, 可多种模式共同运营; 5、支持对 Web 流量的镜像阻断功能, 并且支持指定阻断报文发送接口; 6、支持通过虚拟化技术实现将一台物理设备虚拟成 ≥ 30 个并发虚拟 WAF; 并且可对每个虚拟 WAF 使用的资源进行限制, 例如会话数、新建速率、吞吐量、CPU 及内存使用率; 7、支持流量自学习, 可以自动学习 IP、域名、端口等信息, 将学习到的服务添加到防护策略; 8、支持内置规则弱口令防护功能, 支持自定义表单模式对弱口令登录表单进行识别和校验; 9、支持通过设定前置参数名、正则表达式、参数范围等匹配特定的主机名、URL, 对容易被篡改或者篡改会产生重大风险的参数名的取值进行限定;



22	漏洞扫描	1、配置千兆电口≥ 8个，万兆光口≥ 2个，万兆多模光模块≥ 2个，USB接口≥ 2个，冗余交流电源； 2、采用国产化CPU和操作系统，内存$\geq 16GB$，硬盘存储$\geq 1T$； 3、采取旁路部署模式，支持分级部署与集中管理，IP可达即可进行检测,无需改变网络架构，基于WEB进行管理； 4、支持资产盘点，可下发资产盘点任务导出专用资产盘点报告，支持自定义资产指纹； 5、支持漏洞检测及弱口令的识别能力，支持高危漏洞的专项检测，支持对高危漏洞的自动化验证，可生成专业安全检测报告； 6、产品具备边界完整性检测能力，可检测出目标设备连接智能手机热点、通过智能手机USB共享网络等违规双网卡共享外联行为； 7、产品具备违规内联检测能力，可检测出随身WI-FI、BYOD设备、向日葵； 8、产品具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测； 9、支持配置主机漏洞模板，内置漏洞库数量≥ 300000种，可兼容CVE、CNNVD、CNVD等主流标准，同时支持自定义扫描漏洞库，漏洞库类型可基于操作系统、数据库、中间件等进行分类； 10、产品需集成安全漏洞验证知识库（提供行业迎检知识库、等级保护知识库、安全攻防知识库、安全应急知识库）以及手工漏洞验证工具集； 11、产品具备高危预警能力，能够对最新发布的高危漏洞及时更新推送平台，对最新高危漏洞预警进行立即检测； 12、产品可以联动统一运维管理平台实现对选定终端设备类型的精确探测反馈，实现对终端信息的二次核验；（提供和统一管理平台对接的承诺函）
23	入侵防御（专网区）	1、具备千兆电口≥ 4个，千兆光口≥ 4个，千兆多模光模块≥ 4个，支持扩展SSD硬盘；冗余交流电源； 2、整机网络层吞吐$\geq 4Gbps$，IPS吞吐$\geq 600Mbps$，最大并发连接数≥ 200万，每秒新建连接数≥ 2万，含5年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持丰富的路由协议，例如静态路由、策略路由（路由前策略、路由后策略、本地报文发包策略）、RIP、OSPF、ISIS、BGP； 5、内置丰富的IPS特征库，可针对SQL注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量≥ 9000条； 6、入侵防御日志支持聚合发送，聚合条件包括源IP聚合、目的IP聚合、源端口聚合、目的端口聚合、协议聚合，同时发送的日志服务器≥ 10个； 7、支持将设备划分成多台虚拟的IPS分给不同的租户使用，租户管理各自策略，相互隔离，虚拟IPS数量≥ 30个并发； 8、支持对邮件协议进行访问管控，包括对SMTP命令（至少包含EXPN、MAIL、RCPT、SAML、SEND、SOML、TURN、VRFY等命令）、邮件大小、邮件主题、收发件人、以及文件类型进行控制； 9、支持跨物理设备的端口聚合，扩展带宽节省链路资源以及方便部署。
24	入侵防御（互联网区）	1、具备千兆电口≥ 8个，千兆光口≥ 6个，千兆多模光模块≥ 6个，支持扩展SSD硬盘；冗余交流电源； 2、整机网络层吞吐$\geq 9Gbps$，IPS吞吐$\geq 1Gbps$，最大并发连接数≥ 300万,每秒新建连接数≥ 3万，含5年特征库升级服务；



		3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持丰富的路由协议，例如静态路由、策略路由（路由前策略、路由后策略、本地报文发包策略）、RIP、OSPF、ISIS、BGP； 5、内置丰富的 IPS 特征库，可针对 SQL 注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量≥9000 条； 6、入侵防御日志支持聚合发送，聚合条件包括源 IP 聚合、目的 IP 聚合、源端口聚合、目的端口聚合、协议聚合，同时发送的日志服务器≥10 个； 7、支持将设备划分成多台虚拟的 IPS 分给不同的租户使用，租户管理各自策略，相互隔离，虚拟 IPS 数量≥30 并发； 8、支持对邮件协议进行访问管控，包括对 SMTP 命令（至少包含 EXPN、MAIL、RCPT、SAML、SEND、SOML、TURN、VRFY 等命令）、邮件大小、邮件主题、收发件人、以及文件类型进行控制； 9、支持跨物理设备的端口聚合，扩展带宽节省链路资源以及方便部署。
25	网络安全审计	1、具备千兆电口≥8 个，千兆光口≥2 个，千兆多模光模块≥2 个；冗余交流电源； 2、网络层吞吐量≥9Gbps，并发连接数≥200 万，每秒新建连接数≥1.5 万，含 5 年特征库升级服务； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持透明在线模式、网桥模式、网关模式、旁挂模式部署，支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理； 5、支持策略路由协议、动态路由协议，包括 RIP、OSPF、ISIS、BGP； 7、支持自定义应用：支持通过 IP+端口方式自定义网络应用及基于深度检测方式（应用特征）自定义网络应用； 8、支持应用会话审计，包括 IP、端口、应用类型、会话包数、字节数、时间等的审计； 9、支持用户时长分析：支持分析用户总时长、总流量以及用户具体应用的时长和流量，可通过饼状图或柱状图展示； 10、支持记录 portal 认证账号的最后一次的登陆时间，方便管理员清理长期未使用的账号，避免设备策略冗余；
26	堡垒机(互联网)	1、千兆电口≥6 个，千兆光口≥4 个，千兆多模光模块≥4 个，USB 接口≥2 个，Console 口≥1 个，扩展槽≥2 个；硬盘≥1T；内存≥16G，管理点数≥60 个；采用国产化 CPU 和操作系统； 2、支持 SSHv1、SSHv2、TELNET 等字符协议；支持 RDP、VNC 等图形协议；支持 FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议； 3、支持运维用户对未授权的资源、资源账号申请授权工单，授权工单通过后可运维申请的资源； 4、支持通过协议前置机进行协议扩展，可支持扩展 KVM、Vmware 等虚拟平台上的资源、数据库、B/S 应用、C/S 应用等； 5、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，对动作流配置即可实现单点登录和审计接入； 6、提供运维、监控、回放屏幕水印功能，并可根据实际需求场景选择开启范围，运维本地无法篡改水印内容，震慑不规范的运维和审计行为，提升运维过程数据安全性； 7、支持 linux 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；支持批量导入、导出资源信息，支持手动添加、删除、编辑、检索资源，支持



		变更默认运维端口；支持资源的动态图表管理,系统可自动生成动态全景视图,支持资源的分类统计,提供资源分类可视化页面； 8、支持 web 页面直接发起运维,无需安装任何控件,并同时支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、xftp、RDP 等客户端工具实现单点登录,不改变运维人员操作习惯； 9、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期；用户登录认证方式支持静态口令认证、手机动态令牌认证、Usbkey（国密数字证书）认证、吉大正元网关认证、华测 Ukey 认证、北京 CA 认证、信安 CA 认证、中安云科认证、503CA 认证、AD/LDAP 认证、Radius 认证、短信认证、指纹识别等认证方式,并支持组合形成双因子认证；
27	堡垒机(专网区)	1、千兆电口≥ 6个,千兆光口≥ 4个,千兆多模光模块≥ 4个,USB 接口≥ 2个,Console 口≥ 1个,扩展槽≥ 2个；硬盘$\geq 4T$；内存$\geq 16G$,冗余交流电源；管理点数≥ 300个；采用国产化 CPU 和操作系统； 2、支持 SSHv1、SSHv2、TELNET 等字符协议；支持 RDP、VNC 等图形协议；支持 FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议； 3、支持运维用户对未授权的资源、资源账号申请授权工单,授权工单通过后可运维申请的资源； 4、支持通过协议前置机进行协议扩展,可支持扩展 KVM、Vmware 等虚拟平台上的资源、数据库、B/S 应用、C/S 应用等； 5、支持通过动作流配置提供广泛的应用接入支持,无论被接入的资源如何设计登录动作,对动作流配置即可实现单点登录和审计接入； 6、提供运维、监控、回放屏幕水印功能,并可根据实际需求场景选择开启范围,运维本地无法篡改水印内容,震慑不规范的运维和审计行为,提升运维过程数据安全性； 7、支持 linux 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；支持批量导入、导出资源信息,支持手动添加、删除、编辑、检索资源,支持变更默认运维端口；支持资源的动态图表管理,系统可自动生成动态全景视图,支持资源的分类统计,提供资源分类可视化页面； 8、支持 web 页面直接发起运维,无需安装任何控件,并同时支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、xftp、RDP 等客户端工具实现单点登录,不改变运维人员操作习惯； 9、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期；用户登录认证方式支持静态口令认证、手机动态令牌认证、Usbkey（国密数字证书）认证、吉大正元网关认证、华测 Ukey 认证、北京 CA 认证、信安 CA 认证、中安云科认证、503CA 认证、AD/LDAP 认证、Radius 认证、短信认证、指纹识别等认证方式,并支持组合形成双因子认证；
28	数据库审计	1、业务接口：千兆电口≥ 8个,千兆光口≥ 4个,千兆多模光模块≥ 4个,USBhost 接口≥ 2个,Console 口≥ 1个,扩展槽≥ 2个,采用国产化 CPU 和操作系统； 2、SQL 流量吞吐$\geq 500Mb/秒$,业务流量吞吐$\geq 2Gb/秒$,SQL 语句吞吐≥ 20000条/秒,数据库实例数≥ 10； 3、CPU≥ 8核,内存$\geq 16G$,硬盘$\geq 2T$； 4、支持 Oracle、SQLserver、DB2、MySQL、Cache、Sybase、Informix、Teradata、PostgreSQL、Hive、MongoDB、HANA、HBASE、ES、CacheWeb、Solr、HDFS、Redis、EsgynDB、Tibero、SSDB 等国际主流数据库；支持 DM7、神通、人大金仓、南大通用、湖南上



		容、浪潮 KDB、HWMPP、翰高等国产数据库； 5、支持扫描网络中的开放的服务，自动发现网络中存在的数据库系统，能够对这些数据库系统进行安全审计； 6、支持自动发现敏感数据如身份证号、银行账号等信息，便于进行用户权限控制，支持将扫描到的敏感表信息进行导出； 7、支持自学习功能，能够基于自学习机制的模型策略，审计未授权的客户端 ip 地址、未授权的表操作访问、未授权的数据库用户、未授权的特权操作等； 8、支持跨包的 SQL 语句进行拼接功能，能够完整解析与审计超长 SQL 语句(≥1460 字节)，屏蔽逃逸审计通道； 9、支持查看数据库系统的监视器信息、软件版本信息、补丁信息、表空间情况、会话信息、回退信息、权限等信息来判断数据库系统运行是否正常，保证数据库系统的可用性和响应能力； 10、支持扫描以下系统风险：数据库表级访问的安全性设置，SGA 共享池分配私有空间的限制，每次调用读入的数据块数目的限制，一次会话读入的数据块总数的限制，是否启用资源限制等数据库系统配置等；
29	服务密码机	采用国产化 CPU 和操作系统； 网络接口≥2 个千兆电口，不支持扩展，其他接口≥6 个 USB 口、≥2 个 COM 口 性能参数： SM4 算法加解密：≥540Mbps；SM2 密钥对≥12000 对/秒；SM2 加密：≥2600 次/秒；SM2 解密：≥3400 次/秒；SM2 签名：≥12000 次/秒；SM2 验签：≥4300 次/秒；SM3 杂凑运算：≥520Mbps
30	签名验签服务器	采用国产化 CPU 和操作系统； 提供基于数字证书的数据签名与验证、加解密服务，支持 SM2 等签名算法； 硬件规格：≥2 个 100/1000M 自适应网口，主要性能参数：SM2 签名≥1600 次/秒。
31	安全隔离与信息交换系统	1、业务接口：（内机）千兆电口≥6 个，万兆光口≥2 个，万兆多模光模块≥2 个，满足接口基础要求上扩展槽≥1 个；（外机）千兆电口≥6 个，万兆光口≥2 个，万兆多模光模块≥2 个，满足接口基础要求上扩展槽≥1 个；冗余交流电源；采用国产化 CPU 和操作系统； 2、网络层吞吐量≥1.5Gbps；并发连接数≥40W；视频并发路数≥450 路 D1 视频；数据库同步速率≥3000 条/秒； 3、带液晶屏，液晶菜单可显示内外网机 IP 地址、CPU 使用率和内存使用率等整机信息； 4、支持远程 ftp、远程 SMB、远程 NFS、远程 sftp、本地 ftp、本地 sftp、客户端方式进行文件交换同步； 5、可查看系统每日 CPU、内存、负载使用率以及会话连接数变化情况，提供至少近 7 日变化图查询； 6、提供 API 管理接口，API 管理接口支持访问密钥数字签名验证，确保访问请求身份认证以及数据未被非法篡改；接口支持授权管理，可针对访问请求进行访问权限控制； 7、支持移动网络接入，搭配外置 4G/5G 硬件模块实现电信、移动、联通移动网络拨号接入； 8、多机热备支持自定义服务监测对象，可对关键 IP、服务进行监测，发现服务连接异常，及时进行主备切换； 9、支持批量数据表智能匹配配置，可自动匹配表名、字段相同的数据表建立同步



		关系，满足大批量数据表同步场景下的快速配置需求； 10、支持 SMTP/POP3 协议，支持发件人、收件人地址过滤；支持主题关键字、正文关键字、附件文件名、附件正文过滤；支持文件类型过滤；病毒扫描；
32	态势感知平台	1.千兆电口≥4 个，万兆光口≥2 个，万兆多模光模块≥2 个，USB 接口≥4 个，扩展槽≥2 个；硬盘≥8T；CPU≥8 核；冗余交流电源； 2.单台最大流量处理能力≥1G；采用国产化 CPU 和操作系统； 3.支持 5G 协议解析和威胁检测，可查看 5G 威胁的日志统计数据，包括攻击级别分布、攻击名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表；支持查看 5G 威胁日志的攻击列表展示，包括攻击者、受害者、所属机构、攻击类型、攻击名称、关键字、发现时间； 4.支持从外连地址和受害者的维度展示外连威胁，查看单条外连威胁详情时将外连攻击行为信息进行展示； 5.支持自定义攻击事件分析模型，包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置 38 种及以上安全事件分析模型，如冰蝎 webshell 通信、利用 Sqlmap 上传 webshell、Acunetix 安全工具扫描、APPSCAN 工具扫描等； 6.支持自定义配置的分析条件，包括：URL、HTTP 方法、HTTP 域名、HTTP 状态码、DNS 解析域名、TLS 指纹、TLS 版本、SSH 服务端协议版本、SSH 客户端协议版本、文件类型、文件哈希值、恶意文件家族、SMTP 发件人等； 7.支持时间轴溯源分析，以时间轴的形式展示攻击者在入侵全过程中各个入侵时间节点中的攻击目标、攻击次数、攻击手段以及攻击阶段，同时提供各攻击手段安全处置建议； 8.支持基于 ATT&CK 框架的模型分析； 9.支持多层溯源功能，开启多层溯源后，默认展示两层溯源信息，攻击手段在展示图中消失，右侧展示攻击手段 TOP5 及描述信息； 10.支持攻击关系分析，以攻击者视角展示针对每个攻击目标所采用的攻击手段的攻击关系视图，同时展示攻击事件的攻击手段 TOP 统计，以及每种攻击手段的描述说明，并支持下钻； 11.支持攻击详情分析，基于受害者、目的端口、时间段、攻击手段、攻击类型、攻击级别、攻击名称等七个维度进行网络攻击日志检索，可查看本次攻击事件涉及的网络攻击的详细信息，以及下载原始攻击数据包； 12.支持 AI 判真功能，存在多个攻击手段的攻击事件显示为 AI 判真事件，AI 判真事件存在 AI 判真标识； 13.支持 AI 自动处置功能，支持攻击事件按照昨天的处置历史信息进行处置，攻击事件被盖上相应的处置标签；历史处置记录按时间轴形式显示处置时间、设备信息或备注信息；处置列表新增一条处置信息，显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息； 14.支持展示安全风险评级、攻击事件类型 TOP5、攻击事件级别分布、外部攻击类型 TOP5、外部攻击者 TOP5 等信息，支持在全球地图上展示攻击者到受害者的攻击视图，展示主要攻击类型，展示资产受害者 TOP5，支持展示攻击者数量、受害者数量、攻击总数、已沦陷资产数量和活跃攻击源 TOP5 等信息，同时支持实时滚动攻击日志，每条攻击至少包括攻击者、受害者、攻击类型、攻击等级、攻击名称和时间。
33	态势感知	1、千兆电口≥4 个，万兆光口≥2 个，万兆多模光模块≥2 个，USB 接口≥4 个，



	探针	扩展槽≥2个；硬盘≥4TB；冗余交流电源； 2、流量采集能力≥1G； 3、支持设置标准模式、增强模式、深度模式、专家模式等流量分析策略,可设置不同策略类型，包括攻击策略、审计策略、采样等级、高级设置； 4、支持多种漏洞攻击检测，至少包括：信息泄露、文件包含、文件上传、目录遍历、跨站脚本、代码注入、反序列化、命令执行、未授权访问、模板注入、文件下载、XML 外部实体注入、越权访问、XPATH 注入、SQL 注入、跨站请求伪造、服务端请求伪造、逻辑绕过、缓冲区溢出、DoS 攻击、其他漏洞、可以的 User-Agent 等； 5、支持对 5G 协议解析和威胁检测，可以通过平台查看 5G 威胁的日志统计数据，包括攻击级别分布，攻击名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表； 6、支持基于机器学习的提取攻击者真实访问的 URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者 IP、攻击者 URL、访问行为的原始报文等； 7、支持多种恶意软件检测，至少包括：勒索病毒、挖矿软件、僵尸网络、shellcode、蠕虫病毒、木马病毒、黑客工具、Rootkit、BootKit、恶意文件投放等； 8、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS 等协议的隧道通信； 9、可自定义弱口令规则，低、中、高三种密码规则，结合预定义弱口令字典，对弱口令威胁的检测更准确；界面可展示检测的弱口令威胁日志，有关键字的会展示关键字。
34	杀毒软件	1、产品以纯软件交付，本次配置≥100 点服务器资源且提供不少于三年的软件升级服务，包含管理控制中心软件及终端客户端软件，其中管理控制中心支持云化或者本地化管理平台交付； 2、Windows 桌面支持：WindowsXP（32 位）、Windows7、Windows 8/8.1、Windows10 等；Windows 服务器：WindowsServer2003（32 位）/2008/2012/2016/2019 等，支持国产化操作系统； 3、单一管理控制中心可统一管理分别部署在 WindowsPC、Win 服务器以及 Linux 服务器和国产化操作系统的客户端软件； 4、采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； 5、支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量。
35	日志审计 (互联网区)	1、千兆电口≥8 个，千兆光口≥4 个，千兆多模光模块≥4 个；USB 接口≥2 个，Console 口≥1 个，扩展槽≥2 个；硬盘≥2T+mSATA128G；内存≥16G； 2、日志处理能力≥2000 条/秒，日志存储能力≥1.7 亿条/天，审计授权≥60； 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成； 4、支持日志查询，可根据接收时间、源目 IP、严重级别等信息进行查询，可针对查询到的日志结果进行导出；支持普通模式查询，并且可以根据查询的条件进行模板保存，以便于后续使用；支持专家模式查询，可通过编写表达式进行对日志信息进行更加全面的查询，并且可以根据查询的条件进行模板保存，以便于后续使用； 5、审计策略：内置审计分析策略，包含：DDoS 攻击、Webshell 攻击、XSS 跨站脚本攻击、欺骗攻击、网络蠕虫、数据库高危操作、切换 root 用户、系统重启、硬件故障等。 6、采集方式：支持基于 TCP 和 UDP 的 syslog 协议、kafka、snmptrap、ftp、smb、



		wmi、sftp 等采集协议格式的模式解析; 7、采集策略: 支持被采设备无需安装代理; 支持同一资产多种采集策略; 支持从不同类型系统采集到的日志进行标准化分析, 将不同格式日志映射到固定的解析字段中, 标准化处理后的字段细粒度≥ 90; 8、支持将采集到的日志进行过滤, 可以根据自身业务需求定制过滤策略, 做到将无关日志进行丢弃; 支持将采集到的日志进行归并, 可以根据自身业务需求定制归并策略, 做到在一定条件下将接收到的相同日志归并为一条, 并且显示该日志的接收次数, 使日志信息简明易看; 9、支持三权分立原则, 可设置安全管理员、安全审计员、系统管理员等角色, 通过赋予不同角色不同的权限, 以达到配置权力、审计权力、运维权力的相互制约;
36	日志审计 (专网区)	1、千兆电口≥ 8个, 千兆光口≥ 4个, 千兆多模光模块≥ 4个; USB 接口≥ 2个, Console 口≥ 1个, 扩展槽≥ 2个; 硬盘$\geq 4T+mSATA128G$; 内存$\geq 32G$; 冗余交流电源; 2、日志处理能力≥ 3000条/秒, 日志存储能力≥ 2.5亿条/天, 审计授权≥ 110; 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成; 4、支持日志查询, 可根据接收时间、源目 IP、严重级别等信息进行查询, 可针对查询到的日志结果进行导出; 支持普通模式查询, 并且可以根据查询的条件进行模板保存, 以便于后续使用; 支持专家模式查询, 可通过编写表达式进行对日志信息进行更加全面的查询, 并且可以根据查询的条件进行模板保存, 以便于后续使用; 5、审计策略: 内置审计分析策略, 包含: DDoS 攻击、Webshell 攻击、XSS 跨站脚本攻击、欺骗攻击、网络蠕虫、数据库高危操作、切换 root 用户、系统重启、硬件故障等。 6、采集方式: 支持基于 TCP 和 UDP 的 syslog 协议、kafka、snmptrap、ftp、smb、wmi、sftp 等采集协议格式的模式解析; 7、采集策略: 支持被采设备无需安装代理; 支持同一资产多种采集策略; 支持从不同类型系统采集到的日志进行标准化分析, 将不同格式日志映射到固定的解析字段中, 标准化处理后的字段细粒度≥ 90; 8、支持将采集到的日志进行过滤, 可以根据自身业务需求定制过滤策略, 做到将无关日志进行丢弃; 支持将采集到的日志进行归并, 可以根据自身业务需求定制归并策略, 做到在一定条件下将接收到的相同日志归并为一条, 并且显示该日志的接收次数, 使日志信息简明易看; 9、支持三权分立原则, 可设置安全管理员、安全审计员、系统管理员等角色, 通过赋予不同角色不同的权限, 以达到配置权力、审计权力、运维权力的相互制约;
37	抗 DDOS 攻击设备	1、业务接口: 千兆电口≥ 8个, 千兆光口≥ 2个, 千兆多模光模块≥ 2个, 万兆光口≥ 4个, 万兆多模光模块≥ 4个, 冗余交流电源; 2、网络层吞吐量$\geq 10Gbps$, 最大并发连接数$\geq 800w$, 最大每秒新建连接数(HTTP)$\geq 12w$; 3、产品由专用的国产化硬件平台、国产化操作系统及功能软件构成; 4、支持针对网络层、应用层分别设置清洗策略, 包括但不限于: SYN Flood、UDPFlood、ICMPFlood、DNSQuery/ReplyFlood、HTTPFlood、HTTPSFlood; 5、支持针对不同防护对象, 分别设置不同的异常流量清洗参数、算法等; 6、支持抓包溯源功能, 支持抓取清洗前、清洗后、清洗丢弃的报文进行分析; 针对抓包文件可以进行攻击源 IP 溯源, 并提取攻击报文中的攻击特征下发到清洗设备过滤;



		7、支持连接数新建及并发限制功能，可对 TCP 等协议设置阈值及周期； 8、支持会话数限制，可对源地址/目的地址做会话数限制，设置维度包括：服务类型（可定义服务类型）、用户、新建速率、总会话数、每 IP 会话数、生效时间等； 9、支持针对协议头中各字段配置自定义策略，字段包括但不限于：Method、Cookie、Host、Referer、RequestURI、Verion、User-Agent 等； 10、为保障异常流量安全清洗和业务系统稳定运行，抗 DDOS 攻击设备可以被统一运维管理平台监控。（提供和统一管理平台对接承诺函并加盖抗 DDOS 攻击设备厂商公章）
38	互联网 VPN 接入设备	1、具备千兆电口≥ 8个，千兆光口≥ 2个，万兆光口≥ 4个，万兆多模光模块≥ 4个，冗余交流电源；采用国产化 CPU 和操作系统； 2、整机吞吐量$\geq 9\text{Gbps}$，每秒新建连接数≥ 10万，最大并发连接数≥ 500万；VPN 加密性能：IPsecVPN 吞吐量$\geq 1\text{Gbps}$，IPsecVPN 隧道数≥ 2000个；SSLVPN 吞吐量$\geq 1\text{Gbps}$，SSLVPN 并发用户数≥ 3000个，总用户数不限； 3、支持集群：双机模式下，支持主备两台设备采用同一套 IP 地址，简化配置，节约公网地址； 4、内网攻击防护：基于内网用户流量模型和会话连接、新建连接的异常行为识别攻击，有效防护内网病毒传播、僵尸网络、木马等安全威胁； 5、支持静态路由、RIPv1/2、OSPF、策略路由等。支持 MPLSVPN；支持 MPLS 静态标签转发；支持 LDP 协议，支持 LDP 引入 OSPF 路由、BGP 路由、RIP 路由、静态路由、ISIS 路由、GUARD 路由，支持环路检测；支持 LDP 邻居，MPLS 转发表查看；支持 SVC 方式、CCC 方式、MARTINI 方式、VPLS 方式的 L2VPN；支持 MPLSTE； 6、提供设备的可靠性试验证明，（设备厂商提供证明材料）； 7、支持自动和手动备份，能够保存 5 个以上的文件，支持整机配置文件在线回滚功能，未变化的业务连续不中断； 8、登录公告：支持 VPN 登录前和登录后公告信息显示，登录前后公告内容可配置多条； 9、产品需要支持国密算法，具备商用密码产品认证证书；（提供证书复印件并加盖原厂商公章）
(四)	机房设备	
39	微模块机柜	1.外形尺寸：服务器机柜规格（W*D*H）：600mm*2000mm，前门为玻璃门，后门为钢板门。 2.机柜涂覆层应表面光洁、色泽均匀、无流挂、无露底；金属件无毛刺、无锈蚀。机柜门板、侧板平整，无扭曲、无变形、也不明显抖动；门板开孔均匀。 3.机柜由主框架、顶板、内嵌底板、前后门、侧横梁、矩形管、内立柱和固定层板组成。其中主框架、内立柱的、侧横梁的材料厚度不小于 2.0mm，后门、顶板、和侧板的材料厚度不小于 1.2mm。 4.为方便设备安装及维护，门板为可拆卸式结构，门的开合转动灵活、锁定可靠、施工安装和维护方便。 5.为了保障用电安全，要求机柜内各带电回路对地（或柜体）绝缘电阻不小于 $100\text{M}\Omega$， 6.机柜耐电压强度：要求机柜内各带电回路以及两个非电气连接的带电回路之间，应能承受 2500V，50HZ 正弦试验电压 1min，并不出现击穿或者飞弧现象，漏电流不超过 1mA。



		7.机柜附件：每个机柜含接地组件（接地线 6mm ² ），左后各 1 条垂直理线板，19 英寸安装接地铜排（3*15mm ² ），运输脚轮，LED 灯管+行程开关。
40	列头机柜	1.外形尺寸：服务器机柜规格（W*D*H）：600mm*2000mm，前门为玻璃门,后门为钢板门。 2.要求配电柜主路开关不小于 2*160A/3P，防雷模块不低于 C 级防雷模块。 3.要求配电柜支路开关不小于且不少于两路 24*32A/1P，支路监测参数要求包含：支路额定电流、实际电流，支路负载百分比，支路开关状态。
41	智慧机柜侧板	机柜配件,侧板,1400mm(D)*2000mm(H)
42	机柜锁具	机柜配件,电子锁*2,刷卡一体,带钥匙和 IC 卡 1 张,包含配套线缆
43	智慧机柜 M 型走线槽	顶部 M 型走线槽,600mm(W)*300(D)*150(H),强弱分离,带隔板
44	快开盲板	1U 免工具安装盲板,快开方式,钣金
45	水平理线器	水平理线器,482*44*80MM
46	智慧机柜轻载托盘	100kg 承重开孔托盘,19",适配 600 宽 1100 深以上机柜-微模块
47	L 型托架	50kg 承重 L 型托架 1 副(2 只,左右各 1)
48	智慧机柜专用普通 PDU	1.每个机柜标配 2 条 PDU，为设备 A/B 路供电使用。两条 PDU 应为同一规格,互为备份。 2.交流 PUD 采用黑色涂层，外壳选用优质型材或钢板，应具备强度高，坚固耐用，抗压性能、装配性能、耐蚀性能和装饰性能良好，表面喷涂效果好，工艺先进，纹路平整，美观大方等特点。 3.机柜 PDU 输出接口具有 GB 标准类型，10A 的插座不少于 16 个，16A 的插座不少于 4 个。
49	列间空调	1.总冷量≥35kw，显冷量≥35kw，风量≥6100m ³ /h，加湿量≥1.5kg/h，加热量≥4kW，水平送风模式； 2.可以实现常温情况下最低 10%的 IT 负载（即制冷量的 10%）稳定除湿量功能，降低高湿环境下数据中心低载运行的 IT 设备结露风险。 3.精密空调室内机采用高效工业用直流变频压缩机,可实现 10%~100%宽冷量输出； 4.为了相应国家节能降耗政策，要求空调全年能效比应大于 3.5； 5.具有 LCD 的真彩触摸显示屏，可以显示设备的运行模式与状态，并可设定设备参数，实现良好的人机交互 6.机组具备联动与群控功能，群控采用高速、灵活的 CAN 通讯协议，同一区域可以将≥32 套机组进行统一控制管理； 7.室内风机：要求采用高效后倾离心式 EC 风机。 8.要求空调机组设备符合 GB19413 相关标准。
50	盲柜	规格：≥300*1400*2000mm(W*D*H),黑色
51	机柜监控主机	1.通道动环监控主机，ARM 架构，Linux 系统；双交流供电，支持多路温湿度、烟雾、漏水、端口、天窗、空调、UPS、配电单元、消防、声光告警器等监测和/或控制。
52	微动环监	1.安装在服务器或 PC 端，通过有线连接，后台软件展示模块机房温湿度、通道门禁



	控平台系统软件	状态、能耗等环境实时监控数据; 2.为了保证机房健康运行,要求平台软件具有告警管理功能,可实现实时告警查看,待处理告警统计、历史告警查看以及可自定义设置告警阈值和告警等级等功能,且可自主远程邮件和短信发送相关负责人,可及时发现告警,并能及时处理,保障机房健康安全运行; 3.要求在本软件可实时查看行级空调运行状态和配电模块以及 UPS 电压、电流、电功率、负载百分比以及电池容量等运行状态。
53	电话、短信告警模块	可通过电话或短信的形式对告警内容进行通知。
54	手机 APP 客户端接入接口	手机 APP 客户端接入接口,须能够支持安卓 4.0 及以上智能设备-微模块
55	温湿度传感器	磁吸式温湿度传感器,测温范围:-20℃-70℃,测湿范围:0%-100%RH,12V 接线端子供电
56	烟雾探测器	机柜专用光电烟感探测器,磁吸式,工作电压:DC12V
57	声光报警器	磁吸式电子蜂鸣器,声压 105db,声频 1500 ± 500Hz,60mA,DC12V
58	水浸探测绳	非定位式水浸探测绳,配合非定位水浸传感器使用(5 米)
59	智慧模块化通道电源控制箱	一体柜控制箱,350W12V 开关电源,含照明灯,背景灯电源,2U
60	机房强弱电设备安装及配套辅材	机房强弱电设备安装费及配套辅材费,包括网线、电缆等。
(五)	其他设备	
61	指挥中心大屏	面积≥20m²; 点间距: 1.2mm; 封装方式: COB; 亮度: ≥800cd 分辨率: ≥4K;
62	可视化综合管控一体机	CPU: ≥16 核, ≥2.0GHz; 内存: ≥16GB; 硬盘: ≥2TB; 显卡: 显存≥4GB; 可实现对视频拼接处理的集中统一管理,控制各屏的输出内容,设备带有话筒、投屏器、控制台等外设。 另需包含管理软件,
63	拼接屏处理器	1.1920x1080p@60Hz 信号, 处理平台内部不进行任何抽帧, 满帧输出至显示设备, 支持场景轮循, 2.信号支持: 4096x2160@60hz, 4096x2160@30hz, 3840x2160@30hz, 3840x2400@30hz, 2560x1600@60hz 分辨率, 向下兼容其他分辨率,



		3.支持在输出通道上打开高达 16 个高清信号窗口，且每个窗口支持大小任意调整，图层顺序调整，支持多组屏硬回显，可同时将 4 组不同大屏的整体显示画面通过回显板卡传输至显示器，进行高清显示，回显帧率可达 60hz，可以在控制端实时回显大屏整体画面。 4.配置双控制卡，双电源
二	软件部分	
(一)	系统软件	
1	操作系统	具备文件管理、设备管理、日志管理、服务管理、进程和监控管理、网络管理、资源管理、软件包管理、硬件管理等基本功能，提供语言支持工具、文件共享服务工具、集成开发平台等常用工具，支持 KVM、Docker 虚拟化技术。 硬件支持：支持 X86 和 ARM 架构的处理器，如海光、鲲鹏、飞腾等；符合国家信创要求； 授权方式：按节点授权。
2	数据库	符合国家信创要求；具备数据存储、访问控制、身份鉴别、安全审计和数据备份恢复等功能。产品部署在服务器，以后台服务形式运行，数据库管理员及用户在管理主机上通过图形化管理工具或命令行工具，可实现对数据对象(表、视图、约束、索引、触发器、存储过程等)的配置管理；开发人员可通过标准化数据库访问接口，开发基于数据库的应用系统和软件产品。 授权方式：按节点授权。
3	中间件	用于为上层应用提供运行环境，实现对上层应用的部署和动态管理。主要功能包括 Web 容器、EJB 容器、数据源服务、集群管理等。产品可部署在信创服务器，以后台服务形式运行，用户通过管理控制台或者命令行工具完成上层应用的部署、启动、停止等操作。符合国家信创要求。 授权方式：按节点授权。
(二)	应用软件	
4	项目管理系统	项目管理系统可完整覆盖项目管理的各个过程，帮助企业建立研发管理体系，提高企业管理流程的稳健性和项目管理成熟度，大大提升项目成功的概率。 本系统主要提供标准化模板（如敏捷、瀑布模型），支持项目拆解了任务，设置任务的优先级和依赖性关系，制定预算并关联任务成本，设置交付物和验收标准。
5	统一运维管理系统	统一运维平台可以将本项目涉及的网络和安全设备进行集中管理，对网内安全设备、网络设备、服务器等进行实时运行状态监控，分析研判各类安全事件，通过访问控制策略的配置，实现大规模部署环境下灵活、便捷的安全策略管理，阻止敏感信息外泄和非核心业务的滥用；同时还可以联动现网扫描设备实现对选定终端设备类型的精确探测反馈，实现对终端信息的二次核验，确保网络的整体安全。设备含设备管理、网络监控、攻击监控、系统管理、通用图标等≥65 种大屏展示组件，可以以折线图、环形图、柱状图等形式进行展示。
6	统一门户	统一门户平台集成了本项目的所有应用（除智慧共享药房、针灸数智服务平台以外），实现一键登录，支持 his 集成,用户同步认证。 系统主要功能包括身份认证、身份管理、统一权限、单点登录、信息共享、应用管理与注册、门户管理、页面管理、部件管理、导航管理、内容管理等。
(三)	应用系统开发软件	
7	智慧共享中药房	结合当前中医药数字化的要求和医院的实际情况，为了更好地提高院内管理数字化水平尤其是中医药场景的管理，发挥区域医共体中心医院带头作用，方案主要从



		饮片调剂、煎煮等全流程可追溯追溯入手，满足中药房的数字化管理，将日常繁琐的工序进行优化，通过互联网、物联网等适宜的数字化手段的应用，在整体质量管理、高效管理等方面提高医院的整体数字化管理水平。 系统主要功能包括区县共享中账套管理，煎煮审核，煎药流程管理，流程预警管理，煎药业务查询和汇总，人员绩效管理，药房药库日常管理等。
8	数据整合 交换与数 据集成服 务系统	数据整合交换与数据集成服务系统是一个集数据采集、治理与监控管理为一体的综合性数据处理平台，旨在为医疗业务和管理提供全面、精准、高效的数据支撑。通过构建灵活多样的数据采集机制，包括批量、定时及实时采集，系统可快速整合来自多源业务系统的数据资源，确保数据的及时性与完整性。通过系统建设打通市县乡村各级数据共享和数据交换通道，为分级诊疗体系做好必要的基础准备。 系统主要功能包括大数据基础底座，分布式存储系统，批流一体化计算引擎，医疗数据存储计算，数据采集子系统，数据管理子系统，数据分类分级子系统，数据开放子系统，数据处理子系统，AI 数据中台等。
9	中医针灸 数智服务 系统	以针灸领域权威著作以及大规模临床数据为数据源，构建针灸大模型，针灸知识图谱，并将时空针灸融入其中，形成时空针灸知识图谱，从疾病和症状等多个维度构建针灸处方推荐算法，搭建针对中医针灸诊疗综合服务平台，以针灸大模型技术为特色，支撑针灸辅助诊断、处方审核、诊疗方案推荐、知识学习及查询、患者随访等功能。 系统主要功能包括针灸知识体系，针灸知识管理，针灸处方诊断与治疗决策智能体，针灸处方分析，临床应用服务，针灸疗效评价，针灸患者管理与服务等。
10	中医诊疗 服务质控 系统	通过对海量已完成的中医诊断案例进行流程与结果分析，系统能够识别出共性的诊疗模式与潜在的优化点，为推动中医诊疗流程的标准化提供数据支持。系统将对历史诊疗数据中的关键指标进行统计分析与趋势预警，帮助管理者识别系统性风险，从而在宏观层面指导医疗质量的持续改进，保障患者长远利益。 系统主要功能包括中医诊疗行为规范监控，医疗服务过程追踪与回溯，多模态疗效评价，中医医生实时监控管理分布图，AI 质控，人工质控，门诊病历质控，病案首页质控，住院病历质控，多维度质控结果分析，分类搜索引擎等。
11	中医药业 务智能监 管驾驶舱	中医药业务智能监管驾驶舱整合全市医疗机构中医诊疗与运营数据，主要面向区域卫生监管部门和医疗机构管理者，以“数据赋能中医药管理，智慧驱动业务决策”为核心目标，构建覆盖中医药服务全流程的智能监管体系，通过整合区域中医机构运营数据、疾病监测数据及患者行为数据并进行可视化呈现，管理者能够迅速掌握区域医疗资源的分布、利用情况，以及医疗服务的质量与效率，从而实现精准监管、科学决策，推动区域医疗服务的持续优化与升级。 系统主要功能包括自定义报表分析工具，数据填报，仪表板可视化编辑，组件配置，数据分析报表，业务运营主题分析，患者就诊行为分析，中医健康画像数据应用等。
12	中西医结 合数智类 脑系统	中西医结合数智类脑系统结合前沿 AI 模型搭建理念及技术，深度融合中医“理法方药”理论与西医诊疗理论，构建“中医为主、西医辅助”的智能诊断体系，通过多源数据获取与处理模块解析中西医临床文献、病历及标准规范，经文本分类、清洗、去重等加工形成高质量训练语料，基于渐进式预训练策略与指令微调、强化学习等技术，将中医经典理论与西医病理指标转化为模型算法，实现“中医辨证—西医验证”的协同推理；借助知识图谱构建中西医结合知识体系，通过混合检索与生成技术关联舌象脉象、检验指标等多模态数据，形成动态诊疗路径，既能基于中医辨证思维生成治法治则，又能调用西医检查数据辅助验证用药安全性，为中医智能辅助诊断服务系统，中医诊疗服务质控系统 etc 应用系统提供模型能力支撑。



		系统主要功能包括中西医结合基础大模型，临床智能对话大模型，中西医知识检索增强生成技术，中西医临床诊疗大模型，大模型应用服务系统，分布式程序数据搜索引擎,多云平台 API 资源批量化采集引擎，西医临床标准 word 文档处理套件，临床数据处理、非结构化 pdf 文件解析等。
三	其他	
1	网络租赁	提供 5 年网络带宽
2	数据治理服务	语料库建设 采集计划 历史数据采集范围数据采集标准编制技术准备 历史数据采集 增量数据同步范围实时数据采集 数据预处理 采集数据质量验证问题反馈与处理 数据汇聚 ODS 层模型设计和存储数据质控规则配置 实时质量监控 定期质量评估 问题处理与改进数据落标开发 数据标准规范 数据接口规范



附件 2: 《分项报价表》

序号	标的名称	规格型号	厂商名称	单位	数量	单价 (含税)	总价 (含税)	税率
一	硬件部分						33630000	
(一)	服务器						21610000	
1	大数据服务器	DH-RS2297VT	浙江华启智慧科技有限公司	台	18	190000	3420000	13%
2	应用服务器	DH-RS2297VT	浙江华启智慧科技有限公司	台	15	170000	2550000	13%
3	边缘超融合节点	FusionCube 1000	华为技术有限公司	套	2	900000	1800000	13%
4	高性能存储节点	OceanStor 5610	华为技术有限公司	台	2	2750000	5500000	13%
5	中心智算节点	CS5468H3	浪潮计算机科技有限公司	台	4	1380000	5520000	13%
6	边缘智算节点	DH-GS2298	浙江华启智慧科技有限公司	台	6	250000	1500000	13%
7	备份一体机	OceanProtect X3000	华为技术有限公司	台	2	170000	340000	13%
8	云平台	DCS	华为技术有限公司	套	1	980000	980000	13%
(二)	网络设备						6032000	
9	互联网核心交换机	S8700-10	华为技术有限公司	台	2	135000	270000	13%
10	互联网接入交换机	S6750-S16X10 Y2CZ	华为技术有限公司	台	2	35000	70000	13%
11	核心交换机	CE16804	华为技术有限公司	台	2	785000	1570000	13%
12	接入交换机	H3C S6805-56HP-G	新华三技术有限公司	台	10	132500	1325000	13%
13	存储互联交换机	H3C S6530X-48Y8C-G	新华三技术有限公司	台	2	178500	357000	13%



14	超融合接入交换机	H3C S6805-56HF-G	新华三技术有限公司	台	4	140000	560000	13 %
15	高速互联交换机	H3C S9855-32DH-G	新华三技术有限公司	台	1	1000000	1000000	13 %
16	管理交换机	H3C S5130S-54S-EI-G	新华三技术有限公司	台	4	20000	80000	13 %
17	应用负载均衡器	ADX3000-TM-G-E	杭州迪普科技股份有限公司	台	4	200000	800000	13 %
(三)	安全设备						4565000	
18	万兆防火墙 (专网区)	FW1000-TA-A10	杭州迪普科技股份有限公司	台	2	370000	740000	13 %
19	万兆防火墙 (互联网区)	FW1000-GC-G	杭州迪普科技股份有限公司	台	2	90000	180000	13 %
20	千兆防火墙	FW1000-MA-G	杭州迪普科技股份有限公司	台	2	45000	90000	13 %
21	WEB 应用防火墙	WAF3000-GC-G	杭州迪普科技股份有限公司	台	2	80000	160000	13 %
22	漏洞扫描	Scanner1000-MA-G	杭州迪普科技股份有限公司	台	1	90000	90000	13 %
23	入侵防御 (专网区)	IPS2000-MS-G	杭州迪普科技股份有限公司	台	2	70000	140000	13 %
24	入侵防御 (互联网区)	IPS2000-GC-G	杭州迪普科技股份有限公司	台	2	100000	200000	13 %
25	网络安全审计	UAG3000-GC-G	杭州迪普科技股份有限公司	台	2	110000	220000	13 %
26	堡垒机 (互联网)	LA-OS-7500-M	北京网御星云信息技术有限公司	台	1	100000	100000	13 %
27	堡垒机 (专网区)	LA-OS-7500-M	北京网御星云信息技术有限公司	台	1	115000	115000	13 %



28	数据库审计	DSP1000-MS-G	杭州迪普科技股份有限公司	台	2	100000	200000	13 %
29	服务密码机	HCM-G2500	北京网御星云信息技术有限公司	台	1	150000	150000	13 %
30	签名验签服务器	LeadsecSVT-G2000	北京网御星云信息技术有限公司	台	1	160000	160000	13 %
31	安全隔离与信息交换系统	ISG5000-GS-W-G	杭州迪普科技股份有限公司	台	2	120000	240000	13 %
32	态势感知平台	SAC3000-P-GA-G	杭州迪普科技股份有限公司	台	1	300000	300000	13 %
33	态势感知探针	SAC3000-S-GC-G	杭州迪普科技股份有限公司	套	1	90000	90000	13 %
34	杀毒软件	SW-XDR-PLAT	杭州迪普科技股份有限公司	套	1	60000	60000	13 %
35	日志审计(互联网区)	LSP1000-MS-G	杭州迪普科技股份有限公司	台	1	90000	90000	13 %
36	日志审计(专网区)	LSP1000-GS-G	杭州迪普科技股份有限公司	台	1	140000	140000	13 %
37	抗DDOS攻击设备	Guard3000-GA-G	杭州迪普科技股份有限公司	台	2	150000	300000	13 %
38	互联网VPN接入设备	VPN1000-GC-G	杭州迪普科技股份有限公司	台	2	400000	800000	13 %
(四)	机房设备						1056000	
39	微模块机柜	IC6000-X61420-B	新华三技术有限公司	台	15	7000	105000	13 %
40	列头机柜	PD-JM-160A-80KW-2	新华三技术有限公司	台	1	7000	7000	13 %
41	智慧机柜侧板	JG-CB1420-XW	新华三技术有限公司	套	2	700	1400	13 %



42	机柜锁具	JG-GS6DN	新华三技术有限公司	套	16	3000	48000	13 %
43	智慧机柜 M 型走线槽	JG-ZX-M33	新华三技术有限公司	套	20	350	7000	13 %
44	快开盲板	JG-MB-2U	新华三技术有限公司	个	150	150	22500	13 %
45	水平理线器	JG-LX-1-S	新华三技术有限公司	条	15	150	2250	13 %
46	智慧机柜轻载托盘	JG-TP-100-Q	新华三技术有限公司	块	15	150	2250	13 %
47	L 型托架	JG-TP-50-L	新华三技术有限公司	对	15	150	2250	13 %
48	智慧机柜专用普通 PDU	PDU-3224-S	新华三技术有限公司	个	30	480	14400	13 %
49	列间空调	KT-LFP-35-W S	新华三技术有限公司	套	4	130000	520000	13 %
50	盲柜	JG-JKZJ-300	新华三技术有限公司	套	4	2500	10000	13 %
51	机柜监控主机	IC1000-UA-X 04	新华三技术有限公司	台	1	15000	15000	13 %
52	微动环监控平台系统软件	ICMS-V1	新华三技术有限公司	套	1	10000	10000	13 %
53	电话、短信告警模块	SG-CHM4G7M 7	深圳栅格技术有限公司	个	1	30000	30000	13 %
54	手机 APP 客户端接入接口	APP	新华三信息技术有限公司	套	1	2500	2500	13 %
55	温湿度传感器	SG-TH-RS485	深圳市龙控智能技术有限公司	个	4	8000	32000	13 %



56	烟雾探测器	GD-S833	深圳栅格技术有限公司	个	4	550	2200	13 %
57	声光报警器	HC-103	深圳市豪恩安全科技有限公司	个	1	220	220	13 %
58	水浸探测绳	HW-58	贝特瑞新材料集团股份有限公司	根	4	660	2640	13 %
59	智慧模块化通道电源控制箱	TD-DGKZX-2	新华三信息技术有限公司	套	1	220	220	13 %
60	机房强弱电设备安装及配套辅材	定制	新华三信息技术有限公司(定制)	套	1	219170	219170	13 %
(五)	其他设备						367000	
61	指挥中心大屏	VDS012	利亚德光电股份有限公司	m²	20.25	16296.296	330000	13 %
62	可视化综合管控一体机	M660	联想(北京)有限公司	台	1	22000	22000	13 %
63	拼接屏处理器	MVC-11-C	利亚德光电股份有限公司	个	1	15000	15000	13 %
二	软件部分						37420000	
(一)	系统软件						3810000	
1	操作系统	银河麒麟高级服务器操作系统 V10	麒麟软件有限公司	套	55	7200	396000	13 %
2	数据库	Vastbase G100 V2.2	北京海量数据技术股份有限公司	套	25	78000	1950000	13 %
3	中间件	普元应用服务器软件 V6.5	普元信息技术股份有限公司	套	30	48800	1464000	13 %



(二)	应用软件						1550000	
4	项目管理系统	蓝凌科研项目管理平台软件[简称:RDM]V1.0	深圳市蓝凌软件股份有限公司	套	1	550000	550000	13%
5	统一运维管理系统	SW-UMC-PLAT	杭州迪普科技股份有限公司	套	1	300000	300000	13%
6	统一门户	曼荼罗智能门户系统软件V1.0	无锡曼荼罗信息技术有限公司	套	1	700000	700000	13%
(三)	应用系统开发软件						32060000	
7	智慧共享中药房	数字郑州科技有限公司定制化开发	数字郑州科技有限公司	套	1	1100000	1100000	6%
8	数据整合交换与数据集成服务系统	数字郑州科技有限公司定制化开发	数字郑州科技有限公司	套	1	14710000	14710000	6%
9	中医针灸数智服务系统	数字郑州科技有限公司定制化开发	数字郑州科技有限公司	套	1	4900000	4900000	6%
10	中医诊疗服务质控系统	数字郑州科技有限公司定制化开发	数字郑州科技有限公司	套	1	3950000	3950000	6%
11	中医药业务智能监管驾驶舱	数字郑州科技有限公司定制化开发	数字郑州科技有限公司	套	1	2700000	2700000	6%
12	中西医结合数智类脑系统	数字郑州科技有限公司定制化开发	数字郑州科技有限公司	套	1	4700000	4700000	6%
三	其他						3950000	



1	网络租赁	提供 5 年网络带宽	网络运营商 (数字郑州科技有限公司采购)	年	5	190000	950000	6%
2	数据治理服务	我司提供满足项目要求的数据治理服务	数字郑州科技有限公司	项	1	3000000	3000000	6%
合计		(大写)：柒仟伍佰万元整 (小写)：75,000,000.00 元						



附件 3：阶段性工作量确认报告

序号	系统名称	项目阶段	完成内容	标识物	合同金额 (万元)	涉及金额 比例	涉及金额 (万元)

