采购需求

一、项目背景

国务院办公厅关于推进医疗联合体建设和发展的指导意见国办发〔2017〕32号文："大力发展面向基层、边远和欠发达地区的远程医疗协作网，鼓励公立医院向基层医疗卫生机构提供远程医疗、远程教学、远程培训等服务，利用信息化手段促进资源纵向流动，提高优质医疗资源可及性和医疗服务整体效率。"

医疗集团信息化建设经历了 30 年的发展历程，财务、管理、医疗等部门陆续建立了各自的信息系统。但是，由于建设周期长，信息技术发展快，建设缺乏统一规划，这些信息系统大多数为分散建设，信息不能充分共享和交换，形成大量"信息烟囱"和"信息孤岛"。这就需要提供一个医疗集团信息平台，以解决医疗集团信息系统所包含的各类业务系统集成的问题。

二、项目概况

1、项目名称：武汉大学人民医院昌江黎族自治县医疗集团医疗信息化项目

2、预算金额：4596842.16 元

3、建设周期：12 个月

4、质保期：项目整体质保 24 个月，部分产品按规定质保

5、实施地点：昌江黎族自治县

6、验收方式：由采购人组织有关部门按照国家有关标准的规定进行验收

7、付款方式：签订合同后按合同约定内容付款

8、工作内容

本期项目在医疗集团原有信息系统的基础上，新建智慧医疗集成平台、分级诊疗平台，打通医疗集团内部数据层及业务层，实现各级医院、卫生站之间数据互联互通、并实现分级诊疗。扩充医疗集团网络资源，建设昌江县医疗集团信息中心一个网络汇聚接入点，昌江县人民医院、昌江中西医结合医院、海尾卫生院、七叉卫生院、太坡卫生院、乌烈卫生院 6 个网络分支接入点互联；扩充中心机房计算资源和存储资源，以适应新业务的拓展。

三、项目建设内容需求

（一）硬件部分

序号	名　称	技术参数	单位	数量
一	**中心机房服务器**			
1	应用服务器	4U 机架式 芯片组：Intel C624 芯片组 CPU：4*Xeon Gold 5117 14C 105W 2.0GHz 处理器，最大支持 4 颗 CPU 内存：4*32GB DDR4 2666 MHz，最大 48 条内存 硬盘：2*2.5 英寸 600GB 15K SAS 12Gb 热插拔 512n 硬盘，标配 8 个硬盘位，最大支持 16 个 2.5 英寸硬盘扩展 阵列卡：RAID 730-8i 1GB 高速缓存 PCIe 12Gb 适配器 网卡：4 个千兆网口+1 个千兆管理口 HBA 卡：1 块双口 16G HBA 卡 电源：1+1 冗余电源 服务 三年 7*24 保修	台	1
2	存储设备	2U 高度 12 盘位 双控制器，16GB 缓存 8 个 16G FC 主机接口； IOPS 250K Broadwell 多核（2 Cores），硬件 RAID 加速 本次配置 1 个主柜，10 块 1.2TB 10K 2.5″ SAS HDD，最大支持 240 块 2.5 英寸硬盘扩展 128 Snapshot 标配，自动精简配置，宽条带化 冗余电源，冗余风扇 三年保修服务	台	1
3	KVM	8 口 KVM，一体折叠液晶套件，17 寸显示屏	套	1
4	配件	虚拟媒体连接线缆 VCO （1 根一包）	套	2
5	双机热备软件	HA 双机热备软件	套	1
6	显示器	19.5 英寸 IPS 液晶宽屏显示器 16:9 电脑显示器（VGA 接口），配鼠标键盘	台	4
7	数据整理及迁移服务	1.项目包括所采购设备安装调试、数据库、操作系统群集安装调试、硬件设备优化以及跟据医院的 HIS 等业务的特性的要求，按规划实现相关系统的部署，并安装相关的集成应用系统。 2.项目供应商要完成医院原有业务系统及历史数	项	1

		据整理及迁移工作任务，并确保数据无丢失。		
	小计 1			
二	医院安全等保设备			
1	下一代防火墙(一)	**硬件指标和性能指标：** 1、标准 2U 机箱，冗余电源，配置 6 个 10/100/1000M 自适应电口，4 个千兆光口插槽，2 个万兆光口插槽（含 2 个万兆多模光模块），128GB SSD 固态硬盘存储，1 个 Console 口，支持液晶屏。 2、多核 AMP+架构，网络层吞吐量 18G，应用层吞吐量 7.5Gbps，IPSec VPN 加密速度 1.2Gbps，SSL 最大加密流量 500Mbps，并发连接≥350 万，每秒新建连接数 26 万。 3、配置三年威胁情报升级服务，提供三年硬件维保服务。 **技术功能参数：** 1、支持 VTEP（VxLanTunnelEndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLANNetworkIdentifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定。 2、支持基于 IPv4/v6 地址、应用的会话限制，限制动作包每 IP 新建、每 IP 并发、所有 IP 新建、所有 IP 并发，且可以基于安全域指定限制方向； 3、▲支持与终端管理软件联动，实现基于终端健康状态的访问控制，增强防火墙对木马特征的识别能力（提供功能截图，并加盖厂商公章）。 4、支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMPTrap、邮件、声音、短信等方式告警。 5、支持 IPv4 和 IPv6 流量的 HTTPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，并可同时基于安全域、IPv4 和 IPv6 地址进行例外设置； 6、▲支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看威胁详情和处置详情；支持基于受害主机、威胁情报一键跳转威胁活动统计分析（提供功能截图，并加盖厂商公章）； 7、▲支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为；提供关联	台	1

		的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL 过滤、文件过滤等安全模块检查的日志集中显示（提供功能截图，并加盖厂商公章） **资质要求：** 1.产品具备《计算机信息系统安全专用销售许可证》（增强级）； 2.▲为保证产品大数据分析安全能力，设备厂商应具有《国测信息安全服务资质-大数据安全类证书》（提供证明材料并加盖厂商公章） 3.▲为保证产品自身的开发安全能力，设备厂商应具有《CCRC 信息安全服务资质-软件安全开发服务资质》（提供证明材料并加盖厂商公章）； 4.▲为保证产品自身的开发安全能力，备厂商应具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+）（提供证明材料并加盖厂商公章）； 5.▲具备《中国国家信息安全产品认证证书》（提供证明材料并加盖厂商公章）； 6.▲投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名，（提供证明材料并加盖厂商公章）； 7.▲投标设备厂商具备 ITSS 认证证书，（提供证明材料并加盖厂商公章）；。 8.▲为保证本项目交付后的产品安全运维效果，要求设备厂商具备专业的信息安全运维能力，并取得权威机构的认证资质，设备厂商应具有 CCRC 信息安全服务资质-安全运维服务资质（一级），（提供证明材料并加盖厂商公章）； 9. 为保证信息安全培训的能力，设备厂商应具有《CISP 授权服务机构证书》； 10.▲为保证项目整体交付的综合建设规划能力，设备厂商应具有《信息化建设及服务能力评价资质一级证书》，（提供证明材料并加盖厂商公章）；		
2	下一代防火墙(二)	**硬件指标和性能指标：** 1、标准 2U 机箱，冗余电源，配置 10 个 10/100/1000M 自适应电口，8 个千兆光口插槽，128GB SSD 固态硬盘存储，1 个 Console 口，支持液晶屏； 多核 AMP+架构，网络层吞吐量 8G，应用层吞吐量 5Gbps，IPSec VPN 加密速度 700Mbps，SSL 最大加密流量 400Mbps，并发连接≥230 万，每秒新建连	台	1

		接数 15 万；提供三年硬件维保服务。 **技术功能参数：** 1.支持 VTEP（VxLanTunnelEndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLANNetworkIdentifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定。 2.支持基于 IPv4/v6 地址、应用的会话限制，限制动作包每 IP 新建、每 IP 并发、所有 IP 新建、所有 IP 并发，且可以基于安全域指定限制方向； 3.▲支持与云端联动，至少实现病毒云查杀、云沙箱等功能；支持与终端管理软件联动，实现基于终端健康状态的访问控制，增强防火墙对木马特征的识别能力（提供功能截图，并加盖厂商公章）。 4.▲支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 PingofDeath、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片等；并可在设备页面显示每种攻击类型的丢包统计结果（提供功能截图，并加盖厂商公章）； 5.支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查；支持通过 802.3ad 协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余；支持 MTU≥9016byte 的巨型帧 JumboFrame。 6.▲支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量；支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级；（提供功能截图，并加盖厂商公章）； 7.▲支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果（提供功能截图，并加盖厂商公章） **设备厂商为保证自身产品安全，应具有以下资质要求：** 1.具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级）； 2.▲为保证产品大数据分析安全能力，设备厂商应具有《国测信息安全服务资质-大数据安全类证		

		书》（提供证明材料并加盖厂商公章）； 3.▲为保证产品自身的开发安全能力，设备厂商应具有《CCRC 信息安全服务资质-软件安全开发服务资质》（提供证明材料并加盖厂商公章）； 4.▲具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+）（提供证明材料并加盖厂商公章）； 5.具备《中国国家信息安全产品认证证书》； 6.▲投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名，（提供证明材料并加盖厂商公章）； 7.▲投标设备厂商具备 ITSS 认证证书，（提供证明材料并加盖厂商公章）；。 8.▲为保证本项目交付后的产品安全运维效果，要求设备厂商具备专业的信息安全运维能力，并取得权威机构的认证资质，设备厂商应具有 CCRC 信息安全服务资质-安全运维服务资质（一级），（提供证明材料并加盖厂商公章）； 9.为保证信息安全培训的能力，设备厂商应具有《CISP 授权服务机构证书》； 10.▲为保证项目整体交付的综合建设规划能力，设备厂商应具有《信息化建设及服务能力评价资质一级证书》，（提供证明材料并加盖厂商公章）;		
3	下一代防火墙(三)	1. **硬件指标和性能指标：** 1、标准 1U 机箱，单电源，配置 6 个 10/100/1000M 自适应电口，2 个 SFP 插槽，另有 1 个接口板卡扩展插槽，64GB SSD 固态硬盘存储，1 个 Console 口； 2、多核 AMP+架构，网络层吞吐量 6G，应用层吞吐量 3G，IPSec VPN 加密速度 400Mbps，SSL 最大加密流量 200Mbps，并发连接≥200 万，每秒新建连接数 8 万； 3、配置三年 IPS、AV、URL 过滤、应用过滤、威胁情报检测功能授权及特征升级服务，提供三年硬件维保服务。 **技术功能参数：** 1、▲支持 VTEP（VxLanTunnelEndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLANNetworkIdentifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定。	台	1

		（提供功能截图，并加盖厂商公章）； 2、支持基于 IPv4/v6 地址、应用的会话限制，限制动作包每 IP 新建、每 IP 并发、所有 IP 新建、所有 IP 并发，且可以基于安全域指定限制方向； 3、▲支持与云端联动，至少实现病毒云查杀、云沙箱等功能；支持与终端管理软件联动，实现基于终端健康状态的访问控制，增强防火墙对木马特征的识别能力（提供功能截图，并加盖厂商公章）。 4、支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMPTrap、邮件、声音、短信等方式告警。 5、支持 IPv4 和 IPv6 流量的 HTTPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，并可同时基于安全域、IPv4 和 IPv6 地址进行例外设置； 6、支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看威胁详情和处置详情；支持基于受害主机、威胁情报一键跳转威胁活动统计分析； 7、▲支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为；提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL 过滤、文件过滤等安全模块检查的日志集中显示（提供功能截图，并加盖厂商公章） **资质要求：** 1. 具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级）； 2.▲为保证产品大数据分析安全能力，设备厂商应具有《国测信息安全服务资质-大数据安全类证书》（提供证明材料并加盖厂商公章）； 3.▲为保证产品自身的开发安全能力，设备厂商应具有《CCRC 信息安全服务资质-软件安全开发服务资质》（提供证明材料并加盖厂商公章）； 4.▲具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+）（提供证明材料并加盖厂商公章）； 5.具备《中国国家信息安全产品认证证书》； 6.▲投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名，（提供证		

		明材料并加盖厂商公章）； 7.▲投标设备厂商具备 ITSS 认证证书，（提供证明材料并加盖厂商公章）。 8.▲为保证本项目交付后的产品安全运维效果，要求设备厂商具备专业的信息安全运维能力，并取得权威机构的认证资质，设备厂商应具有 CCRC 信息安全服务资质-安全运维服务资质（一级），（提供证明材料并加盖厂商公章）； 9.为保证信息安全培训的能力，设备厂商应具有《CISP 授权服务机构证书》； 10.▲为保证项目整体交付的综合建设规划能力，设备厂商应具有《信息化建设及服务能力评价资质一级证书》，（提供证明材料并加盖厂商公章）；		
4	日志审计	硬件指标和性能指标： 标准 1U 机箱，6 个千兆电口，2 个扩展插槽，1 个 Console 接口，单电源，4T 硬盘。事件采集 10000EPS，事件处理最高 3000EPS。配置 100 个授权节点，提供三年硬件维保服务。 技术功能参数： 1、支持审计各种网络设备、安全设备、主机操作系统、数据库、中间件配置日志、运行日志、告警日志等；支持各种应用各种应用系统配置日志、运行日志、告警日志等； 2、▲支持自定义实时监视场景，提供可视化规则编辑视图，对关注的事件进行实时展示；支持鼠标放在日志对应字段上界面可悬浮提示资产信息和常用端口信息。（要求提供功能截图证明，并加盖厂商公章）。 3、▲支持自定义实时分析场景，提供可视化规则编辑视图，根据实际业务编写分析规则；支持对于关联事件进行追溯，查看导致该关联事件的所有原始事件（要求提供功能截图证明，并加盖厂商公章） 4、能够在世界地图上实时定位事件源/目的 IP 地址的地理位置（包括二维及三维显示方式） 5、▲可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则；（要求提供功能截图证明，并加盖厂商公章） **资质要求：** 1、▲产品需要提供公安部《计算机信息系统专用产品销售许可证》。（提供证明材料并加盖厂商公章）； 2、▲产品需要提供中国信息安全认证中心《中国	台	1

		国家安全产品认证证书》3C。（提供证明材料并加盖厂商公章）； 3、▲产品需要提供国家信息安全测评中心《信息技术产品安全测试证书》EAL3+。（提供证明材料并加盖厂商公章）； 4、▲投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名，（要求提供证明材料并加盖厂商有效印章）。 5、▲投标网络安全产品制造商具备 ITSS 认证证书，（要求提供证明材料并加盖厂商有效印章）。 6、▲为保证本项目交付后的产品安全运维效果，要求设备厂商具备专业的信息安全运维能力，并取得权威机构的认证资质，设备厂商应具有 CCRC 信息安全服务资质-安全运维服务资质(一级)(资质级别分为三级，其中一级为最高级)，（要求提供证明材料并加盖厂商有效印章）。		
5	终端检测响应（一）	终端安全管理系统控制中心：▲支持控制中心防暴力破解，采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证；（要求提供产品界面和手机动态令牌 APP 截图并加盖厂商公章）	套	1
	终端检测响应（二）	技术功能参数： 1、Windows 服务器系统支持 windows server 2003/2008/2012/2016. 2、支持文件与目录自定义黑白名单的方式来管理全网终端的文件；文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件； 3、支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件； 4、▲具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能；（要求提供功能截图证明，并加盖厂商公章） 5、支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃；	套	15
	终端检测响应（三）	**技术功能参数：** 1.Windows 终端操作系统支持 Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10； 2.支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置 3.能够支持漏洞利用防御，尤其对通过文件漏洞（尤其是 0day 漏洞）的攻击行为进行有效检测与	套	400

		防御； 4.▲对敲诈者病毒提供防护机制，同时提供解密工具，解密工具应为自主研发；（要求提供功能截图证明，并加盖厂商公章） 5.▲具备本地多引擎查杀能力，且引擎可配置；支持对暴力破解事件攻击源 IP 加入黑名单，已加入黑名单的 IP 无法访问网内所有终端。（要求提供功能截图证明，并加盖厂商公章）； 6.支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件 7.支持远程协助终端（不依赖 Windows 远程桌面协议）、远程关机、重启终端； 8.具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端 P2P 补丁分发加速，有效节省外网带宽资源。 9.▲支持与防火墙产品联动，实现基于终端健康状态的访问控制，增强防火墙设备对木马病毒的的识别和防御能力（要求提供功能截图证明，并加盖厂商公章） **资质要求：** 1.产品具备《计算机信息系统安全专用产品销售许可证》，提供证明材料 2.产品具备中国信息安全测评中心 EAL2 证书，提供证明材料 3.▲提供近两年国内市场份额排名前三的第三方权威机构证明文件 4.▲投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名（要求提供证明材料并加盖厂商有效印章）。 5.▲投标网络安全产品制造商具备 ITSS 认证证书，（要求提供证明材料并加盖厂商有效印章）。 6.▲为保证本项目交付后的产品安全运维效果，要求设备厂商具备专业的信息安全运维能力，并取得权威机构的认证资质，设备厂商应具有 CCRC 信息安全服务资质-安全运维服务资质(一级)(资质级别分为三级，其中一级为最高级），（要求提供证明材料并加盖厂商有效印章）。		

6	上网行为管理	1、**硬件指标和性能指标：** 1U 硬件，标配 6 个千兆电接口（其中含 1 个管理接口和 1 个 HA 接口），4 个千兆光口插槽，单交流电源。建议 200M 带宽/1500 人网络环境使用；最大并发连接数为 80 万，最大新建连接数为 26000 个/秒；含专用操作系统与上网行为管理标准软件。 提供三年软件版本升级服务，三年硬件质保服务。 **技术功能参数：** 1.支持网关模式、网桥模式，网桥模式支持多入多出的透明网桥模式部署，旁路部署模式等不影响用户既有网络结构 2.▲支持 key 免审计、key 免管控、key 免认证三者的组合（提供证明截图，并加盖厂商公章） 3.当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈； 4、可以记录应用行为，并对于阻断的应用可以触发告警，并支持邮件及语音双重告警； 5、支持多级虚拟通道，可以将物理带宽分成至少 7 级虚拟通道，合理分配物理带宽资源；支持基于连接数进行流量管理，可以每个人的并发/新建连接数量进行控制； 6、▲支通过 NETBIOS 审计策略对 NETBIOS 通信、登录名及文件、目录进行审计和控制（提供证明截图，并加盖厂商公章） 7、▲设备能够根据终端管理软件检测到的信息配置准入控制策略，准入条件包括系统是否安装了特定的杀毒软件和特定版本；系统是否安装了特定的漏洞补丁；系统是否开启了文件实施防护功能等（提供证明截图，并加盖厂商公章） **资质要求：** 1.公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》 2.▲中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，级别为 EAL3+（提供证明材料并加盖厂商公章） 3. ▲投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名，（要求提供证明材料并加盖厂商有效印章）。 4.▲投标网络安全产品制造商具备 ITSS 认证证	台	1

		书，（要求提供证明材料并加盖厂商有效印章）。 5.▲为保证本项目交付后的产品安全运维效果，要求设备厂商具备专业的信息安全运维能力，并取得权威机构的认证资质，设备厂商应具有 CCRC 信息安全服务资质-安全运维服务资质（一级）（资质级别分为三级，其中一级为最高级），（要求提供证明材料并加盖厂商有效印章）。		
7	堡垒机	1、**硬件指标和性能指标：** 标准 1U 机架式，6 个千兆电口，支持 2 个接口扩展槽位，内置 4TB 硬盘，单电源，支持液晶屏，最大支持 150 路图形会话或 700 路字符会话并发。配置 100 个运维资源授权，提供三年标准售后服务。 **技术功能参数：** 1、▲支持自定义系统事件对应的消息等级;支持基于消息等级、消息类型设置是否告警和告警方式（要求提供功能截图，并加盖厂商公章） 2、▲支持用户的 IP 地址（黑名单或白名单）和 MAC 地址限制（黑名单或白名单）限制，非法地址无法登陆；支持用户的批量修改，包括重置密码、移动部门、更改角色、修改多因子配置、修改有效期、修改 IP 限制、修改 MAC 限制（要求提供截图，并加盖公章） 3、▲访问控制策略基于用户、用户组、资源账户、账户组、有效期、文件管理控制、文件传输控制（上传、下载）、RDP 剪切板控制、时间限制、IP 限制进行设置（要求提供功能截图，并加盖厂商公章） 4、内置常用的系统类型，包括 Linux、Windows、H3C、Huawei、Cisco 5、支持系统负载、内核信息、内存信息、网卡信息、磁盘使用信息、路由表信息、ARP 表信息等运行状态信息的采集； 6、系统内置多种系统报表和运维报表模板，支持按日、周、月为周期，自动生成报表 7、用户多次登录失败将自动锁定账户或 IP，可配置解锁时长、到期自动解锁，也可以手动解锁 **资质要求：** 1.公安部颁发的《计算机信息系统安全专用产品销售许可证》 2.产品需要提供中国信息安全认证中心《信息安全产品认证证书》。	台	1

		3.▲投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名，（要求提供证明材料并加盖厂商有效印章）。 4.▲投标网络安全产品制造商具备 ITSS 认证证书，（要求提供证明材料并加盖厂商有效印章）。 5.▲为保证本项目交付后的产品安全运维效果，要求设备厂商具备专业的信息安全运维能力，并取得权威机构的认证资质，设备厂商应具有 CCRC 信息安全服务资质-安全运维服务资质(一级)(资质级别分为三级，其中一级为最高级)，（要求提供证明材料并加盖厂商有效印章）。		
8	数据库审计	**硬件指标和性能指标：** 标准 1U 机箱，单电源；标配 6 个千兆自适应电口（包含 2 组 bypass），4 个千兆光口插槽，1 个 Console 口，支持 1 个扩展槽位，支持液晶屏。事件处理 12000 条/秒，内置 4TB 磁盘存储空间。提供三年软件升级和硬件维修服务。 **技术功能参数：** 1.支持 Telnet、pop3、smtp、nfs 协议审计，针对 FTP 协议，txt 文件传输可对其内容进行的审计； 2.支持对 MySQL、Oracle、sqlserver、mongodb、redis 数据库的状态监控，主动发现数据库潜在风险； 3.▲提供基于环境动态，整体地洞悉安全风险，以数据为基础，从全局视角提升对安全威胁的发现识别、理解分析的数据库态势感知，及时发现各种异常和危险操作，为整体信息安全管理提供决策依据（要求提供功能截图，并加盖厂商公章） 4.全面支持后关系型数据库 Cache 的集成工具 terminal、portal、studio、Sqlmanager、MedTrak 工具的审计，Terminal 能审计到 M 语句和返回结果（要求提供功能截图，并加盖厂商公章） 5.▲支持 B/S、C/S 应用系统三层架构 http 应用审计，可提取包括应用系统的应用层帐号、数据库帐号、操作系统用户名、客户端主机名、客户端 IP、客户端 MAC 等身份信息，精确定位到人，并可获取 XML 返回结果（要求提供功能截图，并加盖厂商公章） 6.▲本身具备能发现未知仿冒进程工具、防范非法 IP 地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）、	台	1

		设置系统黑白名单等安全功能（要求提供功能截图，并加盖厂商公章）		
	小计 2			
三	**医院核心交换机及卫生汇聚交换机**			
1	主机箱(核心交换机)	交换机主机箱，共 8 个槽位，包含 2 个引擎槽位和 6 个业务槽位	台	2
2	主控引擎(核心交换机)	交换机高性能一代主控引擎，设备性能：交换容量≥80T，包转发性能≥28000Mpps；二层功能：802.11Q 4K,QinQ、SUPER VLAN；链路聚合，端口镜像;三层功能:支持 DHCP SERVER;支持 BGP4/4+、ISISv4/v6、OSPFv2/v3、VRRPv2/v3、支持 BFD 与 RIP/OSPF/BGP 联动；支持 GR for RIP/OSPF/BGP/ISIS 等；支持 MPLS PE；支持配置 POE 线卡，并由独立 POE 电源槽供电，防止因 POE 供电而影响其他业务模块供电稳定性。	台	4
3	电源(核心交换机)	通用电源模块（可以冗余，交流，600W）	个	4
4	线卡(核心交换机)	24 端口千兆以太网光口(SFP,LC)+12 端口千兆以太网电口复用(RJ45)+4 端口万兆以太网光口(SFP+,LC)	块	2
5	千兆单模光模块(核心交换机)	1000BASE-LX 转换模块（1310nm）	个	32
6	万兆单模光模块(核心交换机)	万兆 LC 接口模块（1310nm），10km，适用于 SFP+接口	个	6
7	万兆光缆(核心交换机)	10G Base SFP+ 光纤线缆（包含两边的模块），3 米	个	2
8	千兆交换机(汇聚交换机)	24 个 10/100/1000Base-T 自适应以太网端口+4 个 SFP+端口，固化单风扇，2 个模块化电源插槽，至少需要购买 1 个电源模块		4
9	电源（汇聚交换机）	交流电源模块		8
10	千兆单模光模块(汇聚交换机)	1000BASE-LX 转换模块（1310nm），10km		32
	小计 3			
四	**各接入点路由器**			
1	5 个卫生院-接入层路由器	支持 8 个千兆电口，支持 2 个 WAN 口；支持 7 口 POE 供电，整机 POE 最大输出 135W，单口 PoE 最大输出 30W。支持企业总分 VPN 组网，支持本地微信/短信/WEB 认证，内置无线控制器，支持上网行为管理，内置网监对接。	台	5
2	昌江县人民医院-核心	固化 8 个千兆电口，固化 8 个千兆光口，固化 8	台	1

	路由器	个万兆光口，固化 2 个 40G 光口，32G 内存，两个硬盘插槽，支持 1T 企业级硬盘，硬盘不随机内置，需要单独另配。内置风扇，1+1 冗余电源		
	昌江县人民医院-万兆单模光模块	万兆 LC 接口模块（1310nm），10km，适用于 SFP+接口	块	2
	昌江县人民医院-千兆单模光模块	1000BASE-LX 转换模块（1310nm）	块	2
	小计 4			
	合计			

（二）软件部分：

序号	名　称	模块
一	**医疗集团集成平台基础层**	信息集成引擎
		一体化开发平台
		集成平台接入支持包（供各厂商接入）
	小计 1	
二	**分级诊疗协同服务平台软件**	
1	注册中心	个人注册服务
		医疗卫生人员注册服务
		医疗卫生机构注册服务
2	全景同屏分级诊疗服务	用户管理
		会诊流程管理（会诊申请、资料审核、会诊安排、会诊记录、会诊报告）
		全景同屏会诊管理（即时会诊呼叫及应答服务、音视频交互服务）
3	互联网全景移动会诊服务	移动用户注册
		患者资料订阅/推送
		融合通讯服务
	小计 2	
三	**中心分级诊疗平台**	
1	医疗异构系统信息集成软件	异构数据源定义
		异构数据接口管理
		医院患者索引
		患者诊疗数据获取
		患者诊疗数据存储管理
2	分级诊疗终端	用户登录
		电子病历浏览

		检验结果浏览
		检查报告浏览
		医嘱信息浏览
		会诊通讯录
		会诊申请/会诊报告
		即时会诊呼叫/应答
		会诊实时同屏交互功能
		会诊记录查询
		视音频信号采集交互
3	移动会诊APP（50用户）	用户登录
		患者管理
		病情摘要浏览
		检验结果浏览
		检查报告浏览
		会诊申请/会诊报告
		即时会诊呼叫/应答功能
		会诊实时同屏交互
		融合通讯功能
	小计3	
四	**接入卫生院分级诊疗**	
1	医院管理系统医疗	基本医疗信息管理
		门诊与住院病案书写
		医嘱录入与管理功能
		门诊医生工作组
		住院医生工作站
		门诊护士工作站
		住院护士工作站
		药库管理
		门诊药房管理
		住院药房管理
		中药库管理
		门诊中药房管理
		住院中药房管理
		农合
		城镇居民
		社保
		全国异地农合
		全国异地社保
		耗材管理
		设备管理

		挂号
		门诊收费
		住院收费
		慢病管理
		统计
	异构系统信息集成软件	药品管理系统
		异构数据源定义
		异构数据接口管理
		患者诊疗数据获取
2	分级诊疗终端	用户登录
		电子病历浏览
		检验结果浏览
		检查报告浏览
		医嘱信息浏览
		会诊通讯录
		会诊申请/会诊报告
		即时会诊呼叫/应答
		会诊实时同屏交互功能
		会诊记录查询
		视音频信号采集交互
3	移动会诊APP（5用户）	用户登录
		患者管理
		病情摘要浏览
		检验结果浏览
		检查报告浏览
		会诊申请/会诊报告
		即时会诊呼叫/应答功能
		会诊实时同屏交互
		融合通讯功能
	小计4	
	合计	

（三）系统集成需求：

序号	项目	单位	数量
1	系统集成	项	1

（四）专线电路需求（一年）：

序号	安装地点	产品	电路路由		带宽
			A端	Z端	

1	海尾卫生院	数字电路	昌江医疗集团数据中心	海尾卫生院	50M
2	七叉卫生院	数字电路	昌江医疗集团数据中心	七叉卫生院	50M
3	太坡卫生院	数字电路	昌江医疗集团数据中心	太坡卫生院	50M
4	乌烈卫生院	数字电路	昌江医疗集团数据中心	乌烈卫生院	50M
5	中西医结合医院	数字电路	昌江医疗集团数据中心	中西医结合医院	150M
6	昌江县人民医院	互联网专线		昌江医疗集团数据中心	250M