**桂林市中西医结合医院**

**综合评选文件**

**项目名称：桂林市中西医结合医院信息网络安全**

**等级保护建设（第二期）询价公告**

**2021年11月**

桂林市中西医结合医院信息网络安全等级保护建设（第二期）项目询价公告

桂林市中西医结合医院对信息网络安全等级保护建设（第二期）项目采购进行综合评选，欢迎符合条件的参询单位参加综合评选。

一、项目名称：桂林市中西医结合医院对信息网络安全等级保护建设（第二期）项目

二、对参询单位要求
（一）符合《中华人民共和国政府采购法》第22条要求；
（二）本次询价不接受联合体参询；
（三）本项目未经采购人许可不得转包、分包；
三、报名信息
（一）报名时间：2021年 11 月 24  日至2021年 11 月 30   日下午6点，逾期不再接收报名；
（二）报名地点：桂林市七星区半塘路6号 桂林市中西医结合医院 信息科；
（三）参询单位报名时须提供：具有系统集成资格的证照资料，营业执照、税务登记证、组织机构代码证(三证合一的提供三证合一证)、法人身份证(如是授权委托的提供授权委托人身份证)， 以上文件需提供复印件并加盖单位公章，如是法人授权委托的须提供授权委托书原件并加盖单位公章；近3年内无不良记录，无采取不合法方式解决合同纠纷记录证明或承诺（原件）加盖单位公章；提供在“信用中国”网站(www.creditchina.gov.cn)或中国政府采购网(www.ccgp.gov.cn)等渠道被未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的证明，证明材料需提供网站截图并盖公章。
四、综合评选响应文件要求
（一）本项目预算控制价： 壹佰柒拾捌万元整（￥ 1780000.00元），报价不得超过控制价；
（二）所提供的证书必须合法有效；
（三）超出评选时间，不再接收综合评选响应文件；
（四）所有文件一式七份（一正六副）；
（五）报价文件必须密封；
（六）所有纸质文件必须逐页盖章；
提交的响应文件如有任何一项不符合要求则取消参询资格。
五、综合评选推荐原则
（一）综合评选委员会由医院院内人员组成，评选委员会根据综合得分由高到低排序，若得分相同时，按评选报价由低到高排序；若仍相同的，依次按照技术参数分、综合信誉分、服务承诺分由高到低排序。
（二）采购人将以排名第一的参询报价、参数等内容为主要参照，送第三方招标代理公开招标。
六、评选时间及联系方式
（一）参询具体时间和地点：另行通知。
（二）联系人：杨宜学，电话：18378315570

桂林市中西医结合医院

2021年11月 24 日

**二、服务需求一览表**

**说明：**

**1**、**本服务需求一览表中选注★号的内容为实质性要求和条件。**

**2、本次服务采购最高限价为：178万元。**

**3、参询文件中加盖的参询专用章与公章同等效力。**

4、采购人的信息系统等级安全保护项目（第一期）购置了保垒机、服务器区域防火墙、内网虚拟化安全管理系统、内外网终端安全管理系统、防勒索病毒系统、内网虚拟化数据持续保护软件的部分系统容灾等安全设备设施，并制定了相应的安全策略。

5、第二期项目主要是在第一期建设成果的基础上，按照等保2.0的要求，围绕内外网的移动办公、准入管控、应急灾备等业务开展的实际需要进行相应设计，加强防护。总体设计方案要有兼容性、延续性、拓展性，二期是一期的补充和完善，保障内外网信息系统安全，指导三级等保测评需要涉及的HIS等类的应用系统进行相应的改造，持续整改，完成预测评报告并达到本项目采购内容的预测评目标，确保最终顺利通过三级等保测评。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项号** | **服务名称** | **数量** | **参考品牌** | **服务内容及质量要求** |
| 1 | 内网防火墙 | 1台 | 相当于或者优于360、天融信、山石网科、奇安信 | 1、★多核AMP+架构，网络层吞吐量≥20G，并发连接≥600万，IPsec吞吐量≥6Gbps，防病毒吞吐量≥3Gbps，IPS吞吐量≥4Gbps，每秒新建连接数12万，IPSec隧道数1万个，最大SSLVPN用户数8000个。 冗余电源，≥4个千兆Combo接口，≥4个千兆电口（含一对Bypass接口），≥4个SFP口，≥2个万兆SFP+口，至少提供4个万兆多模光模块，3年标准功能模块升级服务（包含病毒过滤、入侵防御、URL分类库、流控QoS功能模块与特征库升级），初次购买包含功能开通服务，至少含100个SSLVPN并发用户许可；2、支持OSPF、BGP、RIPv1/v2路由，并支持图形化界面配置；3、支持基于角色、用户、服务、应用、URL、IP等的策略路由；支持基于URL的策略路由，支持基于时间、URL的智能引流技术，对具体URL的访问动作进行策略引流，将某个URL的流量引到特定的链路上；4、支持目的路由、目的接口路由、源路由、源接口路由、ISP路由；5、支持BFD 功能，支持BFD与静态路由/OSPF/BGP进行联动。快速检测到与相邻设备间的通信故障，减小设备故障对业务的影响。通过与动态路由协议联动，缩短收敛时间，提升可靠性；6、支持NAT地址可用性探测，支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断。7、支持源NAT、目的NAT、静态NAT，支持一对一、一对多和多对多等形式的NAT；支持源地址和目标地址的同时转换，即BNAT；支持NAT444模式，支持导出NAT444静态映射表。8、支持基于国家地理位置、URL等元素建立安全策略； 9、支持DNS代理功能，可基于入接口、源地址、目的地址、域名、动作、DNS代理失败动作等多维度设置DNS代理策略；10、支持策略命中分析，可基于命中数、首次命中时间、最近一次命中时间、最近未命中天数等维度进行优化统计；11、支持标准802.3ad 链路聚合，多条链路带宽进行捆绑，支持基于源MAC、目的MAC、源IP、目的IP、源端口、目的端口、协议类型等方式组合进行负载。12、支持策略命中分析，可基于命中数、首次命中时间、最近一次命中时间、最近未命中天数等维度进行优化统计；13、具备对应用程序的识别和控制能力。应用程序特征库不少于4000种，并支持在线/手动更新；14、支持内置URL分类过滤库；支持自定义URL分类过滤；支持批量添加自定义URL，支持批量导入URL；支持基于SSL解密的URL过滤；支持基于URL关键字类别进行阻断或记录日志。15、支持对压缩文件类型的病毒检测，必须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型，支持对多重压缩文件的病毒检测，且不小于5层压缩，支持对超出行为自定义处理方式。 |
| 2 | 互联网防火墙 | 2台 | 相当于或者优于360、天融信、山石网科、奇安信 | 1、★多核AMP+架构，网络层吞吐量≥10G，并发连接≥320万，每秒新建连接数9万，IPSec隧道数1万个，最大SSLVPN用户数6000个。IPsec吞吐量≥3.8Gbps，防病毒吞吐量≥2.5Gbps，IPS吞吐量≥4Gbps。 ≥6个千兆电口（含一对Bypass接口），≥4个SFP光口，≥2个万兆SFP+口，至少提供4个千兆多模光模块，3年标准功能模块升级服务（包含病毒过滤、入侵防御、URL分类库、流控QoS功能模块与特征库升级）；至少含100个SSLVPN并发用户许可；2、支持OSPF、BGP、RIPv1/v2路由，并支持图形化界面配置； 3、支持基于角色、用户、服务、应用、URL、IP等的策略路由；支持基于URL的策略路由，支持基于时间、URL的智能引流技术，对具体URL的访问动作进行策略引流，将某个URL的流量引到特定的链路上；4、⯁支持目的路由、目的接口路由、源路由、源接口路由、ISP路由；5、支持BFD 功能，支持BFD与静态路由/OSPF/BGP进行联动。快速检测到与相邻设备间的通信故障，减小设备故障对业务的影响。通过与动态路由协议联动，缩短收敛时间，提升可靠性；6、支持NAT地址可用性探测，支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断。7、支持源NAT、目的NAT、静态NAT，支持一对一、一对多和多对多等形式的NAT；支持源地址和目标地址的同时转换，即BNAT；支持NAT444模式，支持导出NAT444静态映射表。8、支持基于国家地理位置、URL等元素建立安全策略； 9、支持DNS代理功能，可基于入接口、源地址、目的地址、域名、动作、DNS代理失败动作等多维度设置DNS代理策略；10、支持策略命中分析，可基于命中数、首次命中时间、最近一次命中时间、最近未命中天数等维度进行优化统计；11、支持标准802.3ad 链路聚合，多条链路带宽进行捆绑，支持基于源MAC、目的MAC、源IP、目的IP、源端口、目的端口、协议类型等方式组合进行负载。12、支持策略命中分析，可基于命中数、首次命中时间、最近一次命中时间、最近未命中天数等维度进行优化统计；13、具备对应用程序的识别和控制能力。应用程序特征库不少于4000种，并支持在线/手动更新；14、支持内置URL分类过滤库；支持自定义URL分类过滤；支持批量添加自定义URL，支持批量导入URL；支持基于SSL解密的URL过滤；支持基于URL关键字类别进行阻断或记录日志。15、支持对压缩文件类型的病毒检测，必须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型，支持对多重压缩文件的病毒检测，且不小于5层压缩，支持对超出行为自定义处理方式。 |
| 3 | 服务器区WEB应用防火墙 | 2台 | 相当于或者优于360、天融信、山石网科、奇安信 | 1、★多核CPU硬件架构，网络层吞吐不低于22G，网络并发连接数≥250万，HTTP并发连接数≥200万，HTTP新建连接数≥1万。冗余电源，≥4 个 GE 接口（2 组 Bypass 口），≥4个SPF+口，≥4个SPF口，至少提供4个千兆多模光模块和4个万兆多模光模块。16GB内存，1TB硬盘。可防护站点数不少于129个。2、默认包含三年免费WAF特征库升级3、系统具备Web访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御4、系统具备注入攻击防御能力，可以对SQL注入、LDAP注入、SSI指令注入、Xpath注入、命令注入、邮件注入、远程文件包含、本地文件包含以及其他注入进行防御； 5、具备个人敏感信息防泄漏功能，可以检测到个人身份信息（包括中国大陆身份证号、港澳台身份证号、美国社会安全号）、银行卡号、信用卡号、邮件账号的信息泄露；6、支持细粒度的HTTP命令级访问控制策略，可以根据客户端Host、 User-Agent、Accept、Accept-Language、Accept-Encoding、Referer、Cookie等HTTP头部的策略控制；7、系统具备特殊漏洞攻击防御能力，可以对针对Web服务器、Web框架、Web应用程序的漏洞攻击进行防御8、支持包括不限于对HTTP协议异常、注入攻击、跨站攻击、信息泄露、探测访问、特殊漏洞攻击、恶意软件等类型攻击的规则防护9、支持对防护站点设置客户端、URL等方式的白名单策略10、支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略；学习的内容包括：动态URL地址、URL参数、HTTP访问方法等信息。11、★产品支持Web应用漏扫，支持的扫描各种类型的Web漏洞包括：SQL注入漏洞、XSS攻击漏洞、Web服务漏洞、信息泄露漏洞、异常访问漏洞；扫描方式支持普通扫描和侵入式扫描；支持手动扫描和定期扫描，可以定期自动扫描。12、可以根据扫描报告生成虚拟补丁，用户无需中断业务即可针对Web漏洞提供快速保护。13、提供丰富的日志信息，包括设备管理日志、网络安全日志、网页安全日志、防篡改日志、访问控制日志、自学习策略日志等。 |
| 4 | 日志审计 | 1台 | 相当于或者优于360、天融信、亚信、奇安信 | 1、1U设备，内存≥32G，硬盘：4T，≥ 6个千兆电口，≥100个日志源，日志处理性能≥5000EPS,峰值≥6000/秒；2、具备常见标准设备的一键接入能力，支持的设备类型包括：APT、防病毒、路由器、防火墙等。对非标准设备，支持高级创建功能，自定义数据接入和解析方式；3、当采用jdbc、ftp、ssh等主动采集协议采集时，支持采集节点自动热备切换，当数据采集主节点故障时；4、当采用webService、UDP、TCP、SNMP、NetFlow、Syslog、SNMP等被动采集协议采集时，支持多个采集节点负载均衡部署方式；5、支持采集集群管理，可以跨主机进行采集点的添加与删除，支持在集群节点任意主机上发布、删除采集节点，把采集程序发布至另一台主机上运行；6、数据归档支持索引自动下线，根据设置的自动下线时间天数，自动将超时索引转为离线索引以节省资源；7、支持数据处理集群，多个节点可以组成集群，支持在集群节点内任意主机上发布、删除、修改数据处理模块，把数据处理模块进程发布于指定主机上运行；8、支持常见设备日志的格式解析，支持100种以上的品牌和型号，包括各类Unix、Windows、堡垒机、IDS、WAF、IPS、防绕行、防火墙、SSLVPN、服务器、数据库、路由器、流量设备；9、对于默认不支持的新型号设备，支持自定义解析格式配置，无需进行二次开发，即可支持新设备特殊日志格式解析。10、支持采用搜索语言进行高级搜索，支持10种以上搜索语法，包括：关键字搜索、组合条件AND OR进行拼接查询、top分组指令、head取前N条事件、tail取尾N条事件、sort排序，dategap事件量时间轴能力、stats统计能力、table制表能力、pivot多字段分组等；11、支持审计分析场景，包含主机安全审计、中间件安全审计、数据库安全审计、NetFlow流量分析、防火墙安全审计场景；12、在被动采集方式下，支持批量创建模式，可以一次性将一个采集进程发布至所有采集群集节点上；13、支持自定义组合策略，策略中可以包含多种条件，触发告警事件； |
| 5 | 上网行为管理 | 1台 | 相当于或者优于360、天融信、山石网科、奇安信 | 1、★性能参数：网络层吞吐量：≥5Gb，应用层吞吐量：≥1.6Mb，带宽性能≥500Mb，最大并发连接数≥200万，≥4个千兆光口，≥4个千兆电口，含三年上网行为管理特征库授权；2、支持文件缓存，支持安卓和IOS形式的文件，主动缓存文件形式不限于视频、APP等；3、⯁设备智能解析用户流量，针对域名或者文件请求，设备推送文件至终端，帮助用户缓解互联网出口压力，实现文件下载加速的效果；支持本地安全防护，包括但不限于入侵防御、病毒查杀、DDOS、异常包防护等，入侵防御规则不少于8000条，病毒防护规则不少于200万。4、支持路由模式、透明（网桥）模式、混合模式、旁路模式；旁路部署支持加入多个物理接口；部署模式切换无需重启设备5、支持七元组策略路由，支持基于线路权重进行负载转发6、支持7元组的链路负载均衡策略，负载均衡接口支持接口和接口组，支持基于域名进行链路负载，负载算法包括但不少于优先级和权重，负载均衡接口支持pppoe、dhcp、tunnel、物理接口等三层接口。7、支持基于负载链路进行dns-dnat机制，解决用户主机配置DNS解析结果，与实际转发运营商链路解析结果有冲突，从而导致跨运营商访问慢的问题；支持进行DNS探测，针对探测失败情况，支持选择禁用dns-dnat功能或禁用负载链路出接口8、应用特征不少于5000个，移动应用不少于450个。9、支持针对搜索引擎、http、网页内容进行关键字过滤并实时生成日志记录，日志级别包括但不少于紧急、告警、严重、通知、信息、调试、不记录等，方便管理员快速区分用户上网行为属性和定位日志级别。10、支持在设备旁路部署时针对违规上网行为进行阻断过滤。11、针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长12、支持监控用户和应用实时流速，包括用户名、应用名、用户组、上行速率、下行速率、总速率、会话数等信息，帮助管理员快速甄别网络异常行为；支持数据下钻跳转至详细列表，针对用户支持通过趋势图形式，按照时间顺序展示该用户网络会话和流量趋势，支持下钻跳转至详细列表访问的应用组成和流速情况。针对应用支持通过趋势图形式，按照时间顺序展示该应用会话和流量趋势，支持下钻跳转至详细列表使用该应用的用户、速率和会话数等情况。13、支持与行为感知平台进行深入联动，基于上网行为管理的海量上网日志，对用户行为特征进行深度建模分析，不断推出不同场景的行为感知应用，持续挖掘数据价值，帮助组织洞悉行为风险，简化运维管理。 |
| 6 | 漏洞扫描 | 1台 | 相当于或者优于360、天融信、山石网科、奇安信 | 1、标准1U机架式，1T硬盘，标准配置6个10/100/1000M自适应电口，2个扩展插槽,液晶面板显示，2个USB口，1个Console口，单电源。含3年漏洞特征库升级，3年硬件维修服务。2、Web扫描域名无限制，Web扫描任务并发数为10个域名。系统扫描IP地址最大支持1024个，支持扫描A类、B类、C类地址，系统扫描支持100个IP地址并行扫描。3、具备B/S架构设计，并采用SSL加密通信方式，用户可以通过浏览器远程方便的对产品进行管理；4、支持多种扫描方式，提供对IP、域名、资产、批量检测等目标扫描方式；同时具备自定义漏洞扫描方式，提供类别、风险级别等自定义方式。5、具备端口扫描范围自定义功能，支持标准、全部、指定端口等至少4种端口检测；6、支持主流虚拟机管理系统的漏洞检查，支持Vmware ESX\Vmware ESXi等相关漏洞；7、漏洞库列表数量大于60000条，漏洞知识库与CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准兼容。8、具备对iOS、Android、Blackberry、windowsphone等操作系统；9、具备对常见P2P软件的安全漏洞检测，包含对常见的电驴、iTunes、BitTorrent等软件的安全检测；10、具备对后门检测的安全漏洞检查，包括对Microsoft IIS、特洛伊木马检测、Mac OS X恶意程序等常见后门漏洞的安全检测；11、具备对网页暗链、敏感词汇、网站木马的检测。12、具备SMB、TELNET、FTP、SSH、POP3、MSSQL、MYSQL、ORACLE、DB2、SNMP等协议进行口令猜测；13、具备字典上传功能，基于协议、口令类型的字典自定义设置。14、具备告警功能，支持邮件、短信、SNMP、Syslog、FTP等多种告警机制。15、具备自定义报表功能，提供对标题、信息、LOGO等数据的自定义；同时可对导出报表进行加密处理，并设置自定义密码功能。 |
| 7 | 互联网准入认证系统 | 1套 | 相当于或者优于360、天融信、山石网科、亚信 | 1、★≥6个千兆电口、≥4T硬盘，至少支持2000个终端准入认证，至少包含1000客户端三年使用授权； 2、产品支持有线或无线网络环境下的准入管理。3、支持配置网内合法的交换机认证列表，支持导入导出，通过配置密钥控制合法准入通道；支持手动或自动审批终端入网行为；4、支持配置例外终端，对于特殊终端或网络设备，无需进行认证也能接入网络；5、支持多种验证模式，包括用户身份合法即可接入网络、用户和终端身份均合法可接入网络、身份合法用户使用指定合法设备方可接入网络；6、支持用户身份合法性校验方式，包括口令、U-key认证；终端设备合法性校验方式，包括通过入网审批、安装客户端；7、支持终端入网检测，未通过检测的计算机不能接入网络。支持多VLAN、多路由器、NAT形式的地址转换环境；要求准入管理不依赖网络设备，适应任何类型网络，无需修改现有网络配置，不受防火墙限制；8、准入网关的部署方式支持网桥方式、旁路镜像、策略路由方式；9、支持无客户端准入管理，入网方式包括分配用户名（账号）和密码（口令）入网、通过登录授权码入网，支持设置重新认证时长；10、⯁支持Portal准入，可配置临时入网账号；（需提供产品功能界面截图，并加盖参询公章）11、要求支持设置自定义安全检查方案，同时设置多个检查项，并支持与、或关系的叠加组合。检查项内容包括注册表值、注册表项、Windows补丁、进程、服务、文件存在、文件版本、文件修改时间等；12、支持移动终端例外入网，识别移动终端数据包的关键字，而不是通过IP或MAC识别例外设备；13、要求产品具备有效控制私接路由器进入局域网、仿冒合法IP和MAC的入网行为； |
| 8 | 内网准入认证系统 | 1套 | 相当于或者优于360、天融信、山石网科、亚信 | 1、≥6个千兆电口、≥4T硬盘，至少支持2000个终端准入认证，至少包含1500个客户端三年使用授权； 2、产品支持有线或无线网络环境下的准入管理。3、支持配置网内合法的交换机认证列表，支持导入导出，通过配置密钥控制合法准入通道；支持手动或自动审批终端入网行为；4、支持配置例外终端，对于特殊终端或网络设备，无需进行认证也能接入网络；5、支持多种验证模式，包括用户身份合法即可接入网络、用户和终端身份均合法可接入网络、身份合法用户使用指定合法设备方可接入网络；6、支持用户身份合法性校验方式，包括口令、U-key认证；终端设备合法性校验方式，包括通过入网审批、安装客户端；7、支持终端入网检测，未通过检测的计算机不能接入网络。支持多VLAN、多路由器、NAT形式的地址转换环境；要求准入管理不依赖网络设备，适应任何类型网络，无需修改现有网络配置，不受防火墙限制；8、准入网关的部署方式支持网桥方式、旁路镜像、策略路由方式；9、支持无客户端准入管理，入网方式包括分配用户名（账号）和密码（口令）入网、通过登录授权码入网，支持设置重新认证时长；10、支持Portal准入，可配置临时入网账号； 11、要求支持设置自定义安全检查方案，同时设置多个检查项，并支持与、或关系的叠加组合。检查项内容包括注册表值、注册表项、Windows补丁、进程、服务、文件存在、文件版本、文件修改时间等；12、支持移动终端例外入网，识别移动终端数据包的关键字，而不是通过IP或MAC识别例外设备；13、★要求产品具备有效控制私接路由器进入局域网、仿冒合法IP和MAC的入网行为； |
| 9 | 外网核心交换机 | 1台 | 相当于或者优于华为、H3C、迈普 | 三层以太网交换机，至少含24个SFP光口,冗余风扇模块，至少含18个千兆单模光模块，至少含6个千兆多模光模块。 |
| 10 | 内网应急灾备一体机 | 1台 | 相当于或者优于美创、安和金华、精容数安 | ★1、具备≥12个硬盘槽位，≥2颗64位CPU（至强4214，主频2.2GHz，12核，24线程），≥512GB高速缓存；配置≥6块4TB SAS硬盘，≥2个480GB SSD系统盘，≥2个千兆电口，≥2个万兆光口，配置≥1GB缓存 阵列卡（支持RAID 0,1,5,6,10.50,60，含掉电保护电池模块），冗余电源。★2、；配置≥24TB硬盘容量备份许可（初始安装后被保护的硬件平台，软件永久使用）。（1）永久定时备份授权：≥345个x86平台下客户端备份许可；≥79个x86平台下Oracle备份许可；≥48个x86平台下MySQL备份许可；≥102个x86平台下SQL Server 备份许可；≥112个x86平台下DB2备份许可；≥543台个虚拟机备份授权；（2）永久实时容灾备份授权：≥8个数据库复制、≥12个服务器容灾模块：提供业务系统容灾所需的计算、存储、网络资源，以及相关的定时/实时数据同步功能模块，并通过统一界面管理，实现在一套一体机内能同时能接管多个业务系统的运行。3、支持NAT穿透技术，支持将备份系统部署在内网中，也可以同时备份外网的数据。4、内置集成容器平台，可在一体机中创建镜像，容器，用于数据恢复演练及测试相关工作5、为避免病毒及勒索软件对备份数据的破坏，备份系统支持将磁盘介质虚拟成磁带格式，支持（LTO4-LTO8磁带格式）。并提供相关端口映射配置，可将虚拟带库任意机械臂、驱动器映射到指定端口。6、支持以租户为单位无代理备份和恢复OpenStack的实例、卷、快照及镜像7、支持无代理备份Docker的镜像与容器实例8、支持数据库离线恢复，即备份数据不但可直接恢复至数据库，同时也支持将备份数据恢复成文件，恢复的文件可以以离线的方式在异地直接恢复至异地数据库，完全不依赖备份系统，同时也不需要在异地搭建备份系统9、★支持数据库事务级实时同步复制，实时将数据库备份到目标端，目标端数据库实时可读，RPO指标达到秒级，RTO分钟级，数据库实时备份支持主流商业及开源数据库，包括SQL Server、Oracle、MySQL、IBM DB2（提供SQL Server、Oracle、MySQL、IBM DB2。 10、支持模拟备份功能，可在不执行实际备份的前提下，获取到备份目标的文件数量、数据大小等信息，以便更合理地规划配置备份任务。11、备份过程中支持通过安全传输协议（TLS）进行加密，保证数据传输的全过程安全。可自定义加密证书，支持CA证书加密。12、支持VMware、H3C CAS、华为FusionCompute、深信服HCI、XenServer、oVirt、ZStack、OpenStack等主流虚拟化、云平台的无代理备份。13、数据库采用实时同步复制的方式进行保护，当源端出现故障，则将业务手动切换至备用端数据库即可，无需恢复。当源端环境恢复完成后，将数据反向回传，再选择适合时间将业务回切至源端。数据回传过程中无需暂停业务运行，仅需在业务回切时暂停数分钟。14、软、硬质保三年，提供首次上门安装服务，7\*24小时电话、邮件、远程技术支持服务。 |
| 11 | 互联网应急灾备一体机 | 1台 | 相当于或者优于美创、安和金华、精容数安 | ★1、具备≥12个硬盘槽位，≥2颗64位CPU（至强3106，主频1.7GHz，8核，8线程），≥128GB高速缓存；≥4块4TB SAS硬盘，≥2个千兆电口，≥2块240GB SSD系统盘，配置≥1GB缓存阵列卡（支持RAID 0,1,5,6,10.50,60，含掉电保护电池模块），冗余电源。★2、配置≥16TB硬盘容量备份许可。（1）永久定时备份授权：≥215个x86平台下客户端备份许可；≥44个x86平台下Oracle备份许可；≥36个x86平台下MySQL备份许可；≥70个x86平台下SQL Server备份许可；≥29个x86平台下DB2备份许可；≥112台个虚拟机备份授权；（2）永久实时容灾备份授权：≥4个数据库复制、≥4个服务器容灾模块：提供业务系统容灾所需的计算、存储、网络资源，以及相关的定时/实时数据同步功能模块，并通过统一界面管理，实现在一套一体机内能同时能接管多个业务系统的运行。3、内置集成容器平台，可在一体机中创建镜像，容器，用于数据恢复演练及测试相关工作4、为避免病毒及勒索软件对备份数据的破坏，备份系统支持将磁盘介质虚拟成磁带格式，支持（LTO4-LTO8磁带格式）。并提供相关端口映射配置，可将虚拟带库任意机械臂、驱动器映射到指定端口。5、支持以租户为单位无代理备份和恢复OpenStack的实例、卷、快照及镜像。6、支持无代理备份Docker的镜像与容器实例7、支持数据库离线恢复，即备份数据不但可直接恢复至数据库，同时也支持将备份数据恢复成文件，恢复的文件可以以离线的方式在异地直接恢复至异地数据库，完全不依赖备份系统，同时也不需要在异地搭建备份系统8、支持数据库事务级实时同步复制，实时将数据库备份到目标端，目标端数据库实时可读，RPO指标达到秒级，RTO分钟级，数据库实时备份支持主流商业及开源数据库，包括SQL Server、Oracle、MySQL、IBM DB2。9、支持模拟备份功能，可在不执行实际备份的前提下，获取到备份目标的文件数量、数据大小等信息，以便更合理地规划配置备份任务。10、备份过程中支持通过安全传输协议（TLS）进行加密，保证数据传输的全过程安全。可自定义加密证书，支持CA证书加密。11、支持VMware、H3C CAS、华为FusionCompute、深信服HCI、XenServer、oVirt、ZStack、OpenStack等主流虚拟化、云平台的无代理备份。12、数据库采用实时同步复制的方式进行保护，当源端出现故障，则将业务手动切换至备用端数据库即可，无需恢复。当源端环境恢复完成后，将数据反向回传，再选择适合时间将业务回切至源端。数据回传过程中无需暂停业务运行，仅需在业务回切时暂停数分钟。13、软、硬质保三年，提供首次上门安装服务，7\*24小时电话、邮件、远程技术支持服务。 |
| 12 | 容灾软件授权扩容 | 1项 | 相当于或者优于美创、安和金华、精容数安 | 1、≥15个虚拟机保护许可授权与技术服务。2、在数据中心内提供持续数据保护功能，能够在备数据中心保存过去一段时间内应用数据的持续恢复点，最长支持恢复到一年以前的时间点。3、可以捕获并记录每一个写I/O操作，当数据需要恢复时，用户可从时间点中选择，使应用程序能够基于以前的事务快速地从任一时间点恢复。4、提供一致性组功能，可以将某个特定应用程序的所有LUN绑定到一个一致性组中，以确保事务向以前时间点的回滚同时进行，从而确保应用程序的一致恢复5、可以由应用程序和系统自动生成事件书签，也可以由用户向系统输入自己的书签，通过书签，将系统范围的事件（端口故障、系统错误等）与潜在的损坏事件关联起来，管理员可以通过选择书签来恢复数据，从而确保恢复的数据是正确的。6、对于捕获的写I/O，既支持复制到本地站点，也支持复制到远程容灾站点。以上两种方式可以配合使用，提供对同一数据卷的并行本地和远程保护。7、本次配置本地容灾方式。8、I/O拆分功能既能在本项目虚拟化环境上实现，不需要宿主机系统代理实现。9、采用IP连接方式10、提供恢复点整合功能，可以让用户能够决定将捕获的每一个写I/O操作保留多久，在哪一时间点将数据更改整合成一个每日、每周或每月恢复点，从而让用户能够以一致性组为单位优化使用的日志空间，这样只使用其一部分就可以跟踪每一个写操作；余下的空间可用于保存每日、每周或每月恢复点。 11、支持同步和异步复制，捕获的写I/O通过异步复制到远程容灾站点是，可以通过IP网络传输。12、支持在执行故障切换之前装载复制的映像以处理和检查一致性的能力采用“带外”基于网络的应用装置，不在主 I/O 路径中进行监控和数据保护，不影响主机性能。13、支持虚拟化操作系统VMWare ESX，宿主机不限操作系统。14、提供可在多种主机系统上运行的基于 Java 的管理界面，使管理员能够集中管理所有的操作，包括设置复制关系和参数、查看复制状态、恢复到某一时间点，和启动生产故障切换等。 |
| 13 | 主机房改造服务 | 1项 | 国产 | 1、封窗工程：对机房内的3个玻璃窗进行封窗，用防火板从机房里进行封窗，防止雨水等渗透入机房。2、配置2樘1.2米的防火防盗门。3、防静电手环：机房内7个机柜每个机柜配一套防静电手环。4、理线服务：将机柜内的各类线缆进行理线服务，强弱电线路分开整理。 |
| 14 | 灾备机房改造服务 | 1项 | 国产 | 1、封窗工程：对机房内的1个玻璃窗进行封窗，用防火板从机房里进行封窗，防止雨水等渗透入机房2、配置0.9米的防火防盗门3、防静电手环：机房内3个机柜每个机柜配一套防静电手环4、理线服务：将机柜内的各类线缆进行理线服务，强弱电线路分开整理。 |
| 15 | 零信任网关 | 1套 | 相当于或者优于奇安信、天融信、启明星辰、360 | 1、VPN系统主机，标准1U机箱，冗余电源，配置6\*10/100/1000电口，另有2个SFP接口，1T工业级硬盘；2、最大并发用户数800，含100人并发授权，100个ID的授权用户3、网络接口地址配置支持IPv6地址，网络路由地址配置支持IPv6地址；4、支持多链路接入、支持策略路由、支持链路聚合；5、支持B/S和C/S的应用支持单点登录（SSO），并提供加密认证功能。访问多个应用，只须输入一次密码，支持针对不同的访问资源设定不同的SSO用户名和密码。6、支持预防'syn flood'攻击，忽略icmp回显请求（不能被ping）；7、可单独对每个应用发布业务进行负载均衡，具有轮询、加权轮询、最少连接数、静态就近性、动态就近性等算法来实现； 8、支持管理员自定义用户登录帮助文档，通过虚拟门户上传到SSLVPN用户的WEB登录界面，文档格式支持word和TXT；9、支持国产化中选麒麟操作系统客户端APP，在Linux系统平台下不依赖火狐浏览器，具备独立的SSLVPN客户端；10、支持SSLVPN设备的管理端口和用户端口分离功能，管理端口不对公网进行映射，保证设备自身安全，用户可自定义管理端口；11、支持终端使用Win7、win7 64位、win8、win10、Mac、Linux等操作系统登录，保证登录后能够正常访问SSL VPN发布的服务；12、支持智能终端访问的业务和PC端访问的业务分离，可设置具体应用仅允许PC访问或者仅允许智能终端访问，支持智能终端连接网关后，只能走安全隧道，防止互联网访问；13、根据IOS或Android的状态root、越狱、杀毒结果进行准入控制；14、支持15种认证方式，包括本地认证、USBKey、短信认证、数据库认证、邮箱认证、证书认证、动态令牌认证、LDAP认证、windows AD认证、RADIUS认证，并且支持支持本地用户名密码、证书认证、第三方证书、LDAP、短信验证码、邮箱验证码、动态令牌之间的“与”的认证。可实现USBKey认证、LDAP认证、硬件特征码等多种因子绑定认证；15、支持用户访问业务的详细日志记录，如账号、密码、提交POST内容；16、支持RADIUS双机认证，管理员可定义的Radius 属性组与系统中其他组一样作为授权对象，可实时与RADIUS建立联系，保证用户数据更新，保证认证的高可用性；17、支持动态令牌APP根据网关配置的安全策略，实现一人一机绑定，达到硬件token的安全要求； 18、支持LDAP用户动态化和策略化，实现组织单元映射、属性映射，并支持成员组反向映射；19、支持移动应用封装功能，客户上传移动应用APP进行封装、加固；支持对移动应用本身进行病毒、木马检测，以保证移动应用自身安全；20、支持应用防火墙功能，包括能够设置URL、应用的黑白名单；能记录用户访问Http、邮件、QQ等信息；21、支持用户长期不登录时自动锁定，被锁定后需要管理员才能解锁；22、支持与终端安全管理软件联动，可以检查终端安全软件进程，并根据是否安装来判断用户接入情况，并能自动弹出IE链接提示客户下载安装。 |
| 16 | 态势感知分析平台 | 1台 | 相当于或者优于奇安信、天融信、启明星辰、360 | 1、硬件参数：≥20核心40线程CPU，≥128GB内存，冗余电源，≥600GBSAS盘+32TB企业级存储硬盘；2、支持IPv4和IPv6两种部署场景，支持对IPv4和IPv6协议流量分析和还原；提供B/S架构，采用HTTPS方式管理，无需安装管理客户端。3、支持检测暴力破解，可自定义时间范围、登录次数产生暴力破解的告警，如果用户不修改配置，则默认5分钟内尝试登录超过50次将产生暴力破解的告警，支持10种协议包括：FTP、MYSQL、PGSQL、TDS、TNS、RESP、DB2、Sybase、MongoDB、LDAP等；4、提供对流量中邮件协议进行识别和解析，支持SMTP、POP3、IMAP、Webmail；5、提供还原文件传输协议包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB；6、支持主动资产采集能力，支持对服务器资产、域名、端口、应用、网址等资产的探测。7、⯁具备攻击结果判断能力；（提供产品界面截图并加盖参询公章）8、提供常规渗透入侵、内网横向渗透，提供精细化规则65条，例如读取/etc/passwd文件、执行ipconfig命令、执行netstat命令等，提供web木马类型300+种，木马隧道5种，挖矿页面6种等各类黑客攻击和恶意流量进行实时精准入侵动作识别及报警，并能够检测出系统中受控的服务器，定位出当前企业受影响的业务模块；9、支持基于域渗透攻击检测，支持Kerberoasting攻击、票据请求加密降级 、万能钥匙被动检测等；10、支持基于人工智能模型检测各种变种漏洞，如Struts2系列漏洞、SQL注入漏洞、Java反序列化漏 洞、CMS类型漏洞等；11、能够定期接收云端提供的威胁情报，并且威胁情报可支持在线和离线升级两种方式；12、支持威胁情报授权管控：制作授权需包含威胁情报授权；情报授权可控制本机情报使用、检测；13、支持基于威胁情报的威胁检测，检测类型包含僵尸网络、勒索软件、流氓推广、网络蠕虫、远控 木马、黑市工具、其他恶意软件等14、支持检测web漏洞，例如PHP代码执行、扫描器漏洞探测、XSS跨站脚本、PYTHON代码执行、SQL注入攻击等；15、针对模糊检索场景提供关键字全文模糊匹配功能，支持用户自定义数据关键字进行不确定场景下的模糊检索，可视化展示检索后的结果，并针对选定字段取值，提供便捷检索；16、支持对分析集群、探针、扫描节点的统一管理。包括各节点健康状态、节点名称、最后拉取数据时间、是否生效； |
| 17 | 态势感知流量探针 | 1台 | 相当于或者优于奇安信、天融信、启明星辰、360 | 1、★≥8核心16线程CPU，≥64GB内存，≥2个GE流量监听电口，≥2个10GE流量监听光口，冗余电源，≥600GB SAS盘+2TB企业级存储硬盘,网络层吞吐量：≥2Gb。2、提供对网络流量中主流协议进行识别、解析还原并记录，用于取证分析、威胁发现，支持协议包括：HTTP、DNS、SMTP、POP3、IMAP、Mysql、Postgresql、DB2、Oracle、Mongodb、Resp、SMB、NFS、FTP、RIP、Netflow、DHCP、BGP、ICMP、OSPF、Radius、RIP、VNC、NTP、RDP、Rlogin、RSH、Idap、SSH、Oicq、Telnet等，还原内容包括：TCP会话、 行为日志、登录行为等；3、提供对网络流量中的文件进行识别和还原，支持可执行文件（exe、dll、msi等）、文档类文件（docx、pptx、xls、pdf等）、压缩文件（rar、zip等）、移动应用apk等。4、具备攻击结果判断能力； 5、提供流量节点管理：包括各节点健康状态、节点名称、最后拉取数据时间、是否生效； 6、支持检测web漏洞，例如PHP代码执行、扫描器漏洞探测、XSS跨站脚本、PYTHON代码执行、SQL注入攻击等；7、攻击检测覆盖：Web攻击、恶意软件、二进制攻击、网络钓鱼、信息探测、异常行为、网络攻击、横向移动、暴力破解、服务攻击、域内渗透攻击、SHELL命令执行、异常通信等攻击场景。 |
| 18 | 网络安全等级预测评服务 | 1项 | 国产 | 1.依据三级等级保护相关标准规范，使用与测评机构相同的测评工具与实施方法，对采购人的微信公众号(掌上医院)、医院官网、电子签名、综合管理平台(OA移动办公)信息系统进行等级保护等保预测评，找出目标系统与对应等级要求之间的差距，分析安全风险问题情况，计算现状安全得分，并提出针对性整改建议，出具预测评报告，帮助用户在正式测评前提高整体安全保障能力。2.指导采购人对三级等保测评需要涉及的HIS等类应用系统进行相应的改造，完成预测评报告。 |
| 19 | 安全管理体系咨询服务 | 1项 | 国产 | 为建立健全的网络安全体系，协助医院编制网络安全整体规划，并对安全整体规划及其配套文件的合理性和正确性进行论证。根据深入分析、理解单位的现状，对比行业的特性，参考国家标准文件、法律法规、上级标准文件等协助单位建设符合自身安全管理体系。在安全管理上完善制度管理、机构管理、人员管理、系统建设管理、系统运维管理、应急响应等方面机制、制度。 |
| 20 | 安全运维驻场服务 | 1项 | 国产 | 提供1名信息安全运维服务现场驻场人员，处理日常信息安全设备及系统的相关的故障、问题的响应和处理并按要求进行常规巡检等服务，服务周期一年。 |
| 商务条款 | 1、交货时间及地点：自合同签订之日起40日内交货并安装验收完毕；地点：桂林市，客户指定地点。2、质保期：本项目的设备设施、软件、特征库、维保等实行整体质保，质保期为三年（交货验收合格之日起计）。3、验收要求：项目部署上线后，采购人与供应商联合进行初步验收；根据预测评报告结果，持续整改，完成预测评报告并达到本项目采购内容的预测评目标，经双方确认项目建设能满足三级等保要求后，双方联合进行整体验收。4、售后技术服务要求：（1）故障响应时间：中选供应商派驻人员接到故障通知后，30分钟响应，0.5小时以内到达采购人指定现场，4小时内解决故障并恢复系统运行，终身提供技术支持。（2）中选供应商能提供7×24通过远程、上门服务、电话、E-mail等方式为用户提供终身完善的售前和售后技术咨询服务（3）所有设备按产品的要求提供相应的保修期内免费维修服务。（4）供应商需承诺建立常备后援技术团队，为驻场人员提供后援技术支持。后援技术团队提供定期的现场巡检服务。5、付款条件：实施团队工程师进场，设备到货由现场人员与物流人员清点设备数量及检查外观无损坏，收货验收合格后甲方支付合同总金额 40%货款；设备设施软件经实施团队部署上线初步验收后支付至65%；经过持续整改，完成预测评报告并达到本项目采购内容的预测评目标，经整体验收后支付至95%；质保期内供应商配合采购人完成三级等保测评，在质保期到期后10个工作日内支付5%质保金（无利息）。6、参询报价为采购人指定地点的现场交货价，包括：（1）货物的价格；（2）货物的标准附件、备品备件、专用工具的价格；（3）运输、装卸、调试、培训、技术支持、售后服务等费用；（4）必要的保险费用和各项税费；（5）包括安装费用。 |

**三、评分办法**

**评分办法**

**（一）价格分………………………………………………………………………30分**

（1）参询供应商为小型、微型企业，其提供的服务全部由符合政策要求的中小企业承接的（供应商必须按规定提供《中小企业声明函》，或者监狱企业证明文件，或者《残疾人福利性单位声明函》），对供应商的最终竞标价给予10%的扣除，扣除后的价格为评审价，即评审价=参询价×（1-10%）；否则，评审价=参询价。

（2）以进入详细评审的最低评审价为评审基准价，得30分。参询报价分计算公式：

参询报价分= 评审基准价（金额）/参询评审价（金额） ×30分

**（二）技术参数及方案分…………………………………………………………… 49分**

**1. 技术性能及参数分：本项满分20 分**

参询产品完全满足的得基本分20分。带“**★**”项的为实质性技术要求，如不满足，则废标。带“ **⯁** ”号技术规格参数的为重要参数，有一项不满足（负偏离）的，扣2分，扣完为止。不带“**★**”、“ **⯁** ”号技术规格参数的为一般参数，有一项不满足（负偏离）的，扣1分，扣完为止。注：不编列技术偏离表或技术偏离表与项目采购需求不实行一一对照的，扣5分。

**2.总体技术设计方案分：本项满分9分**

一档3分：对项目现状不理解，对项目目标无分析描述，对现状无描述。技术及运行服务方案简单，能提供方案；保证运行服务的技术力量和人力资源安排基本满足要求，技术服务、技术培训的服务内容和措施一般。

二档6分：对项目的理解较浅，对项目描述简单。技术及运行服务方案较详细；保证运行服务的技术力量和人力资源安排满足项目实施要求，技术服务、技术培训的服务内容和措施基本完善。

三档9分：对项目的理解深入，能切合本项目实际提供方案，方案能清楚的表明对本项目的熟悉程度；准确理解本项目的目标、范围、需求、现状，完全把握本项目的技术重点。方案完整合理，技术服务、技术培训及服务体系等服务内容完善，措施得力，满足采购文件要求。

**3.实施组织方案分： 本项满分20分**

**（1）实施方案（满分12分）**

 一档6分：项目实施方案内容不够完整，工作进度计划不具有针对性，或可行性不强的；

 二档9分：项目实施方案内容基本完整，内容包含有工作程序和步骤、实施小组成员的管理机制、考核制度和考核方法等工作进度计划安排基本可行，设置有项目管理组织机构，基本符合项目要求；

三档12分：项目实施方案内容完整，考虑周全，对工作程序和步骤、实施小组成员的管理机制、考核制度和考核方法等有详细的描述，能详细说明各个阶段工作安排，提供实施车辆、有工程实施安全保障措施、工程进度图并有赶工措施、工程质量保证措施、项目风险管理措施、文明施工管理措施等科学合理，可行性强。设置的项目管理组织机构职能完全满足项目要求，对服务质量保证措施均完整具体。

**（2）项目实施人员（满分4分）**

1. 供应商拟投入本项目的相关专业技术人员有高级信息系统项目管理师或PMP证书等相关领域同级别证书的每个得0.5分，满分1分。
2. 供应商拟投入本项目的相关专业技术人员有中级职称（职称专业为：软件、互联网、网络、系统集成专业类）的每个得0.5分，满分2分。
3. 供应商拟投入本项目的相关专业技术人员有高级网络规划设计师的得1分。

（3） **驻场人员 （满分4分）**

供应商拟派出驻场人员具有与本项目相关软硬件及网络相关专业的中级工程师及以上职称的得4分，具有初级工程师的得3分，一般技术人员不得分（须拟驻场人员的社保证明及有效的职称证书复印件并加盖参询单位公章）。

**（三）履约能力分………………………………………………………………9分**

（1）参询单位具有由国家认证认可监督管理部门批准设立的认证机构颁发并在有效期内的ISO9001质量管理体系认证系列、ISO14001环境管理体系认证系列、GB/T45001 职业健康安全管理体系认证系列、ISO/IEC27001信息安全管理体系标准认证证书、ISO/IEC20000信息技术服务管理体系认证证书，每项得1分，满分5分（须提供认证证书复印件并加盖参询单位公章）。

（2）参询单位具有中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书（信息系统安全集成一级、信息安全风险评估一级、信息安全应急处理一级、信息系统灾难备份与恢复一级）的，具有1项得0.25分，满分1分（须提供认证证书复印件并加盖参询单位公章）。

（3）参询单位具有中国信息安全测评中心颁发的信息安全服务资质证书-安全工程类二级及以上、信息安全服务资质证书-灾难恢复类二级及以上，具有1项得0.5分，满分1分（须提供证书复印件并加盖参询单位公章）。

（4）2018年以来，参询单位具有咨询服务或技术服务或等保安全网络系统集成类相关项目业绩的，每满足1个得0.5分，满分2分（提供合同复印件）。

**（四）售后服务方案………………………………………………………………12分**

评委根据参询人提供的售后服务方案（包括人员安排、服务计划、售后服务措施及相关承诺、后续的系统升级服务、日常系统应用技术支持、故障响应时间及处置方式等服务）内容进行综合评价，划分不同档次评分。

**（1）.售后服务方案分：本小项3分**

①有售后方案，有具体的人员安排、服务计划，有具体的售后服务措施、无后续系统完善升级服务、无日常系统应用技术支持服务，得1分。

②售后方案有具体的人员安排、服务计划，有具体的售后服务措施、有后续系统完善升级服务、日常系统应用技术支持服务，得2分；

③售后方案较为详细，有具体的人员安排、服务计划，有具体的售后服务措施、后续系统完善升级服务、日常系统应用技术支持服务，得3分；

**（2）.**供应商的后援技术团队提供**故障响应服务：本小项3分**

在驻场人员现场无法解决故障的情况下，后援技术团队提供以下响应服务：

①遇故障响应时间在1小时内提供远程服务，如无法解决可在10小时内到现场处置；得1分；

 ②遇故障响应时间在20分钟以上提供远程服务，如无法解决可在5小时内到现场处置，得2分；

 ③遇故障在20分钟内提供远程服务，如无法解决可在3小时内到现场处置，得3分。

**（3）.**供应商后援团队的**免费巡检维保服务：本小项共3分**

①质保期内提供到现场免费巡检维保服务，一年2次的，得1分；

②质保期内提供到现场免费巡检维保服务，一年3次的，得2分；

③质保期内提供到现场免费巡检维保服务，一年4次的，得3分。

**（4）.免费质保服务**：**3分**

免费整体质保期超过3年以上的，每增加1年，得1分，本项最多3分。

**（五）总得分 = （一） + （二） + （三） + （四）**

**四、推荐及确定中选结果给委托招标代理**

1. 综合评选委员会由医院院内人员组成，评选委员会根据综合得分由高到低排列次序，若得分相同时，按评选报价由低到高顺序排列；若仍相同的，依次按照项目要求及技术需求响应分、现场演示分、服务承诺分、履约能力分由高到低顺序排列次序。

2. 采购人将以排名第一的参询报价、参数等内容为参照，报第三方招标代理公开招标。