# **上海市养志康复医院(上海市阳光康复中心)**

# **内网核心区计算资源扩容项目招标需求**

# 项目概述

## 项目名称

上海市养志康复医院(上海市阳光康复中心)内网核心区计算资源扩容项目(以下简称“本项目”)

## 项目地点

上海市养志康复医院(上海市阳光康复中心)（以下简称“医院”）

## 项目介绍

本项目拟采购超融合设备及配套扩容组件，对现有IT基础资源进行补充，满足现阶段核心业务运行基本资源要求，支持现阶段医院面向功能障碍人群的“大模型+康复”智能患者服务应用系统计算资源，同时完成配套扩容及业务系统迁移服务。本次需扩容现网环境为：超融合集群1采用aServer-R-2205一体机；超融合集群2采用aServer-W-4000一体机；服务器汇聚交换机为S7506X。

## 本次采购内容

本次医院内网核心区计算资源扩容项目采购内容详见设备采购清单。

本项目预算为1450000元人民币，超预算的投标文件视为废标。

## 建设范围

本项目的建设范围为完成医院超融合资源池的扩容，包括设计、实施、迁移及验证服务。

# 技术需求

## 设备采购清单

**请针对本项目购买的设备提供原厂授权函**。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 型号、规格 | 数量 | 单位 |
| 1 | 超融合一体机1，原厂五年质保 | 详见招标技术参数 | 2 | 台 |
| 2 | 超融合交换机，原厂五年质保 | 详见招标技术参数 | 2 | 台 |
| 3 | 内存扩容 | 详见招标技术参数 | 1 | 套 |
| 4 | 超融合一体机2，原厂五年质保 | 详见招标技术参数 | 2 | 台 |
| 5 | 万兆多模光模块，原厂五年质保 | 详见招标技术参数 | 40 | 块 |
| 6 | 交换机板卡，原厂五年质保 | 详见招标技术参数 | 2 | 块 |
| 7 | 集成服务 | 详见招标技术参数 | 1 | 项 |

## 招标技术参数

## 超融合一体机1

|  |  |
| --- | --- |
| **指标项** | **具体参数** |
| **服务器节点** | 本次提供超融合一体机节点数≥2； |
| **单台硬件配置** | **CPU和内存** | 每台节点配置2颗CPU ，采用Intel Xeon Gold 6326 CPU@2.90GHZ（16C）或以上配置的CPU，每台服务器内存≥24\*32 GB。 |
| **接口** | 千兆电口≥4个，万兆光口 SFP+≥4个（含模块） |
| **硬盘配置** | 每个节点要求配置系统盘≥2\*240G-SATA-SSD 企业级固态硬盘，配置缓存盘≥2\*固态硬盘-1.92T-SSD;，配置数据盘≥6\*4T 7.2K RPM SATA HDD 企业级机械硬盘 |
| **平台兼容性** | 本次招标产品用于现有集群主机扩容升级项目，超融合一体机需要支持被现有云管平台统一纳管。提供厂商承诺函并加盖厂商公章。 |
| **云计算平台要求** | 产品完全自研，非OEM，需提供云计算管理平台的软件著作权证书 |
| 支持大屏展示便于客户直观查看虚拟化资源池的使用情况和健康状态，包括集群资源情况，各主机资源使用情况，存储资源池的IO次数、IO速率、IO时延、存储命中率、主机命中率，以及集群故障与告警，支持Top 5主机CPU和内存利用率、Top 5虚拟机CPU和内存利用率信息大屏展示等  |
| 支持跨地域的多集群管理，可纳管256个物理机节点，支持30000台云主机的规模 |
| 支持主备切换，当主平台发生故障时，能够切换到备平台，保障云平台稳定运行 |
| 支持上传或利用现有云主机创建镜像，可对镜像进行管理、关联资源池等操作，可通过镜像实现一键快速创建云主机及安全组件  |
| 1▲云计算管理平台，和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）均为同一厂商品牌提供，并可以支持扩展同一品牌的网络和安全虚拟化（虚拟应用防火墙、虚拟应用负载均衡等）功能组件，以保障平台的扩展性和兼容性（需提供产品功能截图）  |
| **计算虚拟化要求** | 2▲虚拟化软件非OEM或贴牌产品，禁止借用第三方软件的整合，以保证功能的可靠性和安全性（提供相应的软件著作权） |
| 采用分布式管理架构，去中心化，管理平台不依赖于某一个虚拟机或物理机部署，采用分布式架构保障平台更可靠 |
| 支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态 |
| 支持对超融合平台的硬件进行监控和大屏展示，包含CPU，内存，网卡，硬盘，存储，RAID等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议 |
| 为了更好的保护用户数据，支持设置定期全量备份，支持用户灵活配置备份策略，备份文件保留时间最高可以达到15年，支持将虚拟机的备份文件定期归档到第二存储，最多可以保留100年 |
| 支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员 |
| 此项目核心业务计划部署在超融合平台，平台需定期升级保障平台稳定性，核心业务不能长时间停机，超融合平台需支持在线升级不影响业务；为保证升级时间与步骤可控，升级过程中支持对升级节点进行升级顺序编排、升级暂停（需提供产品功能截图） |
| **存储虚拟化要求** | 产品完全自研，非OEM，需提供存储虚拟化软件著作权证书（提供相应的软件著作权） |
| 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能（需提供产品功能截图）  |
| 支持为虚拟磁盘配置不同的存储策略以满足特定场景的需求, 如系统盘和数据盘选择高性能策略, 备份盘选择低性能策略 |
| 支持对虚拟机业务按照小时/天/周自定义设置定时快照策略，以便业务发生故障时可以快速回滚覆盖原虚拟机或者通过对快照进行克隆的方式生成全新虚拟机，进而恢复至业务健康状态 |
| 3▲硬件故障对平台影响较大，也会影响数据安全，为保障业务在硬件故障后尽快恢复冗余数据保障，支持进行数据重建操作，重建速率达到30分钟/TB；重建过程中可以查看数据重建任务列表信息，包括对象名称、对象类型、数据量和优先级等；支持点击操作中的优先级对数据重建进行优先重建（提供相关证明） |
| 支持针对虚拟机或虚拟磁盘设置数据分布策略，当采用副本聚合策略时，可以保证以性能优先为原则，实现IO本地读效果，当采用副本散列策略时，可以保证虚拟机以分布均匀优先为原则，打散分布均匀在各物理主机上 |
| **网络虚拟化要求** | 产品完全自研，非OEM，需提供网络虚拟化软件著作权证书 |
| 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率【提供官网截图】 |
| 主动探测业务系统，实时监控业务可用性，监控策略包括HTTP、FTP、POP3、SMTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障 |
| 支持链路聚合，为网络中的每个虚拟机提供内置的网络故障切换和负载均衡能力，实现更高的硬件可用性和容错能力 |
| 提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性 |
| **内建安全** | 4▲基于业务安全性和运维高效性考虑，需要虚拟化平台支持在虚拟机安装性能优化工具时自动安装组件功能对操作系统进行安全防护。（需提供相关证明） |
| 云安全中心支持安全事件展示，包括勒索病毒，暴力破解，后门等；支持安全事件报表分析；支持按优先级排序展示虚拟机安全状态，包括操作系统、内部应用、安全事件、是否开启防护等，支持搜索筛选；支持安全告警展示；支持安全事件处置记录展示；支持病毒扫描记录展示；支持查看虚拟机安全防护状态 |
| 提供向导化勒索病毒处理流程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品功能截图） |
| **资质** | 超融合软件获得云计算开源产业联盟颁发的超融合解决方案检验证书 |
|  |
| 为确保云平台在医疗行业的自主可信，超融合软件需获得互联网医疗健康产业联盟颁发的医疗云计算基础设施可信证书，提供证书证明 |
| **保修** | 原厂五年保修服务 |

## 超融合交换机

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| **固定端口** | 万兆SFP+光口≥12个；千兆电口≥12个； |
| **交换机性能** | 交换容量≥1.28Tbps/12.8Tbps |
| 包转发率≥480Mpps |
| **接入方式** | 支持胖瘦一体化，支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时在控制器平台灵活的进行切换 |
| **访问控制策略** | 支持基于交换机单端口、聚合口的ACL策略； |
| 支持基于源目IP地址、MAC地址的ACL策略； |
| 支持基于时间的ACL策略； |
| **服务质量（Qos）** | 流量管理：对于匹配ACL的流量进行重标记从而实现流量监管功能； |
| 优先级映射：支持基于交换机组实现COS、DSCP优先级映射； |
| 拥塞管理：支持多种调度模式（例如：轮询模式、严格优先模式等）实现流量基于报文或端口的优先级 |
| **交换机零配置上线方式** | 二层广播自动发现控制器平台 |
| 配置静态IP地址三层发现控制器平台 |
| DHCP Option43方式发现控制器平台 |
| DNS域名发现控制器平台 |
| **一键替换** | 支持通过控制器平台一键替换“按钮”即可完成故障设备替换，提供平台功能截图证明； |
| **生成树** | 支持STP、RSTP、MSTP协议 |
| **组播** | 支持IGMP v1/v2/v3 Snooping |
| **VLAN** | 支持4K个VLAN |
| **EEE** | 支持IEEE 802.3az 标准的 EEE节能技术：当EEE使能时，从而大幅度的减小端口在该阶段的功耗，达到了节能的目的。 |
| **MAC** | 支持MAC地址≥32K |
| 支持MAC地址自动学习 |
| 支持源MAC地址过滤 |
| 支持接口MAC地址学习个数限制 |
| **端口聚合** | 支持端口聚合≥128个 |
| 支持手工和静态LACP |
| **ARP** | ARP≥16K |
| **DHCP** | 支持DHCP Server |
| **三层功能** | 支持静态路由 |
| 路由表≥1000 |
| **交换机状态显示** | 支持通过控制器平台查看交换机端口负载情况 |
| **安全特性** | 支持防网关ARP欺骗 |
| 管理员分级管理 |
| 支持端口保护、隔离 |
| 支持防止DOS、ARP攻击功能 |
| 支持CPU保护功能 |
| **网络管理** | 支持通过控制器平台跨广域网、NAT远程管理智能交换机 |
| **交换机画像管理** | 支持通过在控制器平台的Web页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan信息，提供功能截图证明； |
| 支持通过控制器平台图形化操作对交换机端口状态的开启与关闭； |
| **运维** | 支持通过控制器平台查看交换机处于工作端口的最近5分钟、1小时、最近1天、最近1周发送与接收的流量趋势；提供功能截图证明； |
| **智能终端类型识别** | 支持终端类型库，基于指纹自动识别PC、路由器、监控终端设备等，提供平台终端类型识别库截图证明； |
| 支持基于终端类型自动识别结果，禁止非法终端(例如私接路由器)接入 |
| **终端安全策略** | 支持终端IP-MAC绑定，当IP+MAC不对应时，可以将终端加入黑名单实现断开终端流量 |
| 支持终端IP-MAC首次部署自动学习绑定 |
| 5▲支持将交换机的端口进行端口组划分，方便配置管理，提供功能截图证明； |
| 支持预留的特权IP必须由管理员审批才可以使用，同时支持IP白名单免审批； |
| 支持终端的MAC与交换机端口变更检测； |
| 支持交换机端口终端类型变更后，通过短信告警 |
| 可以自定义交换机端口接入终端类型，及MAC黑白名单 |
| **终端状态安全分析** | 支持查看终端在交换机端口离线次数、闲置时间、离线趋势 |
| 支持查看安全事件记录、终端类型异常记录、终端在端口迁移次数、终端地址异常记录等安全事件的记录统计 |
| 支持查看终端的的历史接入交换机端口，终端的活跃状态 |
| **保修** | 原厂五年保修服务 |

## 内存扩容

|  |  |
| --- | --- |
| **指标项** | **具体参数** |
| **数量** | 128条 |
| **配置** | 服务器内存32G（X86架构通用），用于现有服务器aServer-W-4000内存扩容 |

## 超融合一体机2

|  |  |
| --- | --- |
| **指标项** | **具体参数** |
| **服务器节点** | 本次提供超融合一体机节点数≥2； |
| **单台硬件配置** | **CPU和内存** | 每台节点配置2颗CPU ，采用Intel Xeon Gold 5318H 2.50 GHz（18C）或以上配置的CPU，每台服务器内存≥32\*32 GB。 |
| **接口** | 千兆电口≥2个，万兆光口 SFP+≥6个（含模块） |
| **硬盘配置** | 每个节点要求配置系统盘≥2\*240G-SATA-SSD 企业级固态硬盘，配置缓存盘≥2\*固态硬盘-3.2T-U.2 NVME SSD;，配置数据盘≥13\*机械SAS硬盘2.4T-SAS2.5寸-万转 |
| **平台兼容性** | 本次招标产品用于现有集群主机扩容升级项目，超融合一体机需要支持被现有云管平台统一纳管。提供厂商承诺函并加盖厂商公章。 |
| **云计算平台要求** | 产品完全自研，非OEM，需提供云计算管理平台的软件著作权证书 |
| 支持大屏展示便于客户直观查看虚拟化资源池的使用情况和健康状态，包括集群资源情况，各主机资源使用情况，存储资源池的IO次数、IO速率、IO时延、存储命中率、主机命中率，以及集群故障与告警，支持Top 5主机CPU和内存利用率、Top 5虚拟机CPU和内存利用率信息大屏展示等  |
| 支持跨地域的多集群管理，可纳管256个物理机节点，支持30000台云主机的规模 |
| 支持主备切换，当主平台发生故障时，能够切换到备平台，保障云平台稳定运行 |
| 支持上传或利用现有云主机创建镜像，可对镜像进行管理、关联资源池等操作，可通过镜像实现一键快速创建云主机及安全组件  |
| 6▲云计算管理平台，和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）均为同一厂商品牌提供，并可以支持扩展同一品牌的网络和安全虚拟化（虚拟应用防火墙、虚拟应用负载均衡等）功能组件，以保障平台的扩展性和兼容性（需提供产品功能截图）  |
| **计算虚拟化要求** | 7▲虚拟化软件非OEM或贴牌产品，禁止借用第三方软件的整合，以保证功能的可靠性和安全性（提供相应的软件著作权） |
| 采用分布式管理架构，去中心化，管理平台不依赖于某一个虚拟机或物理机部署，采用分布式架构保障平台更可靠 |
| 支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态 |
| 支持对超融合平台的硬件进行监控和大屏展示，包含CPU，内存，网卡，硬盘，存储，RAID等硬件健康检测，便于及时发现问题并提供相应异常检测项的恢复指导建议 |
| 为了更好的保护用户数据，支持设置定期全量备份，支持用户灵活配置备份策略，备份文件保留时间最高可以达到15年，支持将虚拟机的备份文件定期归档到第二存储，最多可以保留100年 |
| 支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员 |
| 此项目核心业务计划部署在超融合平台，平台需定期升级保障平台稳定性，核心业务不能长时间停机，超融合平台需支持在线升级不影响业务；为保证升级时间与步骤可控，升级过程中支持对升级节点进行升级顺序编排、升级暂停（需提供产品功能截图） |
| **存储虚拟化要求** | 产品完全自研，非OEM，需提供存储虚拟化软件著作权证书（提供相应的软件著作权） |
| 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能（需提供产品功能截图）  |
| 支持为虚拟磁盘配置不同的存储策略以满足特定场景的需求, 如系统盘和数据盘选择高性能策略, 备份盘选择低性能策略 |
| 支持对虚拟机业务按照小时/天/周自定义设置定时快照策略，以便业务发生故障时可以快速回滚覆盖原虚拟机或者通过对快照进行克隆的方式生成全新虚拟机，进而恢复至业务健康状态 |
| 8▲硬件故障对平台影响较大，也会影响数据安全，为保障业务在硬件故障后尽快恢复冗余数据保障，支持进行数据重建操作，重建速率达到30分钟/TB；重建过程中可以查看数据重建任务列表信息，包括对象名称、对象类型、数据量和优先级等；支持点击操作中的优先级对数据重建进行优先重建（提供相关证明） |
| 支持针对虚拟机或虚拟磁盘设置数据分布策略，当采用副本聚合策略时，可以保证以性能优先为原则，实现IO本地读效果，当采用副本散列策略时，可以保证虚拟机以分布均匀优先为原则，打散分布均匀在各物理主机上 |
| **网络虚拟化要求** | 产品完全自研，非OEM，需提供网络虚拟化软件著作权证书 |
| 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率【提供官网截图】 |
| 主动探测业务系统，实时监控业务可用性，监控策略包括HTTP、FTP、POP3、SMTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障 |
| 支持链路聚合，为网络中的每个虚拟机提供内置的网络故障切换和负载均衡能力，实现更高的硬件可用性和容错能力 |
| 提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性 |
| **内建安全** | 9▲基于业务安全性和运维高效性考虑，需要虚拟化平台支持在虚拟机安装性能优化工具时自动安装组件功能对操作系统进行安全防护。（需提供相关证明） |
| 云安全中心支持安全事件展示，包括勒索病毒，暴力破解，后门等；支持安全事件报表分析；支持按优先级排序展示虚拟机安全状态，包括操作系统、内部应用、安全事件、是否开启防护等，支持搜索筛选；支持安全告警展示；支持安全事件处置记录展示；支持病毒扫描记录展示；支持查看虚拟机安全防护状态 |
| 提供向导化勒索病毒处理流程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品功能截图） |
| **资质** | 超融合软件获得云计算开源产业联盟颁发的超融合解决方案检验证书 |
|  |
| 为确保云平台在医疗行业的自主可信，超融合软件需获得互联网医疗健康产业联盟颁发的医疗云计算基础设施可信证书，提供证书证明 |
| **保修** | 原厂五年保修服务 |

## 万兆多模光模块

|  |  |
| --- | --- |
| **指标项** | **具体参数** |
| **数量** | 40块 |
| **配置** | 中心波长850nm，多模光纤传输，最远距离达300m，提供五年原厂质保 |
| **保修** | 原厂五年保修 |

## 交换机板卡

|  |  |
| --- | --- |
| **指标项** | **具体参数** |
| **数量** | 2块 |
| **配置** | 核心交换机业务接口板卡，提供24个万兆接口，要求能够与现网核心交换机兼容，提供五年原厂质保 |
| **保修** | 原厂五年保修 |

## 集成服务

|  |  |
| --- | --- |
| **指标项** | **具体参数** |
| **数量** | 1项 |
| **配置** | 完成本次采购所有设备、配件的安装、调试服务，确保医院相关在用系统稳定运行。 |
| **保修** | 1年 |

# 服务要求

## **项目工期要求**

本项目整体工期为3个月，包括深化设计、设备供货、设备安装部署、业务系统迁移、试运行及考核验收。

|  |  |
| --- | --- |
| **项目** | **日期** |
| 设备供货、安装部署、集成实施、集成测试 | 合同生效后1个月内 |
| 业务系统迁移 | 设备集成实施后0.5个月 |
| 项目试运行 | 试运行至少1个月 |
| 项目验收交付 | 试运行通过0.5个月内 |

## **实施团队要求**

1. 服务商需要提供不少于15人的系统集成服务团队，保障项目实施与质保工作的响应质量；
2. 为保证项目的顺利实施，响应供应商应成立商务支持小组与技术支持小组，全方位配合用户。
3. 响应供应商应在响应文件中提供项目实施详细的项目小组人员名单及职责，项目负责人具有5年以上工作经历、高级信息系统项目管理师证书或高级工程师证书的优先考虑。项目团队应具有与本项目服务内容相匹配的资质能力，包括但不限于超融合类资质认证、操作系统认证、虚拟化认证、数据库类资格认证、信息系统安全类专业认证、网络类专业认证、IT服务过程管理类认证，项目团队人员具有注册信息安全人员CISP证书的优先考虑。需要提供人员最近一季度内任意一个月的社保证明，并加盖公章。
4. 项目团队人员一旦得到确认，未经用户书面同意，不得随意变动，用户方有权根据实施情况要求更换项目经理和实施人员。

## **系统验收要求**

系统验收合格的条件至少满足以下三个要求：

1. 已提供了合同的全部货物和资料；
2. 试运行时性能满足合同要求；
3. 测试和试运行验收时出现的问题已被解决。

## **服务响应要求**

项目实施及质保期间，服务商需提供7x24小时故障响应人工热线，质保期内满足10分钟内响应，2小时到现场要求。

## **技术文档要求**

项目系统验收前，响应供应商需按院方要求提供详细的技术文档，包含但不限于：设计方案、安装报告、测试报告、试运行报告、随机材料、操作手册等。

## **保密服务要求**

1. 响应供应商承诺参与本项目的所有服务人员需严格保守与本项目有关的技术秘密和商业秘密，任何涉及建设单位及使用单位的信息，包括但不限于数据、特有的功能需求等，未得到建设单位及使用单位的书面同意，不得对任何第三方展示、举例乃至销售，否则响应供应商将承担由此产生的一切后果。
2. 响应供应商不以实施项目为名，侵害本项目各参与单位的技术、商业秘密或者知识产权。
3. **未经甲方书面同意，响应供应商不得对任何第三方泄露本项目所涉及的医院详细网络拓扑、主机集群配置策略等信息。**

## **其他相关要求**

报价说明：本系统所涉及的与现有平台的对接、迁移费用，应包括在本次投报总价中，用户不再另行支付相关费用，提供盖章承诺书。

# 响应供应商要求

1. 响应供应商需提供相应的技术服务，在满足用户方的应用与需求的前提下，完成相关系统集成工作。
2. 响应供应商提供的产品及其配置应该是安全、可靠和成熟的，不是技术上已经或即将淘汰的。
3. 响应供应商需熟悉医院信息化整体架构，提出扩展升级方案。
4. 响应供应商应该保证所提供的所有产品皆不侵犯任何第三方的版权、知识产权和其他合法权利，所采购设备需提供原厂授权及服务承诺函。
5. 供应商具有ISO9001质量管理体系认证证书的、运行维护资质（ITSS）、CCRC 信息安全应急处理服务资质的优先考虑。