主要标的信息：

项号	名称	品牌	规格型号	数量	单价(元)
1	6类24口模块式配线架UTP（含满配模块）	FGT、FGT-24P-6L-K	1、符合中华人民共和国行业标准YD/T1019,符合美国ANSI/TIA-568C标准，ISO/IEC11801标准，ULSubject44标准； 2、1.6mm厚钢板，黑色烤漆 ，标准19寸机架安装，高度1U.插拔次数不小于1000次，端接次数大于等于250次； 3、模块直流电阻0.3欧； 4、绝缘阻抗不低于500MΩ，接点阻抗小于等于20mΩ。	4	¥1,150
2	5类24口模块式配线架UTP（含满配模块）	FGT、FGT-24P-5L	1、支持卡接22-24AWG实心或多股双绞线； 2、支持两种T568A和T568B线序色标； 3、支持155MHZ带宽； 4、性能超越国际ANSI/TIA568-C标准要求，并具有极高的性能余量； 5、RJ45金针下面带垫片,对8根金针进行保护，提高拔插次数与性能的稳定性。	4	¥950
3	电话配线架	FGT、FGT-25P-4T	1、端口数：25*RJ45； 2、面板材质：1.6mm厚钢板； 3、外观颜色：黑色烤漆,安装要求：19英寸机架/机柜,安装高度：0.5U和1U； 4、插座接触针：4针，磷青铜镀镍100uInch,表面再镀金50uInch； 5、插拔次数：不少于1000次,打线工具：110型或Krone型皆可； 6、IDC端接次数：不少于250 次，180度IDC打线方式，斜口刀面设计，可端接0.33-0.5线规铜芯。	2	¥450
4	理线架	FGT、FGT FGT-24P-LX	1、理线器整体材质：采用冷轧钢板，静电喷塑； 2、上下24孔理线出口，后方进线口，方便线缆管理； 3、19英寸1U标准机架式设备 。	10	¥180
5	1米跳线	FGT、FGT-M6-1M	1、符合中华人民共和国行业标准YD/T1019,符合美国ANSI/TIA-568C标准，ISO/IEC11801标准； 2、ULSubject44标准采用多股双绞线设计，低延迟，在100Mbps,155MbpsATM和622Mbps速率下不影响传输。	225	¥30
6	接入交换机	H3C、MS4300V2-28P	一、★单台配置要求 1. 24个10/100/1000Base-TX以太网端口,4个100/1000Base-X SFP端口； 二、技术参数要求 1. ★交换容量≥330Gbps，转发性能≥50Mpps,提供生产厂商官网信息截图及官网查询地址； 2. 支持IEEE802.3x 流量控制（全双工），支持基于端口带宽百分比的广播风暴抑制,支持基于PPS/BPS的风暴抑制；	8	¥5,800

			3. 支持 IPv4 支持静态路由，RIPV1/2，OSPF； 4. 支持基于端口的 VLAN，支持基于 MAC 的 VLAN，基于协议的 VLAN； 5. 支持 QinQ，灵活 QinQ，支持 VLAN Mapping，支持 Voice VLAN，支持 Guest VLAN； 6. 支持最大 9 台设备混合堆叠； 7. 支持智能弹性架构，将多台物理设备互相连接起来，使其虚拟为一台逻辑设备； 8. 支持 L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、TCP/UDP 端口、协议类型、VLAN 的流分类，支持时间段（Time Range）ACL，支持基于端口、VLAN、下发 ACL； 9. 支持 IEEE 802.1X 认证/集中 MAC 地址认证，支持端口隔离，支持端口安全； 10. 支持 802.1p/DSCP 优先级映射，支持队列调度机制； 11. 支持 STP/RSTP/MSTP； 12. 支持 DHCP Server，支持 DHCP Client，支持 DHCP Snooping，支持 DHCP Relay，支持 DHCP Snooping option82； 13. ★支持 VCT 电缆检测功能，支持 DLDP 单向链路检测协议，支持 Loopback-detection 端口环回检测，提供生产厂商官网信息截图及官网查询地址； 14. ★支持端口自动 Power down，端口定时 down 功能（Schedule job）功能，提供生产厂商官网信息截图及官网查询地址； 15. ★ 支持支持业界领先的 9KV 业务端口防雷能力，提供生产厂商官网信息截图及官网查询地址； 16. ★为保障产品代码质量，生产厂商需通过 CMMI5 认证，提供相关证书； 17. ★提供工业和信息化部入网证书； 18. ★设备生产厂商通过 ISO20000 及 ISO27001 认证，提供相应证书。		
7	路由器	H3C 、ER8300G2	一、单台配置要求 1. 提供 2 个 10/100/1000M WAN 口（电口和光口复用），8 个 10/100/1000M LAN 口，1 个 USB 接口，1 个 Console 口； 2. 默认双 WAN 口，最多支持 5 个 WAN 口； 二、技术功能要求 1. 专业的网络处理器 四核 1.2GHz，内存 DDRIII 1024M； 2. 支持智能负载均衡，支持手动负载均衡，支持路由转发模式； 3. 支持 PPPOE，支持 DHCP Server，DHCP client，支持 NAPT，支持 NTP，DDNS； 4. 支持出站/入站通信策略； 5. 路由&AC 合二为一，支持对 AP 自动发现和状态管理，可同时管理 AP 数量 500 个； 6. 支持静态路由；	1	¥13,800

			7. 支持基于 IP/MAC/时间段的组策略配置，URL 过滤(黑白名单)，HTTP 下载文件类型过滤，QQ 访问控制，金融软件控制； 8. 支持历史流量统计，支持网络流量限速，支持 NAT 表项限制，应用通道限制； 9. 支持 AH、ESP 协议，支持手工或通过 IKE 自动建立安全联盟，支持 IKE 主模式及野蛮模式； 10. 支持标准的 IPSec，支持 L2TP Server，支持 L2TP Client； 11. 支持内网异常流量防护，报文源认证（伪装报文直接丢弃不处理），ARP 防攻击/免费 ARP 状态数据包检查，支持防止 WAN 口的 Ping，防止 TCP syn 扫描，防止 Stealth FIN 扫描，防止 TCP Xmas Tree 扫描，防止 TCP Null 扫描，防止 UDP 扫描功能，防止 Land 攻击功能，防止 Smurf 攻击功能，防止 WinNuke 攻击功能，防止 Ping of Death 攻击，防止 SYN Flood 攻击功能，防止 UDP Flood 攻击功能，防止 ICMP Flood 攻击功能，防止 IP Spoofing 功能，防止碎片包攻击，防止 TearDrop 攻击，防止 Fraggle 攻击功能； 12. 支持虚拟服务器，支持静态 NAT（一对一 NAT），支持 DMZ 主机，支持 VPN 透传(PPTP、L2TP、IPSec)； 13. 支持基于 Web 的用户管理接口(远程管理/本地管理)，HTTPS 远程管理，命令行 CLI，SNMP V1/V2C/V3，通过 HTTP 升级系统软件； 14. 故障诊断：Ping / Traceroute，设备自检，故障信息一键导出； 15. ★提供工信部入网许可证复印件； 16. ★为保障产品代码质量，生产厂商需通过 CMMI5 认证，提供相关证书； ★为保障产品代码质量，设备生产厂商须通过 ISO20000 及 ISO27001 认证，提供相应证书；		
8	外网防火墙系统	网神、NSG-1460-Q	1. 标准 1U 设备，配置≥6 个 10/100/1000 Base-T 自适应电口，≥4 个千兆光口， 1 个 Console 口，交流电源；含 3 年硬件质保和全功能模块升级服务； 2. 防火墙吞吐量≥6Gbps，并发连接数≥180 万，每秒新建连接数≥8 万/秒，含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测功能模块； 3. 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求；支持 3G 接入，可实现 3G 及有线链路之间的互为备份； 4. 支持静态路由、动态路由、策略路由，动态路由包括 RIP v1/v2/ng、 OSPFv2/v3、BGP4/4+； 5. 支持静态 DNS，从指定的入接口或源 ISP 接收到的 DNS 请求，防火墙会代替 DNS 服务器将指定的域名与 IP 地址对应关系应答给客户端； 6. 支持防御 IP 地址欺骗，可将 IP 与安全域关联，即指定 IP 或网段从特定安全域流量流入，否则视为 IP 地址欺骗；	1	¥118,000

			7. 支持在 IPv6 环境下配置安全策略、SSL 解密策略等规则，实现漏洞防护、间谍软件防护、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理； 8. 支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制； 9. 支持基于策略的路由负载，支持根据应用和服务进行智能选路，可基于权重做路由负载均衡，支持 12 种均衡方式：源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载； 10. 支持冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略； 11. 支持全面的 NAT 转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式； 12. ★支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持 html、doc、docx、xls、xlsx、ppt、pptx、chm、7z 等多种常见文件类型；（要求提供功能截图） 13. ★支持虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计（提供功能界面截图）； 14. 支持与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱等功能。通过安全云系统提升识别库数量级，补充本地识别库，并加快防火墙对威胁的识别速度； 15. 支持面板下的异常、威胁、重点关注监控、接口信息、系统信息、内容日志、威胁日志、URI 过滤日志、邮件过滤日志、并发连接数； 16. 支持实现 HTTP、FTP、POP3、SMTP、IMAP、SMB 六种应用协议的双向内容过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义，支持阻断及日志两种处理动作； 17. 漏洞防护特征库要求包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； 18. 支持自定义漏洞签名。可标识自定义漏洞的 CVE 编号或 CNNVD 编号。支持自定义基于 TCP、UDP、HTTP 协议的漏洞，并根据各协议的报文结构，指定一个或多个字段的特征值，这些特征值可以被以文本的形式或正则表达式的形式进行匹配，同时支持是否按顺序对这些特征值进行匹配检测。支持自定义漏洞的源端口范围及目的端口范围； 19. 支持与防病毒系统或终端安全管理系统进行联动，增强防火		

			墙对应用特征及木马特征的识别； 20. 支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括 1 天、7 天、30 天、90 天、永久等； 21. 支持在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤等安全功能选项； 22. 支持统计网络中确认失陷的主机及有风险但不能完全确认为失陷的主机数量及风险等级状态，并支持查看失陷时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息，并支持一键跳转处置； 23. 日志支持模糊搜索和按精确策略条件搜索，协助定位异常行为，并通过带条件跳转实现指定行为在分析中心中的关联活动展示，确认异常行为是否具有威胁； 24. ★ 资质要求，提供以下资质证书复印件： 信息安全服务资质--安全运维服务资质。		
9	内网防火墙系统	网神、NSG3000-TE45P-Q	1. 标准 2U 设备，配置≥6 个 10/100/1000 Base-T 自适应电口，≥2 个千兆光口， 支持 1 个接口扩展槽，1 个 Console 口，交流电源；含 3 年硬件质保和全功能模块升级服务； 2. 防火墙吞吐量≥8Gbps，并发连接数≥230 万，每秒新建连接数≥15 万/秒，含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测功能模块； 3. 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求；支持 3G 接入，可实现 3G 及有线链路之间的互为备份； 4. 支持静态路由、动态路由、策略路由，动态路由包括 RIP v1/v2/ng、 OSPFv2/v3、BGP4/4+； 5. 支持静态 DNS，从指定的入接口或源 ISP 接收到的 DNS 请求，防火墙会代替 DNS 服务器将指定的域名与 IP 地址对应关系应答给客户端； 6. 支持防御 IP 地址欺骗，可将 IP 与安全域关联，即指定 IP 或网段从特定安全域流量流入，否则视为 IP 地址欺骗； 7. 支持在 IPv6 环境下配置安全策略、SSL 解密策略等规则，实现漏洞防护、间谍软件防护、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理； 8. 支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能； 9. 支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制； 10. 支持冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略； 11. 支持全面的 NAT 转换能力，支持对源目的地址、端口的转换；	1	¥128,000

			包括一对一，一对多，多对一，多对多地址转换方式； 12. 支持虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计； 13. 支持与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱等功能。通过安全云系统提升识别库数量级，补充本地识别库，并加快防火墙对威胁的识别速度；； 14. 支持面板下的异常、威胁、重点关注监控、接口信息、系统信息、内容日志、威胁日志、URI 过滤日志、邮件过滤日志、并发连接数； 15. 支持实现 HTTP、FTP、POP3、SMTP、IMAP、SMB 六种应用协议的双向内容过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义，支持阻断及日志两种处理动作； 16. 漏洞防护特征库要求包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； 17. 支持自定义漏洞签名。可标识自定义漏洞的 CVE 编号或 CNNVD 编号。支持自定义基于 TCP、UDP、HTTP 协议的漏洞，并根据各协议的报文结构，指定一个或多个字段的特征值，这些特征值可以被以文本的形式或正则表达式的形式进行匹配，同时支持是否按顺序对这些特征值进行匹配检测。支持自定义漏洞的源端口范围及目的端口范围； 18. 支持与防病毒系统或终端安全管理系统进行联动，增强防火墙对应用特征及木马特征的识别； 19. 支持双系统备份，且在系统切换中可实现配置的自动迁移； 20. 支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括 1 天、7 天、30 天、90 天、永久等； 21. 支持在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤等安全功能选项； 22. 基于源目地址、源目端口、协议、域名、URL 多维度的一键式快速运维处置； 23. 日志支持模糊搜索和按精确策略条件搜索，协助定位异常行为，并通过带条件跳转实现指定行为在分析中心中的关联活动展示，确认异常行为是否具有威胁； 24. 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；		
10	安全加密 U 盘	网神、360 移动存储介质管理系统及安全 U 盘 V6.0	1、安全 U 盘性能参数：提供 USB2.0 接口或以上，每个 U 盘容量不低于 8G。采用专用控制模块防止 U 盘介质非授权格式化；使用国产加密芯片对数据进行加解密，安全芯片密级达到检测一级要求。支持产品出厂前 LOGO 定制，可根据用户提供的单位名称进行量身定制；	20	¥750

			2、在身份认证之前，安全U盘的用户数据区属于禁止访问状态，受安全芯片全面保护，安全U盘的启动区属于只读状态，可防止攻击者进行篡改； 3、在身份认证之后，对安全U盘用户数据区的访问，需要通过调用安全芯片接口，接口会对访问的进程进行合法性校验，第三方进程无法成功通过校验，从而阻止第三方的访问与篡改； 4、安全U盘采用私有文件系统接口，主机病毒木马无法自动传播到安全U盘中，安全U盘病毒木马也无法主动传播到主机中； 5、安全U盘数据存储分区分为内网高速区和外网高防交换区，可以通过安全U盘管理系统设置用户安全U盘用户使用权限，在内网电脑使用时，可以使用内网区和外网区，或者只允许使用内网区，外网区加密不可见。在外网电脑使用时只能使用外网区，内网区加密不可见。读写权限可以根据实际需求进行灵活分配； 6、支持通过软件登录界面，或者物理按键的方式，验证用户口令，才可访问U盘； 7、用户口令有尝试次数上限，超过上限后，安全U盘锁定。锁定后即使输入正确的口令也无法访问U盘； 8、安全U盘可以通过内置或外置的功能，来重置安全U盘口令，并清空U盘数据，安全U盘只允许使用企业内部专用初始化工具进行初始化，初始化的功能需要验证管理员身份； 9、数据秘钥安全，在身份认证之前无法访问数据区密文，无法获取数据明文密文的配对；加密方法无法被第三方程序调试，密钥的生成和维护机制受安全芯片保护； 10、安全U盘要求自身采用私有的文件系统，需要通过私有文件系统接口，对文件进行读、写。防止病毒木马主动传播； 11、安全U盘要求支持底层通讯指令经过加密处理，防止通过USB总线嗅探工具获取关键指令，防止“指令重放攻击”； 12、★投标人所提供的设备与技术服务能够与广西高级人民法院现有的安全U盘管理系统，以及内网终端安全管理系统实现对接，对接所涉及到的全部费用均由投标人承担。		
11	机柜系统	超特、CTP-120642	1、 全密封一体柜，含全封闭式冷热通道，通道深度大于200mm，支持上线进线，前单开玻离门，后金属密闭门。 2、 机柜尺寸：600*1200*2000mm。 3、微模块系统机柜需符合ANSI/EIA RS-310-D、DIN41491；PART1、IEC297-2、DIN41494；PART7、 GB/T3047.2- 92标准，兼容19"国际标准、公制标准和ETSI标准。具备很强的兼容性，所有满足EIA-310-D标准的设备都可以安装在机柜中。 4、 微模块系统每个服务器机柜的前后19”安装立柱在机柜内部的安装位置(深度方向)应前后可调，安装立柱正反面均有U高度刻度，安装立柱侧面有安装孔，机柜后部配备2条42U垂直理线槽方便 线缆管理。 5、 微模块系统机柜冷、热通道应与机柜框架整体焊接成型，具	6	¥18,500

			备良好的承载能力和密闭性，不接受拼接式风道。 6、 ★承重≥1600kg，提供第三方检测机构出具的报告。 7、 机柜抗震列度为 8 级，供货时提供认证或检测报告； 8、 ★为了便于快速响应的服务条件，避免因多品牌导致的产品责任问题界定难度，要求机柜、联动及控制组件、配电系统、UPS、空调系统、微模块监控系统采用同一品牌。 9、 机柜侧门 2 套、1U 免工具安装铁质盲板、50KG 设备托放层板、1U 毛刷盲板、42U 垂直理线槽、600 宽机柜顶部走线槽，双通道强弱电分离。 10、 对微模块系统各类传感器及设备进行集中采集及集中控制，安装于机柜热通道不占用机柜 U 位空间 11、 自动开门组件： 1、每个机柜均应配备一套自动开门组件，不应占用 U 位空间。 2、当出现如下紧急状态时，机柜前后门自动打开降低模块内温升，机柜前后门开门角度 90 度： a) 当市电停电情况下，机柜前后门自动打。 b) 当空调故障情况下，机柜前后门自动打。 c) 当出现通道内温度超限时，机柜前后门自动打。 12、LED 照明组件：提供机柜照明，当开门时机柜 LED 灯自动亮起，关门时 LED 灯自动熄灭。 13、状态背景灯光组件：为机机柜提供双色状态背景灯光，系统正常时显示蓝色背景灯光，当发生告警时显示红色背景灯光，背景灯光可手动设置开启关闭。		
12	配电系统	超特、 PCT-30RI	1、机架式配电模块，含主路电能检测，含 RS485 监控接口，含输入输出指示灯，采用施耐德开关器件。	1	¥21,500
13	PDU	超特、 CTPJ2-161010	1、机柜 PDU，单相 16A 输入，10 位 10A 国标输出。	10	¥850
14	UPS、蓄电池	超特、 SU-R10KS	1、 机架式 UPS 10KVA，可直接标准机柜嵌入式安装。 2、12V/100AH 蓄电池：数量 32 只 蓄电池技术要求：额定容量：20 小时放电率 100Ah，适用温度范围：-15℃~45℃。 板栅结构设计减少了使用过程中的板栅伸长；独特的 4BS 铅膏配方，专用紧装配 焊接设备、电池内化成技术，大大延长了电池的使用寿命，浮充设计寿命 10 年（25℃） 3、电池柜及电池连接辅材。 4、★UPS 蓄电池要求与机柜同一品牌，便于整套系统的维护。 5、为保证产品质量，供货时提供 UPS 主机和蓄电池的泰尔认证及检测报告。	1	¥75,800
15	空调系统	超特、 AT-IA80HDUA0	1、 精密空调安装于模块系统内部，采用机架式安装方式，保证系统一致性美观性、易扩容性。 2、 精密空调制冷量 8KW。 3、 精密空调采用电子膨胀阀提高控制精度和响应速度，实现精确制冷且系统稳定，与负荷匹配精准、节能效果好。	2	¥52,000

			4、 采用 EC 风机可以无极调节调速，可以随负荷进行快速响应，具有高风量、高效率、长寿命、低噪声等特性。 5、 机组采用全直流变频压缩机，可实现机组制冷量的灵活调节。压缩机变频控制技术结合机组的送风温度控制，可以使机组在不同的热负荷下能够灵活调节制冷量，从而提供相对恒定的送风温度，降低了送风温度的波动。另外在低热负荷条件下可以尽量降低压缩机的运行频率来保证机组送风温度不会降到太低，并且避免压缩机进入频繁启停状态，如此不仅提高了机组的运行效率和可靠性，还可以避免送风温度太低造成的结露风险。 6、 ★为了便于快速响应的服务条件，避免因多品牌导致的产品责任问题界定难度，要求机柜、联动及控制组件、配电系统、UPS、空调系统、微模块监控系统采用同一品牌。		
16	微模块监控系统	超特、IDU100	1、功能要求： UPS 电源监控、精密空调监控、配电单元监控、漏水监测 1 个、温湿度传感器 5 个、烟感 2 个、联动控制 1 项、10.1 寸触摸屏 1 个安装于微模块机柜前门。 2、硬件性能部分： （1） 为降低机房内噪音，使机房工作能够在一个比较舒适的环境中进行，监控主机必须为低功耗设计的嵌入式主机，必须无风扇。 （2） 为保证被监控设备的正常工作，监控系统必须符合电磁兼容性和电气隔离性能设计要求。 （3） 为方便现场的安装部署、安置美观大方，要求监控采集主机只能为一台，所有被监控设备全部都集中接入监控采集主机，并且接口须标准化，如 RJ45/DB9 等标准化接口，为了方便维护，不能外接接口，设备须符合目前行业最为标准的 19 寸机架式结构要求。 （4） 监控主机设备的质量一定要过硬，能够抗腐蚀，抗变形，密封性好. 3、监控系统软件技术要求： （1） 采用的是 LINUX 嵌入式系统平台，隔绝病毒且稳定可靠。为保证系统的可靠性及避免病毒的影响，监控采集主机设备要求采用最为安全可靠的嵌入式系统平台，如 Power PC linux，ARM linux 等。 （2） B/S 架构，免客户端安装，无需加载控件，由于此系统实现的是机房设备集中管理化要求，软件系统需支持多客户端的访问，方便各级管理人员的登陆，系统需支持 B/S 技术构架，免客户端安装，通过 IE 等网页浏览器，不能够加载控件。 （3） 效率高，稳定安全，可同时支持 5 个客户端同时访问流程，数据加载不超过 5 秒。网页优先需要考虑效率更高、稳定性更好、跨平台性更好、安全性更高的技术架构，需要支持 5 个客户端同时访问流畅，加载数据用时不应该超过 5 秒。 （4） 兼容多品牌多型号的 UPS、精密空调、精密配电等；	1	¥41,750

			（5） 机房动力、环境、空调等设备分区管理，分区展示； （6） 后期系统的扩容及扩建，只需要购买扩展的传感器，在线连接至主机即可实现新增扩展设备的增加，即插即用。 （7） 可根据告警设置进行多种形式的告警，具有至少 3 种告警联动机制（短信/声光/邮件）。每一个告警都可进行关联不同类型的告警方式，报警响应速度快，响应时间少于 5S。 （8） 能够按照实际情况进行设定使用，可以灵活设置报警的条件。对每种监控量的报警设置中，可按报警类别的不同进行不同的设置，也可根据需要对相关告警量的上下限阀值设置进行调整。 （9） 具有多用户管理权限，多层级、多用户、的监控管理系统；可建立多个管理用户，分配用户的查看/管理权限，避免人员误操作。 （10） 具有远程自测、关机及重启 UPS 功能，能够定时任务进行此类操作，并具有相关的记录报表。 （11） 完善的历史记录，并且具有事件处理记录功能，可导出形成报表。 （12） 具有时间一键同步功能，无须繁琐设置。 （13） 监控系统网络通讯协议符合国际网络协议标准，可提供二次接口连接； （14） 应用软件接口具有较强的灵活性和扩充性。 （15） 为了远期功能优化更新，需要具有一键升级的功能。 （16）为避免使用一段时间之后，要进行繁琐的温湿度校准工作，需要具有温湿度校准功能，并且无技术门槛，自由操作。 （17） 为了能够更加清楚的知道自身的存储状态，提早进行数据转移保存等措施，所以系统必须具有检测存储容量功能。 （18） 每次告警的详情都有记录，每次告警解决也必须有记录，每次告警必须有持续时间的记录。 （19） 实现对机房远程监控与管理功能，通过手机 APP 可对远程监控对象进行可靠、准确的监控与控制。使机房无线远程监控达到无人或少人值守，为机房高效的管理和安全运营提供有力的保证。 （20） ★为了便于快速响应的服务条件，避免因多品牌导致的产品责任问题界定难度，要求机柜、联动及控制组件、配电系统、UPS、空调系统、微模块监控系统采用同一品牌。		
17	安装调试+辅助材料	中国、国标	1、对旧设备的拆卸，迁移，标签，分类，安装调试等工作。 2、对线路进行分类、捆扎，并对线路进行编号并贴好标签标识、做到统一、清晰、维护容易查找等工作。 3、电缆、底座、铜鼻子、PVC 管槽 20\25、设备防水箱 、膨胀螺栓、插座、水晶头、扎带、胶布等项目所需全部辅助材料。	1	¥49,900