采购需求

（一）技术要求

1、采购标的名称、数量、单位及技术参数

招标文件在以下技术参数中指出的工艺、参数、型号、尺寸、质量仅作为说明并没有限制性，供应商可以在投标文件中选用同类替代标准，但这些替代标准要相当于或优于技术要求中规定的标准。本项目核心产品：动环监控。

序号	采购标的名称	技术参数		单位	数量
1	精密空调	硬件要求	1、机器采用上送风前回风的气流组织形式,制冷量≥20.0KW，恒温恒湿； 2、机组采用直板式大面积蒸发器，保障换热效率；安装有智能除湿装置，以减少空气过冷及热补偿的能量损失，精密空调机组可以实现低设备负载情况下的稳定除湿功能； 3、机组的工作环境:机组的电气性能符合 IEC 标准，工作电压允许波动范围：380V+10%，工作频率：50HZ±3HZ，温度范围：-40℃-50℃； 4、温度、湿度控制性能：应能按要求自动调节室内温、湿度，具有制冷、加热、加湿、除湿等功能； 5、温度调节范围：+17℃～+32℃，温度调节精度：±1℃，湿度调节范围：30%～80%RH，湿度调节精度：±5%RH，温、湿度波动超限应能发出报警信号。	台	1
2	消防系统	硬件要求	1、烟火灾探测器 5 个、火灾探测器 8 个、声光警报器 6 只、火灾报警控制器/消防联动控制器 1 台、气体灭火控制器/火灾报警控制器 1 台、气体释放警报器 3 只、紧急启停按钮 3 只、智能电源箱 1 台、柜式七氟丙烷灭火装置 4 套、七氟丙烷灭火剂 324 公斤。	套	1
			1、烟火灾探测器 2 个、火灾探测器 2 个、声光警报器 2 只、气体灭火控制器/火灾报警控制器 1 台、气体释放警报器 3 只、紧急启停按钮 1 只、柜式七氟丙烷灭火装置 2 套、七氟丙烷灭火剂 100 公斤。	套	1

3	动环监控	配电柜监测	1、支持测量各相相电压有效值、三相相电压有效值的平均值、电压有效值、三相线电压有效值的平均值、相位角、1～4 回路各相电流有效值、有功功率、总有功功率，全回路总有功功率、各相无功功率、总无功功率、总视在功率、各相功率因数、总功率因数、各相有功电能、总有功电能，全回路总有功电能； 2、支持计量有功电能，掉电不丢失； 3、支持采用 RS485 数字通讯接口采集所有数据； 4、电压支持：测量范围:30~600V(线电压)；20~400V(相电压)，PT:1~10000；连续过载：800V； 5、电流支持:配互感器 withCT0~400A;直入型 0~6A;CT:1~10000；连续过载：2 倍； 6、支持功率测量范围：单相功率：0~80000W/var 总功率：0~240000W/var/VA(按实际输入 3×U×I)； 7、每套配备电流互感器等配件 3 个。	套	2
		市电检测模块	1、支持市电输入接口 6 路 L/N 湿节点输入； 2、市电接入量程 90~275VAC； 3、接口类型支持 RJ45 网口形态； 4、支持 MODBUS 485 协议； 5、波特率支持范围 1200~115200bps； 6、传输距离≥1200 米； 7、防雷等级≥2000W(静电放电)； 8、过压过流保护 30V/200mA； 9、功耗≤0.3W； 10、支持导轨或支架安装； 11、支持动环监测平台统一管理、配置等操作。	套	2
		UPS 监测（采集器）	1、PRS485 接口≥1，DATA 接口≥1； 2、支持 MODBUS485、RS232 两种接口形式的数据采集及对接； 3、RS485 接口速率≥3Mbps，RS232 接口速率≥250kbps； ▲4、支持通过软件自定义 RS485、RS232 接口线序，可实现 RX、TX、GND 的软件自定义（**提供软件功能截图**）； ▲5、可以被数据采集设备统一管理，实现激活、上线、调试等操作（**提供软件功能截图**）； ▲6、为确保物联网网络安全，产品需符合《GB/T 37044-2018 信息安全技术物联网安全参考模型及通用要求》；	套	3

		新风系统对接（采集器）	1、PRS485 接口≥1，DATA 接口≥1； 2、PRS485、DATA 接口均为 RJ45 形态； 3、支持 MODBUS 485、RS232 两种接口形式的数据采集及对接； 4、RS485 接口速率≥3Mbps，RS232 接口速率≥250kbps； ▲5、支持通过软件自定义 RS485、RS232 接口线序，可实现 RX、TX、GND 的软件自定义。（**提供软件功能截图**）； 6、可以被采集主机及动环监测平台统一管理，实现激活、上线、调试等操作。	套	1
		精密空调监测（采集器）	1、PRS485 接口≥1，DATA 接口≥1； 2、PRS485、DATA 接口均为 RJ45 形态； 3、支持 MODBUS 485、RS232 两种接口形式的数据采集及对接； 4、RS485 接口速率≥3Mbps，RS232 接口速率≥250kbps； ▲5、支持通过软件自定义 RS485、RS232 接口线序，可实现 RX、TX、GND 的软件自定义；（**提供软件功能截图**） 6、可以被采集主机及动环监测平台统一管理，实现激活、上线、调试等操作。	套	3
		漏水监测（不定位）	1、漏水反应时间≤2S； 2、支持至少检测 200 米距离范围的漏水情况； 3、支持兼容两芯或四芯测漏传感电缆； 4、支持本地 12~24VDC 供电； 5、存储温度-40℃至 60℃，工作温度-20℃至 50℃，湿度 5%到 95%（无冷凝）； 6、要求搭配 15 米不定位漏水检测线缆，每台配置 1 根。	台	3

		消防监测	1、支持实时监视探测烟雾的存在，有效对火灾进行预警； 2、支持本地供电； 3、支持监控电流：＜4mA，支持火警电流：＜30mA； 4、支持继电器干接点输出，监控时输出开路，报警时输出短路（用户可以自行设定）； 5、支持指示灯提示，正常情况绿灯常亮，检测有烟雾异常时红灯闪烁； 6、支持自动报警且报警音量：＞80dB（正前方 3m 内）； 7、支持正常工作温度：-10℃～+50℃，相对湿度：＜95%； 8、支持与动环监测平台通信跟控制，可实现 APP、语音等告警。	个	10
		温湿度监测	1、支持温度、湿度数据采集与上报的机架式温湿度传感器； 2、支持采集温度范围:-10℃～70℃;误差<±0.3℃，在 25℃时测试； 3、支持采集湿度范围：5%～95%RH（无凝露）；误差<±3%RH，在 25℃时测试； 4、支持液晶显示：显示当前温度，湿度，网络连接状态； 5、支持 RS485 接口：通信协议：MODBUS-RTU 协议；波特率：默认 9600；可选 2400、4800、9600、19200bit/s；数据格式：N,8,1； 6、设备管理：支持动环监测平台统一集中管理，支持设备自定义命名。	个	10
		红外入侵监测	1、工作电源：支 DC12V（可工作在 DC9-24V）； 2、探测距离≥12m； 3、探测角度≥90 度； 4、探测速度≥0.3 米/秒~3 米/秒； 5、防拆输出：常闭，接点容量 DC28V100mA； 6、报警输出：常闭/常开可选，接点容量 DC28V100mA； 7、支持 Web 端、APP 端远程设置设备状态； ▲8、支持联动其他设备，如报警设备、视频监控设备等；（**提供软件功能截图**） 9、支持在动环监测平台可统一管理全部红外人体感应设备	个	2
		视频监控对接	1、能够与现有视频监控系统进行对接，支持对接 ONVIF 协议摄像头； 2、对接后可直接调取监控画面，查看告警事件； 3、至少支持摄像头接入数量授权≥15 路；	套	1

		人脸识别门禁	1、支持触摸显示屏，可显示软件界面及操作提示，设备实时检测最大人脸，具有人脸框提示设计，方便用户校准； 2、支持采用宽动态摄像头，最大视场角 120°，面部识别距离＞2m，适应 1.2m-2.0m 身高范围，支持手机照片、视频防假，支持远程视频预览，支持识别二维码； 3、支持星光级图像传感器，无需白光补光灯，在暗光或无光环境下人脸识别效果不受影响； 4、设备采用深度学习算法，支持至少 5000 人脸库，人脸比对时间≤0.2s/人，人脸验证准确率≥99%，识别速度快，准确率高； 5、设备支持多种认证方式：刷卡、人脸、刷卡+人脸等认证方式； 6、设备支持普通卡/残疾人卡/黑名单/巡更卡/来宾卡/胁迫卡/超级卡/解除卡等多种卡片类型； 7、设备支持多重卡开门功能、首卡开门功能、超级卡和超级密码开门、中心远程开门、多重卡认证+远程授权（N+1）开门功能、在线升级功能、单门反潜回功能； 8、设备支持统一管理； 9、含磁力锁、开门按钮、电源等配件包，每台含 1 套配件包。	套	3
		短信电话告警	1、12V 2A 电源供电，且内置一块电池供断电后应急使用； 2、支持机房动环系统统一管理、配置、监测等功能； 3、支持电话、短信告警两种方式； 4、支持接口类型为 RJ45； 5、支持联通、电信、移动全网通 4G 接入。	套	1
		声光报警器	1、报警音量：MAX 110dB； 2、工作电压：交流 9V～18V 或直流 12V～24V； 3、工作环境：-35℃～55℃； 4、控制方式：采用 Modbus 协议，通过网口形态 RS485 接口与动环监测平台进行通信； ▲5、支持联动告警：支持联动机房动力环境监测系统实现多样化报警，如设备异常、非法入侵、机房漏水、温度过高等告警，支持同时发出声、光两种警报信号（**提供功能截图**）； 6、支持被机房动力环境监测系统管理、配置、展示；	个	1

		数据采集设备	1、以太网口数≥3 个；Console 管理口≥1 个；USB 接口≥1；PDI 接口≥4 个，PRS485 接口≥5 个，DO 接口≥1 个； 2、支持门禁主机功能，具备专门的门禁接口，电源接口≥1；干接点开关接口≥1 个；韦根接口≥1 个； 3、内存≥8GB； 4、所有接口均支持 RJ45 形态，支持对外提供 24V 直流供电； 5、支持传感器类型智能识别，智能上线； 6、支持在多分支机房场景下，与总部网络中断时，本地机房关键数据可以在采集主机实现缓存，时间周期大于 7 天，网络恢复时，数据自动补传给总部平台，保障数据不因网络中断而丢失； 7、支持在多分支机房场景下，与总部网络中断时，本地机房关键数据可以在采集主机实现缓存，时间周期大于 7 天，网络恢复时，数据自动补传给总部平台，保障数据不因网络中断而丢失； 8、支持断电、死机自动开启磁力锁，防止消防状态下人被关在里面； 9、支持对传感器接入是否正常进行监测，LED 灯亮则接入正常；	台	5
		机房动环监控平台	1、千兆以太网口数≥4 个；RJ45 Console 管理口≥1 个；USB 接口≥2； 最大支持 256 个终端接入。 2、支持对接市电监测模块、三相电量仪、UPS、蓄电池、柴油发电机等动力系统，实现对机房动力系统物理安全状态的实时感知； 3、支持接入温湿传感器、精密空调、普通空调、漏水传感器等，实现对机房环境物理安全状态的实时感知； 4、支持接入门禁、门磁、烟雾传感器、视频等，实现对机房安防系统物理安全状态的实时感知； 5、支持 3D 智能引擎，内置网络设备、机柜、UPS、办公资产等素材，可以基于机房真实情况，通过拖拽式真实还原，实现所画即所得； 6、支持基于数字孪生技术的大屏展示，向管理人员展示整体机房整体运行状态，包括 UPS 状态、精密空调状态、电力系统、温湿度情况、告警情况等信息，数据通过友好的大屏直观呈现展示，实现管理可视化； 7、支持多种告警模式，包括电话告警、短信告警、	套	1

			声光告警、APP 告警、WEB 告警、阿里钉钉、微信告警、邮件等； 8、支持多分支机房统一管理，支持本地局域网部署和跨互联网远程部署，通过平台可以对所有分支的接入传感器和物联网关进行统一集中管理，包括统一策略配置、统一运行状态查看、统一数据分析； 9、支持与视频监控对接，实现视频弹窗告警，联动抓拍；支持内置视频中心；支持实时录制告警发生的全过程，并内置视频中心随时查看，实现告警回溯； 10、支持移动 APP 运维，通过手机 APP 即可进行状态查看、设备远程管理、策略远程配置、数据分析查看、巡检任务、空间查看等，并内置常见告警模板，简化运维工作量； 11、支持巡检策略设定，记录并存储巡检报告，比如平台定时对全部设备进行巡检，及时发现异常设备，消除隐患；		
4	新风系统	性能要求	1、风量：≥1600 m^3/h；功率：≥600 w；热回收率：≥75%。	套	1
5	监控系统	性能要求	1、传感器类型：1/2.7 英寸 CMOS； 2、像素：400 万； 3、最大分辨率：2688×1520； 4、最低照度：0.002lux（彩色模式）；0.0002lux（黑白模式）；0lux（补光灯开启）； 5、最大补光距离：50m（红外视频监控距离）； 6、补光灯：2 颗（红外灯）； 7、镜头类型：定焦； 8、镜头焦距：3.6mm； 9、镜头光圈：F1.6。	台	15
			1、PoE 交换机	台	2
			1、网络硬盘录像机 接入路数：32 路；含 4 块 8T 硬盘。	台	1
6	负载均衡	性能要求	1、2U 标准机架式设备，最大吞吐量≥10Gbps，并发连接数≥1100 万，每秒新建会话数≥60 万/秒，PPS（包转发率）≥1400 万，6*GE 电口+8*SFP+万兆接口。	台	1
		工作模式	1、支持透明网桥模式，支持路由模式，支持 NAT 模式，支持旁路分析模式，支持路由、NAT、网桥和旁路分析的混合模式。		
		VRRP	▲1、VRRP 支持 IPv4 和 IPv6 同时部署(**提供功能界面截图**)； 2、支持接口线路工作状态和 VRRP 接口联动； 3、支持对多个 VRRP 物理网卡状态自动调整 VRRP 抢占优先级。		

		IPv6 流量	1、支持对 IPv6 2～7 层流量的识别能力，能够识别主要应用协议； 2、支持对 IPv6 的流量控制，对流量进行放行、阻断、通道限速等； 3、支持对 IPv6 路由，可以对 IPV6 的流量做路由策略； 4、支持 IPv6 到 IPv4 的映射，将 IPv6 的公网 IP 与内网 IPv4 的服务器做映射； 5、支持静态 NAT66 功能； 6、支持 IPv6 的 MAC 管控； 7、支持 V4 到 V6 地址转换。		
		协议识别能力	1、支持 DPI、DFI、节点跟踪、主动探测、加密分析等多种技术； 2、支持对 2～7 层流量的识别能力,特别是针对第 7 层的应用识别能力，能够识别主要应用协议，并逐级细分 P2P 下载、网络视频、网络电话、识别能力、HTTP 协议的子类别和具体客户端名称。		
		智能应用路由	1、支持基于 5 元组、域名、应用协议、DSCP 标签、对象库等条件对流量做路由牵引； 2、支持基于以上组合策略条件对流量做路由牵引； 3、支持虚拟 LAN 接口和 WAN 线路最大支持 4000 条。		
		控制性策略	1、支持基于全局、链路、数据流向、共享用户、移动终端、应用协议/协议组和 IP/IP 群组的速率控制； 2、支持允许、阻断、带宽限速等控制动作，控制参数包含：线路、数据流向、内网地址、用户 MAC、外网地址、传输协议、应用协议、内网端口、外网端口、共享用户数、QQ 用户数、移动终端数、执行动作、优先级、内网 IP 限速等。		
		会话日志	1、日志系统支持会话日志,会话日志包含设备编号、接口、访问时间、源地址、目标地址、NAT 地址、账号信息、域名、协议类型、7 层协议名称、流量、运营商、地理位置一共 13 个元素。同时采用 1:1 的日志输出，完整保留网络中的相关信息。		
		TAP 流量复制	1、支持端口镜像功能；可根据设置条件将类如 HTTP、网桥设备上行方向、某 IP/IP 段、手机上网流量、未知协议等流量等镜像至指定网络接口（包含 VPN 线路），与第三方审计设备联动，便于个性化的数据分析。		

		负载均衡	1、支持基于源 IP、目的 IP、源和目的 IP、四元组、空闲带宽的负载均衡； 2、支持基于域名、应用协议、对象库等混合模式的负载均衡； 3、支持基于最大带宽负载，线路流量达到阈值后切换至其他线路； 4、支持负载均衡策略的生效时间设置； 5、支持服务器负载均衡，最多可以支持 100 台服务器，16 个服务器组； 6、服务器负载均衡支持根据源 IP,源+目 IP 做 HASH 均衡，也支持加权轮询均衡算法； 7、服务器负载均衡支持域名负载。		
		智能 DNS	1、可根据源 IP、目标 IP、访问域名、所在线路等组合条件实现对域名访问的控制，域名控制方式支持阻断、劫持和重定向。		
		PPPoE 服务	1、支持 PPPOE SERVER，单台≥3 万用户在线，PPPOE SERVER 支持与 Radius 认证计费系统对接，并能接收 Radius 服务器下发的限速，踢掉在线用户等指令； 2、可针对用户上线发布公告，用户到期提醒和过期提示； 3、支持 PPPOE 代拨，最少支持 24K 外网代拨账号，PPPOE 代拨支持 CMCC PORTAL 协议，可以账号透传，也可以通过 RADIUS 获取代拨账号； 4、支持 PPPOE 代理，PPPOE 代理账号上线后，可以发送认证日志，日志信息包括账号和 IP 对应关系。		
		嗅探	1、支持在旁路或串接模式下，深度分析 RADIUS、PPPOE、DHCP 数据包，找到账号的带宽限制参数，显示用户真实 MAC，自动对相应 IP 做限速。		
		业务质量测量	1、支持对每条会话监测客户时延，服务时延，应用时延的指标测量。（设备到客户端的网络时延），服务时延（设备到服务器的网络时延），应用时延（会话上下行首包时间差），最大包长（会话上下行最大包的长度）； 2、支持每 IP 用户对端服务应用的质量监测； 3、支持基于五元组、应用、域名进行业务质量分析； 4、支持会话级别的上下行流量查询； 5、支持会话级别的丢包率和重传率查询。		

		威胁情报	1、系统内置数字货币、C&C 节点、APT 攻击、网站后门、钓鱼网址、僵尸网络等 16 种威胁情报，针对网络异常行为进行检测分析； 2、支持对威胁情报的命中监测，支持查看情报命中趋势、情报类型命中分布、以及源 IP、目的 IP、源 MAC 等信息； 3、支持按照威胁情报类型，对命中情报的会话进行自动阻断； 4、支持白名单功能，加入白名单的 IP 和域名，不会命中情报，不会做相应的阻断等动作； 5、情报库支持在线自动同步，支持离线上传； 6、支持对接第三方威胁情报。		
		告警推送	1、支持基于策略的告警功能，可根据定义监控对象阈值，实时向外告警； 2、支持检测系统告警，如 CPU、授权、总连接数、总 IP 数等； 3、支持检测网卡告警，如任意或指定网卡状态、流入/流出速率等； 4、支持检测 WAN 线路告警，如任意或指定 WAN 线路的流入/流出速率、状态变化、心跳时延等； 5、支持检测内网 IP 告警，如任意 IP 的连接数和会话应用； 6、支持检测应用协议告警，如指定应用协议的上、下行流量速率； 7、支持针对各接口 Ping 检测功能，根据检测时延设置阈值，实时向外告警； 8、告警发送方式支持微信公众号、企业微信、邮箱、钉钉等。		
		微信通知和断网	1、通过微信通知，可以随时掌握设备的运行状态，授权信息等内容；通过“一键断网”功能，可以随时通过微信发出指令，阻断内网有问题服务器的 IP 或者域名。		
		VPN	1、支持 L2TP，IPSec、GRE，支持 SD-WAN Tunnel 等。		
		应用商店 APP	1、设备支持以应用商店形式安装所需的功能，可以提供 HA 主备切换能力和通过云服务监控管理多台设备。		
7	入侵防护系统	规格性能	1、标准机架式硬件 2U，交流冗余，≥4T 硬盘，≥4 个万兆光口（含光模块），≥6*扩展槽位，2*USB 接口，1*RJ45 串口，2*千兆电口(管理*1,热备*1)，液晶屏，缺省功能入侵检测、抗拒绝服务、数据防泄漏、应用管理、流量管理、网络层吞吐量≥50Gbps、应用层吞吐量≥10G。	台	1

		安全防护	▲1、系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量为 1 万种以上；（**提供攻击特征库数量截图**）		
			▲2、支持基于 SCADA 等工控协议的相关漏洞攻击检测与防护；（**提供功能截图证明**）		
			3、系统应提供 DoS/DDoS 攻击防护能力，支持双向阻断 TCP/UDP/ICMP/ACK Flooding，以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击。		
			▲4、支持通过 X-Forwarded-For、X-Real-IP、Cdn-Src-IP 来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务的客户端最原始的 IP 地址,并可自定义 X-Forwarded-For、X-Real-IP、Cdn-Src-IP 三个字段的识别优先级顺序;（**提供功能截图证明**）		
			5、系统支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等检测和防护。		
		流量控制	1、支持用户以安全区、IP 地址（网段）、时间、用户、应用多维度的对流量进行管理和控制，包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每 IP 的进行应用流量控制。		
		状态监控	1、首页状态分布支持对威胁事件分布、入侵事件-攻击类别分布、入侵事件-攻击类别趋势、TOP 入侵事件、TOP 入侵事件目的 IP、TOP 入侵事件源 IP、TOP 源 IP 地理分布等威胁事件的下钻分析，点击对应的威胁事件可下钻到对应日志分类查看威胁事件的详细信息。		
		APP 运维管理	▲1、支持设备云端托管服务，将设备上确认威胁告警事件风险上报到云端平台，通过 APP 即时查看告警，实现 APP 运维管理。（**提供界面截图证明**）		
		其他	1、提供三年特征库升级服务； ▲2、产品具有 IPv6 Ready Logo 认证测试证书，**提供有效证书扫描件**。		
8	防火墙	硬件要求	1、2U 标准机架式，含交流双电源，1 个 RJ45 串口，1 个 GE 管理口，1 个 HA 口，2 个 USB 接口，≥4 个万兆光口插槽（含光模块），≥3 个接口扩展槽（4GE4SFP/2SFP+/4SFP+），面板带液晶显示屏，硬盘≥256G 固态硬盘+4T 机械硬盘，≥64G 内存，整体吞吐量≥60Gbps，应用层吞吐≥45Gbps，最大并发会话数≥1800 万，每秒新增会话数≥70 万，**整**	台	1

			机不少于三年升级维保授权,含防病毒模块。		
		链路探测	▲1、支持通过 ICMP、TCP、UDP 协议，完成对目的 IP 地址可达性的探测，支持在策略路由、GRE 隧道、DNAT 策略、HA 中设置链路探测。（**提供配置界面截图证明**）		
		应用识别	▲1、支持国产数据库识别；（**提供配置界面截图证明**）		
			2、支持工业系统类应用协议识别，例如：OPC、IEC、MODBUS、航天云网-INDICS、FOCAS、PCWORX 等工控协议。		
		一体化策略	1、提供基于源/目的 IP 地址、安全区、应用、应用组、协议/端口、时间、安全模板的精细粒度的安全访问控制。		
		策略模拟测算	▲1、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。（**提供配置界面截图证明**）		
		URL 过滤	1、支持内置 Web 信誉库，收录 40 万+恶意站点；		
			2、提供 64+种精细分类（如艺术、商务、新闻论坛、论坛聊天、科技、体育等等）。		
		DDoS 攻击防护	1、支持 ARP/Ping/TCP/UDP/HTTP/SIP/DNS 类型的 Flood 报文攻击；		
			2、支持用户自定义触发流量阈值，保护流量上限，保护时长以及检测周期；		
			3、支持针对 NAT 地址转换后的 DDOS 攻击防护。		
		其他	1、提供三年特征库升级服务； ▲2、产品具有《信息技术产品安全测评证书》(EAL4+及以上），**提供有效证书扫描件**； ▲3、为保障产品在 IPv6 环境下的检测防御能力，产品需具备 IPv6 Enabled Security Logo 认证，**提供有效证书扫描件；**		
9	漏洞扫描系统	规格性能	1、标准 1U，含交流冗余电源，1*串口，4 个千兆电口，4 个千兆光口，扩展插槽≥1，标准配置提供 1 路授权扫描端口,无限个扫描 IP 授权，最大并发主机数≥60,最大并发任务数≥10,默认开通 web 扫描模块、主机扫描模块、云大物扫描模块，支持对云计算平台、大数据组件、物联网设备提供漏洞检测和分析。	台	1

		功能要求	▲1、支持检测的漏洞数大于 30 万条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准；（**提供漏洞数量截图证明**） ▲2、支持扫描国产操作系统、应用及软件的安全漏洞，要求能够扫描大于 70000 条相关漏洞；（**提供漏洞数量截图证明**） 3、支持专门针对 DNS 服务的安全漏洞检测，包括 DNS 投毒等漏洞检测能力；支持“幽灵木马”检测； 4、支持识别多种物联网设备，支持多种物联网设备，能够扫描大于 100 条相关漏洞； 5、支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义； 6、产品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息； ▲7、支持通过多种维度搜索定位资产和查看资产风险，包括并不限于：节点或设备名称、资产 IP 范围、资产管理员、资产操作系统类型、资产风险等级、漏洞名称、开放的端口、资产 banner 信息等；（**提供功能截图证明**） ▲8、支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态；（**提供功能截图证明**）		
		其他	1、提供三年漏洞库升级服务； ▲2、产品具有 IPv6 Ready Logo 认证证书，**提供有效证书扫描件**。		
10	防火墙	硬件要求	1、2U 机架式设备，交流双电源，1*RJ45 串口，1*RJ45 管理口，2*USB 接口，≥6 个千兆电口（含 bypass），≥4 个千兆光口（含光模块），≥4 个万兆光口（含光模块），≥4T 机械硬盘+256G 固态硬盘，包含防病毒模块。	台	2
		性能要求	1、整体吞吐量≥20Gbps，应用层吞吐≥18Gbps，最大并发会话数≥400 万，每秒新增会话数≥25 万。		
		部署方式	1、支持虚拟线，二层透明，三层，混合，旁路监听，单臂接入方式。		
		链路探测	▲1、支持通过 ICMP、TCP、UDP 协议，完成对目的 IP 地址可达性的探测，支持在策略路由、GRE 隧道、DNAT 策略、HA 中设置链路探测。（**提供配置界面截图证明**）		

		应用识别	▲1、支持对 6500+种应用平台及 7600+种的应用进行识别和控制，支持对应用进行二级分类，类型包括媒体类、协作类、一般网络应用、商业系统等，子类包括音频流、游戏、普通商业、工业系统、物联网、文件传输、即时通信、图片视频、社交网络等；（**提供配置界面截图证明**）		
			▲2、支持国产数据库识别；（**提供配置界面截图证明**）		
			3、支持工业系统类应用协议识别，例如：OPC、IEC、MODBUS、航天云网-INDICS、FOCAS、PCWORX 等工控协议。		
		一体化策略	1、提供基于源/目的 IP 地址、安全区、应用、应用组、协议/端口、时间、安全模板的精细粒度的安全访问控制。		
		策略模拟测算	1、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。		
		NAT64	1、支持 NAT64，支持 TCP、UDP、ICMP 报文的 IPv6toIPv4 和 IPv4toIPv6 转换，同时支持有状态和无状态两种转换方式。		
		入侵防护	▲1、支持 11000+种入侵规则过滤并提供服务器、内网等多种规则模板。（**提供配置界面截图证明**）		
		防病毒	▲1、支持 2000w+文件病毒库，病毒查杀率高；（**提供配置界面截图证明**）		
			2、支持 ZIP/ARJ/CAB/RAR/GZIP/BZIP2/TAR 等不少于 20 层压缩文件的病毒查杀。		
		其他	1、提供三年特征库升级服务； ▲2、为保障产品在 IPv6 环境下的检测防御能力，产品需具备 IPv6 Enabled Security Logo 认证，**提供有效证书扫描件**； ▲3、产品具有《信息技术产品安全测评证书》(EAL4+及以上)，**提供有效证书扫描件**。		
11	网络环境动态分析系统	规格性能	1、标准 2U 机架式设备，配置冗余双电源，1 个 RJ45 串口，2 个 GE 管理口，不少于 4 个千兆电口，不少于 4 个千兆光口（含光模块），不少于 2 个接口板扩展槽位，不少于 4T 硬盘。设备自信誉检测、病毒检测、静态检测、动态检测模块。网络吞吐量不低于 3Gbps，样本动态分析性能(个/日)不低于 60000，最大并发连接数不低于 70000。	台	1

		部署模式	1、支持旁路模式，对镜像或分光数据进行检测； ▲2、支持离线扫描模式，对指定的 FTP/SMB 文件目录进行读取检测。（**提供配置界面截图证明**）		
		动态检测	1、提供基于虚拟执行的动态检测技术，可以基于软件在虚拟环境的行为及通用漏洞利用特征（进程行为，逃逸行为），分类识别各种加壳病毒及未知恶意代码。		
			2、支持对 office 文档、pdf、压缩文件、flash、pe 等常见 windows 平台文件进行动态检测；		
			▲3、支持 win xp、win7、win10、安卓虚拟环境，系统至少内置 6 种不同类型的虚拟环境，支持用户自主配置，支持虚拟环境的定制和升级。（**提供配置界面截图证明**）		
		安全情报	1、支持云端安全情报获取，包括且不限于文件、URL、C&C 等安全情报内容；设备能够生成本地安全情报，包括不限于文件、URL、C&C 恶意 IP 地址等。		
		静态检测和 AV 检测	1、支持无签名静态检测技术，主要有无差别的 shellcode 检测；		
			2、支持 YARA 自定义规格检测，能够编辑 YARA 规则文件，导入 YARA 规则；		
			▲3、支持对病毒、木马、蠕虫等已知恶意代码的检测，系统内置不低于两个病毒检测引擎，用户自主配置。（**提供配置界面截图证明**）		
		其他	▲1、支持 IPv6 环境下的部署与配置，产品具有 IPv6 Ready Logo 认证证书，**提供有效证书扫描件**。 ▲2、产品具有《国家信息安全漏洞库兼容性资质证书》，**提供有效证书扫描件**。		
12	网络诱捕系统	硬件性能要求	1、2U 标准机架式，交流冗余电源，2 个 USB 接口，1 个 RJ45 串口，≥2 个千兆管理口，≥4 个千兆电口，≥4 个千兆光口（含光模块），≥2 个接口扩展槽，≥硬盘 256G 固态硬盘，≥1T*2 机械硬盘，≥支持 50 个虚拟蜜罐授权。	台	1
		安全性	1、蜜网部署期间可通过 Vlan 隔离实现真实内网物理隔离。不开放蜜罐访问外网与内网权限，切断蜜罐到其他网络访问路径，防止攻击逃逸。		
		仿真能力	1、支持工控蜜罐类型的仿真，至少支持工控服务类：Bacnet，S7Comm，Modbus，SNMP，IPMI，EN/IP 等。支持 IOT 蜜罐类型的仿真，至少支持 IOT 服务类：GTP 等。系统默认支持 CVE 等漏洞的内置，预置漏洞类型包含 web 漏洞、应用系统漏洞、数据库漏洞等，预置漏洞数量不低于 45 种。		

		攻击诱捕	▲1、针对客户内部各种复杂多变的网络环境，支持提供二层交换机跨网段部署与三层跨路由部署的方式，实现一台设备，多网段仿真蜜罐的部署，极大提高黑客攻击蜜罐的概率。（**提供功能截图证明**） ▲2、可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统，真正有效消耗攻击资源，并直接保护真实资产。（**提供功能截图证明**）		
		攻击感知	▲1、支持攻击诱捕的场景分析，至少包括：WEB 狩猎、物联网狩猎、业务专项狩猎、基础服务狩猎、文件共享狩猎、远程登录狩猎、工业控制系统狩猎、DNS 狩猎、数据库狩猎、邮件狩猎等 10 种攻击感知的狩猎诱捕场景。（**提供功能截图证明**）		
			2、支持攻击长镜头告警分析：可对攻击者的整个攻击过程进行长镜头回放。参考 MITRE ATT&CK，采用多种取证技术手段,还原黑客攻击入侵蜜罐的过程，形成黑客攻击链，攻击链检测包含：侦查、工具制作、投送、攻击渗透、安装工具、命令控制、恶意活动等攻击入侵过程。		
		攻击反制	1、支持反制技术，可对攻击进行精准有效的反制，支持浏览器漏洞反制技术，获取攻击者信息。		
		攻击者溯源	1、设备指纹溯源至少包括：操作系统信息、浏览器指纹、浏览器类型。位置信息溯源至少包括：真实攻击 IP（攻击者拨 VPN 也可获得真实攻击 IP）、代理转发前的 IP 地址、IP 地理位置。		
		狩猎监控可视化	1、支持展示整体狩猎诱捕态势，呈现蜜罐监控概况，包含：高危攻击者数量、失陷主机数量等；威胁狩猎的诱捕结果，按照业务狩猎分类、诱捕结果的分类及各类型的数量。点击每种类型数字和事件名称，均可进行下钻跳转。		
		其他	▲1、产品具有国家信息安全漏洞库兼容性资质证书，**提供有效证书扫描件。**		
13	可视化运维系统	整体要求	1、要求采用标准机架式设备；管理平台底层操作系统应具备安全性和可靠性；	台	1
			2、提供统一的监测管理平台，集中采集各个业务层次和环节中的 IT 元素，包括但不限于：物联网设备、网络设备、安全设备、负载设备、主机操作系统、中间件、数据库、存储、业务进程状态等；		

			▲3、所有的监测器由统一平台调度，license 授权不得按照 IT 元素种类分别授权;本次授权数量:500 个。（**提供功能截图**）		
			4、平台应具有用户角色权限管理功能，可结合此功能配置不同用户具有不同操作权限和资源视图界面；		
			▲5、单套系统在购买 license 情况下能支持 5000 台 IT 设备的监测能力,并且要支持在不更换设备的情况下进行节点扩容。		
			6、具有独立的自身日志审计功能,可对运维系统的：系统日志、操作日志、通知日志、任务日志和内部日志进行审计，按照时间日期查询并导出；		
			7、平台应支持工单管理功能，用户可手工派单也可以根据监测告警信息自动派发工单；		
			▲8、平台应支持资产管理功能，可根据监测信息自动生成资产列表，用户可根据管理需要增加资产属性条目，并且提供资产批量导入功能，实现 IT 资产全面管理；（**提供功能截图**）		
			▲9、支持远程备份功能，用户可通过界面设置备份任务，平台自动把备份的数据通过 FTP、SFTP 上传到用户指定的备份服务器；（**提供功能截图**）		
			10、平台应提供至少包括以下诊断工具：ping，SnmpWalk，IP 网段计算器，MIB 浏览器；		
		自动化、智能化要求	1、监测管理平台整体设计要遵循自动化、智能化原则，添加被监测元素必须提供“自动发现”功能，发现可监测的设备；		
			2、添加的 IT 元素，平台会按照元素类型、品牌进行自动分组；		
			3、需要纳管设备加入监测后，无需人为干预系统会自动去发现可监测内容并添加监测，并且自动添加建议的监测策略和阈值。		
			▲4、平台提供监测策略审查功能，用户调整监测策略后，系统自动审查所有监测内容是否已经正确配置，发现不符合要求的策略用户可进行批量合并，无需逐条去修改。（**提供功能截图**）		
			▲5、平台提供容量预测功能，可预测未来一定周期内资源预计使用情况；（**提供功能截图**）		

		统一的监测采集要求	1、支持 SNMP、Agent、SSH 等多种采集方式，不得采用 Telnet、RPC 等不安全的采集方式；		
			2、平台提供并支持主流操作系统：Unix、Linux、Windows、AIX、Eular、麒麟等。并且 Agent 应采用单一模式，当主机服务器上的被监测项目发生变更或增加时，无需更换或添加其他 Agent，避免增加主机性能消耗；		
			3、监测管理平台应支持对业务系统自身关键性能点的自定义监测。		
		动环监测数据展示	1、支持对接机房内的动环监测平台，显示动力设备、环境、环境设备、安防系统、IT 设备、能耗管理等监控数据；		
			2、支持智能实现机房内多种设备联动，如温度与空调、门禁与视频、压差与新风机、消防与门禁等；		
			3、支持温湿度传感器，漏水监测，空调监测与控制，烟感，UPS 监测等。		
		监测配置要求	1、平台提供批量修改阈值功能，用户可按照监测种类、监测周期等条件筛选进行批量修改，并且无数量限制；		
			▲2、平台监测采集周期等可配置最小间隔为：5 秒；（**提供功能截图**）		
			3、平台应具有对被监控设备、监测器等随意调整分组功能，用户可按需移动或复制监测内容到新的分组；		
			▲4、平台应具有 SLA 管理能力，用户可以指定多个 SLA 计算规则，并提供按时间进行 SLA 计算数据的回滚展示；（**提供功能截图**）		
			5、平台应具有离线计划功能，用户可以指定一个周期或临时离线操作，并能准确地反映到 SLA 计算中。		
		管理视图展现要求	1、平台应全面采用 B/S 结构，无需安装额外客户端，坚决不允许用混合模式（部分 C/S 和部分 B/S）；支持 https 配置；支持全中文 Web 界面；		
			▲2、平台界面内容可以灵活个性化配置，不同用户可以定制独立的显示风格，包括但不限于：主页、界面色调风格；（**提供功能截图**）		
			3、提供集中登陆页面和大屏展示视图，所有页面基于 HTML5 实现，避免采用 flash 等图形方式显示造成大量性能消耗；		

			4、应具有灵活的可视数仓功能，提供多种展示形式，包括：业务视图、网络拓扑、二维机房和数据看板，可以按照展示需求定义各种图形化展示页面，并能嵌入其他系统展现页面；		
			▲5、平台提供二维机房管理视图，用户只需通过点选等简单操作实现机房设备物理位置管理，并具有机房导出为图片功能，设备面板上传功能，用户可按需真实情况定义机柜中的设备呈现视图；（**提供功能截图**）		
			▲6、平台应提供业务管理视图功能，应能够建立业务纵向逻辑视图，建立从业务到监测数据的层次关联，为管理者提供从业务角度看 IT 的方式，并提供数据抓取功能；（**提供功能截图**）		
			7、支持自动拓扑功能，可自动发现设备之间的链路信息，并且提供手工调整功能；支持多个拓扑图的动态刷新功能，用户可以灵活设置拓扑的刷新时间；拓扑图支持全屏显示，支持显示 IP 与设备名的切换，设备间连线可以显示连线的状态，还可以自动根据流量大小来变换连线的粗细；		
			▲8、平台具有数据看板，可以定义看板分辨率，提供至少包含：文本、饼图、仪表盘、柱状、折线、告警列表、Top 排名、旭日图、类比图、环比图，以及内嵌页面等组件。便于用户快速搭建数据看板页面。（**提供功能截图**）		
		告警管理要求	1、平台应具有集中统一的告警管理界面显示所有告警信息，并且默认显示当前：告警、紧急告警、主要告警和过去 5 分钟的告警数量，点击对应标签即可快速筛查出对应的告警列表；		
			▲2、平台应能够记录、统计、查询所有告警从产生到清除的时间，点击详细按钮可查看所有信息，也可以通过派单按钮直接把告警派发给当前值班人员进行处理；（**提供功能截图**）		
			3、平台应具有自动清除当前告警功能，当前告警清除后需保存在历史告警中；提供历史告警的分类查询和统计操作；		

			4、平台应具有告警通知功能，可通过声音、弹窗、Email、短信、电话、微信、钉钉等多种方式，用户可根据需求选择一种或多种方式配置通知规则；并且当告警确认或清除时系统按照配置对通知规则发送相应通知信息给用户。		
		数据分析要求	1、平台应对每个监测器提供原始数据报表，用户可以指定任意查询周期，或拖动鼠标选中展示周期；		
			2、平台应提供常用的网络、系统、通用、SLA 等多种报表模板，用户基于报表模板可以灵活定义报表内容，也可以自定义 TOP-N 报表、历史数据报表；		
			3、平台应提供趋势分析报表，其中包括：可用率汇总报表、流量汇总报表、设备性能汇总报表、通用趋势报表、流量趋势报表；		
			4、数据分析报表应提供定时发送功能，用户可配置把所需报表定期发送到指定邮箱。		
		易用性和可维护性要求	1、系统部署和使用具备易用性。采用一体化的解决方案，能够实现快速实施交付、快速培训、减少人员投入；		
			2、具备灵活扩展性，能快速适应管理需求变更、有效控制上线后需求变更/扩展的全周期性价比；		
			3、提供 REST－API 方式 / 模式接口，其中涵盖：管理对象，性能和故障信息等。		
14	设备维保	规则库升级和质保	1、1 台防火墙 NFNX3-HDB3280，提供售后服务承诺。	年	1
			2、1 台防毒墙 E680，提供售后服务承诺。	年	1
			3、1 台负载均衡 PA26000-HM，提供售后服务承诺。	年	1
			4、1 台 UTS 探针 UTSHD4500，提供售后服务承诺。	年	1
			5、1 台 IPS IPS4720，提供售后服务承诺。	年	1
			6、1 台日志审计 LASNX3-HD5000，提供售后服务承诺。	年	1
			7、1 台态势感知 智能安全运营平台 V3.0-ISOP，提供售后服务承诺。	年	1
15	等保测评	等保评测	1、电子政务网等保评测二级。	次	1
16	运维服务	基础运维服务		年	1
		服务范围	1、管城区电专中心机房、区委大院分支机房及机房内的基础环境系统、消防系统、网络系统、网络安全系统等。城域网传输系统，从运营商接入接口点为界，包括多种路由器、防火墙、核心网络设备、楼层网络设备；核心机房至各局委、办事处专线链路等。		

		机房基础设施运行维护服务	1、机柜设备维护管理：机柜空间位置、光纤配线柜、机柜线路的整理、标签检查更换等。		
			2、机房动环系统维护管理：供配电系统监测、UPS电源监测、蓄电池组监测、精密空调监控、温湿度监测、漏水监测、消防监测等。		
			3、机房空调配电维护管理：空调设备、新风设备、UPS电池、主配电箱。		
			4、机房消防设备维护管理：烟感热感探测器、手动报警按钮和报警控制器、灭火器的控制装置。		
			5、空调供水、电路维护管理：水电路管线及接口的检查维护。		
			6、机房基础维护管理：机房除尘清洁、防火地板、墙面、吊顶、门窗及相关配套的维护管理。		
		硬件设备运行维护服务	1、机房核心设备运行维护机房核心设备运行维护机房核心设备运行维护包括但不限于核心交换机、汇聚交换机、接入交换机、网络安全设备等运行维护，包括硬件设备的检查、清尘、润滑、调整和坏件更换，运行环境、硬件配置、系统策略的检查，以及对系统日志的检查与分析、性能调优、故障隐患排除等。		
		网络及综合布线运行维护服务	1、包括但不限于对政务网、互联网和其他专网的路由器、交换机、通信设备、传输设备和传输链路的运行状态的运行维护，确保系统正常、高效、稳定和可靠运行。		
		运行维护服务方法要求	1、定期对机房基础设施、设备进行日常巡检，季度巡检，掌握设备运行状态和机房环境情况；并提交季度巡检报告。		
			2、定期对机房设施进行清洁保养，如：机房清洁除尘、设备清洁除尘、设备线缆整理、标识标签完整性与准确性检查等；		
			3、进行机房核心设备适应性改进、预防性改进和增强性改进，改进内容包括但不限于系统升级、漏洞补丁加固、固件升级加固和软件版本升级优化、数据备份等，以提升网络设施的稳定性和可靠性。		
			4、进行网络适应性改进、预防性改进和增强性改进，改进内容包括但不限于综合布线系统的布局整改、路由策略调整、固件升级加固和软件版本升级优化。		
		服务响应要求	1、服务响应可通过现场、远程等方式提供，由此产生的一切费用均由供应商承担。		
			2、对于服务请求，达到100%的用户响应度：需要现场解决维修的服务，驻点时间内接报后15分钟到达维修现场响应。		

			3、接到故障报修后，立即实施维护抢修：一般故障（板块级，如外设、电源等）2 小时内排除；较大故障（设备级，如系统、整机等）4 小时内排除；短时间难以修复故障（系统级）应立即启用备用设备，保障业务不长时间中断，并在当日内提交修复方案，报采购人批准后，在修复方案要求时间内修复，及时做出故障原因报告并提出有效措施加以解决。		
		技术支持及咨询服务要求	1、咨询服务：运行维护服务提供者应为运行维护服务使用者和运行维护服务管理者提供 7×24 小时咨询服务。针对采购人提出的技术问题、方案评估作出回复，不定期组织双方进行技术交流。		
			2.技术支持服务： 运行维护服务提供者为运行维护服务使用者和运行维护服务管理者提供的技术支持服务，应包括但不限于电话支持、远程支持和现场支持。 技术支持服务的内容应包括但不限于服务请求、故障处理、设备搬迁和升级优化。 遭遇大面积故障（如病毒等）、项目新建或突发性工作任务，要能保证加派足够的人员、设备、技术力量参与协助工作。		
		2.攻防服务			
		攻防演练	强化各局委网络安全风险防范意识，年度 2 次对授权的重要业务系统进行渗透测试，采用自动化工具或人工测试方法相结合，深度挖掘业务系统存在的安全漏洞，对系统的脆弱性进行分析，验证当前的安全防护措施，找出风险点；渗透测试完成后，提供整理渗透测试服务输出成果。		
		3.应急服务			
		应急演练	落实信息系统应急演练相关工作，年度 2 次组织开展模拟黑客攻击或采取断电、断线、宕机等方式的网络安全实战演练，通过设定发生的安全事件而进行的以检验应急响应工作、评估应急响应预案为目的的演习和检验。		
		4.安全培训			
		安全培训	提升全员网络安全防范意识和网络安全知识水平，年度 2 次对全区局委提供安全意识培训，提高全员的安全意识，强化办公安全意识、安全办公规范，包括信息安全法律法规宣贯、重点安全事件案例、常见攻击手段及防范、日常信息安全防范、上网行为安全规范等内容。		

提供精密空调有效的中国节能产品认证证书扫描件或中国政府采购网节能产品查询结

果截图或全国认证认可信息公共服务平台节能产品查询结果截图。

2、实施方案

供应商提供的实施方案应包含项目部署规划、设备安装、设备调试、功能测试、基础设施维修、特征库升级安全加固 6 项内容。

3、质量保证措施

供应商提供的质量保证措施应包含质量保证目标、质量控制流程、质量检测措施、定期巡检、维护保养、质量保证体系 6 项内容。

4、供货期保证措施

供应商提供的供货期保证措施应包含项目供货进度安排、进度跟进与调整计划、信息反馈机制、供货周期、风险管理、保证措施 6 项内容。

5、供货方案

供应商提供的供货方案应包含供应计划、运输工具选择、运输方案、包装保护措施、供货流程、风险管理 6 项内容。

6、培训方案

供应商提供的培训方案应包含培训方式、培训周期、培训内容、培训计划安排、培训资源、培训进度跟踪 6 项内容。

（二）商务要求

1、供货期：接到采购人通知后 30 日历天内交货并安装调试完毕。

2、质量要求：合格，符合国家及行业标准。

3、付款方式：合同签订后预付合同金额的 30%，货物供货安装、调试完毕并验收合格后按批次支付剩余合同金额。

4、供应商资格要求见供应商须知前附表。如资格证明文件遇年检、换证，则必须提供法定年检、换证单位出具的有效证明扫描件。

5、包装和运输

（1）货物的包装和运输须符合货物特性要求；

（2）为了保证货物在长途运输和装卸过程中的安全，货物包装应符合国家或行业标准规定。由于包装不善导致缺失或损坏等，由中标人承担一切责任。

6、售后服务

（1）负责免费运输及装卸，保证所有产品完好无损和质量达标；

（2）严格执行国家有关产品“三包”(包质、包量、包退换)的规定，从产品交货之日

起，实行“三包”服务；

（3）对一次不合格的产品予以换新，承担一切与之有关的费用；

（4）供应商收到通知后在采购人规定时间内将货物配送至指定地点；

（5）供应商提供的售后服务方案应包括服务内容、服务形式、解决质量问题的响应时间、解决问题时间、后期质保服务、售后服务团队、备品备件7项内容。

7、保险：供应商负责项目交付前货物的保险，负责供应商服务人员服务现场的人身意外保险。

8、质保期：自货物验收合格使用之日起免费质保三年。

9、履约验收：采购人根据国家有关规定、招标文件、中标方的投标文件以及合同约定的内容和验收标准进行验收。验收情况作为支付货款的依据。如有异议，以相关质量技术检验检测机构的检验结果为准，如产生检验检测费用，则该费用由过失方承担。

10、采购人使用中标人中标的货物、技术、资料、服务或其他任何一部分时，享有无偿使用权。免受第三方提出的侵犯其专利权、著作权、商标权或其他知识产权的起诉。如果第三方提出侵权指控，中标人应承担由此而引起的一切法律责任和费用。