采购需求

采购项目要求:

★本次采购产品为非进口产品(进口产品指通过中国海关报关验放进入中国境内且产自关境外的产品）。

★凡属于政府强制采购节能产品，请投标人承诺在交货时提供《节能产品政府采购清单》中的产品。（注：《节能产品政府采购清单》投标人可查询中国政府采购网<http://www.ccgp.gov.cn>。）

★凡属于《中华人民共和国实施强制性产品认证的产品目录》的产品，请投标人承诺在交货时提供该产品的《中国强制认证》（CCC 认证）。

凡属优先采购节能产品，请供应商尽可能提供《节能产品政府采购清单》中的产品。（注：《节能产品政府采购清单》投标人可查询中国政府采购网<http://www.ccgp.gov.cn>。）

凡属优先采购环境标志产品，请供应商尽可能提供《环境标志产品政府采购清单》中的产品。（注：《环境标志产品政府采购清单》投标人可查询中国政府采购网<http://www.ccgp.gov.cn>。）

中标人须提供原制造商制造的全新产品，整机无污染，无侵权行为、表面无划损、无任何缺陷隐患，完全符合国家的有关质量标准，在中国境内可依常规安全合法使用。

产品为原厂商未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追索查阅。

一、项目背景

根据《广州市信息安全等级保护工作协调小组办公室关于设置政府投资信息化项目网络安全等级保护经费的通知》（穗等保办〔2018〕9号）的文件精神，从化区卫生健康局已对区域医疗卫生信息系统和区域公共卫生信息系统等2个系统开展备案、定级和测评环节，现根据评测的结果在物理安全、网络安全、主机安全以及安全管理方面需要进行安全建设和整改，以满足等保二级要求的目的，最大限度地防止或降低网络安全事件的发生。

二、采购项目

采购内容包括以下几个方面:

物理安全: 对机房内UPS不间断电源进行更换及精密空调进行新增;

网络安全: 针对重要设备进行冗余配置，增加网络和安全区域边界安全设备、日志审计、运维审计及终端安全防护;

主机安全: 对操作系统的安全策略进行配置，修复系统漏洞;

安全管理: 结合从化区卫生健康局实际情况，在机房安全管理、人员安全管理及运维管理等方面制定相应的制度，同时制定相关的设备、终端运维手册，制定应急预案及应急报告。

具体采购清单:

序号	产品名称	数量	单位
1	出口万兆防火墙	1	台
2	服务器区万兆防火墙	1	台
3	等保一体机硬件	1	台
4	等保一体机软件授权（含日志审计系统授权100个点，堡垒机授权100个点，Linux服务器终端防护授权1个	1	项

	点，WindowsServer 服务器终端防护授权 50 个点，WindowsPC 客户端终端防护授权 500 个点。		
5	UPS 不间断电源	16	节
6	机房精密空调	1	台
7	等级保护整改服务	1	项

三、设备参数要求

★为保证产品兼容性与用户日常维护方便,本次采购的防火墙及网络安全设备需为同一品牌;

3.1 出口万兆防火墙及服务器区万兆防火墙的基本要求

指标项	详细要求
基本要求	▲所投产品必须为下一代防火墙，产品采用 X86 多核及自主知识产权的多核并行安全操作系统构成；（提供相应资质证明）
	▲防火墙吞吐量：⩾16Gbps；应用层吞吐量：⩾14Gbps；并发连接数：⩾400 万；HTTP 新建连接速率：⩾14 万
	▲2U 标准机架；设备默认配置为⩾6 个 10/100/1000BASE-T 接口和 2 个 SFP 插槽，不少于 2 个端口扩展卡插槽，所有扩展卡插槽均要求位于设备前面板，并且在维护现场即可进行扩展；配置 1T 硬盘。设备配置模块化双冗余电源；
网络接入	▲支持路由、交换、虚拟线、Listening、混合工作模式；（提供截图证明）
	▲支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；（提供截图证明）

	▲支持链路聚合，可根据源/目的 mac、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 10 种链路负载算法;（提供截图证明）
	▲支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供截图证明）;
	支持 SIP 协议的媒体业务接入，实现内外网媒体系统之间上联和下联安全防护，符合 GB/T 28181-2016《安全防范视频监控联网系统信息传输、交换、控制技术要求》及 TC/OP(XZ)2B-185-2017 相关技术要求，提供权威测试报告证明;
安全控制	支持一体化安全策略配置，通过一条策略实现五元组、源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、WAF、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置，简化用户管理;
	提供策略命中、冗余、冲突、包含检查及策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询;（提供截图证明）
	▲内置 P2P 应用、加密应用、数据库应用、工控物联网协议等应用特征库; 支持应用特征库在线或本地更新，支持自定义应用特征;（提供截图证明）
	▲支持超过 80 类、1000 万的 URL 地址分类库，可针对网站类别实施管控，杜绝非法、违规网站的访问行为;（提供截图证明）

	内置文件过滤引擎，支持 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤。
	内置内容过滤功能，可对 FTP 上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤;
	支持将五元组、源 MAC、地址范围、应用、用户等加入静态黑名单，可与 URL 过滤、病毒过滤、防代理功能进行联动实现动态黑名单封锁，支持静态和动态黑名单命中统计和监控;
	▲内置防代理功能，阻断网络用户通过代理主机进行攻击、共享上网等行为; （提供截图证明）
	▲支持连接控制和监控，可对源/目的地理对象、应用制定连接限制策略，可展示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息; （提供截图证明）
安全防护	▲支持独立的入侵防护规则特征库，规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，特征总数在 5000 条以上; （提供截图）能对常见漏洞进行安全防护，兼容国家信息安全漏洞库（提供资质证明）;
	▲入侵防护动作包括告警、阻断、记录攻击报文，支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义，可对自定义规则导入导出; （提供截图证明）
	▲厂商需具备强大的漏洞和攻防研究能力，为 CNNVD 一级支撑单位（提供官网证明材料），能够确保每周至少更新 1 次攻击特征库;

	▲支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；支持至少 2 种专业反病毒厂商的病毒特征库，病毒特征库规模超过 400 万；（提供截图证明）
	▲支持独立的 WAF 防护模块，WAF 防护特征总数在 1000 条以上，支持针对地址、应用设置 WAF 白名单，支持攻击规则搜索以及自定义；（提供截图证明）
	▲支持行为分析，及时发现异常行为并告警，同时能够与 APT 进行联动，实现协同防御；（提供截图证明）
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；
	支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；支持 UDP 关联认证，对源地址进行合法性认证；
	支持 DNS FLOOD 防护，能对 DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒、DNS 格式等攻击提供 DNS REPLY 源认证、源限速、目的限速、域名限速等综合防护手段；
	▲支持 NTP 流量检测清洗，能对 NTP REQUEST FLOOD、NTP REPLY FLOOD 等攻击进行检测并提供基于 NTP 请求限速、NTP 响应限速、源认证、会话认证的防御策略；（提供截图证明）
安全接入	支持 IPSec VPN 功能，支持 AES、DES、3DES、MD5、SHA-1 等 VPN 加密、认证算法，支持对隧道内网络流量进行监控展示；
	支持 SSL VPN 功能，满足远程用户安全接入内网，支持 windows、Android、iOS 等远程客户端接入；
系统管理	支持多个配置文件并存，配置文件备份能力不少于 4 个；配置文

	件支持选择部分配置和全部配置导入导出;
	▲支持主、备双系统以及多个系统版本文件并存，系统版本数量不少于 5 个（提供截图证明）;
数据中心	支持独立审计策略，可对 URL 地址、网页标题、网页内容、邮件行为、邮件内容、FTP 上传/下载行为及文件内容进行审计;
	▲提供完善的审计数据查询功能，可对用户访问网站、邮件收发、论坛微博、FTP、TELNET 等上网行为以及用户上网流量时长等内容进行查询; （提供截图证明）
	支持日志本地存储，可对不同类型日志设置存储空间，（提供截图）支持日志外发至多个服务器，可设置日志传输协议、时间类型、日志语言、是否合并及加密传输等参数;
显示监控	支持对设备 CPU、内存、磁盘、整机流量、新建、并发进行统计，展示设备 CPU、内存、硬盘实时利用率及其历史走势图;
	▲支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数; （提供截图证明）
资质要求	提供计算机信息系统安全专用产品销售许可证;
	提供防火墙密码检测证书;

3.2 等保一体机及软件授权要求

指标项	详细要求
硬件要求	等保一体机硬件平台，Intel 处理器*2 颗，8 核心支持超线程，内存≥96G，256G*1 SSD 系统盘，2T*2 数据盘，支持 raid 0; 接口≥6 个千兆电口和 4 个万兆光口

系统架构	软硬件解耦，底层硬件使用 x86 架构服务器；底层 x86 服务器数量支持线性增加；支持集群部署模式；
页面定制	支持修改云安全管理平台的系统名称、单位名称以及页面 logo 等信息。
安装部署	▲支持在资源池管理平台通过初始化方式自动部署云安全管理平台和终端威胁防御系统；（提供截图证明）
	支持安全实例热迁移功能，服务器故障后安全实例可以自动迁移到正常运行的服务器上；
	云安全管理平台和安全网元部署标准 X86 服务器下，与硬件设备的解耦，无需专用硬件设备。安全网元的容量可以随着 X86 服务器数量的扩容而横向扩容。
云安全能力	▲支持提供虚拟化防火墙、虚拟化堡垒机、虚拟化日志审计、虚拟化数据库审计、虚拟化网络审计、虚拟化基线管理、虚拟化 Web 应用防火墙、虚拟化负载均衡、虚拟化终端威胁防御（EDR）、虚拟化 VPN、虚拟化漏扫安全产品的能力；（提供截图证明）
	▲等保一体机内所有虚拟化安全产品皆为云安全管理平台安全厂商自研；（提供官网产品截图）
资源配置	按需选择网元规格、区域、时长等开通安全网元，支持在线申请安全网元；
	根据实际业务场景自主选择功能。平台可提供场景化服务，基础安全、安全运维、网站安全及等级保护等场景服务。
	支持可以通过控制台单点登录到安全网元管理页面，无需再次输入账号密码。

	支持在云安全管理平台控制台页面显示SAAS化EDR模块授权信息、可视化方式显示EDR服务Agent总数、agent在线数、agent离线数等相关信息。
	▲支持纳管无代理分布式防火墙。（提供截图证明）
业务编排	▲支持为不同区域配置云安全管理平台底层平台，实现多区域部署，可通过为不同的区域配置不同的安全组件（提供截图证明）
	服务编排支持以可视化的方式方便用户规划创建自己的业务网络，可以通过拖拽的方式直观的管理自己的计算网络资源。可基于资产信息定义IP五元组流量信息，并可定义流量路径，并关联流量定义实现流量编排。
用户管理	▲默认支持平台管理员、租户管理员、普通用户三种角色支持自定义用户权限对功能模块进行控制，并且可设置功能权限只读或者读写。（提供截图证明）
	支持创建、删除、修改、查询租户、租户账号。
	支持管理员在创建用户时生成初始密码，并可重置用户密码。
运维管理	支持显示平台资源信息，如宿主机运行状态、CPU利用率、内存利用率、磁盘利用率;
	支持显示申请的实例状态、实时流速、网络总流量、CPU温度等信息，并用可视化图表的方式展示CPU、内存、磁盘占用趋势，网络总流入流出速率趋势;
	支持显示安全实例运行状态，可查看安全实例详细信息，如（cpu/内存/磁盘信息、历史流量/流量趋势信息、网络接口状态等）;

	▲支持安全实例态势大屏展示，以可视化的形式显示安全实例列表、安全实例告警状态、安全实例资源信息以及安全实例资源分布（提供截图证明）
	支持运维监控态势大屏展示，以可视化的形式显示系统服务状态、物理主机资源信息、IP 使用率信息、平台告警信息;
	支持安全态势大屏展示、以可视化的形式显示攻击类型排名、攻击源 Top5、被攻击主机 Top5、安全事件趋势、安全事件排行、威胁终端排行等信息。
	支持实时监测日志中包含的关键事件信息和日志产生的频率，从频繁发生的事件日志中发现潜在的危害事件，并产生潜在危害告警日志。可根据不同的事件场景灵活配置监测的事件相关信息、监测时间窗口、监测阀值和告警日志内容。
	▲支持新建、编辑、复制、删除、启用和停用告警策略；告警日志支持按时间和告警类型等维度筛选；告警类型至少包括：网络攻击告警、WEB 攻击告警、DDoS 攻击告警、防病毒告警、未知威胁事件告警等；支持自定义告警规则；支持查看告警策略详情，详情至少包括：策略名称、过滤规则、报警级别、规则分组、报警内容等。（提供截图证明）
系统管理	支持单个 license 可实现云安全管理平台授权和安全网元授权导入；支持许可自动化导入激活安全产品，实现安全产品自动化激活，包括云防火墙、云 WAF、云堡垒、云日志审计、云数据库审计、云网络审计、云负载、云基线等等所有安全产品许可的自动化导入激活。

	云安全管理平台相关运行日志，包括服务状态、调试日志等
	所有用户登录到云安全管理平台以后执行的存在风险的操作，如安全实例关机、重启、删除，用户删除，租户删除，开通新服务等
	支持系统运行诊断分析，诊断系统各平台的服务状态；支持网络抓包诊断分析，可设置区域、物理主机、物理网口、租户、IP、端口等条件进行抓包分析。
	支持查看磁盘使用情况显示磁盘节点信息、磁盘使用情况以及操作日志、告警日志、审计数据所占磁盘空间大小；支持以磁盘利用率、数据类型、时间等条件设置磁盘清理规则，定期清理磁盘空间。
	▲支持级联管理功能，一个主管理平台可以管理多个分支管理平台，并且主管理平台能够显示下级管理平台的 IP 地址、地理位置、在线状态、上线时间等信息（提供截图证明）
	支持修改云安全管理平台的系统名称、单位名称以及页面 logo 等信息。
	支持通过云安全管理平台下载安全网元技术白皮书和用户手册等相关附件信息。
	支持双因素认证功能
底层平台功能	虚拟机提供跨地域的计算、网络、存储资源配额管理功能，提供资源的使用情况。
	物理机管理提供计算、存储、网络物理资源池的管理，支持主机集群功能；线性扩容主机数量；

	支持分布式存储集群以保证存储的可靠性，支持存储节点线性扩容。
	▲支持在资源池管理平台通过初始化方式自动部署云安全管理平台和终端威胁防御系统；（提供截图证明）
	支持通过恢复出厂设置一键恢复到出厂状态进行重新配置。
	▲支持查看等保一体机服务器内部网络拓扑图并且支持拓扑图自动调整；支持以集群模式方式查看跨服务器之间网络连接信息。（提供截图证明）
	支持自定义安全镜像的标签，包括不限于 cpu 规格、内存规格、磁盘规格等；支持自定义网络虚拟机标签，配置安全组件网口需要连接到哪个网络中，应对负责网络环境。
	支持在系统页面上创建多个虚拟的软件交换机。
云运维审计	支持 H5 运维，所有运维操作通过 web 页面进行，不需要调用第三方运维工具。
	支持自动化运维，可按每日、每周、每月或者定期自动执行。
	支持自动化运维脚本自定义。
	▲支持 RDP、VNC 图形操作过程中键盘输入操作记录、剪贴板和鼠标点击行为记录。（提供截图证明）
	支持超级管理员、系统管理员、保密管理员、密码管理员、安全审计员、保密员、运维管理员、操作员角色。
	支持本地认证和三方认证服务器接入认证，包括 AD、LDAP、Radius 服务器。
	支持密码认证、证书认证、USBKEY 认证等双因素认证方式。

	▲支持运维命令审批、阻断。（提供截图证明）
	▲支持定期改密，密码采用信封加密后自动外发至指定邮箱或者 FTP 服务器。（提供截图证明）
云日志审计	支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于 10s;
	数据存储能力：压缩加密存储，压缩比不低于 10:1；日志存储不低于 10000 条/M;
	支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出;
	▲支持独立展示每个被采集源最近 24 小时的日志数量趋势,便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态;（提供截图证明）
	▲支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集;（提供截图证明）
	▲支持对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击;（提供截图证明）
	▲支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数;（提供截图证明）
	支持首页以全国地图、全球地图展示最近 24 小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息;

	支持为不同类型日志设置不同的查询条件和显示条件;
	支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息;
	▲支持在日志查询结果上针对源 IP、目的 IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源 IP 和目的 IP(公网地址)还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果; （提供截图证明）
	▲支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析; （提供截图证明）
	支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备 IP、源 IP、目的 IP 等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出;
	▲支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息; （提供截图证明）
	支持基于拓扑图的日志源相关数据信息快速查看; 支持通过拓扑下钻查看对应日志源的日志、报表、告警数据。
云 EDR	▲ 客户端安装后至多占用 50M 硬盘资源，病毒库 3M 大小，日常内存占用不到 30M，有效节省 PC/Server 资源; （提供截图证明）;
	管理中心支持实时显示客户端的状态及终端基本信息，包括客户端连接状态、服务状态; 终端机器名称、客户端版本、病毒库版本、IP 地址、MAC 地址、操作系统版本、危险及功能漏洞、

	主板信息、显卡信息、内存大小、当前版本信息和物理位置等信息，并支持终端信息导出。
	产品具备漏洞集中修复，强制修复；可以展示全网补丁情况，分为高危补丁、功能更新等，并展示已打补丁和未打补丁的信息。
	▲ 支持对 webshell 后门进行扫描检测 ，webshell 后门库数量大于 100000。（提供截图证明）；
	当文件被执行、修改、访问时，反病毒引擎对相应文件进行扫描，如扫描到威胁则阻断用户对该恶意威胁的触碰并根据需要进行隔离操作。
	设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。
	▲对系统关键位置进行防护，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度阻止无文本攻击、流氓、广告程序对系统的恶意篡改等行为。对系统进行防护。（提供截图证明）；
	支持终端对外攻击检测，根据自定义 SYN、UDP、ICMP 数据包的检测阈值，自动阻止并记录攻击行为。
	通过协议（TCP、UDP、ICMP、IGMP、GGP、PUP、IDP、ND、ESP、AH、RDP、GRE、SKIP、RAW），端口号，IP 地址、业务流量进出口方向等控制规则对终端进行防护,从网络层保护终端安全。
	▲ 支持文档防泄漏功能，针对终端存储的 word、pdf、ppt、Excel、rtf、txt 等文档的名称、内容进行包含关键字检查，对含有指定关键字的文档进行禁止发送、禁止拷贝等管控，消

	息提醒的同时将文档违规信息上报管理平台。(提供截图证明);
	▲支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读-运行）和启用读写、启用（读写-运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外USB设备。（提供截图证明）;
	▲对流氓软件、弹窗广告能够实现智能拦截，同时也可以自定义添加截图拦截弹出，避免了各类骚扰弹窗。(提供截图证明);
资质要求	云安全管理平台需具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》
	云安全管理平台需具备《云计算产品信息安全认证证书》
	▲云安全管理平台需具备《IPv6 Ready logo》

3.3 UPS不间断电源

指标名称	主要参数
性能要求	1.▲电压/V≥12; 2.▲容量/Ah≥100; 3.▲W/cell≥320; 4.内阻mΩ≤4; 5.重量(Kg)≤30; 6.工作温度范围：-20℃－55℃; 7.材质要求：采用符合UL 94-V0 的阻燃材质电池壳体; 8.采用专业的板栅制造工艺，电池设计浮充寿命长达10年以上; 9.在产品设计上更加侧重与UPS的兼容匹配及系统成本优化，实现与UPS 的高度结合;

	10.采用统一的嵌入式端子设计，电池过大电流性能好，安装维护简单方便;

3.4 机房精密空调

指标名称	主要参数
性能要求	1.▲总冷量≥12.5kw,送风方式：上送风; 2.▲风量≥3100（m3/h）; 3.▲加湿量≥1.5（kg/h）; 4.▲加热量≥4（kw）; 5.机房专用空调机组的电气性能应符合 IEC 标准; 6.材质要求：空调设备外壳应采用全金属防腐材质，室内风机应采用全金属防腐材质; 7.机房专用空调应能按要求自动调节室内温度，具有制冷、加热、除湿等功能; 8.机房专用空调系统应具有高可靠性，应选用高可靠性的谷轮（Copeland）品牌涡旋压缩机、高可靠性机械热力膨胀阀、全金属室内风机等高可靠性部件，满足全年 365 天，每天 24 小时不间断运行; 9.▲每台机房专用空调应具备一个主回风口和两个侧面辅助回风口，有利于提高机组性能。空调应具备来电自启动功能，满足机房无人值守的要求。 10.▲应采用远红外加湿器，加湿器可以重复利用及长期使用; 11.▲机房专用空调应具备高全年能效比，在室内回风条件 24℃，50%湿度条件下全年能效比>3.75; 12.应具有先进的微处理控制器，可存储 200 条历史告警信息;

	13.机房专用空调机组的风冷型室外冷凝器应采用无级全调速装置，保证系统冷凝压力的稳定并降低噪声; 14.机房专用空调机组的风冷冷凝器的电控部分应有良好的防水性能 15.室内空调机组需要全正面维护，可以靠墙安装。
产品证书要求	▲CQC 节能认证证书; ▲节能测试报告 ▲3C 认证报告 ▲抗震测试报告 ▲CRAA 认证证书。

四、等级保护整改服务

以下是差距测评 65 个高风险，具体整改服务以现场实际为准。

序号	安全层面	安全控制点	测评项	符合情况	测评对象	整改措施
1	安全物理环境	湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	部分符合	机房	精密空调
2	安全物理环境	电力供应	应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	部分符合	机房	UPS
3	安全物理环境	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	不符合	机房	机房整改
4	安全通信网络	网络架构	应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	部分符合	安全通信网络	防火墙
5	安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	部分符合	安全区域边界	防火墙
6	安全区域边界	访问控制	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。	部分符合	安全区域边界	防火墙
7	安全区域边界	恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	不符合	安全区域边界	防火墙

8	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	tomcat	安全服务
9	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	区域公共卫生信息系统	安全服务
10	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	数据库服务器	安全服务
11	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	应用服务器,管理机 1	安全服务
12	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	数据库	安全服务
13	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	接入交换机	安全服务
14	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	H3C M9000-A 防火墙模块,H3C M9000-B 防火墙模块	安全服务
15	安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	部分符合	H3C M9000-A,H3C M9000-B	安全服务
16	安全计算环境	身份鉴别	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	不符合	tomcat	安全服务
17	安全计算环境	身份鉴别	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	不符合	应用服务器,管理机 1	安全服务
18	安全计算环境	身份鉴别	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	不符合	数据库服务器	安全服务
19	安全计算环境	身份鉴别	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	部分符合	数据库	安全服务
20	安全计算环境	身份鉴别	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	不符合	接入交换机,H3C M9000-A,H3C M9000-B	安全服务
21	安全计算环境	身份鉴别	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	不符合	H3C M9000-A 防火墙模块,H3C M9000-B 防火墙模块	安全服务

22	安全计算环境	身份鉴别	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	不符合	tomcat	堡垒机
23	安全计算环境	身份鉴别	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	不符合	应用服务器,管理机 1	堡垒机
24	安全计算环境	身份鉴别	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	不符合	数据库	堡垒机
25	安全计算环境	身份鉴别	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	不符合	H3C M9000-A 防火墙模块,H3C M9000-B 防火墙模块	堡垒机
26	安全计算环境	身份鉴别	当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	不符合	接入交换机,H3C M9000-A,H3C M9000-B	堡垒机
27	安全计算环境	访问控制	应重命名或删除默认账户，修改默认账户的默认口令。	不符合	tomcat	安全服务
28	安全计算环境	入侵防范	应关闭不需要的系统服务、默认共享和高危端口。	不符合	应用服务器,管理机 1	安全服务
29	安全计算环境	入侵防范	应关闭不需要的系统服务、默认共享和高危端口。	不符合	接入交换机,H3C M9000-A,H3C M9000-B	安全服务
30	安全计算环境	入侵防范	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	不符合	应用服务器,管理机 1	入侵防御
31	安全计算环境	入侵防范	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	不符合	数据库服务器	入侵防御
32	安全计算环境	入侵防范	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	不符合	数据库	入侵防御
33	安全计算环境	入侵防范	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	不符合	H3C M9000-A 防火墙模块,接入交换机,H3C M9000-B 防火墙模块,H3C M9000-A,H3C M9000-B	入侵防御
34	安全计算环境	入侵防范	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	不符合	区域公共卫生信息系统	入侵防御
35	安全计算环境	入侵防范	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	不符合	区域公共卫生信息系统	入侵防御

36	安全计算环境	入侵防范	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	不符合	数据库服务器	入侵防御
37	安全计算环境	入侵防范	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	不符合	应用服务器,管理机 1	入侵防御
38	安全计算环境	入侵防范	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	不符合	数据库	入侵防御
39	安全计算环境	入侵防范	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	不符合	H3C M9000-A 防火墙模块,接入交换机,H3C M9000-B 防火墙模块,H3C M9000-A,H3C M9000-B	入侵防御
40	安全计算环境	安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	不符合	tomcat	日志审计
41	安全计算环境	安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	部分符合	区域公共卫生信息系统	日志审计
42	安全计算环境	安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	不符合	应用服务器,管理机 1	日志审计
43	安全计算环境	安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	不符合	数据库	数据库审计
44	安全计算环境	安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	部分符合	H3C M9000-A 防火墙模块,接入交换机,H3C M9000-B 防火墙模块,H3C M9000-A,H3C M9000-B	日志审计
45	安全计算环境	安全审计	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	不符合	tomcat	日志审计
46	安全计算环境	安全审计	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	不符合	应用服务器,管理机 1	日志审计
47	安全计算环境	安全审计	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	不符合	数据库	数据库审计
48	安全计算环境	剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	不符合	数据安全	

49	安全计算环境	个人信息保护	应仅采集和保存业务必需的用户个人信息。	不符合	数据安全	
50	安全计算环境	个人信息保护	应禁止未授权访问和非法使用用户个人信息。	不符合	数据安全	
51	安全建设管理	安全方案设计	应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。	不符合	安全建设管理	安全服务
52	安全建设管理	安全方案设计	应根据保护对象的安全保护等级进行安全方案设计。	不符合	安全建设管理	安全服务
53	安全建设管理	安全方案设计	应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	不符合	安全建设管理	安全服务
54	安全建设管理	工程实施	应制定安全工程实施方案控制工程实施过程。	不符合	安全建设管理	安全服务
55	安全建设管理	测试验收	应制订测试验收方案，并依据测试验收方案实施测试验收,形成测试验收报告。	不符合	安全建设管理	安全服务
56	安全建设管理	测试验收	应进行上线前的安全性测试，并出具安全测试报告。	不符合	安全建设管理	安全服务
57	安全建设管理	系统交付	应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。	不符合	安全建设管理	安全服务
58	安全建设管理	系统交付	应对负责运行维护的技术人员进行相应的技能培训。	不符合	安全建设管理	安全服务
59	安全建设管理	系统交付	应提供建设过程文档和运行维护文档。	不符合	安全建设管理	安全服务
60	安全建设管理	外包软件开发	应在软件交付前检测其中可能存在的恶意代码。	不符合	安全建设管理	安全服务
61	安全建设管理	外包软件开发	应保证开发单位提供软件设计文档和使用指南。	不符合	安全建设管理	安全服务
62	安全运维管理	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	不符合	安全运维管理	漏洞扫描
63	安全运维管理	恶意代码防范管理	应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。	不符合	安全运维管理	安全服务
64	安全运维管理	备份与恢复管理	应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	不符合	安全运维管理	安全服务

65	安全运维管理	应急预案管理	应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。	不符合	安全运维管理	安全服务

五、技术服务要求

技术服务内容具体要求如下：（中标供应商必须承诺达到以下服务标准）

在保修期内提供以下支持：为确保信息化设备安全、可靠地运行，本次项目需要在质保期内对设备每季度巡检一次生成巡检报告及调优评估分析报告。

（一）热线电话支持

提供 7*24 小时的电话热线支持服务，其中：

1.工作日 9:00-18:00 提供电话直线支持服务；

2.其它时间段则由专人通过指定的移动电话提供支持服务；

（二）远程故障排除

对于电话、传真或 E－MAIL 中无法讨论解决的复杂问题，技术工程师将利用远程测试手段，对故障进行远程诊断，进行远程故障排除或向客户方提供详尽解决方案，可要求客户方提供远程接入的线路保障，在需要进行故障处理时，提供远程接入需要的相关信息，为客户远程提供故障处理；

（三）重大故障的现场支持

当医疗单位开展业务系统时，无法使用或大面积不能正常使用，而且在远程调试也无法解决的情况下，中标供应商需要派遣技术服务人员 2 小时到使用现场提供现场服务，通过现场服务修正错误或故障，并将系统恢复至最佳状态；

六、项目管理要求

（一）项目实施时间要求

★供应商需承诺，在合同签定后 3 个月内完成全部设备和软件部署，通过二级等保评测并测试上线，必要时可申请信息系统服务商配合。

（二）系统安装调测要求

1、系统的软、硬件安装和调试由供应商负责。供应商在安装调试前应提出完整的计划并经用户方确认，包括设备安装的内容、项目、指标、方法和进度，并提供相应的仪器和工具。

2、供应商根据应答标书提供的系统方案，承担完成系统建设、网络连接及所有要求的功能，不存在电缆、网卡或其它附件的短缺，不存在服务设备和软件性能不满足业务需求和系统功能的情况，否则供应商须在两周内免费补齐所缺设备和软件，避免因此造成系统延期开通而引起市民投诉及信访。

（三）系统上线要求

1、系统安装调试并通过二级等保验收后，需经用户方确认后方可进入正式运行期。

2、系统上线测试内容与本技术条款应相一致；供应商应提供测试条件、方法和过程的方案。

3、验收测试合格后，双方签署验收协议，作为上线验收依据；系统入网上线运行。供应商有义务配合用户方完成相关业务的交接工作。

（四）技术文档要求

1、供应商应提供软硬件的配置清单；

2、用户方为供应商提供的所有业务技术资料、文档，供应商有责任对第三方保密；

3、供应商应提供详细的服务计划和服务日志。

4、供应商提供的书面技术资料应能满足确保系统正常运行所需的管理、运营及维护有关的全套文件。同时还包括用户方认为必要的其他技术文件。文件要求用中文书写。

5、供应商应提供书面技术资料详细清单，所有文件均应有简洁明了的名称和编号。各种文件的文字说明应通俗易懂，所有图纸的图幅及图形符号等均应规范化。

6、供应商应根据用户方的业务需求及相关的技术文件要求，提出完整的项目管理、系统设计、项目施工、项目验收、技术支持方案以及供应商人力资源供给方案。供应商负责提交项目实施日报或周报。

（五）技术培训要求

供应商在系统正式上线后，须为用户方参与系统维护相关技术人员进行系统操作和维护等方面的技术培训。

（六）售后服务及培训要求

1、质保期要求：采购的设备需提供 3 年的保修服务。

2、售后服务要求

（1）所有保修服务方式均为中标人上门保修，即由中标人派员到采购人使用现场维护。由此产生的一切费用均由中标人承担。

（2）在项目验收后的免费服务期内，如因需要增加系统功能而产生的费用，双方另议;

（3）项目免费服务期满后，供应商必须承诺在法定工作时间内，可以提供免费的技术指导和咨询，如需其他技术支持服务，则费用由双方另议。

3、培训要求

对组织机构系统管理员及相关人员进行专业的产品操作培训，杜绝由人员误操作导致的系统故障及数据丢失，帮助区卫健局 IT 管理人员了解并掌握产品使用方法，保证产品的价值最大化实现。

（一）应根据合同清单提供详细的产品说明书，系统使用说明书和系统维护说明书。

（二）对区卫健局的人员分为运行维护人员的培训、工程技术人员的培训和管理人员的培训。

（三）运行维护技术人员经过培训应能进行日常设备运行维护工作，掌握

软件、硬件的操作，熟悉硬件基本功能。能熟练地分析软件、硬件信息等工作，并能有效的组织、开展业务应用能力。

（四）保障高级工程技术人员培训后，能够处理一般维护人员不能处理的技术问题。

（五）管理人员经培训后，应能负责全面的技术管理工作，了解系统建设的过程，系统功能及未来建设的规划。

（六）进行全员信息安全意识的培训。

（七）当系统升级或者改造时，应进行免费系统升级及改造专门培训，具体时间由双方协调培训时间。

（八）培训费用计入总价。

七、付款方式

（一）合同签订后，按照供应商提供的完整资料，十五个工作日内，支付总价的 30%的货款。

（二）硬件设备到货，安装调试完毕，十五个工作日内，支付总价的 65%的货款。

（三）调试完成，各医疗机构现有信息系统使用稳定，通过信息系统二级等保整改项目，支付合同总价的 5%的货款。

八、评审标准

本次采用综合评分法，综合评分=技术评分+商务评分+价格评分+综合信用评价得分，投标人的最终得分为所有评标小组成员有效的综合评分的算术平均数，且所有分值计算保留小数点后二位，小数点后三位四舍五入，评分比重构成如下:

评分项目	技术评分	商务评分	价格评分	综合信用评价得分
分值	47 分	28 分	20 分	5 分

（一）技术及参数评分：47 分

分值（47）	评审内容	评分细则
5	整体网络安全等级保护方案响应情况：整体技术方案完整、规范	根据响应情况进行比较，对比最优得 5 分；对比次之得 3 分；对比一般得 1 分；对比差得 0 分。
10.5	出口万兆防火墙及服务器区万兆防火墙响应情况	完全满足采购需求得满分，共 21 项为▲号，每一项▲号指标不满足扣 0.5 分，扣完为止（要求提供证明材料而没有提供的视为不满足）。
14	等保一体机及软件授权响应情况	完全满足采购需求得满分，共 28 项为▲，每一项▲号指标不满足扣 0.5 分，扣完为止（要求提供证明材料而没有提供的视为不满足）。
1.5	UPS 不间断电源响应情况	完全满足采购需求得满分，共 3 项为▲，每一项▲号指标不满足扣 0.5 分，扣完为止
6	机房精密空调响应情况	完全满足采购需求得满分，共 12 项为▲，每一项▲号指标不满足扣 0.5 分，扣完为止
7	等级保护整改服务	整改服务方案根据整改措施进行比较，对比最优得 7 分；对比次之得 5 分；对比一般得 3 分；对比差得 0 分。
3	售后服务和技术培训方案	对比采购需求，优：得 3 分；良：得 2 分；中：得 1 分；差：得 0 分。

（二）商务评分：28 分

分值（28）	评审内容	评分细则
6	安全设备产品具有追溯性且保证质量	1.投标人所投安全产品原厂商具有网络安全应急服务支撑单位资质，提供证书复印件并加盖公章，得 2 分；有一款产品不满足，该项不得分。 2.投标人所投安全产品原厂商具有信息化建设及服务能力评价证书，提供证书复印件并加盖公章，得 2 分；有一款产品不满足，该项不得分。 3.投标人所投安全产品原厂商具有 TL9000 电信质量体系认证，提供证书复印件并加盖公章，得 2 分；有一款产品不满足，该项不得分。
4	投标人提供 2019 年以来完成的同类型项目经验相关合同，提供合同要点扫描件。（分公司投标的，总公司业绩可纳入评审）	每个得 1 分，最高 4 分。
2	财务报告权威性	财务报告能提供有审计资质的第三方出具的 2019、2020 年度《审计报告》：同时提供得 2 分，提供一个得 1 分，无得 0 分
10	本项目组成员技术实力	具有以下专业资格证书：网络工程师中级或以上职称证书、信息系统项目管理师证书、H3C 认证

		高级工程师、集成开发工程师、爱数技术认证工程师，每个得 2 分，最高 10 分，每缺少一个扣 2 分，扣完为止。提供证书扫描件及提供资质证明材料及在本项目投标截止日之前在本单位任职至少三个月的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等的扫描件）
3	安全设备服务能力	可以同时提供产品生产厂家项目授权函及服务承诺函得 3 分，提供一个得 1.5 分，无得 0 分
3	团队服务能力	供应商直接跟踪服务，服务便捷，承诺 2 小时内能到达现场，得 3 分；2-4 小时内能到达现场得 2 分；超过 4 小时到达现场得 1 分。

（三）价格评分：20 分

在性能技术参数相当的前提下，按以下情况打分，如功能或配置缺少，在评标过程中，其价格将加上其他投标商相应分项价格的最高价格；如若中标，该缺漏项费用将由中标商自行承担。

取最低价为评标基准价，其价格分为满分 20 分，其他投标人的价格分统一按照下列公式计算： 价格评分=（评标基准价／评标价）×20 分

（四）综合信用评价得分（属于商务评分的一部分）：5 分

综合信用评价得分=供应商未被列入“信用中国”网站中“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”的记录名单；不处于“中国政府采购网”中“政府采购严重违法失信行为信息记录”的禁止参加政府采购活动期间(请供应商提供采购前一个月信用信息查询记录截图并加盖公章）。

以上各项得分按四舍五入原则精确到小数点后两位。将综合评分由高到低

顺序排列。综合评分相同的，按评标价由低到高顺序排列；综合评分相同，且评标价相同的，按技术评分由高到低顺序排列。综合评分相同，且评标价和技术评分均相同的，名次由评标工作人员抽签决定。

九、投标文件制作要求

投标文件不应有涂改、增删和字迹潦草之处，无论投标人是否中标，其投标文件恕不退还，投标文件组成:

（一）封面

（二）投标函（详见格式一）

（三）报价一览表（详见格式二）

（四）技术规格条款偏离表（详见格式三）

（五）资格证明文件: 法定代表人授权书（详见格式四）及有效营业执照副本、税务登记证、组织机构代码证（复印件盖公章）

（六）投标供应商 2019 年至今同类项目业绩一览表（详见格式五）

（七）项目实施人员汇总表（详见格式六）

（八）等级保护整改服务

（九）售后服务和技术培训方案

封面

项 目 名 称： XXX

投
标
文
件

供应商全称（公章）:

地　　址:

时　　间:

投标函（格式一）

致：（）：

（投标人名称）系中华人民共和国合法企业，经营地址_____。

（XXX）是（供应商全称）的法定代表人，我方愿意参加贵方组织的（XXX项目）的投标，为此，我方就本次投标有关事项郑重声明如下：

1、投标方已详细审查全部招标文件，同意招标文件的各项要求。

2、我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3、若中标，我方将按招标文件规定履行责任和义务。

4、我方不是采购人的附属机构。

5、投标书自开标日起有效期为 45 天。

6、以上事项如有虚假或隐瞒，我方愿意承担一切后果。

法定代表人签名（或签名章）：_____ 日 期：_____

供应商全称（公章）：_____

报价一览表（格式二）

供应商全称（公章）：_____

项目名称	品牌	规格型号	数量	单价（元）	投标总价（元）
合计金额大写:			小写: ￥_____		
备注	1、此表报价单可按项目实际的需求规范合理列报。 2、项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、税费及其他一切费用。				

法定代表人签名（授权代表签名）：_____

日　期：_____

技术规格条款偏离表（格式三）

供应商全称（公章）：_____

招标文件要求	投标文件响应	偏离情况（出口万兆防火墙及服务器区万兆防火墙响应情况）	偏离情况（等保一体机及软件授权响应情况）	偏离情况（UPS 不间断电源响应情况）	偏离情况（机房精密空调响应情况）	备注

注：投标人应根据投标设备的性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”，并在“备注”栏列明满足 XX 个▲号指标。

法定代表人签名（授权代表签名）：_____

日　期：_____

法定代表人授权书（格式四）

:

XXX 是（供应商全称）的法定代表人，现委托本单位在职职工 XXX 为授权代表，以我方的名义参加 XXX 项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件，我方对授权代表的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效，授权代表签署的所有文件不因授权的撤销而失效。

授权代表无权转让委托权，特此委托。

授权代表签名：_____ 职务：_____

授权代表身份证号码：_____

法定代表人签名（或签名章）：_____ 职务：_____

供应商全称（公章）：_____ 日 期：_____

附法定代表人身份证复印件并加盖公章、授权代表身份证复印件并加盖公章

项目业绩一览表 （格式五）

供应商全称（公章）：_____

采购单位名称	设备或项目名称	合同金额（万元）	合同签订时间

注：须附投标人同类项目合同复印件

法定代表人或授权代表签名：_____

日　期：_____

项目实施人员汇总表（格式六）

供应商全称（公章）：_____

姓名	项目中担任角色	专业技术资格	参加本单位工作时间

注：须附工程师认证证书或毕业证复印件

法定代表人或授权代表签名：_____

日　期：_____