**重庆应用技术职业学院**

**信息安全实训室建设项目**

**竞争性谈判文件**

**重庆应用技术职业学院制**

2025年4月29日

**第一部分 谈判项目书**

**项目名称及编号：**2025-X005

**信息安全实训室建设**

**二、资格要求：**

1. 须具有独立法人资格，具有独立承担民事责任的能力，具备合法有效的营业执照并通过年审。注册资金100万元以上。经营范围包含信息系统集成服务、人工智能应用软件开发、智能控制系统集成、计算机软硬件、教学专用仪器销售、网络技术服务、网络与信息安全软件开发、计算机信息系统安全专用产品销售。

2.在重庆地区拥有固定的经营场所或售后服务常驻机构。

3.具有良好的商业信誉、健全的财务会计制度和完善的售后服务体系。

4.确保能够提供符合要求的合格产品，有稳定、强有力的技术维护队伍，能够提供及时、良好的售后服务。

5. 近三年内无行政处罚及重大违法违规记录。

**三、产品质量及服务要求：**

1.所有产品必须符合国家相关法律法规要求。

2.保质期内发生的质量问题由供货商免费负责解决。

3.供应商须在竞谈书中单独提供一份切实可行的售后服务承诺书。

4.竞谈文件要注明工期及质保时间，售后服务响应时间。

5.竞谈文件一式肆份，壹正叁副。

**四、设备名称、数量及参数要求：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **单位** | **数量** | **参数要求** |
| 1 | 管理节点 | 台 | 1 | 一、功能要求  为所有用户访问平台的统一接口，负责设备监控和调度使用，提供实验拓扑的虚拟子网路由交换功能，对学生实验流程的监控，及综合评分等功能。  1、支持在管理系统中对服务器进行远程重启，关机操作，支持一键关机；  2、支持管理员、参赛队员和观众三种角色的使用与验证，同时支持对并发用户数量的控制；  3、支持对管理节点及计算节点的资源使用率进行监控；  4、支持系统状态监控，包括：系统用户数量、在线用户数量、竞赛数量、练习数量、虚拟机母本数量、正在运行的虚机数量等内容；  5、内置DHCP服务，可以设置多个地址池，能够为竞赛中的资源分配IP地址，包括：网段、掩码位、适用模块等；  二、硬件要求  1. 标准2U机架式硬件，配置安装导轨；  2. 主机：2U服务器产品，采用INTEL C621芯片组，支持两颗Intel® Xeon® Processor Scalable可扩展家族CPU；  3. CPU：≥1\*Intel Xeon Silver 4310 12C 2.10GHz 18MB 120W；  4. 内存：≥64GBD DR4-3200 ECC REG RDIMM；  5. 硬盘：≥2.5" 1.92T GEN4 读取密集 U.2；  6. 接口：≥4个千兆网口，为减少网络延迟，集成的双口千兆网卡必须支持I/O AT、负载均衡、链路汇聚、绑定冗余等特性；  7. 扩展槽：支持≥6个PCIE 4.0 ；  8. 远程管理：标配远程管理控制端口，可实现与操作系统无关的远程对服务器的完全控制，虚拟电源可远程开机、重启、关机，主板集成iBMC，可实现远程iKVM。 |
| 2 | 计算节点 | 台 | 2 | 一、功能要求  支持VT-X，VT-d功能，使用qemu-kvm和Docker虚拟化技术提供底层技术支持。接收管理节点的调度任务，是计算任务的承载体。  1.支持将竞赛数据至网络靶场竞技系统管理节点的实时传输；  2.支持计算节点的系统资源被管理节点实时调用；  3.支持实时监控挂载运行虚拟机数量，并实时提供虚拟机占用资源情况；  4.支持自动对系统内闲置资源的实时释放，防止资源被消耗浪费；  5.支持KVM虚拟化技术，内置轮询算法，支持最优算法测算及选择；  二、硬件要求  1. 标准2U机架式硬件，配置安装导轨；  2. 主机：2U服务器产品，采用INTEL C621芯片组，支持两颗Intel® Xeon® Processor Scalable可扩展家族CPU；  3. CPU：≥2\*Intel Xeon Silver 4310 12C 2.10GHz 18MB 120W；  4. 内存：≥128GBD DR4-3200 ECC REG RDIMM；  5. 硬盘：≥2.5" 1.92T GEN4 读取密集 U.2；  6. 接口：≥4个千兆网口，为减少网络延迟，集成的双口千兆网卡必须支持I/O AT、负载均衡、链路汇聚、绑定冗余等特性；  7. 扩展槽：支持≥6个PCIE 4.0 ；  8. 远程管理：标配远程管理控制端口，可实现与操作系统无关的远程对服务器的完全控制，虚拟电源可远程开机、重启、关机，主板集成iBMC，可实现远程iKVM。 |
| 3 | 汇聚交换机 | 台 | 1 | 1、≥24 个 10/100/1000BASE-T 端口,≥4 个 1G/10GBASE-X SFP Plus 端口,≥1 个 Slot；  2、背板带宽：≥598Gbps/5.98Tbps；  3、包转发率：≥222Mpps ；  4、支持基于端口的VLAN（4K个）；  5、支持静态路由；  6、工作环境：0℃～45℃；  7、支持IEEE802.3x 流量控制(全双工)，支持PPS/bps风暴抑制；  8、支持基于端口/MAC/协议/IP子网的VLAN；  9、支持PMTU支持IPv6 Ping,IPv6 Tracert,IPv6 Telnet；  10、支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2；  11、支持报文的802.1p和DSCP优先级重新标记；  12、支持802.1X认证, 单端口最大用户数限制；  支持SSH 2.0、RADIUS、HTTPS。 |
| 4 | 机柜 | 1 | 台 | 1、尺寸：宽度600mm，深度1000mm，高度42U；  2、前门：网门材质，带锁，可拆卸；  3、后门：全金属材质，散热网孔设计，带锁，可拆卸；  侧板：速装卸侧板，全金属材质。 |
| 5 | 智能云调度模块 | 套 | 1 | 1、支持系统资源的调度，提供高度贴近实战的仿真网络信息安全对抗环境； 2、系统调度虚拟靶机资源为上层的业务系统提供环境支撑，网络拓扑资源为竞赛环境提供拓扑支撑，题库资源主要为竞赛提供试题资源的支撑； 3、系统实时监控系统硬件资源的利用率，为平台提供稳定、高效、高并发的虚拟化能力，实现资源最大化利用； 4、管理员可自行创建竞赛或练习场景，可自行选择题目类型、题目数量、竞赛时间并自动计算总体分值； 5、支持靶机环境自动生成，包括练习使用靶机与竞赛使用靶机； 6、系统根据题目拓扑类型生成对应的网络环境，网络环境数量会随比赛队伍数或练习队伍数智能生成。每一套网络环境，是完全隔离的、独享的； 7、智能建立参赛团队与虚机环境之间的联系，学生作答登录指定环境； 8、为保证攻防阶段比赛的公平公正性，每套环境中虚机密码不同；（为证明此功能的真实性，必须提供截图并加盖投标人公章） |
| 6 | 竞赛过程管理模块 | 套 | 1 | 1、支持竞赛用户管理，包括添加/批量添加用户、批量初始化密码、删除/批量删除用户、添加团队、删除/批量删除团队等； 2、支持工具的上传和下载，管理员可预置工具分类，参赛者登录客户端后可以进行工具查询并下载； 3、系统支持管理员用户自定义创建赛题，支持批量添加赛题； 4、支持用户自定义创建竞赛试卷，试题类型可自由组合，系统自动统计试题数量和分值； 5、支持用户自定义创建竞赛，竞赛启动分手动开启和自动开启两种，竞赛结束后系统自动清除靶场环境； 6、自动开启竞赛阶段支持设置竞赛阶段的开始时间和结束时间，到指定时间时自动开始该阶段的比赛，未到指定时间时也可手动开启该阶段，不影响下一阶段自动开启；（为证明此功能的真实性，必须提供截图并加盖投标人公章） 7、每场竞赛中支持多个竞赛阶段同时开启，最多6个竞赛阶段；（为证明此功能的真实性，必须提供功能视频） 8、靶场环境中的flag推送时间可自定义设定； 9、系统支持同时进行多场竞赛，支持启动竞赛、暂停竞赛、关闭竞赛三种操作方式； 10、竞赛过程中，支持查看所有队伍的靶机的使用情况，支持对靶机环境进行管理操作；（为证明此功能的真实性，必须提供截图并加盖投标人公章） 11、支持练习模式。练习模式下，选手可以在登录界面中查看题目的详细解题指导文档；（为证明此功能的真实性，必须提供功能视频） 12、支持八种竞赛阶段：基础理论阶段、夺旗闯关阶段、主机渗透阶段、攻防对抗阶段、取证溯源阶段、企业环境渗透阶段、安全加固固阶、自定义竞赛阶段；（为证明此功能的真实性，必须提供截图并加盖投标人公章） 13、支持管理员在取证溯源阶段控制题目、关卡、靶机访问权限的开放和关闭；（为证明此功能的真实性，必须提供截图并加盖投标人公章） 14、竞赛支持针对不同用户发布不同的公告信息，支持实时弹出公告功能，支持向指定参赛队伍发送公告；支持向指定队员发送公告。（为证明此功能的真实性，必须提供截图并加盖投标人公章） |
| 7 | 态势展示模块 | 套 | 1 | 1、竞赛过程中，参赛端展示系统当前时间、竞赛及阶段相关的时间信息，方便选手合理分配； 2、支持同时开启多场竞赛，用户可自主选择观看的竞赛； 3、八个竞赛阶段，支持八种不同的态势展现形式，具体表现为基础理论阶段、夺旗闯关阶段、主机渗透阶段、攻防对抗阶段、取证溯源阶段、企业环境渗透阶段、安全加固阶段、自定义竞赛阶段八种不同的竞赛态势展现效果；（为证明此功能的真实性，必须提供功能视频） 4、取证溯源阶段，支持以态势图的形式展示本阶段的参赛队伍的答题情况。支持显示每个参赛队伍本阶段的答题数量、得分、当前排名、支持参赛队伍的总得分及总名次统计； 5、企业环境渗透阶段，直观展示企业环境的网络拓扑结构，智能发现拓扑中的新网络，发现后可被显示。选手攻击了拓扑中某台机器，可以动态展示攻击效果，攻击成功有加分效果。支持显示每个参赛队伍本阶段的答题数量、得分、当前排名、支持参赛队伍的总得分及总名次统计； 6、安全加固阶段，支持展示所有队伍的加固情况，以及对拓扑中的哪个区域进行了加固。支持显示每个队伍此阶段的答题数量、得分、当前排名、支持参赛队伍的总得分及总名次统计； |
| 8 | 分析评估模块 | 套 | 1 | 1、支持分析每个参赛团队每个阶段中的实时得分、赛题提交时间、所有题目的提交答案历史； 2、支持通过团队名称、所属院校查询团队成绩详情； 3、支持竞赛成绩导出，导出内容包含参赛队伍信息、各阶段分值等信息，导出格式Excel； 4、能够将任意一支队伍的所有阶段答题详情进行导出，导出格式为图片，导出内容包含各阶段得分占比图、正确率占比图、整场比赛的得分走势图、答题详情； 5、支持展示本场竞赛中所有团队的总体得分、阶段得分，包括每个队伍得分时间现状图；（为证明此功能的真实性，必须提供截图并加盖投标人公章） 6、支持按照团队统计与题目统计两种方式统计成绩，团队统计为每个团队的得分情况进行统计，题目统计以每道题目在各个团队的答题正确率进行统计； 7、团队统计以图形化展示统计，包括图形化展示各个阶段的得分占比、正确率占比、整体竞赛的得分走势图、手动加减分详情及时间； 8、按题目统计中有每道题的分值，答对题目团队的数量，所有团队的正确率等信息； 9、按题目统计中可以查看每道题的答题详情，其中体现每道题的作答用户，所属院校，提交答案，提交时间，提交状态等信息； 10、支持对历史竞赛的查看功能，支持演练任务库存储不少于1000个历史任务； |
| 9 | 场景设计模块 | 套 | 1 | 1、系统内置多种靶机、防火墙、路由器等资源； 2、竞赛场景无限制，用户根据需求可自定义任意场景，创建虚拟主机及网络拓扑等； 3、支持用户自定义靶机，包含选择所使用的镜像、操作系统等； 4、靶机上传过程中，支持超大文件的断点续传，靶机格式支持qcow2、img、iso； 5、支持用户以拖拽方式自主设计网络拓扑，可拖拽多个网络和主机，组成不同vlan，提供可视化展示，并支持按网络拓扑图自动生成虚拟网络环境； 6、支持防火墙功能，防火墙作用于不同网络之间，实现网络间的阻隔与放行设置，支持给防火墙增加策略和防火墙规则，以实现不同功能；（为证明此功能的真实性，必须提供截图并加盖投标人公章） 7、支持安全组功能，安全组作用于不同虚拟机主机之间，实现主机间不同协议和端口的阻隔与放行设置，支持给安全组增加规则；（为证明此功能的真实性，必须提供截图并加盖投标人公章） 8、支持给网络设置ip段，支持给主机设置固定ip； 9、支持镜像库管理功能，支持添加、删除、查询等操作，根据镜像大小可选择网页上传或工具上传两种形式。 |
| 10 | 用户授权许可 | 点 | 40 | 单用户授权 1、作为用户登录网络靶场竞技系统的唯一入口，用户能使用本角色的所有功能； 2、单用户授权，可以自动识别选手、管理员用户，无需在登录时选择用户角色。学生用户可以实现参与竞赛或练习答题相关操作，管理员用户可以实现对竞赛本身的管理以及资源使用情况的监控。标准产品可实现40用户并发。 |
| 11 | 基础考核资源库 | 套 | 1 | 1、包含基本编码、MySQL数据库安全、SQL注入利用、信息隐藏、XSS与编码、MSSQL数据库安全、MD5算法、缓冲区溢出之shellcode提取、移动应用的安全防护、逆向工程等内容； 2、包含密码破解、SQL注入、源码分析、欺骗技术、缓冲区溢出、溢出攻击安全防护、编码解析等内容； 3、包括Windows操作系统主机安全防护、Linux/Unix操作系统主机安全防护、DNS系统的安全防护、扫描与探测、DOS及DDOS类攻击的安全防护、网络层攻击的安全防护； 4、包含主机恶意代码防护、网络单元信息的收集、暴力破解、Web入侵安全防护、安全设备与工具、系统压缩文件密码破解、代码审计等内容； |
| 12 | 夺旗闯关资源库 | 套 | 1 | 1、题目类型必须包括WEB安全、密码学、安全杂项、逆向工程、编程、溢出等6大类型； 2、web安全方面包含SQL注入，宽字节注入，盲注，报错注入，字符串黑名单绕过、SSRF服务端请求伪造获取数据，文件包含(本地和远程)，文件上传和各种检查绕过和解析漏洞，php代码审计中的变量覆盖，命令执行，反序列化等漏洞和hash函数的不当使用等； 3、密码学包含古典密码中单表代换加密：凯撒密码 ，多表代换加密，以及其他类型加密如JSFuck，培根密码，栅栏密码，RSA加密，选择密文攻击，hash长度扩展攻击、DSA数字签名，以及伪随机数生成相关攻击； 4、杂项包括Morse 编码、格雷编码、曼彻斯特编码、XXencoding、Base64、ASCII 编码、以及条形码、二维码相关技术。元数据提取，像素值转化，png图片的lsb信息隐藏，图片长宽调整隐藏，gif图片多帧、时间轴中隐藏信息。pcap文件修复，http，dns等各种协议分析。压缩包暴力破解，明文攻击，伪加密。音频隐写： mp3 、 波形、频谱、LSB音频隐写。Ext，Fat等文件格式分析，内存数据分析； 5、逆向工程包括脱壳技术、反调试技术、Linux逆向技术、python smali java 等语言的逆向技术，windows PE 和 Linux ELF 文件的逆向； 6、pwn栈溢出包括保护机制绕过、ROP技术，SROP，BROP等、栈指针劫持，动态链接绕过ASLR（ret2dl\_resolve）、Partial overwrite 绕过ASLR，绕过canary(leak)。pwn堆溢出方面包括UAF ，double free、off by one 、Fastbin Attack、Unsorted bin attack、Chunk Extend / Shrink、House Of Einherjar、House of Lore、House Of Force、Unsorted Bin Attack、House of Orange。溢出其他漏洞包括格式化字符串漏洞造成任意地址读写、整数溢出漏洞、条件竞争漏洞、linux内核漏洞exploit编写； |
| 13 | 主机渗透资源库 | 套 | 1 | 1、包含mailpress RCE漏洞、弱口令漏洞、权限提升、注入漏洞、失效的身份认证、安全配置错误、目录遍历漏洞、任意文件读取漏洞、后台密码爆破、认证绕过漏洞、网页编辑器漏洞、任意文件上传漏洞、敏感文件泄露漏洞、上传绕过漏洞、自定义页面上传木马、中间件解析漏洞等漏洞内容； 2、包括信息收集、php-fpm未授权访问、redis未授权访问、Web入侵安全防护、主机入侵与防护、数据库攻击与防护、溢出攻击、提权攻击与防护、后门技术与防护措施、操作系统漏洞等漏洞类型； 3、包含基本编码、MySQL数据库安全、SQL注入利用、XXE实体注入利用、LDAP注入、OS命令注入、文件包含、代码注入、数据库远程登录、信息隐藏、XSS与编码、CSRF利用、MSSQL数据库安全、MD5算法、缓冲区溢出之shellcode提取； 4、包含端口扫描、密码破解、SQL注入、源码分析、欺骗技术、缓冲区溢出、组件安全、编码解码、防火墙防护配置及绕过技术等内容； 5、包含系统压缩文件密码破解、代码审计、密码哈希破解等内容； |
| 14 | 攻防对抗资源库 | 套 | 1 | 1、包括但不限于通信企业、交流平台、涉密企业、电商平台、金融机构等比赛场景； 2、包含任意文件读取漏洞、敏感文件泄露漏洞、网页编辑器漏洞、任意权限getshell、后台任意目录上传和执行、弱密码爆破、宽字节配合万能密钥等漏洞； 3、包含mailpress RCE漏洞、弱口令漏洞、注入漏洞、权限提升、失效的身份认证、安全配置错误、php-fpm未授权访问、中间件解析漏洞、目录遍历漏洞、爆破密码、认证绕过漏洞、任意文件上传漏洞、上传绕过漏洞、自定义页面上传木马等漏洞内容； 4、包含基本编码、数据库安全、溢出攻击、信息隐藏、XSS与编码、MD5算法、缓冲区溢出之shellcode提取； 5、包含密码破解、主机入侵与防护、SQL注入、XXE实体注入、LDAP注入、OS命令注入、文件包含、代码注入、数据库远程登录、源码分析、欺骗技术、组件安全、提权攻击与防护、编码解码等内容； 6、包含各类信息收集、php-fpm未授权访问、redis未授权访问、Web入侵安全防护、主机入侵与方式、压缩文件密码破解、数据库安全、后门技术与防护、代码审计、操作系统漏洞； 7、可以对各队伍主机的运行情况进行监控，如果选手恶意关闭必要服务，监控程序自动扣分。 |
| 15 | 取证溯源资源库 | 套 | 1 | 1、包含子域名爆破、伪造邮件、c段扫描、awvs扫描网站、爆破后台、sql注入、sqlmap扫描、编辑网站模板写shell、数据库下载、反弹内网shell； 2、包含文件上传、xss、系统口令爆破、ftp爆破、ssh口令爆破、web口令爆破、mysql数据库密码爆破、sqlserver数据库密码爆破、vnc密码爆破； 3、包含wordpress网站、dedecms网站、drupal网站、joomla网站、discuz网站、phpcms网站； 4、包含ssh后门、定时任务执行恶意代码、web代理、socks5代理、socks4代理、端口转发，插入js恶意代码； 5、包含ntscan的使用、vlan划分、web指纹识别工具的使用、nessus的使用、java反序列化工具的使用、apache解析漏洞的使用、钓鱼邮件的构造、邮件挂马应用、webshell密码爆破、portscan的使用、ftp爆破、john的使用、hydra的使用、linux定时任务、php越权访问、rootkit木马的使用、js探针的使用、伪造邮箱地址、vpn暴力破解、wwwscan的使用、子域名爆破、awvs的使用、php木马的使用、c段扫描工具的使用、nslook的使用、使用ftp提权、撞库攻击、iTop系统的使用； 6、包含sqlmap注入流量识别、sql注入流量识别、菜刀流量识别、js代码分析、js代码解密、webshell流量识别、远程命令流量识别、爆破流量识别、ftp流量识别、mysql协议识别、反序列化力量识别、weblogic后门识别、jsp木马识别、redis流量识别、arp流量识别、mail协议分析； 7、ftp交互流量分析、ftp数据端口计算、流量中文件提取、webshell代码分析、网站密码hash破解、linux系统密码破解、joomla密码破解； 8、pam后门查找分析、分析bash\_history、查找隐藏webshell、查找系统后门、计划任务后门分析； |
| 16 | 企业环境渗透资源库 | 套 | 1 | 1、包含5个虚拟机以上的网络拓扑环境、必须包括多个vlan、必须有模拟的外网地址、且选手只能通过外网地址访问环境； 2、包含web口令爆破、ftp口令爆破、ssh口令爆破、后台地址爆破、目录爆破、绝对路径获取、hash密码破解； 3、包含文件上传绕过漏洞、敏感信息泄露漏洞、远程代码执行漏洞、java反序列化命令执行漏洞、php反序列化命令执行漏洞、xxe注入漏洞、文件包含漏洞、认证绕过漏洞、sql注入漏洞、sql二次注入漏洞、sql注入绕过waf、密码重置逻辑漏洞、任意文件读取漏洞、条件竞争泄露hash漏洞； 4、包含数据库获取webshell、修改配置文件注入so共享库漏洞、邮件服务器协议利用、metinfo后台getshell、jymusic后台getshell； 5、包含wordpress插件任意文件下载漏洞office命令执行漏洞、snmp信息泄露漏洞、Supervisord 远程命令执行漏洞、读取chrome保存的账号密码、双重md5解密； 6、包含python、php源码分析； 7、包含Joomla二阶注入漏洞、appcms的前台sql注入漏洞、zoom client远程命令执行漏洞； 8、包含Apache ActiveMQ Fileserver远程代码执行漏洞、Haraka远程代码执行漏洞、Xplico未授权远程命令执行、OFFICE-CVE-2017-11882漏洞、CVE-2017-12629漏洞、MS15-077漏洞、CVE-2014-3704漏洞、CVE-2017-12635漏洞、CVE-2017-12636漏洞、JTRT Responsive Tables注入漏洞； 9、包含防毒墙的认证绕过漏洞、防毒墙的认证绕过漏洞； 10、包含内网扫描、端口转发、nc反弹shell、msf木马获取meterpreter-shell、web代理、socks4代理、socks5代理、windows系统提权、linux系统提权。 |
| 17 | 安全加固资源库 | 套 | 1 | 1、包含口令加固、文件上传绕过加固、sql注入加固、密码重置加固、重装漏洞加固； 2、包含webshell清理加固、文件及目录权限加固、用户权限加固、代码执行加固、php反序列化加固、java反序列化加固； 3、包含端口加固、系统服务权限加固、命令注入加固、任意文件读取加固、穷举用户加固、web未授权访问加固； 4、包括权限提升加固、信息泄露加固、接口暴露加固、数据库未授权访问加固； 5、包括对所有加固点的监控，检测到异常自动扣分，检测到加固成功自动加分，检测时间可以根据智能算法控制，防止选手猜测出检测时间。 |
| 18 | 工具资源库 | 套 | 1 | 1、安全工具类别包含漏洞扫描、扫描嗅探、密码破解、加密解密、逆向工程、木马后门、远程控制、代理工具、综合工具等； 2、工具数量不少于38款，须包含但不限于以下内容： (1)御剑后台扫描超强85W字典 (2)小葵多功能转换工具 (3)Android逆向助手 (4)Seay源代码审计系统 (5)caidao2016 (6)Burpsuite\_pro (7)Proxifier (8)verify\_CVE-2017-12149 |
| 合计 |  |  |  |  |

**备注：以上参数仅供参考，报价产品达到或优于以上参数即可，参与竞谈单位根据以上功能需求，提供自有品牌产品的详细技术方案，技术方案中提供详细的功能描述、技术参数。**

**五、最终报价及相关文件要求：**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **（一）报价文件格式** | | | | | | | | | |
| 序号 | 产品名称 | 品牌 | 规格型号 | 详细技术参数 | 数量 | 单位 | 单价（元） | 小计（元） | 备注 |
| 1 |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |
| 4 | 合计 | 大写： （小写：￥000,000.00） | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **（二）技术文件格式** | | | | | | | | |
| 序号 | 产品名称 | 品牌 | 规格型号 | 招标参考参数 | 投标产品参数 | 偏离 | 说明 | 备注 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**投标相关文件要求：**

1.所有报价均以人民币最终报价，含设备费用、安装调试费、运费、清洁费、退换货费、税费(提供增值税普通发票)、售后服务等全部费用。报价文件中须提供详细报价清单并提供安装调试时间，并满足项目建设方案技术要求

2.竞谈人须在竞价文件中单独提供一份切实可行的售后服务承诺书，明确质保期内、外的服务条款。

3. 竞谈人在投标的同时请附上企业现行合法有效的营业执照原件（或营业执照公证件）及复印件（盖公章）以及售后服务承诺等相关证明。

4.如竞价人单位法定代表人未能到现场参与，委托单位其他人员参与竞谈的，需提供法定代表人授权委托书及竞谈人在本公司购买的近6个月社保证明。

5. ★标书中的报价文件和技术文件需分别独立封装。其中报价文件应包含详细的设备清单及报价；技术文件则必须涵盖资质证明、竞价人提供的近三年内3个以上同类产品的业绩合同复印件（需加盖单位公章）或竞价人提供的厂家近三年内3个以上同类产品的业绩合同复印件（需加盖厂家公章）。此外，技术文件还应包括谈判代表的授权书、社保证明、详细清单、技术参数偏离表、建设方案以及售后服务方案等，且技术文件中严禁包含任何产品报价信息。投标现场还需提供一份U盘，存储上述资质证明、业绩合同复印件、谈判代表的授权书及社保证明等文件的盖章件电子档。

6. 对于代理产品的供应商，若中标，在签订合同前，必须提供原厂家的授权书及售后承诺书（需加盖厂家公章）。

**六、交货及货款的结算方式：**

在合同签订后，严格按照院方指定的时间、地点安装调试完毕，并作好人员培训等相关工作，经验收合格后支付总货款的 95 %，余款5%在质保期满后支付。

**七、谈判有关说明：**

1.谈判地点：重庆人文科技学院后勤处一楼会议室。

2.谈判时间：另行通知

3.有关规定：超过谈判截止时间、不密封的谈判文件或不按《谈判文件》规定提交相关资质的谈判，我处恕不接受。

**八、联系人及联系方式：范老师 023-42460570**

**九、凡涉及本次谈判文件的解释权归竞争性谈判管理小组。**

**十、一切与谈判有关的费用，均由竞谈人自理。**

**第二部分 竞争性谈判相关附件**

**附件1：买卖合同主要条款**

**买卖合同主要条款**

**甲方（买方）：**

**乙方（卖方）：**

甲乙双方就甲方向乙方购买 事宜，经友好协商一致，达成如下条款供双方遵守：

（注：以下内容为买卖合同的主要条款）

**一、标的物情况及价格**

（二）合同总价格为（大写）： （小写：￥000,000.00），本价格包含产品（设备）价格、运输费、搬运费、质保期内售后服务费、退换货运费、清洁费、安装调试费（设备）、税金等全部费用在内，除本合同约定外，乙方不得要求甲方另行支付任何费用。

（三）乙方承诺本合同销售产品（设备）单价不高于乙方销售给第三人的价格或市场平均价格（含网络销售平台平均价格）。若甲方发现向乙方购买的产品（设备）单价高于第三人的购买价格或市场平均价格，则乙方按高出部分的两倍向甲方支付违约金。价格承诺期为 年 月 日起至 年 月 日止。

**三、交货时间**

甲乙双方签定合同后，乙方须在 年 月 日之前将甲方订购的产品送到甲方指定的地点（设备须在此期限按要求安装完毕，并能投入正常使用）并经甲方验收合格。否则每延迟一日，按合同价款的千分之五向甲方支付违约金。乙方逾期十日仍不能交货的，甲方有权解除合同，尚未支付的货款不予支付，已经支付的货款乙方须全额返还，同时乙方须按本合同交易总金额的20%向甲方承担违约金。

**六、付款方式**

（一）乙方将全部产品（设备）送达甲方指定地点（设备须安装调试完毕），经甲方代表验收合格，在验收单上签字确认后，甲方向乙方支付合同总金额的 95 %，质保期满后支付余款（因乙方未能按本合同约定提供售后质保服务，质保金应扣除部分除外）。

（四）在甲方支付合同款项前，乙方须向甲方送交合法有效的全额增值税**普通**发票。若乙方未按期送交合法有效的全额发票，则甲方付款时间自动顺延，甲方不承担迟延付款的任何责任。

**七、售后服务**

1、所有物品自验收合格之日起 年为质保期。质保期内产品（设备）出现质量问题，乙方必须无条件免费维修或更换。

2、乙方在质保期内接到甲方维修、换货、技术支持等售后服务需求的电话、短信息或电子邮件通知后，乙方需在2小时内作出售后服务承诺，并在24小时内上门服务。

**（备注：《买卖合同》的其他条款详见届时双方签订的合同）**

**附件2：谈判申请及声明**

致： （竞争性谈判人）

根据贵方项目编号 的谈判文件，我方正式提交响应性文件正本壹份，副本叁份。

据此函，签字人兹同意如下：

1.我方同意提供贵方可能要求的与本次谈判有关的任何证据或资料。

2.一旦我方成交，我方承诺将根据谈判文件与贵方签订书面合同，并严格履行合同义务。

3.我方指派 （姓名）（身份证号码： ）为我方全权代表，代表我方参加贵方本次项目的竞争性谈判活动，负责处理与本次竞争性谈判相关的一切事宜。

4.我方决不提供虚假材料谋取成交，决不采取不正当手段诋毁、排挤其他竞价人，决不与竞争性谈判人、其它竞价人恶意串通，决不向竞争性谈判人及谈判小组进行商业贿赂。如有违反，我方无条件同意贵方不退还我方已交纳的竞争性谈判保证金，赔偿竞争性谈判人因此遭受的全部损失，并接受相关管理部门的处罚。

5.与本申请有关的正式通讯地址为：

地 址：

电 话：

传 真：

电子邮箱：

法定代表人（签字）：

竞价人（盖章）：

日 期： 年 月 日

**附件3：法定代表人授权委托书**

**法定代表人授权委托书**

本授权委托书声明：我 (姓名)（身份证号码： ）系

(竞价人名称)的法定代表人，现授权委托 (姓名)（身份证号码： ）为我公司代理人，参加 (竞争性谈判人)的 竞争性谈判活动。代理人在谈判、合同签订过程中所签署的一切文件和处理与之有关的一切事务，我本人及我单位均予以承认并承担与之相关的一切法律后果。

代理人无转委权。特此委托。

代理人： 性别： 年龄：

单位： 部门： 职务：

竞价人：(盖章)

法定代表人：(签字或盖章)

日期： 年 月 日

（粘贴双方身份证复印件）