重庆人文科技学院
信息系统等级保护定级评审及评测项目
竞争性谈判文件

重庆人文科技学院制

2024年11月6日

第一部分 竞争性谈判项目书

项目名称及编号：

财务收费系统、网站群管理系统等级保护定级评审及评测

项目编号：2024060

一站式服务平台、校园视频监控系统等级保护定级评审及评测

项目编号：2024061

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，并具有公安部认可的等级保护测评资质认证。。

2.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。

6. 供应商应必须是国家网络安全等级测评与检测评估机构（提供网络安全等级测评与检测评估机构服务认证证书）。

7. 供应商应为重庆市网络与信息安全信息通报机制成员单位或重庆市网络与信息安全信息通报中心支撑单位。

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、项目内容及主要参数要求：

一、项目概况

为应对日益高发的网络攻击破坏活动，提高信息系统的安全防护能力，加强信息安全管理，落实《中华人民共和国网络安全法》的明确要求，根据《信息安全等级保护管理办法》、GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》等法规和标准的要求，在充分了解被测系统的情况下从实际出发，结合该系统的构成特点，确定具体的测评对象，组织评审专家对评测对象进行定级评审，建立测评方案和测评指导书，通过访谈、检查和工具测试等方式判断该系统安全管理和安全技术的各个方面相对于测评指标的符合程度。针对互联网 Web 应用特点，重点对 Web 应用常见的 SQL 和代码注入漏洞、跨站脚本、缓冲期溢出、信息泄漏等进行工具扫描和检测，并对系统进行渗透测试，以发现系统存在的高危漏洞和风险。通过测评、风险评估、安全扫描和渗透测试，准确反映待测信息系统的安全防护能力现状，对发现的问题进行深入分析，提出安全整改建议，帮助我单位对系统进行安全建设和改进，确保被测系统达到安全保护相应能力的要求。最终出具网络安全等级保护测评报告，并协助我单位完成公安机关指定的定级备案工作，向公安机关提交相关定级备案材料。

二、测评对象

序号	系统名称	测评备案等级
1	财务收费系统	二级
2	网站群管理系统	二级
3	一站式服务平台	二级
4	校园视频监控系统	二级

三、测评依据

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）
《信息安全等级保护管理办法》（公通字[2007]43 号）
《中华人民共和国国家标准 GB/T 17859-1999 计算机信息系统安全保护等级划分准则》
《中华人民共和国国家标准 GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》
《中华人民共和国国家标准 GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》
《中华人民共和国国家标准 GB/T 28449-2018 信息安全技术网络安全等级保护测评过程指南》
《中华人民共和国国家标准 GB/T 20984-2007 信息安全风险评估规范》

四、测评具体内容

本次测评应严格按照《GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》标准的要求实施，加强质量监督和复查，确保测评工作质量。测评指标和对象选择须符合《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》标准的相关要求。具体测评要求如下：

测评范围主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

技术测评：

（1）安全物理环境测评（物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护）；

（2）安全通信网络测评（网络架构、通信传输、可信验证）；

（3）安全区域边界测评（边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证）；

（4）安全计算环境测评（身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护）；

（5）安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

管理测评：

（1）安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

（2）安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

（3）安全管理人员测评（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）；

（4）安全建设管理测评（定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统支付、等级测评、服务供应商选择）；

（5）安全运维管理测评（环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理）。

五、实施内容

供应商在测评过程中要求按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术信息系统安全等级保护实施指南》（GB/T25058-2010）、《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）、《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共 10 个层面进行安全等级保护测评。测评指标如下：

等级保护技术要求（二级）

安全层面	安全控制点	测评指标
安全物理环境	物理位置选择	a）机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
		b）机房场地应避免设在建筑物的高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应有专人值守，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标记；
		b）应将通信线缆铺设在隐蔽安全处；
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a）机房应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；
		b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
	防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	温湿度控制	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。
	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；
		b）应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
		b）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于段。
	通信传输	应采用校验技术保证通信过程中数据的完整性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
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。

安全层面	安全控制点	测评指标
	访问控制	a）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；
		b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
		c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
		d）应能根据会状态话信息对进出数据流提供明确的允许/拒绝访问的能力；
	入侵防范	应在关键网络节点处监视网络攻击行为。
	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。
	安全审计	a）应在网络边界、重要网络节点处进行安全审计，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；
		b）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；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a)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；
		b）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；
		c)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。
	访问控制	a）应对登录的用户分配账户和权限；
		b）应重命名或删除默认账户，修改默认账户的默认口令；
		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d）应授予管理用户所需的最小权限，实现管理用户的权限分离。
	安全审计	a）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；
		b)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；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b)应关闭不需要的系统服务、默认共享和高危端口；
		c）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；
		d）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；
		e）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；
	恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
	数据和备份恢复	a）应提供重要数据的本地数据备份与恢复功能；
		b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
	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。
	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；
		b）应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

安全层面	安全控制点	测评指标
	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
		b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
	管理制度	a)应对安全管理活动中的各类管理内容建立安全管理制度；
		b)应对要求管理人员或操作人员执行的日常管理操作建立操作规程。
	制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定。
		b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理机构	岗位设置	a)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
		b)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。
	授权和审批	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b)应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。
	沟通和合作	a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通,定期召开协调会议，共同协作处理网络安全问题；
		b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
		c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	应定期进行常规安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况。
安全管理人员	人员录用	a)应指定或授权专门的部门或人员负责人员录用；
		b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查。
	人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
	安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。
	外部人员访问管理	a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
		b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
		c)外部人员离场后应及时清除其所有的访问权限。
安全建设管理	定级和备案	a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
		b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
		c)应保证定级结果经过相关部门的批准；
		d)应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a)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；
		b)应根据保护对象的安全保护等级进行安全方案设计；
		c)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。
	产品采购和使用	a)应确保网络安全产品采购和使用符合国家的有关规定；
		b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
		b)应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。
	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
		b）应保证开发单位提供软件设计文档和使用指南。
	工程实施	a） 应指定或授权专门的部门或人员负责工程实施过程的管理；
		b）应制定安全工程实施方案控制工程实施过程。
	测试验收	a）应制定测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

安全层面	安全控制点	测评指标
		b)应进行上线前的安全性测试，并出具安全测试报告。
	系统交付	a)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；
		b)应对负责运行维护的技术人员进行相应的技能培训；
		c)应提供建设过程文档和运行维护文档。
	等级测评	a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
		b)应在发生重大变更或级别发生变化时进行等级测评；
		c)应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a)应确保服务供应商的选择符合国家的有关规定；
		b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
安全运维管理	环境管理	a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
		b)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；
		c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
安全运维管理	介质管理	a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
		b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a)应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理；
		b)应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
	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。
	网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
		c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
		e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
	恶意代码防范管理	a)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；
		b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
安全运维管理	恶意代码防范管理	c)应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
	配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
	密码管理	a)应遵循密码相关国家标准和行业标准；
		b)应使用国家密码管理主管部门认证核准的密码技术和产品。
	变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审，审批后方可实施。
	备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；
		b)应规定备份信息的备份方式、备份频度、存储介质、保存期等；
		c)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。
	安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件；
		b)应制定全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
		c)应在事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

安全层面	安全控制点	测评指标
	应急预案管理	a)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；
		b)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
	外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定；
		b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

六、实施要求

1、在项目实施过程中，投标方应做好计划与安排，确保项目实施不影响系统的正常运行。

2、供应商必须承诺对本项目技术文件以及由用户提供的所有内部资料、技术文档和信息予以保密。供应商须按用户的要求签订保密协议，未经用户书面许可，不得以任何形式向第三方透露本项目标书以及本项目的任何内容。

2、在服务实施过程中,对项目进行规范化管理，确保项目服务质量可控和过程文档完整。要有项目管理组织、项目管理计划、服务资产管理等。同时，供应商应根据项目实际情况制定项目实施计划，严格按照项目实施计划推动项目实施，确保项目进度。

3、供应商应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。供应商应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

4、在项目实施过程中，供应商应成立相应的项目组，指定一名专职的项目经理协调和调度项目实施工作。

5、依据《网络安全等级保护测评机构管理办法》相关规定：“属于异地测评项目的，测评机构应从项目管理系统中生成测评项目基本情况表,并于测评项目实施前报送或传至被测评网络备案公安机关”。属于异地测评项目的,成交供应商应在合同签订前提交审核通过的《测评项目基本情况表》。如出现不能按时提交或备案不通过的，视为成交供应商不具备签订合同的基本条件，采购人有权按评审排名依序顺延。

6、协助甲方填写专家评审意见表及系统定级备案材料，协调开展现场专家评审现场会议并取得备案证。

7、测评方经初步测评后出具该测评系统差距分析报告，并协助甲方完成整改工作直至出具合格的测评报告。

8、项目实施过程中取得的成果报告：（1）渗透测试报告

（2）差距分析报告

（3）最终合格的测评报告（纸质档）

五、最终报价及相关文件要求：

项目名称	测评内容及要求	小计（元）	备注
系统等级保护定级评审及评测项目	财务收费系统（二级）		
	网站群管理系统（二级）		
	一站式服务平台（二级）		
	校园视频监控系统（二级）		

1.所有报价均以人民币最终报价，含系统测评费、税费(提供增值税普通发票)、报告制作等全部费用。报价文件中须提供详细报价清单并提供详细测评方案，并满足项目要求。

2. 竞价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）以及网络安全等级测评与检测评估机构服务认证证书等相关证明。

3.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。

4.★标书中**报价文件和技术文件须分别单独封装**；其中报价文件含详细系统评测清单及报价；技术文件中须含有资质、竞价人提供近三年同类业绩合同复印件（加盖单位公章）或谈判代表的授权和社保、资质文件和实施方案等，**技术文件中不得有报价；投标现场提供一份 U 盘，U 盘内包含竞价人资质、竞价人近三年同类产品业绩合同扫描件（加盖单位公章）、谈判代表的授权和社保等文件盖章件电子档。**

六、交货及货款的结算方式：

在合同签订后，中标人严格按照校方指定的时间、地点实施完毕，并作好评测报告相关资料交接等相关工作。免费提供为期两年的网络安全服务，工作内容包括针对被测系统每年两次漏洞扫描和两次渗透测试,以及校方所有新上线系统的渗透测试服务;中标人应确保测试对象选择合理，接入点和测试路径符合国家网络安全相关要求，并协助校方进行整改加固工作。免费协助校方填写专家评审意见表及系统定级备案材料，协调开展现场专家评审现场会议并取得备案证。协助校方完成公安机关指定的定级备案工作，向公安机关提交相关定级备案材料。

付款方式：测评实施阶段结束后，中标人向校方提供等额有效发票及等保测评合格报告电子版和测评报告纸质版并经校方验收合格后，一次性向中标人支付全额

测评费用。

七、谈判有关说明：

1.谈判地点：重庆人文科技学院后勤一楼会议室。

2.谈判时间：2024 年 11 月 22 日上午 9 时 30 分。

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，均由竞价人自理。

十一、投标保证金：1,000.00 元（大写：壹仟元整）于开标前汇入如下账户：

单　位：重庆人文科技学院

开户行：工商银行合阳支行

账　号：31000　　94009　　02492　　5680

★竞谈现场提供一份纸质投标保证金回执单

未中标的投标人的投标保证金将于定标后的 7 个工作日内予以退还(不计利息)，中标人的投标保证金，自动转为履约保证金，采购方和使用单位对项目共同验收合格后退还投标保证金（不计利息）。

如投标人发生下列情况之一时，投标保证金不退还：

1.中标人未能在规定期限内提交履约担保或签订合同协议。

2.开标后投标人在投标有效期内撤回投标。

3.投标人有违纪违规现象的。

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：

乙方：

甲乙双方根据相关关法律规定，遵循自愿、公平、诚实信用的原则，就甲方向乙方购买 _____产品（系统、软件、数据库等），并由乙方负责安装实施该产品等事项，经双方协商一致，签订本协议，供双方履行：

一、标的物

币种及单位： 人民币（元）

序号	产品名称和型号	数量	金额（元）
1			
2			
3			
4			
合计：　　元（大写：　　）			

（注：以上表格不够填写的，按此格式另行打印标的物清单，作为本合同附件）

二、产品交货时间、地点

1、交货时间：乙方应在签订合同后_____日内，将本合同约定的产品（所有硬件和软件）交付给甲方并安装调试完毕，经甲方验收合格并能正常使用。

2、交货地点：甲方所在地或甲方指定地点。

三、付款方式及时间

1、付款方式：□ 支票　□电汇 □银行汇票 □LC　□T/T

2、付款时间：乙方完成所有产品交付并安装调试完毕，经验收合格后投入使用，甲方应在收到乙方要求付款通知及发票后向乙方一次性支付合同总额的95%，即人民币_____元（大写：_____）。

3、甲方应在质保期届满后向乙方付清剩余5%的余款。

4、甲方支付合同金额至乙方以下账户：

公司名称：

开户银行：

帐　　号：

5、乙方在收款前，需向甲方出具足额正规、真实、有效、足额、收付款人准确、内容完整的完税发票，否则，甲方有权拒付货款，并不承担逾期付款违约责任。

四、质量保证

1、乙方向甲方销售的产品必须与本合同约定的产品名称、型号、功能模块、使用目的、授权范围、使用期限等要求完全符合，并能持续正常使用。

2、乙方向甲方销售的产品必须为原厂正版产品，使用产品的作品等内容得到著作权人授权，须具备原厂正版授权许可证及著作权人授权。

五、质保条款

1、本产品自验收合格并投入正常使用之日起，乙方提供___年的免费服务期，其中一年为产品原厂提供的标准服务，三年为乙方提供的服务，包括安装培训、本地问题处理、技术支持及产品升级服务。

2、普通问题的服务方式包括电话、传真、电子邮件、远程登录(如 FTP)等，及时了解用户的产品使用情况；在远程维护无法解决问题的情况下，48 小时内派出项目实施工程师上门服务。

3、乙方接收通知的电话、传真和电子邮件为：_____，甲方按前述联系方式通知乙方视为有效通知。

4、乙方售后服务机构在服务期内免费为用户提供各种技术服务，包括：每年四次定期回访，在线答疑，产品更新等。

5、乙方为甲方建立完整、准确的产品档案，包括项目实施日志、问题及需求记录的等。

6、甲方需要乙方提供其他服务由双方另行协商约定。

六、知识产权

1、乙方应保证拥有该产品的永久使用权，并有原厂授权证书、许可证以及作者的著作权授权书，确保甲方及用户能够合法正常的使用该产品及相关作品、文章等。

2、乙方所提供的该产品件不应存在任何权利瑕疵，乙方应保证甲方免于遭受因第三方提起侵权索赔而产生的任何损失。任何第三方向甲方提起侵权索赔，乙方应负责与之进行交涉，并承担由此引起的一切法律责任。

3、因乙方提供的产品侵犯第三方知识产权，导致甲方无法使用的，乙方应赔偿甲方因此产生的所有损失或支付合同总金额 30%的违约金。

4、甲方享有该产品在本合同约定范围内的使用权。

（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）