合肥市第八中学信息化系统
安全等级保护测评服务

招
标
采
购

招标单位：合肥市第八中学

项目编号：2020HFBZXJCG014

招标时间：2020 年 12 月

一、投标前须知

尊敬的投标单位：

根据《中华人民共和国政府采购法》的规定，合肥市第八中学拟就“合肥市第八中学信息化系统网络安全等级保护测评服务”项目以公开招标的方式进行采购。

投标前须知附表	
序号	内 容
1	项目名称：合肥市第八中学信息化系统安全等级保护测评服务 项目性质：服务类 预算价：壹拾贰万元整
2	采购机构：合肥市第八中学 地址：合肥市政务区习友路 1688 号

3	投标文件递交地点： 合肥市第八中学现教处 投标（报名）截止时间：2020 年 12 月 7 日 下午 5:00，逾期递交的竞标文件或不符合规定的竞标文件恕不接受。 投标（报名）时间：2020 年 12 月 1 日- 12 月 7 日 （每天上午 8：30-11：00；下午 2：30-5:00 不含节假日） 评标时间： 北京时间 2020 年 12 月 8 日 上午：10：00 评标地点：合肥八中行政楼会议室 项目联系人和投标文件接收人：阮老师 电话/传真：63688843
4	付款方式：本项目合同以人民币付款，招标人全过程按实施完成一次结算（遇假期顺延）。
5	联合体投标：☐允许 ☑不允许
6	服务内容：按照服务要求中规定的相关服务内容执行。（附件中服务要求为必须满足要求，其它增值服务内容以实际踏勘为准）
7	服务地点：合肥市第八中学
8	服务期：甲方通知后 30 日历天；质量要求： 合格 。

9	投标评定方法：综合评分法。即得分最高的前二名投标人为本项目预中标人和预中标候选人。如果综合得分出现两家或两家以上相同者，按投标报价由低到高排序；总得分且投标报价均相同的，则采取抽签方式确定排序。
10	竞标文件份数：正本壹份，副本贰份（正副本叙述有差异时以正本为准），密封提交。
11	合同有效期：签订之日起 贰年 年期。
12	备注：投标人必须对项目现场及环境进行踏勘，并应充分考虑设备及环境复杂程度，服务过程可能调整及其它等风险因素，结合现场踏勘情况，综合报价。

二、招标需求

1、招标范围：合肥八中信息化系统安全等级保护测评服务

2、项目内容：合肥八中智慧校园系统、一卡通消费系统的二级等级保护测评及主流设备网络安全培训服务。

3、报价说明：

包含测评、安全测试等服务与完成整改指导、培训等，提供合肥市第八中学信息化系统安全等级保护第二级的等保测评服务，出具测评分析和整改建议，出具符合安徽省公安厅要求的正式测评结果报告。

4、其他相关要求

工期要求：30 日历天；

质量要求：符合安徽省公安厅要求的正式测评报告。

三、终止竞争性招标

出现下列情况之一时，合肥市第八中学有权宣布终止竞争性招标采购，并将理由通知所有供应商：

1、有效供应商数量不足，导致本次招标缺乏竞争的；

2、出现影响采购公正的违法、违规行为的；

3、因重大变故，采购任务取消的；

4、政府采购法律法规规定的其他情形。

四、确定成交供应商

招标小组根据详细评审的结果确定成交候选供应商，并标明排列顺序。排名第一的成交候选供应商经采购人确定为成交供应商后，由合肥八中予以公告。

如招标小组认为有必要，可以对排名第一的成交候选供应商就响应文件所提供的内容是否符合招标文件的要求进行资格后审。如果确定排名第一的成交候供应商无法履行合同，将依次对其他成交候选供应商进行类似的审查。

排名第一的成交候选供应商放弃成交、不按照招标文件要求提交履约保证金、无故不能履行合同，或者被查实存在影响成交结果的违法行为等情形，不符合成交条件的，采购人可以按照招标小组提出的成交候选供应商名单排序依次确定其他成交候选供应商为成交供应商，也可以重新招标。

供应商对采购过程、成交结果提出质疑，质疑成立且影响或者可能影响成交结果的，合格供应商符合法定数量时，可以从合格的成交候选供应商中另行确定成交供应商的，应当依法另行确定成交供应商；否则应当重新招标。

不接受最终审查或在最终审查过程中提供虚假资料的成交供应商，成交供应商资格将被取消，同时按照政府采购的相关法律、法规予以处罚。

最低报价并不是被授予合同的保证。

凡发现成交候选供应商有下列行为之一的，其成交无效，并移交监督管理部门依法处理：

1、以他人名义参加招标或提供虚假材料弄虚作假谋取成交资格的；

2、以他人名义参加招标，是指使用通过受让或者租借等方式获取的资格、资质证书参加招标。

3、供应商下列情形之一的，属于提供虚假材料的行为：

4、使用伪造、变造的许可证件；

5、提供虚假的财务状况或者业绩；

6、提供虚假的项目负责人或者主要技术人员简历、劳动关系证明；

7、提供虚假的信用状况；

8、其他弄虚作假的行为。

9、与采购人、其他供应商或者合肥八中工作人员恶意串通的；

10、向采购人、评审专家、合肥八中工作人员行贿或者提供其他不正当利益的；

11、有法律、法规规定的其他损害采购人利益和社会公共利益情形的；

12、其他违反政府采购法律、法规和规章强制性规定的行为。

13、确定成交供应商前，合肥八中可能会同采购人对成交候选供应商进行约谈。约谈包括诚信承诺、履约承诺以及原件核查等内容，约谈确认成交候选供应商无法实质性响应招标文件要求的，成交无效。

五、技术要求

为深入贯彻落实习近平总书记关于网络安全工作的重要指示精神和《网络安全法》要求，根据公安部、国信办联合印发《信息系统安全等级保护管理办法》（公通字【2007】 43 号）、《关于信息系统安全等级保护工作的实施意见》（公通字【2004】66 号）、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安【2007】861 号）等相关文件要求，对本次招标采购测评项目及服务按照以下标准和要求开展网络安全等级保护

测评、安全加固工作及服务：

1、测评依据

《网络安全等级保护基本要求》（GB/T 22239-2019）

《网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

2、测评原则

（1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据 进行任何侵害招标人的行为，否则招标人有权追究投标人的责任。

（2）标准性原则：测评方案的设计与实施应依据国家 等级保护的相关标准进行。

（3）规范性原则：投标人的工作中的过程和文档，具 有很好的规范性，可以便于项目的跟踪和控制。

（4）可控性原则：测评服务的进度要跟上进度表的安 排，保证招标人对于测评工作的可控性。

（5）整体性原则：测评的范围和内容应当整体全面， 包括国家等级保护相关要求涉及的各个层面。

（6）最小影响原则：测评工作应尽可能小的影响系统 和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

3、单元测评

（1）物理安全

物理安全测评将通过访谈、文档审查和实地察看的方式测评

信息系统的物理安全保障情况。在内容上，物理安全层面测评实施过程涉及 10 个测评单元。各个测评指标的具体内容和测评要求见表 3.1。

表 3.1 物理安全测评实施内容表

序号	测评指标	测评要求
1	物理位置的选择	通过访谈物理安全负责人，检查主机房等过程，测评主机房等信息系统物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈物理安全负责人，检查主机房出入口、机房分区域情况等过程，测评信息系统在物理访问控制方面的安全防范能力。
3	防盗窃和防破坏	通过访谈物理安全负责人，检查主机房主要设备、介质和防盗报警系统等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	通过访谈物理安全负责人，检查机房设计/ 验收文档，测评信息系统是否采取相应的措施预防雷击。

5	防火	通过访谈物理安全责任人，检查机房设计/ 验收文档，检查机房防火设备等过程,测评信息系统是否采取必要的措施防止火灾的发生。
6	防水防潮	通过访谈物理安全负责人，检查主机房和除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。
7	防静电	通过访谈物理安全负责人,检查主机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	通过访谈物理安全负责人,检查主机房恒温恒湿系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。
9	电力供应	通过访谈物理安全负责人，检查主机房供电线路、设备等过程，测评信息系统是否具备提供一定的电力供应的能力。
10	电磁防护	通过访谈物理安全责任人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。

（2）网络安全

网络安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的网络安全保障情况。在内容上，网络安全层面测评实施过程涉及 7 个测评单元。各个测评指标的具体内容和测评要求见表 3.2。表3.2 网络安全测评实施内容表

序号	测评指标	测评要求
1	结构安全	通过访谈网络管理员，检查网络拓扑情况、抽查核心交换机、接入交换机和接入路由器等网络互联设备，测试系统访问路径和网络带宽分配情况等过程，测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	访问控制	通过访谈安全员，检查防火墙等网络访问控制设备，测试系统对外暴露安全漏洞情况等过程，测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。
3	安全审计	通过访谈审计员，检查核心交换机和接入交换机等网络互联设备的安全审计情况等，测评分析信息系统

		审计配置和审计记录保护情况。
4	边界完整性检查	通过访谈安全员，检查边界完整性检查设备，接入边界完整性检查设备进行测试等过程，测评分析信息系统私自联到外部网络的行为。
5	入侵防范	通过访谈安全员，检查网络边界处的入侵检查设备 IDS/IPS 等过程，测评分析信息系统对攻击行为的识别和处理情况。
6	恶意代码防护	查看系统在网络边界及核心业务网段处是否有对恶意代码采取相关措施，查看代码库是否更新，询问更新策略。
7	网络设备防护	通过访谈网络管理员，检查核心交换机，接入交换机和接入路由器等网络互联设
	备；IDS 和防火墙等网络安全设备，查看它们的安全配置情况，包括身份鉴别、权限分离、登录失败处理、限制非法登陆和登陆连接超时等，考察网络设备自身的安全防范情况。	

（3）主机安全

主机系统安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的主机安全保障情况。在内容上，主机系统 安全层面测评实施过程涉及 7 个测评单元。

各个测评指标的具体内容和测评要求见表 3.3。表 3.3 主机安全测评实施内容表

序号	测评指标	测评要求
1	身份鉴别	检查各主机服务器和终端设备相应操作系统或数据库的身份标识与鉴别和用户登录的配置情况。
2	访问控制	检查各主机服务器和终端设备相应操作系统或数据库的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。
3	安全审计	检查各主机服务器和终端设备相应操作系统或数据库的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。
4		检查各主机服务器相应操作系统的剩余信息保护情况，查询有关维

	剩余信息保护	护手册和操作手册，查看文件、目录和数据库记录等资源所在的存储空间被释放或重新分配前的处理情况。
5	入侵防范	检查各主机服务器和终端设备相应操作系统的自我监控能力；检查操作系统对入侵的防范情况。
6	恶意代码防范	检查各主机服务器和终端设备相应操作系统的恶意代码防范情况。
7	资源控制	检查各主机服务器和终端设备相应操作系统或数据库的系统资源控制情况，如会话限定、用户登录限制、最大并发连接以及服务优先级设置等。

（4）应用安全

应用安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的应用安全保障情况。在内容上，应用安全层面 测评实施过程涉及 9 个测评单元。

各个测评指标的具体内容和测评要求见表 3.4。表

3.4 应用安全测评实施内容表

序号	测评指标	测评要求
1	身份鉴别	检查业务应用系统的身份标识与鉴别功能设置和使用配置情况；检查业务应用系统对用户登录各种情况的处理，如登录失败处理、登录连接超时等。
2	访问控制	检查业务应用系统的访问控制功能设置情况，如访问控制的策略、访问控制粒度权限设置情况等。
3	安全审计	检查业务应用系统的安全审计配置情况， 如覆盖范围、记录的项目和内容等； 检查业务应用系统安全审计进程和记录的保护情况。
4	剩余信息保护	查看应用系统设计、验收文档，是否采取措施保证对存储介质中的用户鉴别信息进行及时清除。
5	通信完整性	检查业务应用系统客户端和服务器端之间的通信完整性保护情况。
6	通信保密性	利用协议分析仪检查业务应用系统客户端和服务器端之间的通信保密性保护情况。

7	抗抵赖	询问管理员，应用系统是否采取抗抵赖措施，具体措施有哪些。
8	软件容错	检查业务应用系统的软件容错能力，如输入输出格式检查、自我状态监控、自我保护、回退等能力。
9	资源控制	检查业务应用系统的资源控制情况，如会话限定、用户登录限制、最大并发连接以及服务优先级设置等。

（5）数据安全及备份恢复

数据安全测评将通过访谈、配置检查的方式测评信息系统的数据安全保障情况。在内容上，数据安全层面测评实施过程涉及 3 个测评单元。

各个测评指标的具体内容和测评要求见表 3.5。

表 3.5 数据安全及备份恢复测评实施内容表

序号	测评指标	测评要求
1	数据完整性	检查信息系统的数据完整性保护情况，包括传输完整性、存储完整性保护措施等；
2	数据保密性	检查信息系统的数据保密性保护情况，包括传输保密性和存储保密性保护措

		施等。
3	备份和恢复	数据的备份情况，包括软、硬件方面的支持情况等。

（6）安全管理制度

测评对象主要为安全主管人员，安全管理人员、各类其它 人员、各类管理制度、各类操作规程文件等，涉及工作单元 3 个。各个测评指标的具体内容、测评对象和测评要求。见表 3.6。表 3.6 安全管理制度测评实施内容表

序号	测评指标	测评要求
1	管理制度	通过访谈安全主管，检查有关管理制度体系文档等过程，测评管理制度体系在内容覆盖上是否全面、完善。
2	制定和发布	通过访谈安全主管，检查有关制度制定要求文档等过程，测评管理制度的制定和发布过程是否遵循一定的流程。
3	评审和修订	通过访谈安全主管，检查管理制度评审记录等过程，测评管理制度定期评审和修订情况。

（7）安全管理机构

测评对象主要为安全主管人员、安全管理人员、相关的文件资料和工作记录等，涉及工作单元 5 个。各个测评指标的具体内容和测评要求见表 3.7。

表 3.7 安全管理机构测评实施内容表

序号	测评指标	测评要求
1	岗位设置	通过访谈安全主管，检查部门/岗位职责文件,测评被测评单位的安全主管部门设置情况以及各岗位设置情况。
2	人员配备	通过访谈安全主管，检查人员名单等文档,测评被测评单位内各个岗位人员配备情况以及关键岗位的轮岗情况。
3	授权和审批	通过访谈安全主管，检查相关文档，测评被测评单位对重要活动的授权和审批情况。
4	沟通与合作	通过访谈安全主管，检查相关文档，测评被测评单位对内部部门、外部单位间的沟通与合作情况。
5	审核与检	通过访谈安全主管，检查相关制度文档和管理要求文档等过程,测评被测评单位

	查	对安全工作的审核和检查情况。

（8）人员安全管理

人测评对象主要为安全主管人员、人事管理人员、相关管理制度、相关工作记录等，涉及工作单元 5 个。各个测评指标的具体内容和测评要求见表 3.8。

表 3.8 人员安全管理测评实施内容表

序号	测评指标	测评要求
1	人员录用	通过访谈人事负责人，检查人员录用文档等过程，测评被测评单位在录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。
2	人员离岗	通过访谈人事负责人，检查人员离岗要求文档等过程，测评被测评单位在人员离岗时是否按照一定的手续办理。
3	人员考核	通过访谈安全主管，检查有关考核记录等过程，测评被测评单位是否对人员进行日常的业务考核和工作审查。
4	安全意识教育和培训	通过访谈安全主管，检查培训计划和执行记录等文档，测评被被测评单位是否对人员进行安全方面的教育和培训。

5	外部人员访问管理	通过访谈安全主管，检查有关文档等过程,测评被测评单位对第三方人员(物理逻辑)信息系统是否采取必要控制措施。

（9）系统建设管理

测评对象主要为安全主管人员、系统建设负责人、各类管 理制度、操作规程文件、执行过程记录等，涉及工作单元 9 个。各个测评指标的具体内容和测评要求见表 3.9。

表 3.9 系统建设管理测评实施内容表

序号	测评指标	测评要求
1	系统定级	通过访淡安全主管，检查系统定级相关文档等过程，测评信息系统是否按照一定要求确定其等级。
2	安全方案设计	通过访谈系统建设负责人，检奄系统安全建设计划等文档. 测评被测评单位对系统整体的安全规划设计是否按照一定流程进行。
3	产品采购	通过访谈安全主管、系统建设负责人，检查相关采购制度等过程，测评被测评单位是否按照一定的要

		求进行信息系统的产品采购。
4	自行软件开发	通过访谈系统建设负责人，检查相关软件开发文档和管理制度文档，测评被测评单位对自行开发的软件是否采取必要的措施保证开发过程的安全性。
5	外包软件开发	通过访谈系统建设负责人，检查相关文档，测评被测评单位对外包开发的软件是否采取必要的措施保证开发过程和日后的维护工作能够正常开展
6	工程实施	通过访谈系统建设负责人，检查相关制度文档和实施文档，测评被测评单位对系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。
7	测试验收	通过访谈系统建设负责入，检查相关制度文档和测试验收文档，测评被测评单位在信息系统运行前是否对其进行测试验收工作。
		通过访谈系统运维负责人，检查系

8	系统交付	统交付清单和系统交付管理制度等过程，测评被测评单位是否采取必要的措施对系统交付过程进行有效控制。
9	系统备案	访谈安全主管，了解系统备案及相关资料管理情况,访谈文档管理员，了解系统备案相关资料的查阅控制情况。
10	等级测评	访谈是否安排专人负责系统等级测评管理,三级系统是否每年进行测评，对测评不符合项是否及时整改。
11	安全服务商选择	通过访谈系统运维负责人，测评被测评单位是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

（10）系统运维管理

测评对象主要为安全主管人员、安全管理人员、各类运维 人员、各类管理制度、操作规范文件、执行过程记录等，涉 及工作单元 12 个。各个测评指标的具体内容、测评对象和测评要求见表 3.10。

表 3.10 系统运维管理测评实施内容表

序号	测评指标	测评要求
1	环境管理	通过访淡物理安全负责人，检查主机房安全管制度和办公环境管理文档等过程，测评被测评单位是否采取必要的措施对主机房的出入控制和办公环境的人员行为等方面进行安全管理。
2	资产管理	通过访谈资产管理员，检查资产清单和系统、网络设备等过程，测评被测评单位是否采取必要的措施对信息系统资产进行分类标识管理。
3	介质管理	通过访谈资产管理员，检查介质管理记录、介质安全管理制度以及各类介质等过程，测评被测评单位是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。
4	设备管理	通过访谈资产管理员、系统管理员，检查设备使用管理文档和设备操作规程等过程，测评被测评单位是否采取必要的措施确保设备在使用、维护和销

		毁等过程安全。
5	监控管理和安全管理中心	访谈运维负责人，了解监控对象范围、采用的监控工具、监控指标等情况，检查监控记录，是否记录了监控对象、监控内容监控异常现象处理等内容。
6	网络安全管理	通过访谈安全主管、网络管理员，检查网络安全管理制度、网络审计日志和网络漏洞扫描报告等过程，测评被测评单位是否采取必要的措施对网络的安全配置，网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。
7	系统安全管理	通过访谈安全主管、系统管理员，检查系统安全管理制度、系统审计日志和系统漏洞扫描报告等过程，测评被测评单位是否采取必要的措施对信息系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。
8	恶意代码防范管理	通过访谈系统运维负责人，检查恶意代码防范管理制度和恶意代码检测、分析记录等过程，测评被测评系统是否采取必要的措施对恶意代码进行集中管理，确

		保信息系统具有恶意代码防范能力。
9	密码管理	通过访淡安全员，检查密码管理制度等过程，测评被测评单位是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。
10	变更管理	通过访谈系统运维负责人，检查变更方案和变更管理制度等过程，测评被测评单位是否采取必要的措施对系统发生的变更进行有效管理。
11	备份和恢复管理	通过访谈系统管理员、网络管理员、检查系统备份管理文档和记录等过程，测评被测评单位是否采取必要的措施对数据、设备和系统进行备份，并确保必要时能够对信息系统进行有效地恢复。
12	安全事件处置	通过访谈系统运维负责人，检查安全事件记录分析文档、安全事件报告和处置管理制度等过程,测评被测评单位是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。

13	应急预案管理	通过访谈系统运维负责人，检查应急响应预案文档，应急预案培训记录等过程，测评被测评单位是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。

4、整体测评与风险分析

针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。

依据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。

5、测评报告编制

完成上述测评工作和招标方实施整改后，出具符合公安机关要求的（年度）保护等级测评报告。

6、售后服务

售后服务内容主要包括以下几个方面：

（1）管理制度完善

根据差距分析报告，分别从人员安全管理、安全管理机构、安全管理制度、系统建设管理以及系统运维管理四个方面进行梳理，协助招标方制定适宜的管理制度体系文件。

（2）技术培训

测评结束后，提供网络安全法规、网络安全防范、网络安全管理及客户主要核心设备生产商指定的安全中级培训等有关的网络安全培训 2 次，以增强招标方技术人员网络安全意识以及网络安全防范技能，其中包含测评中主流设备网络安全培训服务。

（3）安全应急

要求中标后为招标方提供日常安全技术咨询服务，必要时提供远程或现场指导。

7、其他要求

（1）投标人中标后，服务不能满足招标文要求的， 采购人有权取消中标人资格或合同，并按有关规定进行处理。

（2）违约责任问题，合同执行中若发生纠纷由采购人 和中标人双方协商解决，协商不成通过采购人所在地仲裁或诉讼解决。

（3）遵守采购人纪律，注意保密。

（4）知识产权：中标人保证对其出售的标的物享有合 法的权利，中标人应保证其所出售的标的物没有侵犯任何第三方的知识产权和商业秘密等权利。

（5）投标价若超出该项目预算金额（控制价）将做无 效投标处理。

（6）招标人将保留对预中标单位的资质、资格证明文 件、投标文件的真实性进行标后核查的权力，如发现有弄虚 作假行为，一律按规定上报有关监督部门依法处理。

六、投标单位资格

1、在中华人民共和国境内合法注册的，具有独立法人资格的企业；

2、本项目不接受联合体投标；

符合《中华人民共和国政府采购法》第二十二条规定；

4、投标人存在以下不良信用记录情形之一的，不得推荐为中标候选供应商，不得确定为中标供应商：

（1）供应商被人民法院列入失信被执行人的；

（2）供应商被工商行政管理部门列入企业经营异常名录的；

（3）供应商被税务部门列入重大税收违法案件当事人名单的；

（4）供应商被政府采购监管部门列入政府采购严重违法失信行为记录名单的。

5、投标人须具备国家网络安全等级保护工作协调小组办公室颁发的网络安全等级保护测评机构推荐证书。

七、投标单位必须提交的投标文件内容

投标授权委托书；

投标函；

服务要求响应、服务方案；

近五年内没有不良记录和生产责任事故证明材料；

报价书：投标供应商须根据招标内容和要求，报出投标总价。报价为完成本次项目的全费用价格，包含完成本次项目所发生的一切费用，其他各项取费项目由投标人自报，漏项自负，并根据附件三填写报价书封面；

以上材料均要求加盖公司公章。

八、评审方法及标准

1、本次评标活动将采用综合评分法评审：采购人对符合投标人资格的，实质上响应招标文件要求的投标文件按照综合评分表进行综合评分；

2、对某一投标文件的每一个指标项，每位评委进行评分并四舍五入保留至小数点后两位数，然后将各指标项得分进行汇总得到一个合计评分。再将该投标人的各位评委的合计评分取平均值，得到该投标人的综合总得分；

3、评标过程中，如果评标小组一致认定投标人报价不合理的，评标小组可以认定其投标无效；

4、按照有效投标人综合总得分由高到低依次排出中标供应商及中标候选供应商。

招标小组按下表内容对响应文件进行初审和综合评审，各供应商的得分分值一经得出，并核对无误后，任何人不得更改。招标小组对供应商某项初审指标如有不同意见，按照少数服从多数的原则，确定该项指标是否通过。

（一）初审

合肥八中信息系统等级保护测评服务项目初审表				
序号	实质性响应评审指标	评审要求	是否通过	响应文件格式及提交资料要求
1	营业执照	合法有效		提供有效的营业执照和税务登记证的扫描件或影印件，应完整的体现出营业执照和税务登记证的全部内容。已办理“三证合一”登记的，响应文件中提供营业执照扫描件或影印件即可。事业单位提供事业单位法人证书、民办非企业提供民办非企业单位登记证书、非企业专业服务机构提供执业许可证即可。
2	税务登记证	合法有效		
3	招标响应函	符合招标文件要求		
4	无重大违法记录声明函、无不良信用声明函	符合招标文件要求		
5	招标授权书	符合招标文件要求		法定代表人参加招标的无需此件，提供身份证明即可。六响应文件格式附件

6	招标响应情况	付款响应、服务期限响应等。		
7	投标报价	符合招标文件要求		主要考虑：①报价是否响应本招标文件的实质性要求；②报价是否会降低本招标文件规定的质量、服务期限、服务内容；③是否有重大缺项漏项或错项。
8	其他要求	法律、行政法规规定的其他条件或招标公告、招标文件列明的其他要求。		
评审指标通过标准：供应商必须通过上述全部指标。				
评委签字： 评审时间：				

（二）综合评分细则

序号	评分指标		评分标准	分值
	一级指标	二级指标		
1	技术部分（80分）	投标人资质（27分）	测评机构在安徽省公安厅备案（提供证明材料）；	3分
			具有ISO9001质量管理体系认证；ISO14001环境管理体系认证、OHSAS18001职业健康安全管理体系认证；每提供一个得2分，满分6分；（提供证书复印件）	6分
			具有企业3A资信等级证书、3A信用等级证书；每提供一个得2分，满分4分；（提供证书复印件）	4分
			为政府采购优秀供应商；（提供证明材料）；	4分
			ISO/IEC27001信息安全管理体系认证证书（认证方向：网络安全等级保护测评、信息系统风险测评）	5分
			为行政事业单位提供渗透技术支持、漏洞检测等服务不少于三个单位，提供公安网安部门授权函（或授权书）的；	5分
		业绩（15分）	自2019年1月1日以来，承担教育行业信息系统测评案例的，1个得1.5分，最高15分（投标时提供合同复印件或扫描件加盖投标人公章，合同原件备查）	15分
		测评方案（6分）	测评内容与项目要求吻合程度较好，技术方案完备，人员配备、项目周期、质量控制等较合理，测评方案总体优良得5-6分； 测评内容与项目要求吻合程度较好，技术方案较好，人员配备、项目周期、质量控制等较合理，测评方案总体较好得3-4分； 测评内容与项目要求吻合程度一般，技术方案一般，人员配备、项目周期、质量控制等不合理，测评方案总体一般得1-2分； 未提供测评方案的不得分。	6分

		项目团队人员资质（32 分）	项目经理须由高级测评师担任，同时具有信息系统测评高级工程师、网络安全工程师、数据中心运维工程师、软件架构师、信息安全测评师、注册信息安全专业人员（CISP）认证；每提供一项证书得 1 分，满分 6 分；提供证书复印件及及近期半年社保证明；项目经理须满足高级测评师，否则该项整体不得分；	6 分
			团队人员具有网络安全工程师的，每一人得 1 分，满分 6 分,提供证书复印件及近期半年社保证明;查询网址：http://www.ccat.net.cn；	6 分
			团队人员具有数据中心运维工程师的，每一人得 1 分，满分 6 分,提供证书复印件及近期半年社保证明；证书查询网址：http://www.ccat.net.cn；	6 分
			团队人员具有国家注册信息安全专业人员（CISP），每一人得 1 分,满分 6 分,提供证书复印件及近期半年社保证明；证书查询地址：http://www.itsec.gov.cn；	6 分
			团队人员具有大数据技术工程师证书，每一人得 1 分，满分 6 分,提供证书复印件及近期半年社保证明；证书查询地址：http://www.ccat.net.cn；	6 分
			团队人员具有软件架构师，每一人得 0.5 分，满分 2 分,提供证书复印件及近期半年社保证明；证书查询网址：http://www.ccat.net.cn；	2 分
		备注	所有项目团队人员必须为测评师，否则提供的其它证书不予加分；同一人员的单项证书不能重复计算得分；	
2	商务部分（20 分）	投标报价（20 分）	满足招标文件要求且投标价格最低的投标报价为评标基准价并得满分，其他投标人的价格分按下列公式计算：价格分=（评标基准价/投标报价）×20%×100。	

九、投标人须知

投标报价为投标人在投标文件中提出的各项支付金额的总和。包括本次招标文件的全部内容及工程的材料、人工、成本、利润、税金、开办费、技术施工措施费、机械进出场费、风险费、材料调差、政策性文件规定费用等所有费用、安全文明施工、道路跟踪清洁、二次搬运、投标方报价要包含解决此问题所采取的一切费用；

投标人应对现场和周围环境进行勘察，投标人应对不清楚或疑问之处书面提出答疑，并要求业主单位给予答复，以获取编制投标文件和签署合同所需的资料。勘察现场所发生的费用由投标人自己承担。业主单位向投标人提供的有关现场的资料和数据，是业主单位现有的能使投标人利用的资料。业主单位对投标人由此而做出的推论、理解和结论概不负责。投标人因现场实地踏勘不仔细的，成交后签订合同时和履约过程中，投标人不得以不完全了解现场情况为由，提出任何形式的增加工程造价或索赔的要求；

投标人应确保其所提供的投标资料的真实性、有效性及合法性，否则，由此引起的任何责任由其自行承担；

如果评标小组认为有必要，可要求投标人在规定时间内提交投标文件的补充资料或证明材料；

投标人对本函如有不清楚之处，请及时以书面形式与招标人联系，招标人将尽快予以答复；

投标文件应字迹清晰、内容齐全、表达准确，不应有涂改。若有修改，修改处应加盖公章。

投标人应保证其服务人员在招标前现场勘查、招标评审、中标服务期间，对所接触的招标人各种文件、数据库资料、系统安全策略、网络拓扑等信息严格保密，遵守招标人保密制度，不得向第三方透露。

十、废标

出现下列情况之一时，评标小组有权宣布废标，并将理由通知所有投标人：

出现影响采购公正的违法、违规行为的；

报价人的报价均超过了采购预算，采购人不能支付的；

报价人的报价不能确保基本规费缴纳的（如：税金等）；

因重大变故，采购任务取消的；

评标小组评审后一致认定应予废标的；

十一、合同签订

1、成交人应按采购规定的时间、地点与招标单位签订合同。双方应按照投标文件、报价文件及评标过程中的有关澄清、说明或者补正文件的内容与采购人签订合同。成交人不得再与招标委托单位签订背离合同实质性内容的其它协议或声明；

2、采购双方必须严格按照投标文件及承诺签订合同，不得擅自变更。合同风险由双方自行承担；

3、合同格式：制式合同。专用条款未明确部分根据投标文件及评标内容签订；

4、招投标文件是将来签订正式合同的组成部分，与正式合同具有同等法律效力；中标后，签订合同价格为固定价格，定标后不做任何添补。

十二、附件

本招标文件的最终解释权归合肥市第八中学。

附件一：投标授权委托书

附件二：投标函

附件三：项目报价书

附件四：服务要求

附件五：招标业绩承诺函

附件六：无重大违法记录声明函、无不良信用记录声明函

附件一：

投标授权委托书

致：合肥市第八中学

本授权书声明：_____（投标单位名称）授权_____（被授权人的姓名）为我方就“合肥市第八中学信息化系统安全等级保护测评服务”投标活动的合法代理人，以我方名义全权处理该项目相关事宜。

特此声明。

代理人（被授权人）签字：_____

职务：_____

投标单位名称（公章）：

日期：

附件二：

投标函

致：合肥市第八中学

根据贵方所发“合肥市第八中学信息化系统安全等级保护测评服务”项目招标公告，正式授权下述签字人 _____（姓名）代表投标人_____（投标单位全称），提交投标文件。

据此函，签字人兹宣布同意如下：

1、按招标文件规定及投标文件承诺完成本次服务所有需求。

2、我们根据招标文件的规定，严格履行合同的责任和义务,并保证于买方要求的日期内完成合同内容。

3、我们已详细审核全部招标文件，包括招标文件附件、参考资料、招标文件修改书或图纸（如果有的话），我们知道必须放弃提出含糊不清或误解的问题的权利。

4、我们同意从投标人须知规定的招标日期起遵循本投标书，并在投标人须知规定的招标有效期之前均具有约束力。

5、如果在招标后规定的招标有效期内撤回投标，我们的投标保证金可被贵方没收。

6、同意按贵方要求在招标现场规定时间内向贵方提供与其投标有关的任何证据或补充资料，否则，我们的投标文件可被贵方拒绝。

7、我方（投标人）对投标文件中所提供资料、文件、证书及证件的真实性和有效性负责。

8、我们完全理解贵方不一定接受最低报价的投标。

与本投标有关的通讯地址：_____电话：_____

投标人（单位公章）：

日　　期：

附件三：

项目报价书

项目名称	**合肥市第八中学信息化系统安全等级保护测评服务**
投标单位名称（盖章）：	
投标报价	（大写）： （小写）：
工期	接甲方通知后 30 日历天内完成
质量要求是否响应招标文件	（请填写“响应”或者“不响应”）
其他说明：	

法人代表或代理人签字：

日期：

附件四：

服务要求

1、投标人需根据测评业务系统的数量自行评估并配置不少于 3 人（至少包括 1 名高级测评师，1 名中级测评师）的测评实施团队，测评实施团队在合同约定期内派驻采购人指定地点办公；成交供应商在成交后需保证在实施阶段主要技术人员必须是全职，上述人员由成交供应商在合同签订后服务实施前向采购人提供相应人员证书材料进行查验。

2、测评内容应包括安全技术测评和安全管理测评，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、工具测试等各方面的内容。

3、需勘察现场，提供符合招标人信息化系统的测评方案。

4、需提供售后信息安全培训等服务方案。

附件五：

招标业绩承诺函

我公司同意评审结果公告中公示以下业绩并承诺：响应文件中所提供的业绩均真实有效，甲方采购单位均真实有效。若被发现存在任何虚假、隐瞒情况，我公司承担由此产生的一切后果。

供应商签章：_____

日　　期：_____

序号	项目名称	服务范围	合同总金额	备注
1				
2				
3				
4				
5				
……				

备注：

1、表中所列业绩应为供应商满足本招标文件要求的业绩；

2、成交供应商提供的以上业绩情况，如招标文件《供应商须知前附表》有约定的，将按约定随评审结果公告。

附件六：

无重大违法记录声明函、无不良信用记录声明函

（本声明函将随成交结果一并公告）

1、本公司郑重声明，根据《中华人民共和国政府采购法》及《中华人民共和国政府采购法实施条例》的规定，参加政府采购活动前三年内，本公司在经营活动中没有重大违法记录，没有因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

2、本公司郑重声明，我公司无以下不良信用记录情形：

（1）公司被人民法院列入失信被执行人；

（2）公司、法定代表人或拟派项目经理（项目负责人）被人民检察院列入行贿犯罪档案；

（3）公司被工商行政管理部门列入企业经营异常名录；

（4）公司被税务部门列入重大税收违法案件当事人名单；

（5）公司被政府采购监管部门列入政府采购严重违法失信行为记录名单。

我公司已就上述不良信用行为按照招标文件中供应商须知前附表规定进行了查询。我公司承诺：合同签订前，若我公司具有不良信用记录情形，贵方可取消我公司成交资格或者不授予合同，所有责任由我公司自行承担。同时，我公司愿意无条件接受监管部门的调查处理。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商签章：_____

日　　期：_____