太湖职业技术学校信息系统网络安全等级保护测评服务
竞价公告

有关企业：

根据工作安排,学校现拟对校园信息系统进行网络安全等级保护测评，兹请有资质的单位参与报价。

一、服务内容和预算：太湖职业技术学校信息系网络安全等级保护测评；总预算 50000.00 元，最高限价 50000.00 元。

二、基本资格要求（提供有关佐证材料）：

（一）投标人必须具有独立的法人资格，合法有效的营业执照（提供营业执照副本扫描件或复印件并加盖单位公章）；

（二）具有履行合同所必需的设备和专业技术能力；

（三）供应商存在以下不良信用记录情形之一的，不得推荐为成交候选人，不得确定为成交人。

1.被人民法院列入失信被执行人的；

2.被工商行政管理部门列入企业经营异常名录的；

3.被税务部门列入重大税收违法案件当事人名单的；

4.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。

三、具体要求：

对智慧校园系统进行安全技术测评，安全管理测评，工具测试，编制系统安全整改方案，编制和完善安全管理制度等。按等保要求，完成规定工作内容，合同签订后 30 个工作日完成（不涉及整改情况）交付所有信息系统测评报告。验收合格后一次性付款。

四、报价时间和地点：太湖职业技术学校。报价一经我校认可，即为签订合同的最终依据。

五、报价人复函须知：

（1）营业执照、税务登记证、组织机构代码证（已办理“三证合一”的，提供统一营业执照）复印件并加盖公章。

（2）报价函。报价函应由报价人加盖公章。

（3）无不良信用、无重大违法记录声明函。

（4）此项目不收取标书费和报价保证金。

（5）我校将依据同等条件下最低价原则且不超过最高限价确定成交人。如出现多家报价人报价相同且最低，则由学校基建采购小组投票决定成交人。

六、截止时间： 2023 年 10 月 19 日 17:00。

七、联系人：吴力锋 电话：13705565916

地址：安徽省安庆市太湖县晋湖路 340 号职业技术学校。

附件 1：采购需求

附件 2：报价函

附件 3：无不良信用、无重大违法记录声明函

附件 1：

采购需求

一、项目概况

依据《中华人民共和国网络安全法》《信息安全等级保护管理办法》的相关要求，对太湖职业技术学校信息系统进行网络安全等级保护测评，包括：安全技术测评，安全管理测评，工具测试，编制系统安全整改方案，编制和完善安全管理制度等。

二、项目实施范围

序号	服务系统名称	数量	级别	备注
1	智慧校园系统	1	贰	
2				
3				
4				

三、采购内容

（一）指导思想和基本准则：

根据公安部、国家保密局、国家密码管理局、国信办联合印发的《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）、公安部《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信[2009]1429 号）等文件精神，结合太湖职业技术学校工作实际情况，现拟对太湖职业技术学校信息系统实施等级保护测评，以进一步完善太湖职业技术学校信息系统安全管理体系和技术防护体系，切实提高太湖职业技术学校信息系统信息安全防护能力，为太湖职业技术学校信息化建设的健康有序发展提供可靠保障。

（二）等级保护测评主要包括以下几个方面：

1、安全技术测评：针对太湖职业技术学校信息系统进行全方位的技术方面的测评工作，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、安全管理中心等五个方面的安全测评及漏洞扫描。

2、安全管理测评：针对太湖职业技术学校信息系统在安全管理方面进行测评工作，包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理层等五个方面的安全测评。

3、形成差距分析报告：依据测评结果和《信息系统安全等级保护基本要求》（GB/T22239），对太湖职业技术学校信息系统的安全现状和风险进行整体、全面的分析和评估，形成相应的差距分析报告。

4、提供系统安全整改建议：依据《信息系统安全等级保护基本要求》和《信息系统等级保护安全设计技术要求》，结合太湖职业技术学校信息系统差距分析报告，针对太湖职业技术学校信息系统安全现状的提供安全整改建议，作为建设方和承建方进行系统整改的辅助依据。

5、为委托单位编制和完善安全管理制度提供咨询和服务：依据《信息系统安全等级保护基本要求》和《信息系统等级保护安全设计技术要求》，为太湖职业技术学校制订和完善各项信息安全管理制度提供相关的咨询和服务，以达到规范信息安全日常管理工作，提高信息安全基础管理水平。

6、完成上述测评工作和实施整改后，出具符合公安机关要求的（年度）信息系统安全保护等级测评报告。

四、实施原则

1、规范性原则：成交人工作中的过程和文档，应具有良好的规范性，可以便于项目的跟踪和控制；

2、可控性原则：测评的工具、方法和过程需在双方认可的范围之内并符合进度表的安排，保证采购人对服务工作的可控性；

3、整体性原则：测评和分析的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患；

4、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采购人网络的行为，否则采购人有权追究责任。

5、最小影响原则：测评工作应尽可能小的影响系统和网络的正常运行，不能对现网的运行和业务的正常提供产生显著影响。

五、测评要求

（一）测评对象

测评对象种类上应抽查主要的设备、设施、人员和文档等。在对象选择上应做到基本覆盖、数量进行抽样，等级测评的测评对象在抽样时应主要考虑以下几个方面：

1）主机房（包括其环境、设备和设施等）和灾备机房；

2）存储被测系统重要数据的介质的存放环境；

3）办公场地；

4）整个系统的网络拓扑结构；

5）安全设备，包括防火墙等；

6）边界网络设备，包括路由器、楼层交换机等；

7）对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

8）承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

9）管理终端和主要系统终端；

10）能够完成信息系统不同业务使命的业务应用系统；

11）业务备份系统；

12）信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

13）涉及到信息系统安全的所有管理制度和记录。

根据信息系统的测评强度要求，在执行具体的核查方法时，在广度上要做到从测评范围中抽取充分的测评对象种类和数量；在执行具体的检测方法，在深度上要做到对功能等各方面的测试。

（二）测评流程

等级保护测评实施过程包括以下四个阶段：

1、测评准备阶段

1）测评项目组组建：明确项目经理、测评人员及职责分工。

2）项目计划书编制：项目计划书包含项目概述、工作依据、技术思路、工作内容和项目组织等。

3）信息系统调研：通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，明确被测系统的范围（特别是信息系统的边界），了解被测系统的详细构成，包括网络拓扑、业务应用、业务流程、设备信息（服务器、数据库、网络设备、安全设备、数据库等）、管理制度等。

4）工具和表单准备：根据被测系统的实际情况，准备测评工具和各类测评表单。

2、方案编制阶段

1）测评对象确定：根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，确定出本次测评的测评对象。

2）测评指标确定：根据已经了解到的被测系统定级结果，确定出本次测评的测评

指标。

3）测评工具接入点确定：确定需要进行工具测试的测评对象，选择测试路径，根据测试路径确定测试工具的接入点。

4）测评内容确定：确定现场测评的具体实施内容，即单元测评内容。

5）测评实施手册开发：编制测评实施手册，详细描述现场测评的工具、方法和操作步骤等，具体指导测评人员如何进行测评活动。

3、现场测评阶段

现场测评应分别从技术上的安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个层面和管理上的安全管理制度、安全管理机构、安全人员管理、安全建设管理和安全运维管理五个方面分别进行：

1）安全物理环境：通过人员访谈、文档审查和实地察看的方式测评信息系统的安全物理环境保障情况。主要涉及对象为物理基础设施。在内容上，安全物理环境层面测评实施过程涉及 10 个测评单元，包括：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：通过访人员访谈、配置检查和工具测试的方式测评信息系统的安全通信网络保障情况。主要涉及对象为网络互联设备、安全通信网络设备和网络拓扑结构。在内容上，安全通信网络层面测评实施过程涉及 7 个测评单元，包括：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、网络设备防护、恶意代码防范。

3）安全区域边界：通过人员访谈、配置检查和工具测试的方式测评信息系统的安全区域边界保障情况。主要涉及对象为各类服务器的操作系统、数据库管理系统。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，包括：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制。

4）安全计算环境：通过人员访谈、配置检查和工具测试的方式测评信息系统的安全计算环境保障情况，主要涉及对象为各类应用系统。在内容上，安全计算环境层面测评实施过程涉及 9 个测评单元，包括：身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错、资源控制。

5）安全管理中心：通过人员访谈、配置检查的方式测评信息系统的安全管理中心保障情况，主要涉及对象为信息系统的管理数据及业务数据等。在内容上，安全管理中心层面测评实施过程涉及 3 个测评单元，包括：数据完整性、数据保密性、备份和恢复。

6）安全管理制度：通过人员访谈、文档审查和实地察看的方式测评信息系统的安全管理制度情况。在内容上，安全管理制度方面测评实施过程涉及 3 个测评单元，包括：管理制度、制定和发布、评审和修订。

7）安全管理机构：通过人员访谈、文档审查的方式测评信息系统的安全管理机构情况。在内容上，安全管理机构方面测评实施过程涉及 5 个测评单元，包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

8）安全管理人员：通过人员访谈、文档审查的方式测评信息系统的人员安全管理情况。在内容上，人员安全管理方面测评实施过程涉及 5 个测评单元，包括：人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理。

9）安全建设管理：通过人员访谈、文档审查的方式测评信息系统的安全建设管理情况。在内容上，安全建设管理方面测评实施过程涉及 11 个测评单元，包括：系统定级、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、系统交付、安全服务商选择、系统备案、系统测评。

10）安全运维管理：通过人员访谈、文档审查的方式测评信息系统的安全运维管理情况。在内容上，安全运维管理方面测评实施过程涉及 13 个测评单元，包括：环境

管理、资产管理、介质管理、设备管理、安全通信网络管理、系统安全管理、恶意代码防范管理、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、监控管理和安全管理中心。

4、分析与报告编制阶段

1）单项测评结果分析：针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据。

2）单元测评结果判定：将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。

3）整体测评：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。

4）风险分析：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）等级测评结论形成：在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。

6）测评报告编制：根据等级测评结论，编制测评报告，包括概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等。

（三）测评方法

在等级保护测评过程中，应采用以下测评方法：

1、工具测试

利用技术工具（漏洞扫描工具、渗透测试工具、压力测试工具等）对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透测试等。

2、配置检查

利用上机验证的方式检查主机、服务器、数据库、网络设备、安全设备、应用系统的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等），测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，从而测试系统是否达到可用性和可靠性的要求。

3、人员访谈

与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，不同等级信息系统在测评时有不同的要求，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

4、文档审查

检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档）的完整性，以及这些文件之间的内部一致性。

5、实地查看

通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否达到了相应等级的安全要求。

6、测评工具

在等级保护测评过程中使用的测评工具须严格遵循可控性原则，即所有使用的测评工具将事先提交给甲方检查确认，确保在双方认可的范围之内，而且测评过程中采用的技术手段确保已经过可靠的实际应用。

六、测评依据

1、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

2、《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

3、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

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

七、报价要求

本项目报总价，报价包含完成本项目服务期间所产生的一切费用（含验收费用），采购人后期不再另行追加费用。

八、人员配备及要求

成交人拟派的安全服务团队不得少于4人（至少包括1名高级测评师、2名中级测评师）。安全服务团队在合同约定期内派驻采购人到指定地点办公；成交供应商需保证在实施阶段主要技术人员必须是全职。

九、验收标准

1、成交人按等保要求，完成规定工作内容，合同签订后30个工作日完成（不涉及整改情况）交付所有信息系统测评报告。

2、提供相关过程文档和系统测评报告。

附件 2:

报价函格式

致：太湖职业技术学校

根据贵方“校园信息系统网络安全等级保护测评服务竞价公告”，正式授权　　（姓名）代表报价人参加该项目的采购活动。我方已详细审查全部采购文件和有关附件，据此我方郑重声明以下诸点，并对之负相应的法律责任。据此函，签字人兹宣布同意如下：

1、按询价文件规定提供报价总价为（大写）　　元人民币。

2、我方根据询价文件的规定，严格履行合同的责任和义务。

3、我方已详细审核全部竞价文件，我方知道必须放弃提出含糊不清或误解的问题的权利。

4、如果在询价后规定的有效期内撤回报价，我方愿意赔偿由此给采购人造成的相关一切损失。

5、我方同意向贵方提供贵方可能另外要求的与其报价有关的任何证据或资料。

报价单位：　　（公章）

日　　期：

电子邮件：

附件 3：

无不良信用记录承诺函

本公司郑重承诺，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的；

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询价通知书中的规定进行了查询。

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。

供应商公章：

日　　期：