云南省特殊教育资源中心综合管理与服务平台

等保三级测评采购询价公告

根据有关要求，昆明学院学前与特殊教育学院受云南省教育厅委托建设和管理云南省特殊教育资源中心，根据我国《网络安全等级保护管理办法》的相关规定，按《云南省教育行业信息安全等级保护工作实施规范》及昆明学院有关要求，须完成“云南省特殊教育资源中心综合理及服务平台”等级保护三级测评。按照采购计划，拟对2024年云南省特殊教育资源中心综合管理与服务平台等保三级测评服务项目进行询价采购，潜在供应商应在网上下载获取采购文件，并于北京时间2024年1月12日12点前提交响应文件。

一、项目基本情况

项目名称：云南省特殊教育资源中心综合管理与服务平台等保三级测评

采购方式：询价

预算金额：伍万元整（人民币）

采购需求：三级等保测评服务

合同履行期限：自合同签订之日起至60日历日之内

工期（供货期）要求：自合同签订之日起至60日历日之内

本项目不接受联合体投标。

二、申请人的资格要求

**（一）服务商应当具备下列一般条件**

1. 具有独立承担民事责任的能力；

2.具有良好的商业信誉和健全的财务会计制度；

3.具有履行合同所必需的人员和专业技术能力；

4.有依法缴纳税收和社会保障资金的良好记录；

5.参加政府采购活动前3年内，在经营活动中没有重大违法记录；

6. 法律、行政法规规定的其他条件。

**（二）服务商需具备以下特殊条件**

服务商具有公安部第三研究所颁发的“网络安全等级测评与检测评估机构服务认证证书”。

**（三）拒绝下述供应商参加本次采购活动**

供应商被“信用中国”网站（ww.creditchina.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

三、项目需求

**（一）项目范围**

|  |  |  |
| --- | --- | --- |
| **序号** | **等保测评系统名称** | **定级** |
| 1 | 云南省特殊教育资源中心综合管理与服务平台 | 三级 |

**（二）项目测评内容**

**1.项目依据**

按照网络安全等级保护2.0标准开展本次等保测评工作，测评的指标、内容及其程序需严格执行如下规范要求：

《中华人民共和国网络安全法》

《信息安全等级保护管理办法》(公通字[2007]43号)

《信息系统安全保护等级定级指南》（GB/T 22240-2008）

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

《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）

《信息安全技术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定级指南》（GB/T 22240-2020）

《信息系统安全管理测评》（GA/T 713-2007）

《信息安全等级保护等级测评实施细则》

《信息安全风险评估规范》（GB/T 20984-2007）

《信息安全风险管理指南》（GB/Z 24364-2009）

《信息安全管理体系要求》（GB/T 22080-2008）

《信息安全管理实用规则》（GB/T 22081-2008）

《信息系统安全管理要求》（GB/T 20269-2006）

《信息安全事件分类分级指南》（GB/Z 20986-2007）

《信息安全事件管理指南》（GB/Z 20985-2007）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全应急响应计划规范》（GB/T 24363-2009）

**2.服务内容及说明**

**（1） 等保保护测评**

等保测评覆盖安全技术测评和安全管理测评两大类10个方面。安全技术测评包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等5个层面上的安全控制测评；安全管理测评包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等5个方面的安全控制测评。

**（2）等保测评内容**

根据国家对网络安全等级保护工作的相关法律和技术标准要求，结合本项目的系统保护等级开展实施与之相应的检查工作，具体检查内容应包括：

①安全物理环境

测评内容主要包括：物理位置选择、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、电磁防护等。

②安全通信网络

测评内容主要包括：网络架构、通信传输、可信验证等。

③安全区域边界

测评内容主要包括：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、可信验证等。

④安全计算环境

测评内容主要包括：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、个人信息保护等。

⑤安全管理中心

测评内容主要包括：系统管理、审计管理、安全管理、集中管控等。

⑥安全管理制度

测评内容主要包括：安全策略、管理制度、制定和发布、评审和修订等。

⑦安全管理机构

测评内容主要包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等。

⑧安全管理人员

测评内容主要包括：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等。

⑨安全建设管理

测评内容主要包括：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、系统交付、等级测评、服务供应商选择等。

⑩安全运维管理

测评内容主要包括：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、外包运维管理等。

**（三）等保测评目标**

1.识别信息安全风险。通过对信息系统在安全技术和安全管理方面的分析，发现信息系统在安全技术和安全管理方面与相应安全等级保护要求之间的差距，并进行风险分析，出具差距分析报告，明确信息系统面临的风险。

2.增强安全防护能力。依据差距分析报告的结果，并结合实际情况，区分轻重缓急，制定针对性的安全整改计划，通过安全整改不断提高信息系统的整体安全保护水平。

3.测评结果分析

* 单项测评结果判定
* 单元测评结果判定
* 整体测评分析
* 形成测评分析报告
* 针对测评分析报告的整改建议

**（四）渗透测试**

选取可能发起攻击的测试点，使用渗透测试的方式查找可能存在的渗透点,发现信息系统防护体系的薄弱环节，找出可能发生的恶意攻击事件和违规行为。

**（五）渗透测试内容**

工作内容包括渗透测试及提供漏洞修复方案。本次渗透测试工作为黑盒测试。

**1.需要包含如下阶段**

* 前期交互阶段：与用户组织进行讨论，确定渗透测试范围和目标。
* 信息搜集阶段：采用各种方法搜集用户方的所有相关信息。
* 威胁建模阶段：使用在信息搜集阶段所获取到的信息，标识出目标系统上可能存在的安全漏洞与弱点。
* 漏洞分析阶段：综合前面几个环节获取到的信息，从中分析和理解，找出攻击途径和攻击方法。
* 渗透攻击阶段：针对确定好的攻击途径和攻击方法实施渗透攻击，获取系统相关权限。
* 后渗透攻击阶段：以特定的业务系统作为目标，识别出关键的基础设施，找出用户组织最具价值和尝试进行安全保护的信息和资产，找出能够对用户组织造成重要业务影响的攻击途径。
* 报告阶段：将渗透测试结果编制成文档提交给用户，提供安全解决方案；同时将在渗透测试阶段产生的垃圾数据进行清理。

**2.渗透测试工作要求**

本次渗透攻击测试工作应当以不破坏用户应用系统为前提条件，不做危害用户应用系统的工作行为，遵守职业道德，遵守行业规则，严格遵守保密制度，保密要求，不得擅自修改、拷贝用户数据，不得泄露、传播用户的敏感信息，如有违反将负法律责任。

**（六）服务成果**

本次安全服务应提交以下成果：

《信息系统等级测评报告》，包括单元测评分析结果、整改测评分析结果、测评结论和安全整改建议等。

《信息系统渗透测试报告》，包含但不限于如下方面的内容：渗透测试的方法、目标、范围；测试的人员、时间、策略。测试的工具、风险规避措施；测试的过程、漏洞利用截图，测试的结果等。

**（七）项目总体要求**

1．合同签订后60个日历日内完成相关测评工作。测评单位需根据学校及学院和系统云平台管理要求实际情况合理安排测评进度，学校及学院和系统云平台可能因为各类突发状况导致测评周期的不确定性，供应商需要配合学校和学院进行进度的合理安排。项目工作人员需遵守等保检测规定，采用符合标准的检测工具和检测方法实施检测，如因违规操作造成对检测系统的破坏，则应承担相应责任。

2.测评单位必须针对此次测评给出详细方案，内容包含测评计划、测评实施、风险管控、协助整改。要求方案充分考虑到高校和系统云平台特性，结合业务要求，提出切实可行的整改方案。

3.测评单位需针对此次测评列出本项目组织管理架构及主要参与人员情况介绍。要求组织管理架构及人员配备科学完整，项目负责人、项目组人员有参与高校项目的管理经验。项目实施过程中实行专人专职原则，保证各安全层面的测评全面有效，能够发现实际存在安全风险，现场实施人员均需持有等级保护测评师证书。项目组人员必须熟练掌握信息安全相关标准与规范，具备丰富的信息安全测评工作经验，具有成熟的信息安全技术和项目管理能力，能够应对可能的突发性安全事件应急工作。

4.供应商必须单独配备安全测评工具，包含但不限于以下种类工具：网络漏洞扫描系统、web 漏洞扫描系统。供应商必须在技术方案内明确专项检查所需要的所有技术检测工具，至少包含以下内容：名称、型号、主要功能、数量等。

5.在测评过程中保证客观性和公正性原则，测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案开展。

6.测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。详细描述在测评过程中如何通过技术手段控制和规避可能对学校及学院和系统云平台业务系统造成的影响。对于项目实施过程中出现的异常情况如何处理，保证系统正常运行以及测评的可进行性。

7.协助整改，针对差距测评结果，给学校及学院和系统云平台业务管理部门提出合理、可行的整改方案和建议，并在整改完毕后给出系统定级报告。

8.提供详尽、明确的技术培训，同时提供本次乃至后续的培训方案，方案应包含网络安全相关课程内容以及详细培训体系流程。

9.本次等级保护测评项目不得转包或者分包，所有驻场测评师必须持证上岗，未经采购方同意，项目组成员不得更改。

**（八）项目实施方案要求**

供应商需根据本项目服务内容编制详细的项目实施方案，包括测评内容、测评指标以及测评方法的详细方案；测评工作流程；测评工作的详细实施方案；测评过程中的渗透测试服务方案；测评工具的详细介绍；培训方案；人员配置方案以及供应商认为需要提供的其它方案。

**（九）项目服务期限**

供应商应当在合同签订后60个日历日内完成采购文件规定的项目并交付学校使用。

**（十）项目验收标准及要求**

项目完成后，供应商须按照项目采购服务内容及要求，按国家、行业或企业等标准，提供相应的服务内容及交付成果，供应商完成全部项目内容并经采购人验收合格后，项目整体验收合格。

**（十一）付款条件**

项目合同签订、成交供应商人员服务到位且成交供应商完成项目合同的所有工作，采购人于一个月内完成项目验收，成交供应商应向采购人开具发票，采购人收到发票并确认无误后10日内向成交供应商支付相应款项。

四、评标方法和定标原则

参加询价采购活动的供应商，应当按照询价文件的规定一次报出不得更改的价格。

询价小组应当从质量和服务均能满足采购文件实质性响应要求的供应商中，根据报价选择价格最低者为供应商。

五、响应文件提交

截止时间：北京时间2024年1月12日12点

地点：昆明学院（云南省·昆明市 昆明经济技术开发区浦新路2号)博学楼409室

**1.响应文件的组成**

(1) 在有效期内的企业营业执照副本复印件；

(2) 响应单位法定代表人身份证复印件；

(3) 响应单位代理人身份证复印件；

(4) 授权委托书（格式见附件）；

(5) 《响应报价一览表》、《询价采购表》（格式见附件）；

(6) 《承诺书》（格式见附件）；

**2.文件的签署和密封要求**

（1）询价响应单位对所响应的采购内容需严格按照《询价采购表》填写；

（2）响应文件叁份且装订成册，并明确标明“正本”和“副本”。响应文件正本和副本如有不一致之处，以正本为准；

（3）询价响应文件均应采用打印或使用不能擦去的黑色或蓝色墨水书写，由响应单位法定代表人或其授权代表在询价文件要求处亲自签署或盖章，并在询价响应文件（正本）的每一页上加盖公章，未加盖公章的视为无效页；

（4）询价响应文件须装袋密封，封口处须加盖单位公章，密封袋及相应文件封面上应注明采购项目名称、项目编号、响应单位名称、地址、联系人、联系电话等；

（5）采购单位有权拒绝未按上述要求制作的询价响应文件。

六、合同模板（经学院和律师审核后的合同）

 见附件。

七、凡对本次采购提出询问，请按以下方式联系。

项目联系人：徐老师

电　话：0871－65098949