山东城市服务职业学院

采购综合管理系统、预算（项目库）管理系统安全等级保护测评服务询价公告

#### 一、 采购内容

山东城市服务职业学院采购综合管理系统、预算（项目库）管理系统安全等级保护测评服务，具体要求详见附件。

二、投标人资格

（1）在中国境内注册，持有合法的营业执照，具有独立承担民事责任能力的法人、其他组织或自然人；

（2）供应商具有《网络安全等级测评与检测评估机构服务认证证书》；

（3）财务状况报告，依法缴纳税收和社会保障资金的相关材料（需提供财务报告或资信证明或自拟格式承诺、近6个月内任意一个月的纳税证明和缴纳社保证明）；

（4）具有履行合同所必需的设备和专业技术能力；

（5）无不良信用信息记录（供应商自拟格式承诺）；

（6）本项目不接受联合体参加。

三、报价要求

1. 2024年10月10日14时30分—15时00分，到山东城市服务职业学院（山东省烟台市高新区科创西路60号）图信楼619提交报价文件。联系人和联系电话：丛老师，2246687。

2. 报价人须提供包含以下内容的加盖单位公章的报价资料一份：工商营业执照副本复印件、法定代表人身份证复印件、报价单、服务承诺（包括优惠条件承诺）、联系人及联系方式、投标人资格要求等。上述资料装订成册（需提供纸质版文件2份、电子扫描件1份），自行密封并在封面加盖单位公章，否则视为无效投标。所交资料因存档需要，采购人不予返还。

3. 报价为完成采购综合管理系统、预算（项目库）管理系统安全等级保护测评服务全部内容的总价，包括人工费、交通费、设备租赁费、培训费、住宿费、利润、税金等所有费用，且综合考虑价格上涨的不确定风险。

四、其他要求

1.采购人不组织统一考察现场，无论供应商对现场考察与否，都将被视为熟悉该项目的一切情况，并承担一切与报价有关的风险、责任和义务。

2. 采购人未设置最低限价，但投标人报价不得明显低于其他通过符合性审查投标人的报价，也不允许低于成本价报价。否则，采购人将认为其报价有可能影响产品质量、服务质量或不能诚信履约。投标人现场不能对其低报价做出合理解释的，采购人可根据《政府采购货物和服务招标投标管理办法》（财政部87号令）等法律法规认定为无效报价。

3.中标人因自身原因放弃中标人资格，将不允许再次参与该项目，一年内不允许参与采购人其他项目。

4.报价资料应符合完全响应山东城市服务职业学院采购综合管理系统、预算（项目库）管理系统安全等级保护测评服务所有要求，要求见附件。

五、控制价、付款方式、服务期限

控制价：本项目总控制价为人民币80000.00元。

付款方式：本项目无预付款，服务完成并验收合格后支付合同价款的100%。

服务期限：自合同签订之日起1个月内完成测评备案。

六、截止报价时间，报价人不足3家或在评审过程中实质性响应询价文件要求的报价人不足3家，采购人可改为竞争性谈判采购。

七、报价人提交报价资料视为同意该询价公告条款，采购人享有对该条款的解释权。

附件：1.报价单

2.采购综合管理系统、预算（项目库）管理系统安全等级保护测评服务实施方案

山东城市服务职业学院

2024年9月28日

附件1：报价单

报价单

山东城市服务职业学院：

我单位在山东城市服务职业学院采购综合管理系统、预算（项目库）管理系统安全等级保护测评服务中的报价为人民币\_\_\_\_\_\_\_元，大写\_\_\_\_\_\_\_\_元。

联系人：

联系电话：

报价单位（章）：

2024年 月 日

附件2：采购综合管理系统、预算（项目库）管理系统安全等级保护测评服务实施方案

**一、项目概况：**

为了落实《中华人民共和国网络安全法》的有关法律要求，提高信息系统的安全保护水平，选择具备资质的第三方专业机构，在全面了解现有信息化现况的基础上，开展网络安全等级保护测评工作。通过本次工作，发现信息系统中存在的安全风险，分析信息系统安全现状与相关政策文件、技术标准内容要求的差距，提出安全建设整改建议。切实加强信息安全防范水平，提高系统抵御风险的能力。

**二、总体要求**：

1.按照网络安全等级保护定级标准和工作要求，开展信息系统安全等级保护系统梳理和定级工作，协助完成系统的定级报告，并协助完成到公安机关的备案工作。

2.按照国家等级保护2.0相关标准和要求，采购综合管理系统（二级）开展网络安全等级保护测评工作，找出系统现状与相关标准要求之间的差距，遵循适度原则，提出切实可行的整改建议，最终完成等级保护测评报告。

3.针对测评中发现的信息安全管理漏洞和薄弱环节，并深入分析下一步信息系统建设和管理的实际安全需求，协助开展相关的安全整改指导工作，确保重要信息系统的安全防护水平满足当前和未来建设发展的安全要求。

**三、定级梳理：**

按照公安部网络安全等级保护工作要求，开展信息系统安全等级保护定级备案工作。要求完成以下系统的定级报告，并协助到公安机关完成备案。系统情况如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 级别 | 系统所在部门 |
| 1 | 采购综合管理系统 | 二级 | 资产管理处 |
| 2 | 预算（项目库）管理系统 | 二级 | 财务处 |

**四、测评依据：**

公安部、国家保密局、国际密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）；

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》（公通字 [2007]43号）。

《计算机信息系统安全保护等级划分准则》GB/T 17859-1999

《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 网络安全等级保护定级指南》GB/T 22240-2020

《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 网络安全等级保护实施指南》GB/T 25058-2019

《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 数据库管理系统安全评估准则》（GB/T 20009-2019）

《信息安全技术 路由器安全技术要求》（GB/T 18018-2019）

《信息安全技术 操作系统安全技术要求》（GB/T 20272-2019）

《信息安全技术 数据库管理系统安全技术要求》（GB/T 20273-2019）

《信息安全技术 网络交换机安全技术要求》（GB/T 21050-2019）

《信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法》（GB/T 37931-2019）

《信息安全技术 数据交易服务安全要求》（GB/T 37932-2019）

《信息安全技术 工业控制系统安全检查指南》（GB/T 37980-2019）

《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）

《信息安全技术 工业控制系统专用防火墙技术要求》（GB/T 37933-2019）

《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》（GB/T 37934-2019）

《信息安全技术 工业控制系统网络审计产品安全技术要求》（GB/T 37941-2019）

《信息安全技术 工业控制网络监测安全技术要求及测试评价方法》（GB/T 37953-2019）

《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》（GB/T 37954-2019）

《信息安全技术 工业控制系统产品信息安全通用评估准则》（GB/T 37962-2019）

《信息安全技术 可信计算规范》（GB/T 37935-2019）

《信息安全技术 网络存储安全技术要求》（GB/T 37939-2019）

《信息安全技术 桌面云安全技术要求》（GB/T 37950-2019）

《信息安全技术 移动终端安全管理平台技术要求》（GB/T 37952-2019）

《信息安全技术 数控网络安全技术要求》（GB/T 37955-2019）

《信息安全技术 网站安全云防护平台技术要求》（GB/T 37956-2019）

《信息安全技术 个人信息去标识化指南》（GB/T 37964-2019）

《信息安全技术 智慧城市安全体系框架》（GB/T 37971-2019）

《信息安全技术 云计算服务运行监管框架》（GB/T 37972-2019）

《信息安全技术 大数据安全管理指南》（GB/T 37973-2019）

《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）

《信息技术 安全技术 消息鉴别码 第3部分:采用泛杂凑函数的机制》（GB/T 15852.3-2019）

《信息安全技术 云计算服务安全指南》（GB/T 31167-2014 ）

《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）

《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）

《信息安全技术 信息系统密码应用测评要求》GBT43206-2023

《信息安全技术 信息系统密码应用设计指南》GBT43207-2023

《商用密码应用安全性评估测评过程指南》(GM/T 0116-2021 )

《商用密码应用安全性评估测评作业指导书》

项目涉及的其它相关国际、国内标准或规范

**五、测评内容**

测评的内容包括但不限于以下内容：

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、安全管理中心等五个方面的安全测评。

安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

1.安全物理环境

根据信息系统机房和现场安全测评记录，针对机房和现场在“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”和“电磁防护”等安全物理环境方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

2.安全通信网络

根据信息系统安全通信网络测评记录，针对通信网络方面在“网络架构”、“通信传输”、“可信验证””等方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

3.安全区域边界

安全区域边界现场测评包括“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”等边界区域防范措施进行检查。

4.安全计算环境

安全计算环境现场测评包括“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”等几个方面的测评。

5.安全管理中心

安全管理中心现场测评包括“系统管理”、“审计管理”、“安全管理”、“集中控制”等方面。

6.安全管理制度

根据现场安全测评记录，针对信息系统在安全管理制度方面的“安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

7.安全管理机构

根据现场安全测评记录，针对 信息系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

8.安全管理人员

根据现场安全测评记录，针对 信息系统在安全管理人员方面的“人员录用”、“人员离岗”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

9.安全建设管理

根据现场安全测评记录，针对 信息系统在安全建设管理方面的“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”以及“服务供应商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

10.安全运维管理

根据现场安全测评记录，针对 信息系统在安全运维管理方面的“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”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。对运维管理方面与ITIL体系的融合适应性进行评估。

11.人员安全能力提升

成交供应商应提供包含等保2.0标准体系、信息安全政策法规、商用密码应用技术在内的安全培训。

通过现场测评，逐项找出系统现状与国家相关标准要求之间的差距，进行逐项分析、整体分析，给出差距分析报告，并给出整改建议方案。

待整改完毕后，进行结果确认，完成网络安全等级保护测评，出具测评报告，并将测评报告报当地公安机关备案。

**六、成果交付**

项目实施完成后，要求供应商提供满足国家及公安部门审核要求的交付物（包括但不限于）如下：

《xx系统（二级）网络安全等级保护测评报告》

**七、其他要求**

1.项目团队人员不少于5人，其中高级测评师不少于1人。所有成员必须全程全职参与本次项目。项目成员不得随意变动，确需变动，必须提前征得采购人同意。

2.项目实施过程中所收集、产生的所有与本项目相关文档、资料，包括文字、图片、表格、数字等各种形式所属权均归属于山东城市服务职业学院，成交供应商有义务对所涉及到的内容保密，并在签定合同时签署保密协议。

**八、其他要求**

1.项目团队人员不少于5人，其中高级测评师不少于1人。所有成员必须全程全职参与本次项目。项目成员不得随意变动，确需变动，必须提前征得采购人同意。

2.项目实施过程中所收集、产生的所有与本项目相关文档、资料，包括文字、图片、表格、数字等各种形式所属权均归属于山东城市服务职业学院，成交供应商有义务对所涉及到的内容保密，并在签定合同时签署保密协议。

**九、验收合格标准**

1.服务应符合相应的国家标准（无国家标准的按部标或者行业标准）。

2.成交供应商应将所有制作的有关资料等交付采购人。

3.服务达不到质量要求，采购人有权拒收，并可以解除合同；由此引起采购人损失及赔偿责任由成交供应商承担。