**采购公告**

武汉设计工程学院拟就“重要信息系统等级保护测评项目”进行询价采购，欢迎合格的供应商参加报价。现将有关事项公告如下：

**1、项目名称：**重要信息系统等级保护测评服务

**2、项目概况：**按照等保2.0标准开展重要信息系统等级保护测评服务

**3、供应商资格要求：**

3.1供应商必须具备《政府采购法》第二十二条的规定：

具有承担民事责任能力的独立法人机构；具有良好的商业信誉和健全的财务会计制度；有依法缴纳税收和社会保障资金的良好记录；参加政府采购活动前三年内，在经营活动中没有重大的违法记录。

3.2须具备有效营业执照或者三证合一的营业执照（经营范围需满足本次询价的相关要求）、组织机构代码证、税务登记证及相关证书。

3.3须具备公安部第三研究所（国家认证认可委员会批准的认证机构）认证发放的《网络安全等级测评与检测评估机构服务认证证书》。

3.4供应商项目组成员中，其中须提供至少一名高级测评师资格证明或测评人员具有CISP证书（种类涵盖CISO、CISE和CISP-pte等）。

3.5投标人须具有本地化服务能力，如为异地机构在参与本项目过程中严格落实异地测评备案手续，必须提供省级网络安全等级保护领导小组办公室出具盖章版的《等级测评机构异地测评项目备案表》，本地化分支机构证明材料和本地化常驻人员近一年的社保证明。

**4项目实施内容与要求**

* 1. 4.1、服务内容及范围：

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **系统等级** |
| 1 | 学工一站式服务系统 | 二级 |
| 2 | 资产管理系统 | 二级 |

* 1. 4.2、项目定级备案

投标方应梳理现有的信息系统，严格按照《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》的要求，对信息系统的级别进行划定。完成信息系统定级报告及定级材料的准备、整理，完成信息系统去公安机关的备案工作。

4.3、项目测评内容

根据国家等级保护相关标准《GBT22239-2019 网络安全等级保护基本要求》，对重要信息系统等级保护测评项目应包括以下内容：

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：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、安全运维管理等五个方面的安全测评。

服务内容：

1. 协助开展系统和重要信息系统的自查自评估工作，对存在的风险隐患和安全问题及时提供有针对性的安全整改建议，保障整改措施的落实，完成重要信息系统的定级、备案等相关工作；
2. 依据《网络安全等级保护基本要求》，从安全技术和管理两个方面共十个层面对信息系统进行等级测评，出具等级测评报告；
3. 针对信息系统等保测评实施过程中发现的安全隐患和薄弱环节，提供安全建设整改和安全加固方面的咨询。
4. 提供安全服务，及时发现信息系统中存在安全隐患和威胁，进一步开展安全建设整改工作，及时、有效、正确的预防和阻止各种黑客攻击。职责清晰，能快速及时的帮助客户处理网站安全事件。

|  |  |  |
| --- | --- | --- |
| 项目 | 服务内容 | 工作描述 |
| 等级测评 | 项目准备及现场调研 | 协助对信息系统物理环境、网络、终端、数据、安全管理等进行调研。 |
| 信息系统定级、备案 | 疏理信息系统定级工作，完成信息系统定级报告及定级材料的准备；整理、补充信息系统备案所有相关的文档，完成相应信息系统等级保护备案工作。 |
| 信息系统差距分析 | 对定级的信息系统，依照《网络安全等级保护基本要求》进行逐个对照，分析信息系统安全情况与等级保护基本要求的差距，完成信息系统等级保护差距分析报告。 |
| 等级保护安全整改 | 协助落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、辅助进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。 |
| 等级保护测评 | 参照《GBT22239-2019 网络安全等级保护基本要求》和《GB/T28448-2019 网络安全等级保护测评要求》等标准规范要求，对信息系统开展信息系统等级保护测评工作。  |
| 成果 | 服务目标为：协助用户取得公安机关备案证明；通过公安部门的等级保护检查，输出《信息系统等级保护测评报告》。 |

* 1. 4.4、测评要求

（1）安全物理环境物理安全测评是对信息系统的机房和办公场所的物理位置选择、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、电磁防护等方面的安全状况。

（2）安全通信网络

网络安全测评是对信息系统的网络系统安全防护情况进行测评，包括网络结构安全、网络访问控制、网络安全审计、网络边界完整性测评、网络入侵防范、网络恶意代码防范、网络设备防护等方面的安全状况。

1. 安全区域边界

安全区域边界是对信息系统的边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的安全状况。

（4）安全计算环境

安全计算环境是对信息系统的身份鉴别、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、个人信息保护等方面的安全状况。

（5）安全管理中心

安全管理中心是对信息系统的系统管理、审计管理、安全管理、集中管控进行测评。

（6）安全管理制度

安全管理制度测评是对信息系统的安全策略、管理制度、制定和发布、评审和修订等情况进行测评。

（7）安全管理机构

安全管理机构测评是对信息系统的岗位设置、人员配备、授权与审批、沟通和合作、审核和检查等情况进行测评。

（8）安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗安全意识教育和培训、外部人员访问管理等情况进行测评。

（9）安全建设管理

系统建设管理测评是对信息系统建设过程中的、测试验收、系统交付、等级测评服务供应商管理等情况进行测评。

（10）安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、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、外包运维管理等情况进行测评。

* 1. 4.5、测评风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

（1）操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

（2）操作时间控制

* + 1. 对测评直接影响系统工作时，尽可能避开敏感时期。

（3）人员与数据管理

* + 1. 必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

（4）制定应急预案

* + 1. 根据测评范围界定的系统情况，在实施前制定应急预案。

（5）关键业务系统风险控制

* + 1. 对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

（6）优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

（7）数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

* 1. 4.6、整改实施内容

投标方严格按照差距分析报告内容，落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。

* 1. 4.7、汇总项目材料并验收

投标方对整改后的内容进行最终确认，并汇总信息系统等级保护测评报告，完成公安机关的材料报备，取得信息系统备案证明。

投标方汇总等级保护测评阶段性文档（不限于定级备案材料、差距分析报告、整改实施方案、测评报告、备案证明等），保证通过评审及验收。

**5、询价文件的递交：**

5.1请投标供应商认真报价，其报价包括整个服务项目的进场实施、售后服务、利润、税金等一切费用。

5.2投标人应将纸质报价文件密封包装，并在外包装上注明项目名称、投标人名称（投标人名称应写全称），且在封口处加盖单位印章。