**采购需求**

**一、采购内容及数量**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目内容 | 数量  | 预算金额(元) | 备注 |
| 1 | 重要信息系统信息安全等级保护测评 | 1批 | 200000.00 |   |

1. **商务要求（技术要求里另有注明的以技术要求为准）**

|  |  |
| --- | --- |
| **▲**付款条件 | 1、在合同签订后5个工作日内，供应商须向采购人支付合同总金额5%的履约保证金，如不提供，采购人有权拒签合同。签订合同生效后，20个工作日内，采购人向供应商支付50%合同款。2、完成等级保护测评工作后通过市公安部门定级备案工作，并通过项目最终验收后20个工作日内，采购人待财政资金下达后支付50%合同款，验收一年后无质量和服务问题，一次性无息退还履约保证金。 |
| 交货时间及地点 | 2021年12月31日前完成测评工作并将相关报告按校方指定地点进行移交。 |
| 验收要求 | 验收应按照采购人确认的验收测试大纲进行，全过程必须由采购人在场见证。1. 信息系统等级保护测评项目目标是输出符合当地公安部门的等级保护测评报告，该项目将产生一定数量的文档。
2. 响应供应商应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责。
3. 响应供应商应提交验收流程、验收方法和验收依据。
4. 响应供应商应提供交付件归档办法和方式。
5. 响应供应商应提供详细的验收测试大纲或计划，大纲中应明确规定验收项目和必须满足的要求。大纲必须经采购人确认后方可生效。
6. 验收报告需双方代表签字认可。
 |

1. **技术要求**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 总则引言为了落实公安部信息安全等级保护要求，进一步增强信息系统安全防护能力，确保系统安全稳定运行，依据《信息系统安全等级保护基本要求》（GB/T 22239-2019）、《信息系统安全等级保护管理办法》等国家相关文件和标准的要求，制定本技术规范书。响应供应商应仔细阅读本技术规范书所列的各项规范，所提供的测评服务应满足本技术规范书提出的要求。响应供应商也可以推荐满足本技术规范的其他方案，但必须对其在技术规范方面与本技术规范书之间所存在的差异加以详细说明。若无说明，则按对响应供应商不利的方面理解。本项目实施单位应具备如下资质：1. 实施单位应具有公安部门颁发的测评认证资质；
2. 实施单位应提供专业技术人员的信息安全专业认证证书，机构内部具有等级保护测评资质人员不少于15人；
3. 实施单位应具有近两年内等级保护安全测评业绩，并提供相关资质和业绩证明。
4. 不接受联合体单位；

响应供应商应在规定时间内，向采购人提供符合本技术规范书要求的详细的项目实施建议书和报价清单。响应供应商应提供测评成员的技术背景资历资料、从事测评的经验、人力资源的组织方式、项目实施的管理方式、项目成员的角色和责任。响应供应商在项目建议书中，对本技术规范书中提出的技术及项目要求应逐项予以说明和答复。对涉及到的主要需求、技术及服务应做详细的说明。响应供应商对本技术规范书各条目的应答应为“满足”、“不满足”、“部分满足”，不得使用“明白”、“理解”等词语，在答复中，应明确满足的程度，并做出具体、详细的说明，凡采用“详见”、“参见”方式说明的，应指明参见文档中的具体的章节或页码，否则将视技术建议书不符合要求且该应答无效。如果响应供应商提供的系统与本规范书的要求有差异，应在技术建议书中以“技术偏差”为标题的专门章节中加以详细描述。响应供应商应承诺在等级保护安全测评过程中所使用的工具软件本身不能有任何安全隐患，对此应承担责任。同时提供的安全服务必须在技术上先进和成熟，使用工具软件版本是最新的并且成熟稳定，响应供应商应在等级保护测评过程中保证系统的稳定性。响应供应商现场工作结束后，如果采购人对提出的安全问题有疑义，响应供应商应予解答。适用范围本技术规范适用于信息系统等级保护测评的招标采购，包括技术服务要求和验收要求。* + - 本技术规范提出的是最低限度的技术要求。凡本技术规范中未规定，但在相关国家标准、能源行业标准或IEC标准中有规定的规范条文，响应供应商应按相应标准的条文进行服务供应说明。
		- 如果响应供应商没有以书面形式对本技术规范的条文提出异议，则采购人认为响应供应商提供的服务完全符合本技术规范。如有异议，应在投标书中以“投标偏差表”为标题的专门章节中加以详细描述。
		- 本技术规范所建议使用的标准如与响应供应商所执行的标准不一致，响应供应商应按更严格标准的条文执行或按双方商定的标准执行。
		- 本技术规范经招标、投标双方确认后作为订货合同的技术附件，与合同正文具有同等的法律效力。

规范性引用文件下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本规范。1. 《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
2. 《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》
3. 《GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南》
4. 《GB/T 20984-2015 信息安全技术 信息安全风险评估规范》
5. 《信息系统安全等级保护测评要求》
6. 《信息系统安全等级保护测评过程指南》

权利和职责为切实保障本项目的工作质量，确保测评工作达到预期目标，对响应供应商及采购人双方技术工作责任约定如下：采购人责任：1. 负责测评实施过程中同相关单位和部门的协调
2. 为响应供应商提供良好的工作场地和环境
3. 按工作要求提供相关的资料和信息
4. 准备应急措施，负责实施过程中的紧急情况的处理响应供应商责任
5. 按照采购人工作章程开展工作
6. 项目内容的变更即时与采购人代表沟通
7. 按照协议要求提供技术服务和成果
8. 确保测评工作质量
9. 配合采购人准备应急预案和实施过程中的紧急情况处理
10. 负责按时完成所有工作

同时，双方都必须遵循保密要求。测评范围和需求2.1本次测评系统清单：

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 级别 |
| 1 | 办事服务大厅（含流程引擎、契约锁） | 二级 |
| 2 | 教学综合信息服务平台 | 二级 |
| 3 | 高校科研创新服务平台 | 二级 |
| 4 | 人脸门禁管理系统 | 二级 |
| 5 | 网站群类：双年展官方主站、6个二级学院网站、电子图书 | 二级 |
| 6 | 一卡通类：智能报表系统、资产采购管理系统、座位预约系统、自助借阅系统、自助打印系统 | 二级 |

信息安全等级保护测评系统类型应完整，涵盖原等级保护定级备案涉及的二级信息系统。测评结束后，应由测评机构出具符合当地公安部门的测评报告。同时，响应供应商应协助采购人办理信息系统安全等级保护备案手续等相关工作。2.2、等保安全整改方案设计服务(1)协作完成等保整改服务中标人在出具整改意见以后，安排人员上门驻场协助采购人完成整改。坚持管理和技术并重的原则，落实信息安全责任制，修订并落实各类安全管理制度，开展人员安全管理、系统建设管理和系统运维管理等工作，协助采购人完成等保安全管理制度的修订。(2)技术咨询中标方能够提供信息安全方面的技术咨询服务，安全专家咨询服务、安全策略与规范拟定服务。技术规范测评原则等级保护测评实施方案设计与具体实施应满足以下原则：**保密性原则**：响应供应商应与采购人签订等级保护测评保密协议，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，不得利用此数据侵害采购人的权益，否则采购人有权追究响应供应商的责任。**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。**规范性原则**：响应供应商工作中的过程和文档，应具有规范性，便于项目跟踪和控制。**可控性原则**：测评服务的进度应符合进度安排，保证采购人对测评工作的可控性。**整体性原则**：测评的范围和内容应系统、全面、规范，满足国家等级保护相关基本要求。**最小影响原则**：技术测评工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评应在采购方许可的条件下进行。实施要求响应供应商应详细描述等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、时间安排、阶段性文档提交和验收标准等。响应供应商应详细描述测评人员的组成、资质及各自职责的划分。响应供应商应配置经验丰富的测评人员进行等级保护测评工作。测评方法测评方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地察看等多种方法。如需在等级保护测评实施过程中采用在线测评工具的，各种工具软件由响应供应商推荐，经采购人确认后由响应供应商提供并在测评中使用。应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。等级保护测评应有详细的实施方案和严格的操作步骤，采取的措施应是经过测试、稳定可靠的。安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由响应供应商推荐，经确认后由响应供应商提供并在测评中使用。安全测评需要的运行环境（如场地、网络环境等）由采购人提供，响应供应商应详细描述需要的运行环境的具体要求。测评流程信息系统安全等级保护测评流程分为四个阶段：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评完成后，提供整改建议书。风险控制测评工作本身也会引入安全风险，必须加强测评过程中的风险控制。测评实施前，双方应充分讨论并明确测评对系统可能带来的风险和隐患，确定测评对象、测评方法和工具，并制定应急恢复措施。（1）操作的申请和监护测评操作必须遵守现场运行规章制度，确保系统安全稳定运行。如需在线测试，按照相关工作规程，事前申请，并在专责人员的指导和监护下进行。（2）人员与数据管理重视测评保密工作，加强测评过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。（3）测评对象选择优先选择备用设备（系统）或临时搭建的模拟环境进行测评，避免影响在线系统运行。（4）制定应急预案根据被测评系统情况，在测评实施前制定应急预案，加强系统在线应急处置能力。（5）关键业务系统风险控制关键在线运行系统禁止采用渗透测试工具进行测评。测评内容根据国家等级保护相关标准，信息系统安全等级保护测评应包括以下内容：**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、安全计算环境和安全管理中心等五个方面的安全测评；**安全管理测评**：包括安全管理机构、安全管理制度、安全人员管理、安全建设管理和安全运维管理等五个方面的安全测评。**安全物理环境**安全物理环境测评是对信息系统的机房和办公场所的物理环境安全防护情况进行测评，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、电力供应和电磁防护等方面的安全状况。**安全通信网络**安全通信网络测评是对信息系统的网络系统安全防护情况进行测评，包括网络架构、通信传输、可信验证等方面的安全状况。**安全区域边界**安全区域边界测评是对信息系统的网络系统边界防护、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。**安全计算环境**安全计算环境是对信息系统的计算环境安全防护情况进行测评，包括应用系统层面的身份鉴别、访问控制、安全审计、入侵防范、可信验证、数据完整性、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。**安全管理中心**安全管理中心测评是对信息系统的集中管理情况进行测评，包括系统管理、审计管理等方面的安全状况。**安全管理机构**安全管理机构测评是对信息系统的安全管理组织和岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。**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、管理制度的制度和发布、评审和修订等情况进行测评。**安全人员管理**安全人员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，以及外部人员访问管理等情况进行测评。**安全建设管理**安全建设管理测评是对信息系统建设过程中的系统定级备案、安全方案设计、产品采购和使用、自主软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务商供应商选择等情况进行测评。**安全运维管理**安全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。工程管理技术联络会为了确认系统等级保护测评方案，明确等级保护测评的范围，准备必需的测评资料，协调工程进度。在整个工程进展过程中响应供应商可根据采购人要求召开两次技术联络会。技术联络会应记录会议纪要，包括会议议题和结论。联络会纪要应由双方代表签字，并且具有与合同相同的法律效力。第一次技术联络会在合同生效后约4周内在采购人地举行，响应供应商派代表参加。1. 审查并确定等级保护测评初步方案及流程。
2. 讨论并澄清合同文件中的技术条款及相应的实施方案，确定信息系统等级保护测评范围。
3. 响应供应商应提供测评所用工具及相关资料，以保证测评的顺利实施。
4. 讨论并确认工程实施方案及工程进度。

第二次技术联络会在现场测评阶段完成后举行，包括以下议题：双方确认现场测评结果，对后续整改情况的介绍和计划。项目验收验收应按照采购人确认的验收测试大纲进行，全过程必须由采购人在场见证。1. 信息系统等级保护测评项目目标是输出符合当地公安部门的等级保护测评报告，该项目将产生一定数量的文档。
2. 响应供应商应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责。
3. 响应供应商应提交验收流程、验收方法和验收依据。
4. 响应供应商应提供交付件归档办法和方式。
5. 响应供应商应提供详细的验收测试大纲或计划，大纲中应明确规定验收项目和必须满足的要求。大纲必须经采购人确认后方可生效。
6. 验收报告需双方代表签字认可。

项目文档响应供应商完成项目后应提供以下文档：表4-1 响应供应商完成项目提供文档列表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **文档名称** | **提交时间** | **备注** |
| 1 | 《信息系统系统安全等级保护测评报告》 | 完成现场测评后8周 |  |
| 2 | 《信息系统安全等级保护测评整改建议》 | 完成现场测评后8周 |  |

质量保证响应供应商在等级保护测评方案设计、实施、验收的各个阶段，均应满信息系统正常稳定运行的要求。响应供应商出具的相关报告应得到等级保护行业主管单位认定。报告正本一式四份，采购人保留两份。保密要求响应供应商承担被测评单位敏感信息的保密责任，在项目实施过程中，双方需要复制对方提供的相关资料时，应提交书面申请，在得到对方书面同意后方可复制，并将数据内容记录成表，签字确认。未经双方书面同意，不得向第三方透露项目和涉及双方企业信息安全、技术成果的任何内容。项目结束后，双方必须互相确认测评过程中提供的相关资料，相互承担保密责任。 |

1. **其他**

**1、标“▲且加下划线”的有关技术和商务要求为实质性条款，响应方必须做出实质性响应，否则视为无效响应文件。除此之外其余的指标、服务要求以及合同条款可在磋商现场，根据磋商小组与供应商的磋商进行变动。**

**2、除磋商文件中所明确的采购需求规格外，欢迎其他能满足本项目采购需求且性能相当于或高于所明确的产品参加磋商报价。同时在采购需求偏离表中作出详细对比说明。**

**3.如技术部分中未特别注明需执行的国家相关标准、行业标准、地方标准或者其他标准、规范，则统一执行最新标准、规范。**