**信息系统等级保护测评项目需求**

**一.项目简介：**

为做好重要信息系统网络安全防护，我院需对三个信息系统进行等级保护测评，通过测评工作及时发现系统安全隐患并迅速进行整改，从而全面提升重要信息系统的网络安全防护水平，以保障系统的安全、高效、稳定运行。现对信息系统等级保护测评项目组织询价采购活动，预算9万元。

1. **采购内容及要求**

1、等级保护测评

协助用户完成三个信息系统的定级备案工作，按照用户现状参照所定等级对应的技术要求进行测评分析，对评估对象的现状作记录，包括物理安全、网络安全、主机安全、应用安全、数据安全及备份和恢复；按照用户系统现状对应的管理要求进行测评分析，对评估对象的现状作记录，包括安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理。

（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

①单项测评结果判定

②单元测评结果判定

③整体测评分析

④形成测评分析报告

⑤针对测评分析报告的整改建议

2、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。

（1）渗透测试的内容

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。

（2）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。并将在渗透测试阶段产生的垃圾数据进行清理。

（3）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。

3、服务成果

本次安全服务应提交以下成果：

（1）《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。

（2）《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。

4、服务人员要求

（1）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。

（2）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。

5、工具配备要求

（1）投标人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。

（2）投标人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。

6、复测要求

根据测评报告，完成整改后，投标人需进行复测，并出具公安部门认可的测评报告。

评分标准

|  |  |  |  |
| --- | --- | --- | --- |
| **评分项** | **评分标准** | **分值** | **备注** |
| **一、报价部分（20分）** |
| 服务价格（20分） | 满足招标文件要求且投标报价最低的报价为评审基准价，其价格为满分。其他投标人的价格分统一按照下列公式计算：报价得分=（评审基准价/报价）×20（小数点后保留两位）。 | 20分 |  |
| **二、商务部分（48分）** |
| 综合实力（22分） | 投标人具有中国信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）技术支撑单位等级证书》二级及以上的，得4分，没有不得分。 | 4分 | 须提供证书或证明复印件并加盖公章。 |
| 投标人具有中国网络安全审查技术与认证中心颁发的（信息安全风险评估）《信息安全服务资质认证证书（CCRC）》一级服务资质，得4分，没有不得分。 | 4分 |
| 投标人具有中国网络安全审查技术与认证中心颁发的（信息系统安全运维）《信息安全服务资质认证证书（CCRC）》一级服务资质，得4分，没有不得分。 | 4分 |
| 投标人获得过省级及以上网络攻防演练一等奖的得4分，其他一等奖奖项仅得1分。 | 4分 |
| 投标人具有ISO27001（信息安全管理体系）认证，且认证范围包含网络安全等级保护测评的得2分 。 | 2分 |
| 投标人具有ISO9001（质量管理体系）认证，且认证范围包含网络安全等级保护测评的得2分 。 | 2分 |
| 投标人具有ISO20000（信息技术服务管理体系）认证，且认证范围包含网络安全等级保护测评的得2分 。 | 2分 |
| 人员资质（20分） | 项目经理资质（10分） | 项目经理具有《信息安全等级测评师证书（高级）》，且同时具有《项目管理专业人士资格认证（PMP）》、《注册信息安全工程师（CISP）》、《信息系统安全认证专业人员（CISSP）》、《注册数据安全治理专业人员证书（CISP-DSG）》的得10分；每具有一个证书得2分，没有不得分。 | 10分 | 须提供证书或证明复印件并加盖公章。 |
| 项目组成员资质（10分） | 项目组成员（除项目经理外）具有《信息安全等级测评师证书（高级或中级）》、且同时具有《信息安全保障人员证书（CISAW）》、《数据安全工程师(高级)》得6分;每具有一个证书得2分，没有不得分。 | 6分 |
| 投标人提供的项目组渗透人员具备《注册信息安全渗透测试工程师（CISP-PTE）》证书和《国家网络安全应用检测专业防御人员（NSATP-D）》证书的，每提供一位人员得2分，最高得4分。其他情况不得分。 | 4分 |
| 等级保护测评案例（6分） | 投标人2022年1月1日以来完成过类似等级保护测评项目案例，每个案例得2分，最高得6分。 | 6分 | 须提供合同复印件并加盖公章。 |
| **三、技术部分（32分）** |
| 测评方案（20分） | 测评内容（20分） | 测评内容包含安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、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10个方面的，单项内容科学合理，可行性强的得2分，最高可得20分； | 20分 |  |
| 组织方案（12分） | 服务组织架构（3分） | 测评服务组织架构：具体负责技术、调研、管理、实施人员分工明确，可行性强的得3分；测评服务组织架构：具体负责技术、调研、管理、实施人员分工明确，可行性较强的得2分；测评服务组织架构：具体负责技术、调研、管理、实施人员分工明确，具有一定可行性的得1分；测评服务组织架构分工不明确或未提供的不得分。 | 3分 |  |
| 项目进度安排（3分） | 项目进度安排根据工作量、工作强度合理规划，内容完整，可行性强的得3分；项目进度安排根据工作量、工作强度合理规划，内容完整，可行性较强的得2分；项目进度安排根据工作量、工作强度合理规划，内容完整，具有一定可行性的得1分；进度安排不合理或未提供的，不得分。 | 3分 |  |
| 风险管控能力（3分） | 测评风险控制方案内容全面完整，可行性高的，得3分；测评风险控制方案内容全面完整，可行性较高的，得2分；测评风险控制方案内容全面完整，具有一定可行性得，得1分；测评风险控制方案不合理或未提供得，不得分。 | 3分 |  |
| 渗透测试方案（3分） | 渗透测试方案内容完整，科学合理，可行性强的，得3分；渗透测试方案内容完整，较科学合理，可行性较强的，得2分；渗透测试方案内容基本完整，基本科学合理，具有一定可行性的，得1分；渗透测试方案不合理或未提供得不得分。 | 3分 |  |