**喀什地区维吾尔医医院等保测评服务**

**一、采购单位**：喀什地区维吾尔医医院

**二、项目名称：**喀什地区维吾尔医医院HIS系统、EMR系统、PACS系统、LIS系统网络安全等级测评服务采购项目

**三、项目预算:**人民币350000元以内

**四、资质要求**

1.等级保护测评资质：《网络安全等级测评与检测评估机构服务认证证书》2.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服务资质二级及以上认证证书.

3.近三年投标方没有被“中国网络安全等级保护网”（http://www.djbh.net）公示责令整改或取消资质的情况.

4.提供营业执照；

5.本项目不接受联合体投标。

**五、项目团队**

1、对拟派项目经理须具备高级网络安全等级测评师证书和商用密码应用安全性评估测评能力证书、渗透测试高级工程师证书、数据安全工程师(高级)证书。

2、技术负责人：具有网络安全服务能力评价证书中级（CCSS-R）、软件测评工程师（STE）证书。

3、团队人员资质要求：具有中级测评师证书、网络安全能力认证-网络安全管理（CCSC）（Ⅱ级）、公安部信息安全等级保护评估中心颁发的CIIP-D证书。

（以上涉及人员资质，需提供证书扫描件并加盖公章，同时提供社保证明。）

**六、服务内容及要求**

**（一）测评范围：**

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **拟定达到级别** |
| 1 | HIS系统 | 三级 |
| 2 | EMR系统 | 三级 |
| 3 | PACS系统 | 三级 |
| 4 | LIS系统 | 三级 |

**（二）服务**

1、商用密码咨询及培训服务

对网络信息安全等保测评系统开展商用密码咨询服务：主要分为密码技术和密码技术应用，密码技术主要包括：功能、密钥管理、密码配用策略、密码实现机制、密码安全防护。密码技术应用主要包括：物理安全密码、网络安全密码、主机密码安全、应用安全密码、数据安全及备份恢复密码。

3、风险评估服务

对网络信息安全等保测评项目开展风险评估服务。根据风险评估要素关系模型，进行风险评估需要分析评价各要素，按照各要素关系，风险评估的过程主要包括:风险评估的准备，即信息收集与整理、对资产、威胁、脆弱性的分析、己有采取安全措施的确认以及风险评价等环节。

4、每年提供两次（上半年一次下半年一次）信息安全检查服务，根据公司信息部门安排，每次实施三次安全扫描，分别对应着信息安全检查的自查初级阶段、自查复核阶段、最终整改阶段。每个阶段保证7个工作日完成扫描结果和整改措施的提报。提报的结果以简单、方便阅读的图表或其他方式呈现，方便用户根据扫描结果进行整改。

5、对该系统进行信息安全评估，通过资产梳理、资产识别、资产赋值、脆弱性赋值、威胁性赋值，形成最终的安全风险评估报告和安全加固建议。

6、渗透测试：通过对重点服务器进行准确、全面的测试，可以发现系统最脆弱的环节，以便对危害性严重的漏洞及时修补，以免后患。出具渗透测试报告，并根据渗透测试结果指导应用厂商进行修复和加固；修复后进行渗透测试复查，验证漏洞修复情况，出具复查报告。

7、安全培训：宣贯国家信息系统等级保护政策，明确开展等级保护工作的目标、内容和要求。

8、应急响应服务：在国家法定节假日、国家或自治区重要会议、安全事件大规模爆发等重要时刻，提供7x24小时现场应急支撑服务。

**（三）项目技术规范**

1.质量标准：应依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准。

* 《中华人民共和国网络安全法》
* 《网络安全等级保护条例》（征求意见稿）
* 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
* 《网络安全等级保护定级指南》（GB/T 22240-2020）
* 《网络安全等级保护实施指南》（GB/T 25058-2019 ）
* 《网络安全等级保护基本要求》（GB/T 22239-2019）
* 《网络安全等级保护测评要求》（GB/T 28448-2019）
* 《网络安全等级保护设计技术要求》（GB/T 25070-2019）
* 《网络安全等级保护测评过程指南》（GB/T 28449-2018）
* 《信息技术安全技术信息安全管理体系要求》（GB/T22080-2008）
* 《计算机信息系统安全等级保护通用技术要求》（GA/T390-2002）
* 《信息安全技术信息系统安全管理要求》（GB/T 0269-2006）
* 《信息系统安全工程管理要求》（GB/T20282-2006）
* 《网络安全等级保护设计技术要求》（GB/T 25070-2019）
* 《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）
* 《信息安全技术网络安全等级保护测试评估技术指南》（GB/T36627-2018）

**2.测评内容**

**（一）系统调研：**在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统、网络环境资产现状。

**（二）现场测评：**根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果。

**（三）分析整改：**根据前述工作内容，分析信息系统安全情况与等级保护基本要求的差距,提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合采购单位安全整改工作。

**（四）结论报告：**根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评,提供安全等级符合性测评服务，出具相关系统测评报告。

**（五）配合验收：**整理项目过程中所有相关的过程文档，提交系统相关资料。

**3、等级保护测评要求：**

供应商在测评过程中要求按照《信息安全技术 信息安全等级保护定级指南》（GB/T22240-2020）、《信息安全技术 网络安全等级保护实施指南》（GB/T25058-2019）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、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、安全运维管理共10个层面进行安全等级保护测评。

**4、项目实施管理**

**（一）服务保证：**乙方将严格执行甲方的项目管理规定，从项目组织管理、项目进度管理、项目质量保障和安全保密等方面加强项目管理，确保服务质量。

**（二）质量保证：**乙方将建立严格的质量保证体系，制定项目过程的质量控制方案和实施措施，并督促落实各环节质量控制内容和目标；保证项目各个阶段工作满足采购人对质量的要求。

乙方将根据项目的工作计划，对阶段性工作成果进行审核，并向项目单位提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个项目的质量。

**（三）完成时限：**自合同签订后45日内完工。

（1）付款方式：完成技术服务、验收合格，若无质量问题一次性付清。