附件：

信息系统等级保护测评项目采购需求

一、项目概述

2017年6月1日《中华人民共和国网络安全法》的正式施行，其中第二十一条明确了国家实行网络安全等级保护制度。为了提升我院信息安全性，我院拟按照网络安全等级保护制度2.0标准对核心信息系统进行等保测评。

二、采购项目标的清单、预算、时间、时限

（一）采购项目清单：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 标的名称 | 计量单位 | 数量 |   |
| 1 | 医院信息系统(HIS、EMR)三级等保测评 | 项 | 1 |   |
| 2 | 医院信息集成平台三级等保测评 | 项 | 1 |   |
| 3 | 互联网医院三级等保测评 | 项 | 1 |   |
| 4 | 门户网站二级等保测评 | 项 | 1 |  |
| 5 | 信息安全服务 | 项 | 1 |   |

1. 采购预算：22万元内
2. 采购时间：预计2025年10至11月份
3. 项目完成时限：合同签订后90天内

注：以最终发布的采购公告及采购文件为准

三、技术要求：

（一）主要服务规范及产品（如涉及）配置要求、服务量。

本次测评的主要是根据GB 17859-1999《计算机信息系统安全保护等级划分准则》信息安全的相关标准，对清单中的业务系统，在技术和管理两个方面的10个大项内容进行逐一的检查和测试，其内容涉及信息系统的物理安全、网络安全、主机安全、应用安全、数据安全和管理安全等，以核查内江市中医医院信息系统已有的信息安全防护措施是否达到国家关于信息安全等级保护相应等级的防护要求，找出系统在信息安全方面存在的脆弱点，并提出安全整改建议。通过测评来发现问题、解决问题，从而帮助系统的使用者规避信息安全风险。

经我院初步测算，信息系统共有3个三级信息系统、1个二级信息系统需要进行等级保护测评服务。潜在供应商将在采购人指定地点完成所有信息系统的等级保护测评服务，并提出整改建议。

系统情况如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 系统级别 |
| 1 | 医院信息系统(HIS、EMR)三级等保测评 | 三级 |
| 2 | 医院信息集成平台三级等保测评 | 三级 |
| 3 | 互联网医院三级等保测评 | 三级 |
| 4 | 门户网站二级等保测评 | 二级 |
| 5 | 信息安全服务 |   |

（二）项目管理

潜在供应商必须提供完整的项目管理方案，针对以下项目管理要求进行项目管理服务要求进行承诺，未提供项目管理服务承诺为无效投标人。

1. 潜在供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任；
2. 应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力；
3. 潜在供应商在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留；

4、潜在供应商的岗位配置要至少配置测评师、项目经理、渗透工程师、质量主管等并明确各个岗位的相关职责。

5、测评工具要求

（1）、采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件；

（2）、采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品；

（3）、采用的测评工具的生产商应为正规厂商，能够对产品进行持续更新并提供质量和安全保障；

1. 、测评机构所使用的测评工具不会对单位系统产生破坏或负面影响。
2. 网络安全等级保护测评要求
3. 潜在供应商应详细描述本次项目整体实施方案，包括项目概述、等保测评服务方案、项目实施方案等。
4. 潜在供应商应详细描述服务人员的组成、资质及各自职责的划分。投标人应配置有经验的测评人员进行本次等级保护测评工作。
5. 网络安全等级保护测评的具体要求

1、信息系统技术安全测评

（1）、安全物理环境测评：物理安全检测应当包含：物理位置的选择、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、电磁防护等十个单元。

（2）、安全通信网络测评：安全通信网络测评应当包含：网络架构、通信传输、可信验证等。

（3）、安全区域边界主机安全测评：安全区域边界测评应当包含：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。

（4）、安全计算环境测评：安全计算环境测评应当包含：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。

（5）、安全管理中心测评：系统管理、审计管理、安全管理、集中管控。

2、信息系统管理安全测评

（1）、安全管理制度测评：安全管理制度测评应当包含：安全策略、管理制度、制定与发布、审批和修订。

（2）、安全管理机构测评：安全管理机构测评应当包含：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

（3）、安全管理人员测评：安全管理人员测评应当包含：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。

（4）、安全建设管理测评：安全建设管理测评应当包含：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、服务。

（5）、安全运维管理测评：安全运维管理测评应当包含：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。

（五）项目交付文档

项目实施过程及完成后，应向采购人提交包含但不限于以下的文档：

《网络安全等级测评方案》

《网络安全等级测评整改建议》

《网络安全等级测评报告》

《公安部门备案证明》

《渗透测试报告》

注：《网络安全等级测评方案》应在正式测评前提交，《网络安全等级测评整改建议》应在测评中提交，《网络安全等级测评报告》及《渗透测试报告》应在正式测评开始后22个工作日后提交。

（六）信息安全服务

以合同签订时间为期一年，其中包含漏洞扫描一次，重大节日安全保障（全年），网络安全培训一次，攻防演练一次，突发网络安全事件30分钟响应，2小时内到达现场进行应急处理，每季度出具医院网络安全分析报告。