桐城市人民医院网络安全等级保护测评服务

公开三次询价

# 一、项目概述

### （一）政策依据

依据《信息安全等级保护管理办法》（公通字〔2007〕43号）第十四条规定，第三级信息系统应当每年至少进行一次等级测评。桐城市人民医院作为三级综合医院，其核心业务系统需严格遵循等保要求，保障网络安全与数据合规。

### （二）项目背景

### 桐城市人民医院2024年通过的测评内容为两个三级系统【面向公众服务的信息系统（含医院信息集成平台、HIS）、互联网医院】和一个二级系统（官方网站）。根据等保要求，2025年需对两个三级系统进行年度测评，确保其安全防护能力持续符合三级标准。

### （三）项目目标

通过采购专业测评服务，对医院两个三级信息系统进行全面安全评估，出具合规的《测评报告》，并针对发现的问题提供整改建议，提升系统安全防护水平，满足公安部门监管要求。

## 二、采购内容

### （一）测评对象与等级

|  |  |  |
| --- | --- | --- |
| **系统名称** | **安全保护等级** | **测评次数** |
| 面向公众服务的信息系统（含医院信息集成平台、HIS） | 三级 | 1次 |
| 互联网医院系统 | 三级 | 1次 |

### 采购方式：公开招标

### 最高限价(人民币)：5万。

### （二）服务范围

1. 依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）和《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019），对两个三级系统进行安全技术测评（包括物理安全、网络安全、主机安全、应用安全、数据安全）和安全管理测评（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）。
2. 出具《网络安全等级保护测评报告》，并针对测评发现的问题提供详细的整改建议方案。
3. 配合医院完成整改后的复测工作，确保系统通过公安部门备案审核。

## 三、技术要求

### （一）测评标准

严格遵循等保2.0标准体系，包括但不限于：

* 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
* 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
* 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

### （二）测评内容

1. **安全物理环境**：检查机房的物理访问控制、防火、防水、防雷、电力供应等措施是否符合三级要求。
2. **安全通信网络**：评估网络架构的合理性、网络设备的配置策略、通信传输的保密性和完整性等。
3. **安全区域边界**：核查边界防护设备的部署与策略配置，确保边界访问控制、入侵防范、恶意代码防范等措施有效。
4. **安全计算环境**：检测主机操作系统、数据库管理系统、应用系统的安全配置，漏洞扫描与修复情况，以及访问控制、审计日志等功能的完整性。
5. **安全管理中心**：验证安全管理中心的集中管控能力，包括安全策略下发、日志分析、事件响应等。
6. **安全管理制度**：审查医院现有的安全管理制度文件，评估制度的完备性、适用性和执行情况。
7. **安全管理机构**：检查安全管理机构的设置、人员分工及职责落实情况。
8. **人员安全管理**：评估人员录用、离岗、培训等环节的安全管理措施。
9. **系统建设管理**：核查系统定级备案、安全方案设计、产品采购与使用、工程实施、测试验收等过程的合规性。
10. **系统运维管理**：审查系统日常运维管理流程，包括配置管理、漏洞管理、事件处置、应急预案等。

## 四、服务要求

### （一）测评流程

1. **项目启动阶段**：签订合同后，供应商应在5个工作日内组建项目团队，与医院对接并制定详细的测评方案，明确测评范围、方法、时间安排等。
2. **现场测评阶段**：
	* 医院提前10天通知供应商进场时间。
	* 供应商进场后20个工作日内完成现场测评工作，包括数据采集、漏洞扫描、策略核查、人员访谈等。
	* 现场测评结束后5个工作日内，向医院提交《整改建议报告》，明确列出系统存在的安全问题及整改措施。
3. **整改与复测阶段**：
	* 医院根据整改建议进行系统整改，整改完成后通知供应商进行复测。
	* 供应商在收到复测通知后10个工作日内完成复测工作，并在复测结束后10个工作日内出具正式的《网络安全等级保护测评报告》。
4. **验收阶段**：供应商协助医院将测评报告提交至公安部门备案，并配合完成验收工作。

### （二）售后服务

1. 提供为期1年的免费安全咨询服务，解答甲方在网络安全方面的疑问，提供技术支持和建议。
2. 对于测评过程中发现的漏洞和安全问题，在整改完成后1年内，免费提供远程技术支持，协助甲方进行漏洞修复和安全加固。
3. 若甲方在服务期内进行系统升级、架构调整或发生安全事件，供应商应在接到通知后24小时内响应，提供紧急技术支持。
4. 提供为期1次的免费网络安全知识课程培训服务，加强巩固甲方工作人员网络安全相关知识，为防护网络安全信息泄漏保驾护航。

（三）保密要求

供应商应对测评过程中获取的医院敏感信息（包括但不限于业务数据、系统架构、用户信息等）严格保密，不得向任何第三方披露。在项目结束后，应将所有涉及甲方的资料（包括纸质文档、电子数据等）进行销毁或归还，确保信息安全。

## 五、商务要求

### （一）合同期限

### 服务期1年。

### （二）付款方式

1. 合同签订后，甲方在10个工作日内支付合同金额的50%作为预付款。
2. 供应商完成现场测评并提交《整改建议报告》后，医院在10个工作日内支付合同金额的30%。
3. 供应商完成复测并提交正式《测评报告》，且测评结果通过公安部门备案审核后，医院在10个工作日内支付合同金额的20%。

### （三）违约责任

1. 若供应商未按合同约定的时间和质量要求完成测评工作，每逾期一天，应按照合同金额的0.1%向医院支付违约金；逾期超过30天的，医院有权解除合同，并要求供应商承担相应的赔偿责任。
2. 若医院未按合同约定支付款项，每逾期一天，应按照未支付金额的0.1%向供应商支付违约金。

### （四）争议解决

双方在履行合同过程中如发生争议，应首先通过友好协商解决；协商不成的，任何一方均有权向合同签订地有管辖权的人民法院提起诉讼。

## 六、供应商资质要求

1. 供应商须为在中华人民共和国境内注册的独立法人，具有有效的营业执照，且经营范围包含网络安全等级保护测评相关服务。
2. 供应商须具备公安部颁发的《网络安全等级测评与检测评估机构推荐证书》，并在《全国网络安全等级保护测评机构推荐目录》中备案。
3. 供应商须具有良好的商业信誉和健全的财务会计制度，提供近三年（2022-2024年）的财务审计报告或财务报表。
4. 供应商须具有依法缴纳税收和社会保障资金的良好记录，提供近三个月（2025年2-4月）的纳税证明和社保缴纳证明。
5. 供应商须具备至少3个类似项目经验（提供合同复印件或中标通知书），且在医疗行业有成功案例者优先。
6. 供应商拟派项目团队成员须具备网络安全等级测评师资质，其中项目负责人须具有高级测评师证书。
7. 供应商须承诺在本地设有固定的服务机构或能够提供本地化服务支持，确保在接到医院通知后2小时内到达现场。

## 评标办法

## 最低投标价法

## 八、报价表（报价需包含完成本项目的所有费用）

|  |  |  |  |
| --- | --- | --- | --- |
| **系统名称** | **安全保护等级** | **测评次数** | **报价（元）** |
| 面向公众服务的信息系统（含医院信息集成平台、HIS） | 三级 | 1次 |  |
| 互联网医院系统 | 三级 | 1次 |  |
| 合计 |  |

## 九、其他事项

1. 本采购需求书未尽事宜，双方可在合同签订时另行协商补充。
2. 供应商应仔细阅读本需求书的所有条款，如对本需求书有任何疑问或建议，应在投标截止时间前以书面形式向医院提出，医院将视情况进行澄清或修改。
3. 本采购需求书自发布之日起生效，有效期至项目验收完成。

## 十、报价表加盖公章密封，于8月7日16：00时前送至桐城市人民医院(新院区)，门诊2楼，行政办公区综合采购办公室，本着自愿原则，逾期视为放弃！不接收快递报价文件。若本次询价仍不足三家，将转为竞争性谈判或其他方法确定供应商

## 联系方式：综合采购办：0556-6197331 信息工程科：0556-6197366

**桐城市人民医院**

**2025年08月1日**