**长沙市中心医院信息安全等级保护测评服务要求**

**一、项目背景**

长沙市中心医院是在市委市政府领导下的综合性三级甲等医院。医院已备案的三级信息系统五个，分别是HIS系统、EMR系统、LIS系统、PACS系统、互联网医院，本次计划对这五个系统进行信息安全等级保护测评。

### 二、测评范围

|  |  |  |  |
| --- | --- | --- | --- |
| 服务名称 | 系统名称 | 系统级别 | 数量 |
| 信息系统安全等级保护测评 | LIS系统 | 三级 | 1 |
| PACS系统 | 三级 | 1 |
| EMR系统 | 三级 | 1 |
| HIS系统 | 三级 | 1 |
| 互联网医院 | 三级 | 1 |

### 三、测评目标

根据《GB/T 22239—2019信息安全技术 网络安全等级保护基本要求》等标准组织开展信息系统等级保护符合性测评，衡量系统的安全保护管理措施和技术措施是否符合等级保护基本要求（三级），是否具备了相应的安全保护能力，判断现有的安全保护水平与国家信息安全等级保护管理规范和技术标准要求项之间的符合情况。通过对信息系统进行整体、全面、公正的评估，对不符合项进行风险分析，编写信息安全等级保护测评报告，以帮助和促进被测评信息系统达到国家规定的信息安全要求。

### 四、评估标准

竞价人应依据国家相关政策标准开展工作，依据标准包括但不限于如下国家政策标准：

1. 《信息安全等级保护管理办法》（公通字[2007]43号）
2. 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）
3. 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）
4. 关于进一步推进全省信息安全等级保护工作的函（湘公函[2011]21号）
5. 关于对全省重要信息系统开展信息安全等级保护专项检查工作的函（湘公函[2011]74号）
6. GB/T 22240-2016《信息安全技术信息系统安全等级保护定级指南》
7. GB/T 20269-2006《信息安全技术 信息系统安全管理要求》
8. GB/T 22239-2019《信息安全技术 网络安全保护等级基本要求》
9. GB/T 25058-2019《信息安全技术 网络安全保护等级实施指南》
10. GB/T 25070-2019《信息安全技术 网络等级保护安全设计技术要求》
11. GB/T 28448-2012《信息安全技术 信息系统安全等级保护测评要求》
12. GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》

### 五、测评原则

1. 规范性原则：严格遵循国家、行业相关规范、标准开展工作。
2. 最小影响原则：做好风险预防措施，尽可能避免对网络和信息系统造成影响；测评人员应该仅以发现系统安全漏洞为目的，不得采取对被测系统带有破坏性的信息安全测试。
3. 公平公正原则：按照统一标准开展等级保护测评工作，确保等级保护测评工作能够客观、真实地反应各被测系统网络安全等级保护现状。

### 六、测评内容

1. 对系统进行安全现状测评，以找出系统与相应等级基本要求之间的差距，明确系统安全运行现状。
2. 进行系统安全等级测评，包括安全物理环境、安全区域边界、安全通信网络、安全计算环境、安全管理中心等内容、安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等内容，以确保系统在其相应等级保护要求下运行。
3. 参照《GBT22239-2019信息安全技术网络安全等级保护基本要求》、《GBT25070-2019信息安全技术网络安全等级保护安全设计技术要求》、《GBT28448-2019信息安全技术网络安全等级保护测评要求》等相关规范，对信息系统进行等级测评，找出系统与国家标准要求之间的差距，对存在的风险进行评估，并出具公安部门认可的《信息安全等级测评报告》和《渗透测试报告》。

**七、技术服务要求**

1. 本次等级测评应满足的原则

保密原则：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，不得利用此数据进行任何侵害招标人的行为，否则招标人有权追究竞价人的责任。

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：测评工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

可控性原则：测评服务根据进度表进行安排，保证测评工作的进度可控。

整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的的正常运行、业务的正常开展产生任何影响。

竞价人应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

1. 本次等级测评的整体要求

竞价人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

竞价人应详细描述测评人员的组成、资质及各自职责的划分。竞价人应配置有测评资质的专业人员进行本次信息安全等级保护测评工作。

本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件由竞价人推荐，经招标人确认后由竞价人提供并在信息系统等级保护测评中使用。

竞价人使用的漏洞扫描工具应具有以下风险发现功能：风险管理、基线检查、Websell检查、二进制后门、病毒扫描、补丁扫描、漏洞扫描、弱口令扫描。

**八、项目成果要求**

测评完成后，竞价人须提交包括但不限于以下成果：

1. 《信息系统安全等级保护测评报告》：描述被测评系统的信息安全现状，找出存在的安全隐患，描述系统安全防护措施与国家标准要求之间的差距，对存在的漏洞进行风险分析，最后提出整改建议。
2. 《渗透测试报告》：针对等级保护测评过程中发现的安全问题，进行远程渗透性技术验证测试。
3. 上述报告作为验收依据。
4. **其它要求**
5. 竞价人须采取有效管理措施，确保被测评系统在测评期间的安全管理，切实防止测评人员在被测评系统中种植木马、病毒等危害性程序，防止发生测评人员非法获取、删改被测评系统数据等安全事件。相应安全管理措施须写入竞价文件中。
6. 中标人中标后不得转包、分包。
7. 中标人须配合医院在重要检查和大型活动时，提供现场信息安全技术支持。
8. 要求竞价人是《全国网络安全等级测评与检测评估机构目录》中的服务单位，并提供网上（www.djbh.net）查询的证明材料。
9. 要求项目负责人必须具备高级网络安全等级测评师资格，提供证书复印件及负责人的社保证明。
10. 业绩要求中标人近三年中标过三级甲等医疗机构等级评测项目。
11. 组织信息科工作人员进行一次专业信息安全培训，在在等级保护测评之外根据院方要求至少提供一次漏洞扫描、一次渗透测试服务，并提供相应的测试报告。
12. 针对重大信息安全突发事件提供应急响应服务，保障1小时内安全应急人员到场，迅速确定事件原因，缩小事件影响，遏制事态发展，快速恢复系统运维，并提交应急响应报告。
13. 提供4次安全巡检服务，根据院方时间安排进行。
14. 为院方护网行动提供技术支持服务。
15. **付款方式**

★按照上述要求完成测评并验收合格后，支付合同总金额的90%，余款10%自验收合格之日起1年后无息付清（无售后服务问题）。