马鞍山市中医院信息系统等保测评内容及相关要求

1. **采购预算**

预算金额（人民币）： 14 万元；最高限价（人民币）： 13.3 万元。

1. **采购内容及相关要求**

 **（一）采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评系统名称 | 定级情况 | 预算单价（万元） |
| 1 | 医院综合医疗管理系统 | 三级 | 7 |
| 2 | 互联网医院综合医疗运营管理平台 | 三级 | 7 |
| 合计 |  |  | 14 |

**（二）服务内容**

**1.项目简介**

**1.1项目背景**

网络安全等级保护是我国关于信息安全的基本政策，《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发(2003) 27号）明确要求我国信息安全保障工作实行等级保护制度。2007年6月发布的关于印发《信息安全等级保护管理办法》的通知(公通字(2007)43号）进一步强调了开展网络安全等级保护工作的重要意义，规定了实施网络安全等级保护制度的原则、内容、职责分工、基本要求和实施计划，确立了实施网络安全等级保护工作的操作办法。

2017年6月国家颁布实施《中华人民共和国网络安全法》，进一步明确，国家实行网络安全等级保护制度，正式将网络安全等级保护制度写进国家法律，从法治层面推动网络安全等级保护制度的落实。

**1.2项目概述**

为深入贯彻落实习近平总书记关于网络安全工作的重要指示精神和《网络安全法》规定，根据网信办、公安部、上级主管部门关于网络安全的指示要求，我单位将委托第三方有测评资质的测评机构，对马鞍山市中医院按照等级保护基本要求开展网络安全等级保护测评，出具相应的测评报告。

**1.3.项目目标**

通过网络安全等级保护测评，全面了解和掌握马鞍山市中医院的安全保护状况，找出其与《网络安全等级保护基本要求》对应级别的差距。同时从风险管理角度，运用科学的方法和手段，系统地分析被测系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护策略和整改措施，为防范和化解网络安全风险、最大限度地防止由于网络安全事件引发公共安全事故以及全面提升单位网络安全防护水平提供科学依据。

**2.项目实施**

**2.1实施依据**

本次项目实施，主要遵循以下国家标准：

《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

**2.2实施原则**

（1）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中标人的责任。

（2）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。

（3）规范性原则：中标人的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。

（4）可控性原则：测评服务的进度要跟上进度表的安排，保证招标人对于测评工作的可控性。

（5）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。

（6）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正常运行、业务的正常开展产生任何影响。

**2.3实施范围**

本次项目主要对以下系统，按照已定级标准，开展网络安全等级保护测评：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评系统名称 | 定级情况 | 简要说明 |
| 1 | 医院综合医疗管理系统 | 三级 |  |
| 2 | 互联网医院综合医疗运营管理平台 | 三级 |  |

**2.4实施内容**

对已定级备案的系统进行十个安全层面的网络安全等级保护测评（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）。

测评包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

安全控制测评使用测评单元方式组织，分为安全技术测评和安全管理测评两大类。安全技术测评包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个层面上的安全控制测评；安全管理测评包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的安全控制测评。具体见下图2.1：



图2.1 网络安全等级保护测评框架

**3.过程控制**

网络安全等级保护测评分为测评准备、方案编制、现场测评、分析与报告编制四个阶段，各阶段主要工作如下：

**3.1测评准备阶段**

主要包括以下工作内容：

测评项目组组建：明确项目经理、测评人员及职责分工。

项目计划书编制：项目计划书包含项目概述、工作依据、技术思路、工作内容和项目组织等。

信息系统调研：通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，明确被测系统的范围（特别是信息系统的边界），了解被测系统的详细构成，包括网络拓扑、业务应用、业务流程、设备信息（服务器、数据库、网络设备、安全设备、数据库等）、管理制度等。

工具和表单准备：根据被测系统的实际情况，准备测评工具和各类测评表单。

输出文档：《项目计划书》、《系统调研表》、《工具清单》、各类表单。

**3.2方案编制阶段**

主要包括以下工作内容：

测评对象确定：根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，确定出本次测评的测评对象。

测评指标确定：根据已经了解到的被测系统定级结果，确定出本次测评的测评指标。

测评工具接入点确定：确定需要进行工具测试的测评对象，选择测试路径，根据测试路径确定测试工具的接入点。

测评内容确定：确定现场测评的具体实施内容，即单元测评内容。

测评实施手册开发：编制测评实施手册，详细描述现场测评的工具、方法和操作步骤等，具体指导测评人员如何进行测评活动。

输出文档：《测评方案》、《测评指导书》。

**3.3现场测评阶段**

现场测评主要指单项测评，分别从技术上的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心和管理上的安全管理机构、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分别进行。

安全物理环境：通过人员访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况。主要涉及对象为物理基础设施。在内容上，安全物理环境层面测评实施过程涉及10个测评单元，包括：物理位置选择、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。

安全通信网络：通过访人员访谈、配置检查和工具测试的方式测评信息系统的网络通信安全保障情况。主要涉及对象为网络整体架构、网络拓扑结构、通信传输方式等。在内容上，安全通信网络层面测评实施过程涉及3个测评单元，包括：网络架构、通信传输、可信验证。

1. **商务要求**

1、进场时间：成交供应商自合同签订之日起15日内完成测评工作，提交测评报告并通过验收。

2、服务期限：自合同签订之日起1年内。

3、服务地点：马鞍山市中医院（招标人指定地点）。

4、付款方式：成交供应商完成测评并出具马鞍山市中医院综合医疗管理系统、互联网医院综合医疗运营管理平台评测报告后，采购人在30日内按合同支付费用。

5、本项目投标人特定资格要求：投标人持有《网络安全等级测评与检测评估机构服务认证证书》（证书在有效期内），且未被主管部门暂停业务或处于整改期内。

6、服务规范：有国家标准的执行国家标准；无国家标准的执行行业标准；无行业标准的执行地方标准；无地方标准的执行企业标准。

7、中标人在项目实施过程中，国家对相关项目有资质要求的，进场单位和人员的资质、资格符合国家、省、市有关规定。实施期间中标人所发生的或中标人实施场地内发生的或中标人原因造成的安全事故，均应由中标人负责按有关规定处理善后事宜，并承担给采购人造成的损失。

8、投标文件中为本项目配备的人员力量，在合同履行期间，中标人须按采购人要求到达本项目现场提供相应服务，否则采购人有权解除采购合同。

9、服务响应时间：中标人需设有专门的服务队伍，建立完备的响应机制。如出现服务问题，电话响应无法解决，中标人必须在接到电话2小时内到达现场，4小时内解决问题。

10、验收：

10.1采购人和相关部门按照招标文件和招标响应文件进行验收。招标文件没有规定和招标响应文件没有相应承诺的，按照下列原则进行验收：有国家标准的按照国家标准验收，没有国家标准的按行业标准验收，无行业标准的按地方或企业标准验收，成交投标人予以配合。涉及需要由其他相关行业主管部门验收的项目，采购人须约请相关部门和专家参加项目验收。

10.2采购人及相关行业主管部门对项目进行全面的验收，对验收中暴露出来的问题，成交投标人应及时进行整改，整改后仍达不到验收标准的，采购人有权取消成交投标人资格。

11、本项目总投标价包含了交付使用前的全部费用及所有价内价外税金及合理利润等，不再产生任何二次费用。