附件1：

马鞍市中医院信息系统三级等级保护评测项目采购内容及相关要求

一、采购预算

项目预算（人民币）：14万元；

最高限价（人民币）：14万元。

二、采购内容及相关要求

**（一）采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目名称** | **项目内容** | **单位** | **预算单价（万元）** | **预算数量** | **预算金额（万元）** |
| 马鞍山市中医院信息系统三级等级保护评测项目 | 医院综合医疗管理系统等级评测 | 次 | 7万元 | 1 | 7万元 |
| 互联网医院综合医疗运营管理平台 | 次 | 7万元 | 1 | 7万元 |

**（二）技术要求**

**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，对马鞍山市中医院的信息系统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**

通过信息系统三级等级保护测评，全面了解和掌握马鞍山市中医院的信息系统的安全保护状况，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，开展信息系统三级等级保护测评：

|  |  |  |  |
| --- | --- | --- | --- |
| **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。

安全区域边界：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边界安全保障情况。主要涉及对象为网络边界互连设备、网络边界安全设备以及安全控制策略等。在内容上，安全区域边界层面测评实施过程涉及6个测评单元，包括：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。

安全计算环境：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边界安全保障情况。主要涉及对象为网络设备、安全设备、主机、数据库以及应用系统等。在内容上，安全计算环境层面测评实施过程涉及11个测评单元，包括：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、个人信息保护等。

安全管理中心：通过访人员访谈、配置检查的方式测评信息系统的集中安全管理保障情况。主要涉及对象为系统各类安全审计系统、综合网管系统、网络拓扑以及集中安全管理功能系统等。在内容上，安全管理中心层面测评实施过程涉及4个测评单元，包括：系统管理、审计管理、安全管理、集中管控等。

安全管理制度：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安全管理制度情况。在内容上，安全管理制度方面测评实施过程涉及4个测评单元，包括：安全策略、管理制度、制定和发布、评审和修订。

安全管理机构：通过人员访谈、文档审查的方式测评信息系统的安全管理机构情况。在内容上，安全管理机构方面测评实施过程涉及5个测评单元，包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

安全管理人员：通过人员访谈、文档审查的方式测评信息系统的人员安全管理情况。在内容上，安全管理人员方面测评实施过程涉及4个测评单元，包括：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。

安全建设管理：通过人员访谈、文档审查的方式测评信息系统的系统建设管理情况。在内容上，安全建设管理方面测评实施过程涉及10个测评单元，包括：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、服务供应商选择。

安全运维管理：通过人员访谈、文档审查的方式测评信息系统的系统运维管理情况。在内容上，安全运维管理方面测评实施过程涉及14个测评单元，包括：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。

输出文档：现场测评结果记录。

**3.4分析与报告编制阶段**

主要包括以下工作内容：

单项测评结果分析：针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据。

单元测评结果判定：将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。

整体测评：针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。

风险分析：据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。

等级测评结论形成：在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。

测评报告编制：根据等级测评结论，编制测评报告，包括概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等。

输出文档：《等级测评报告》。

**3.5交付成果**

本项目输出的主要工作产品中，交付给采购单位的主要有：

|  |  |  |
| --- | --- | --- |
| 阶段名称 | 任务名称 | 输出文档 |
| 准备阶段 | 项目计划 | / |
| 系统调研分析 | / |
| 方案编制阶段 | 测评方案制定与确认 | 测评方案 |
| 测评阶段 | 现场实施 | / |
| 整改复核 |
| 报告编制阶段 | 测评报告的编制与评审 | 等级保护测评报告 |

**4.项目管理**

为确保本项目顺利开展，要求测评机构结合本项目实际，组建适宜项目组，负责项目的具体推动落实。

**4.1人员要求**

成交供应商为本项目配备的项目组成员**不少于3名**，项目组成员应与响应文件中配备人员一致，未经采购人同意，中途不得更换。

**4.2质量要求**

测评机构应具有运行良好的质量管理体系，同时为本项目配备质量经理，加强项目测评过程中的质量管理控制，确保项目按照相关标准实施。

配备的质量经理应具有丰富管理经验及管理能力。

**4.3进度要求**

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。

**4.4风险控制**

测评机构应具有良好的保密机制，确保测评过程获悉的相关资料不被泄露。此外，为确保测评过程的风险可控，测评机构应针对测评过程可能出现的风险，编制风险规避措施，将可能的损失降到最低。

**4.5测评工具**

本次测评过程中使用的测评工具需满足三级系统等级保护测评所需，至少包括系统漏洞检查工具、网站安全检查工具、主机病毒检查工具、主机木马检查工具等工具。优先选择经公安部门认可推荐的测评工具。

工具接入系统前，需经被测单位认可同意后，方可接入系统。

**5.项目验收**

完成信息系统三级等级保护测评工作，测评单位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，由采购人确认并验收。

**6.其他要求**

（1）本项目总报价包含了履行合同所有内容的全部费用，包括人工费（含社会保险费和住房公积金）、餐费、办公费、交通费、服务费、技术服务费、仪器设备使用费（含耗材）、采购代理服务费、人工费、资料费、打印费、保险费其他费用（如编写费、资料费）以及供应商认为完成本项目所需要的其他费用及所有价内价外税金及合理利润等。

（2）成交供应商服务不能满足招标文件要求的，采购人有权解除合同，不予退还履约保证金，并按有关规定进行处理。

（3）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。

三、投标人资质要求

1、具备《中华人民共和国政府采购法》第22条规定的条件。

2、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。

3、投标人应具有二级与三级系统等级保护测评所需的测试工具和技术手段。

4、在本项目实施期间，未经用户同意，中途不得更换人员。

5、本项目不接受联合体投标，不允许转包、分包。

6、投标人须符合下列情形之一（不良行为记录以《马鞍山市公共资源交易主体不良行为信息处理暂行办法》（马公管〔2016〕35号）为准）：

（1）开标日前两年内未被马鞍山市、县公共资源交易监督管理部门记不良行为记录或记不良行为记录累计未满5分的。

（2）最近一次被马鞍山市、县公共资源交易监督管理部门记不良行为记录累计记分达5分到9分(含9分)且公布日距日超过3个月。

（3）最近一次被马鞍山市、县公共资源交易监督管理部门记不良行为记录累计记分达10分到19分(含19分)且公布日距开标日超过6个月。

（4）最近一次被马鞍山市、县公共资源交易监督管理部门记不良行为记录累计记分达20分到29分(含29分)且公布日距开标日超过12个月。

（5）最近一次被马鞍山市、县公共资源交易监督管理部门记不良行为记录累计记分30分以上(含30分)且公布日距开标日超过24个月。