**招标要求**

**项目名称：南京鼓楼医院集团仪征医院网络安全等级保护测评服务项目**

**南京鼓楼医院集团仪征医院**

**二○二二年九月**

# 第一部分投标人须知

**前附表**

|  |  |
| --- | --- |
| **序号** | **内容** |
| 1 | 项目全称：南京鼓楼医院集团仪征医院网络安全等级保护测评采购项目 |
| 2 | 招标人全称：南京鼓楼医院集团仪征医院招标人地址：仪征市仪化生活区环南路1号 |
| 3 | 采购方式：公开招标 |
| 4 | 评分标准：综合评分法 |
| 5 | 标书制作要求：编制一式三份响应文件（包括一份正本和两份副本），每份响应文件必须清楚标明“正本”或“副本”字样。一旦正本和副本不符，以正本为准。 |
| 6 | 招标范围：等级保护测评服务 |
| 7 | 施工总工期：30日历天，具体开竣工时间以发包人书面通知为准。计划开工时间：2022年9月；计划竣工时间：2022年10月。 |
| 8 | 投标截止时间：2022年9月13日09:00投标文件递交地点：南京鼓楼医院集团仪征医院信息部各投标单位可将投标文件邮寄至递交地点。也可在开标截止时间前带至开标现场。 |
| 10 | 开标时间：2022年9月13日09:00 |
| 11 | 评标时间：2022年9月13日09:00 |
| 12 | 招标联系人：南京鼓楼医院集团仪征医院 顾皓 联系电话：18260650800 |
| 13 | 投标人提疑截止时间：2022年9月13日09:00 |
| 14 | 招标人答疑截至时间：2022年9月13日09:00 |

1. **投标人的资格要求**

1、满足《中华人民共和国政府采购法》第二十二条规定：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

2、落实政府采购政策需满足的资格要求：无

3、本项目的特定资格要求：无

4、本项目不接受联合招标。

**二、项目进度要求**

本项目要求在签订合同后30日内完成。

**三、文档资料管理要求**

文档是保证项目的实施连贯性的重要保证，报价人需要按管理规范提供完善的文档，并对项目进行过程中的文档进行有效的管理。

**四、实施要求**

中标单位必须在签订合同后3个工作日内安排项目组进场，对本项目信息系统、网站开展调研工作，调研内容包括测评系统情况、安全运维现状和已有规范标准等，调研方案需经采购人确认通过后才能开展测评工作。

在项目实施过程中，中标测评机构如需采购人配合，要详细描述需要配合的内容。

本项目中可能需要的软硬件平台（如笔记本电脑、测试软件等）均由中标测评机构提供。中标测评机构在服务期内未经采购人许可不得使用任何未经确认的存储设备对测评数据进行复制。中标测评机构必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件的可用性和可靠性。由此产生的一切责任由中标测评机构承担。

现场测评人员应严格遵守甲方制定的规章制度，遵守机房和信息安全管理制度。因安全测评疏忽所造成的安全事故，中标单位应该承担相应责任。

**五、报价要求**

所有报价均以人民币报价，总报价响应包括但不限于上述采购需求包含的所有人工、保险、劳保、交通、加班、培训、会议、管理、设备、耗材、税费等费用及为完成整个项目所产生的其它所有费用，以及政策性文件规定及合同包含的所有风险、责任等各项应有费用。招标文件未列明，而投标人认为其他必需的费用也需列入报价。在合同实施时，采购人将不予支付中标人没有填列的项目费用，并认为此项目的费用已包括在投标价格中。

**六、资格证明文件**

1、企业法人营业执照（复印件）

2、税务登记证（复印件）

3、法人代表授权书（原件）

**七、付款方式**

具体付款方式如下：签订合同后，相关人员开始进场施工，甲方需根据合同缴纳首付款（合同总价30%）；实施及培训完成且验收合格后支付合同总价60%，验收合格一年后支付合同总价10%。

**八、谈判方式**

院方在对报价人的品牌、实力、信誉、价格、业绩、性能及服务等综合因素进行综合评定确定报价人排名，优先选择第一名，其余作为备选对象。对未被选中报价人，院方将不作任何解释。

**九、其他说明**

谈判文件是合同不可分割的一部分，参与谈判即视为对本邀请文件要求的接受。请报价人务必认真阅读本文件，严格遵照谈判文件内容，谈判文件不符合要求的即视为无效文件。

# 第二部分项目需求

**一、采购项目简要说明**

南京鼓楼医院集团仪征医院为贯彻落实《中华人民共和国网络安全法》，根据信息网络安全等级保护工作要求，拟通过购买服务的形式委托第三方专业机构，对本单位信息系统、网站开展等保测评工作，提升网络安全防护水平，确保安全高效稳定运行。

**二、项目对象及目标**

1、项目对象

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 备案等级 |
| 1 | 南京鼓楼医院集团仪征医院信息系统 | 三级 |
| 2 | 南京鼓楼医院集团仪征医院信息网站 | 二级 |

2、委托具备资质的第三方信息安全等级测评机构（以下简称测评机构）对信息系统、网站开展等级保护测评，查找与分析现有系统安全防护的不足。

3、根据等保测评成果，由测评机构提出合理可行的安全整改建议，协助采购人进行相关整改工作，整改后的系统达到对应的等级保护的要求和标准。

**三、项目原则**

1、客观公正原则：测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案开展。

2、保密原则：在测评过程中，需严格遵循保密原则，双方签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害采购人利益。

3、最小影响原则：测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应提前做出说明并经采购人同意后组织实施。

4、规范性原则：信息安全等级保护测评服务的实施必须由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

5、质量保障原则：在整个测评过程中，高度重视项目质量管理。项目的实施严格按照项目实施方案和流程进行，并由项目协调小组开展监督，控制项目的进度和质量。

6、系统安全原则：测评机构工作人员需遵守等保检测规定，采用符合标准的检测工具和检测方法实施检测，如因违规操作造成被检测信息系统受损，则测评机构承担相应责任和损失。

7、测评师规范原则：测评机构工作人员必须通过公安部的等级保护等级测评师认证，持证上岗，经项目委托方确认资格后方可实施检测。

**四、技术要求和规范**

《中华人民共和国网络安全法》

《关于加强党政机关计算机信息系统安全和保密管理的若干规定》

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)

《信息安全等级保护管理办法》(公通字[2007]43号)

《信息系统安全保护等级定级指南》（GB/T 22240-2008）

《信息系统安全等级保护基本要求》（GB/T 22239-2008）

《信息系统安全等级保护测评要求》

《信息系统安全等级保护测评过程指南》

《信息系统安全管理测评》（GA/T 713-2007）

《信息安全等级保护等级测评实施细则》

《信息安全风险检查规范》（GB/T 20984-2007）

《信息安全风险管理指南》（GB/Z 24364-2009）

《信息安全管理体系要求》（GB/T 22080-2008）

《信息安全管理实用规则》（GB/T 22081-2008）

《信息系统安全管理要求》（GB/T 20269-2006）

《信息安全事件分类分级指南》（GB/Z 20986-2007）

《信息安全事件管理指南》（GB/Z 20985-2007）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全应急响应计划规范》（GB/T 24363-2009）

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

《江苏省电子政务外网建设规范》（DB32/T 3514.1-2019）

以及本项目完成前国家、省对信息系统等级保护的最新规范和要求。

**五、服务内容**

（一）等级保护测评。中标测评机构依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）对本项目信息系统进行信息收集和测评分析，对测评对象的现状作记录，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；按照用户系统现状对应的管理要求进行测评分析，对测评对象的现状作记录，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。

1、识别信息安全风险。通过对信息系统在安全技术和安全管理方面的分析，发现信息系统在安全技术和安全管理方面与相应安全等级保护要求之间的差距，并进行风险分析，出具差距分析报告，明确信息系统面临的风险。

2、增强安全防护能力。依据差距分析报告的结果，并结合实际情况，区分轻重缓急，制定针对性的安全整改计划，通过安全整改不断提高信息系统的整体安全保护水平。

3、测评结果分析

（1）单项测评结果判定

（2）单元测评结果判定

（3）整体测评分析

（4）形成测评分析报告

（5）针对测评分析报告的整改建议

（二）渗透测试

选取可能发起攻击的测试点，使用渗透测试的方式查找可能存在的渗透点,发现信息系统防护体系的薄弱环节，找出可能发生的恶意攻击事件和违规行为。

1、渗透测试内容

* 工作内容包括渗透测试及提供漏洞修复方案。
* 本次渗透测试工作为黑盒测试。

2、需要包含如下阶段

* 前期交互阶段：与用户组织进行讨论，确定渗透测试范围和目标。
* 信息搜集阶段：采用各种方法搜集用户方的所有相关信息。
* 威胁建模阶段：使用在信息搜集阶段所获取到的信息，标识出目标系统上可能存在的安全漏洞与弱点。
* 漏洞分析阶段：综合前面几个环节获取到的信息，从中分析和理解，找出攻击途径和攻击方法。
* 渗透攻击阶段：针对确定好的攻击途径和攻击方法实施渗透攻击，获取系统相关权限。
* 后渗透攻击阶段：以特定的业务系统作为目标，识别出关键的基础设施，找出用户组织最具价值和尝试进行安全保护的信息和资产，找出能够对用户组织造成重要业务影响的攻击途径。
* 报告阶段：将渗透测试结果编制成文档提交给用户，提供安全解决方案。并将在渗透测试阶段产生的垃圾数据进行清理。

3、渗透测试要求。渗透攻击测试工作以不破坏用户应用系统为前提条件，不做危害用户应用系统的工作行为，遵守职业道德，遵守行业规则，严格遵守保密制度，保密要求，不得擅自修改、拷贝用户数据，不得泄露、传播用户的敏感信息，如有违反将负法律责任。

（三）信息安全风险检查

对本项目信息系统实施风险检查服务，明确信息系统存在的问题和不足，主要包括：

1、对信息系统相关的资产进行调查梳理，分析资产重要性及安全需求。

2、识别对信息系统构成潜在破坏的威胁，通过过去的事件报告记录、入侵检测系统获取的统计数据和近几年国际机构发布的对于整个社会或特定行业安全威胁发生概率的统计数据，分析威胁发生的可能性和破坏的影响程度。

3、检查信息系统在物理环境、组织、过程、人员、管理、配置、硬件、软件、信息等技术和管理两方面存在的安全问题，通过但不限于实地勘察、人员访谈、工具扫描、手动检查、文档审查等方式分析安全问题的严重程度。

4、检查但不限于防火墙、入侵检测、交换机等网络设备的安全配置、操作系统、数据库安全功能、应用软件安全功能验证，分析已有安全措施有效性。

5、在完成了上述资产识别、威胁识别、脆弱性识别、以及对已有安全措施确认后，按照标准要求对风险检查要素做关联分析，计算安全事件发生的可能性以及发生后的损失，给出风险分析结论，划分风险优先处理等级，确定可接受风险与不可接受风险，给出风险处置建议，出具风险检查报告。

（四）安全整改服务

1、安全整改技术服务。在等保测评和风险检查完成后，测评机构提供安全整改技术服务，协助采购人开展安全整改。采购人完成整改后，测评机构为采购人提供整改复查，直至符合整改要求。

（1）协助采购人建立信息安全等级保护管理体系。根据信息安全技术网络安全等级保护标准要求，结合《差距测评报告》提出的安全管理体系与等级保护基本要求之间的差距，在信息安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面指导并协助建立健全符合相应等级要求的安全管理制度。

（2）协助采购人对本项目信息系统开展安全等级保护安全技术整改。根据信息安全技术网络安全等级保护标准要求，结合《差距测评报告》提出的安全防护现状与等级保护基本要求之间的差距，综合重要信息系统的特点，明确安全需求，设计符合相应等级要求的信息系统安全技术建设整改方案，协助开展信息安全等级保护安全技术措施建设，落实符合信息安全技术网络安全等级保护标准要求的措施。

（3）协助采购人对本项目信息系统的应用系统进行安全整改，完成开发安全管理规范的编制和建立完善的安全控制机制，包括：人员授权、软件需求风险检查、代码管理、版本发布等。

2、安全整改培训服务

中标测评机构依据测评分析成果以及国家、省对信息安全技术网络安全等级保护最新要求，协助采购人开展信息安全技术网络安全等级保护等网络安全方面的培训讲座，旨在通过培训让相关人员了解国家网络安全新动向、新趋势，理解如何进行等级测评，掌握常见的攻击手段及有效的防护措施。

**六、资料成果提交**

本项目的资料成果包括但不限于：

1、测评实施方案；

2、等保测评报告；

3、安全整改方案；

5、迎检服务台账、漏洞扫描报告、渗透测试报告；

**七、服务期限**

1、本项目完成等保测评时间为合同签订之日起30个日历天内。

2、本项目等保测评服务期为一年，覆盖安全整改服务时间。

**八、人员要求**

本项目采用项目经理负责制，除了项目经理之外，项目组至少由5名信息安全等级测评师（由公安部信息安全等级保护评估中心颁布）组成，项目组人员名单经采购人确认后，未经采购人确认同意不得随意更换。

**九、服务要求**

（1）中标单位必须在签订合同后3个工作日内安排项目组进场，对本项目信息系统开展调研工作，调研内容包括测评系统情况、安全运维现状和已有规范标准等，调研方案需经采购人确认通过后才能开展测评工作。

（2）在项目实施过程中，中标测评机构如需采购人配合，要详细描述需要配合的内容。

（3）本项目中可能需要的软硬件平台（如笔记本电脑、测试软件等）均由中标测评机构提供。中标测评机构在服务期内未经采购人许可不得使用任何未经确认的存储设备对测评数据进行复制。中标测评机构必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件的可用性和可靠性。由此产生的一切责任由中标测评机构承担。

（4）现场测评人员应严格遵守甲方制定的规章制度，遵守机房和信息安全管理制度。因安全测评疏忽所造成的安全事故，中标单位应该承担相应责任。

**第三部分谈判办法和确定原则**

1、本项目由甲方招标小组与报价人现场谈判确定最终报价，最终结果由医院领导研究确定。

2、报价表

**投标报价汇总表**

项目名称： 金额单位：人民币元

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评项目名称 | 金额 | 备注 |
| 1 | 南京鼓楼医院集团仪征医院信息系统 |  |  |
| 2 | 南京鼓楼医院集团仪征医院网站 |  |  |
|  | 合 计 |  |  |
| 投标总价（大写） 元 |

投标人：（盖章）

法定代表人或其授权法定代表人：（签字或盖章）

日期： 年 月 日

招标人备注：

1. 本次投标人的投标报价为固定报价, 该报价为完成本项目提供合格服务所需要的全部费用，包括测评费、服务费、资料费、管理费、利润、税收等。

2．投标报价包含价格风险等费用，中标后不因市场、相关政策及其它风险变化在结算时作任何调整。

3．投标人在清单中报价以人民币为单位。