**万载县人民医院信息系统网络安全等级保护测评服务项目**

#  询价采购文件

万载县人民医院就信息系统网络安全等级保护测评服务项目（项目编号：WZXRMYY-2025-0827) 进行询价采购，欢迎符合资质条件的供应商参加。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目内容 | 简要技术说明 | 数量 | 总预算金额（元） |
| 1 | 信息系统网络安全等级保护测评服务 | 三级等级保护测评。提交符合国家有关标准的评测报告，同时提供网络安全培训服务，网络安全应急响应服务等。 | 1项 | 45000 |
| 合 计 （大写） ：肆万伍仟圆整（¥:45000元） |

**注：响应供应商的报价须包含与本项目有关的一切费用。**

**1.1、响应人须具备的资格条件（资格审查）：**

**特别提醒：开标时响应人须提供下述有效证明材料的原件或复印件加盖鲜章用于资格审查，同时须将所有资格审查所需材料的复印件制作在响应文件内，否则将视为无效响应。**

**1.1、响应人须具备的资格条件（资格审查）：**

**1.1.1、**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。 特别提醒：依据赣财购〔2023〕8号文《江西省财政厅关于推行政府采购供应商资格信用承诺制的通知》，以上1-6项可提供江西省政府采购供应商资格信用承诺函（格式见《江西省政府采购供应商资格信用承诺函》），特别要求：（1）、公安部第三研究所认证发放的《网络安全等级测评与检测评估机构服务认证证书》；（2）、中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD)技术二级及以上支撑单位证书。其他材料需以彩色扫描件形式放入投标文件中，未按要求提供或者提供的资质证明材料不齐全的，其资格审查不通过 。

**1.1.2、**单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的采购活动；为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商不得参加该采购项目的采购活动，提交产品属于政府强制采购节能产品的，必须为询价公告发布之日前财政部、国家发展改革委公布节能产品政府采购清单最新一期的产品；

 **1.1.3、**供应商被“信用中国”网站列入失信被执行人和重大税收违法案件当事人名单的、被“中国政府采购网”网站列入政府采购严重违法失信行为记录名单（处罚期限尚未届满的），不得参与本项目的政府采购活动。

**1.2、评标方法和原则：**最低评标价法。即指响应文件满足询价文件全部实质性要求且报价最低的响应人为排名第一的成交候选人。报价相同的，采取随机抽取方式确定。

**1.3、询价文件获取：**有意向的供应商可通过万载县人民医院官网：http://ycxyyfywy.com/获取询价采购文件。

**1.4、响应文件递交截止及开标时间**：2025年9 月3 日 下午3：00整 （北京时间）；

开标地点：万载县人民医院行政楼一楼B06询价议价招采室；

**1.5、采购单位**：万载县人民医院 ；

 地址：宜春市万载县康乐街道大北关路95号；

联系人：唐海洋； 电话：18970524002

**1.6、采购方式**：院内询价采购

**1.7、招标公告期限**：自本采购公告发布之日起3个工作日。

**1.10、万载县人民医院纪检监察室电话：0795-8981429**

**1.11、采购信息发布、补充、变更、修改平台：**

万载县人民医院官网：http://ycxyyfywy.com/

本项目相关澄清、变更、修改、补充等事宜均在以上网站发布，不再电话通知，请各拟响应人密切关注。

万载县人民医院

2025年8月27日

一、项目基本情况：

项目名称：万载县人民医院信息系统网络安全等级保护测评服务项目

采购方式：院内询价采购

采购限价：45000元

二、采购需求：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务对象** | **服务内容** | **服务要求** |
| 1 | 万载县人民医院互联网医院平台 | 三级等级保护测评 | 提交符合国家有关标准的评测报告，同时提供网络安全培训服务,网络安全应急响应服务等 |

三、服务技术要求：

1、 信息系统等级保护测评

供应商需具有等保测评资质。遵照“GB/T 28448-2019”、“GB/T 28449-2018”、“GB/T22239-2019”等技术标准，从安全物理环境、安全通信网络、安全区域边界、计算和设备安全、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理等10个层面进行等保测评，并参考被测单位自身信息安全管理要求，从安全控制间、层面间、区域间和系统结构间的综合分析进行深入剖析，根据分析出的安全隐患和薄弱环节，找出信息系统与国家技术标准要求之间的差距。 完成定级、备案、测评工作。

合同签订后50天内交付成果：备案证明、等级保护测评报告。

2、应急响应支撑服务

为单位提供网络安全应急响应服务。网络安全应急响应服务：发生重大信息安全事件后应及时响应，响应时间不得超过一小时,对包括计算机运行在内的业务运行进行维持或恢复，安排具有信息系统安全资深人员和应急响应工作经验丰富技术人员完成实施工作，根据每次应急响应的情况，必要时提供软、硬件设备参与应急响应工作，并进行分析，出具《安全事件分析报告》。供应商必须具有中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）技术二级及以上支撑单位证书，且证书在有效期内，提供证书复印件。同时，尽可能地减少和控制住网络安全事件的损失，提供有效的响应和恢复指导，并努力防止安全事件的发生。

3、安全培训服务

对网络安全技术和网络安全保护意识等进行培训，分析最前沿的网络安全形势，了解网络安全技术、网络安全的入侵常见手法及防范的有效培训，提升单位全员安全意识，建立长效机制促使网络安全管理措施的落实到位。为单位提供单位全员网络安全培训，提高网络安全风险防范意识，每年不少于一次。

以上技术需求均需满足，不满足视为无效响应。

四、服务商资格条件：

1、在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）近三年没有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合规定条件的服务商；

2、在中华人民共和国境内合法注册，具有独立法人资格，符合国家法律规定，有能力提供相应服务的服务商；

3、具有公安部第三研究所认证发放的《网络安全等级测评与检测评估机构服务认证证书》。

4、具有中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）技术二级及以上支撑单位证书。

五、响应材料要求：

1、响应书。

2、营业执照（组织机构代码、税务登记证）复印件、法人身份证复印件。

3、法定代表人授权书。

4、公安部第三研究所认证发放的《网络安全等级测评与检测评估机构服务认证证书》。

5、中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）技术二级及以上支撑单位证书。

6、无重大违法记录声明函。

7、技术承诺函。

六、付款方式：交付备案证明付30%，交付等保测评报告付70%。