# 福建省肿瘤医院采购调研公告

**第一部分 须知前附表**

|  |  |
| --- | --- |
| **序号** | **主　　　要　　　 内　　　 容** |
| 1 | 项目名称： 等级保护安全测评及安全加固服务  |
| 2 | 调研报名时间： 2025 年 6 月 5日至 6 月 12 日 (节假日除外)8：00-12：00或14：30-17：30(北京时间）调研会时间： 2025 年 6 月 19日 9:00 |
| 3 | 投标文件正本壹份,副本壹份胶装并密封加盖投标人公章。文件未胶装将视为无效。 |
| 4 | 投标文件递交处：福建省肿瘤医院网络技术中心 |
| 5 | 上述时间、地点如有变动，以单位届时通知为准。 |
| 6 | 采购报名、采购调研等采购过程中有任何异议，可联系我院监督科室。电话：83660063-8407；83660063-8467。 |

地　址： 福建省福州市福马路420号

福建省肿瘤医院科研楼四楼网络技术中心

邮　编： 350014

报名联系电话： 0591-83660063-8822

联系人：钱工、金工

第二部分 具体要求

**一、采购内容**

|  |  |  |  |
| --- | --- | --- | --- |
| **合同包** | **名称** | **数量** | **预算（万元）** |
| **（一）** | 等级保护安全测评及安全加固服务 | 1项 | 80 |

**二、技术及服务要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **数量** | **技术参数要求** |
| 1 | 等级保护测评服务 | 1项 | 1.对医院重要信息系统（HIS、LIS、PACS、EMR、协同办公系统、移动APP、门户网站、互联网医疗及处方流转服务平台（含慢病管理）、福建省肿瘤登记信息直报平台、医院信息集成平台、病理质控与资料管理系统、分子病理质控管理系统）进行三级等级保护测评服务。2.测评内容覆盖安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度等方面的内容。3.由中标方委托具备等保测评资质的机构实施，最终正式测评报告需由机构盖章，并通过官方备案。4.服务期限自合同签订起1年，或测评完成，以先到为止。 |
| 2 | 网络安全运营服务 | 1项 | 1 等级保护咨询服务（1）对上述12个等保测评信息系统提供资产分析服务、风险评估服务、差距评估、安全加固服务、等保制度建设服务、辅助测评一站式服务。（2）交付成果包括：《信息系统基本情况调查表》、《等级保护安全评估与整改建议》、《等级保护安全管理制度汇编》等。（3）服务期限自合同签订起1年，或测评完成，以先到为止。2 网络安全运营服务对医院关键业务系统提供网络安全运营服务，服务内容包括：（1）安全评估服务(4次/年): 为信息系统的使用、管理部门开展信息安全等级保护提供依据，制定安全规划及开展安全建设提供安全决策支持。交付成果：《安全评估报告》4份1. 渗透测试服务(1次/年):针对目标系统开展黑客模拟攻击渗透测试服务，全面检测被测系统安全性;在网络攻防演练提供专业攻防人员和相关安全设备支持。

交付成果：《渗透测试报告》1份1. 应用安全检测服务(4次/年)：采用自动化检测工具和专业攻防人员全面检测Web应用程序安全，提供安全加固指导。

交付成果：《应用安全检测报告》 4份3.MS安全运营托管服务通过云端安全运营专家，面向医院提供7\*24小时互联网网络安全监控，对安全告警日志进行实时分析、研判、告警和提供处置建议。（1）云端安全监控：结合安全专家人工分析和处置，提供安全威胁分析和安全威胁情报服务，形成处置和整改建议。交付成果：每日安全简报。（2）威胁情报共享：云端安全运营管理平台可与医院安全运营管理平台交换恶意软件、攻击特征数据等数据，实现安全威胁情报实时共享，可与医院防火墙、Web应用防火墙等设备进行策略联动，实现网络安全告警微信小程序推送、自动封堵阻断。交付成果：按需提供《威胁情报更新记录》。（3）网站安全监控（全年）：对网站提供可用性、域名劫持、敏感词、弱口令、挂马、暗链等监控服务，覆盖主流网络运营商线路，提供7\*24小时值班，第一时间人工验证告警。交付成果：《网站安全监控报告》4份；1. 告警与处置服务：运营过程中根据发生的告警情况，进行分析和处置，同时给出设备策略等准确的优化与加固建议。

交付成果：《安全处置建议》。（5）服务期限自合同签订起1年。为保障安全服务实施质量，供应商拟投入的项目团队需至少包含1名项目经理，项目成员需具备中国网络安全审查技术与认证中心认证的信息安全保障人员工程师CISAW证书（安全集成专业级或以上）、注册渗透测试工程师（CISP-PTE）证书、网络安全应急管理能力证书。 |
| 3 | 安全加固服务 | 1项 | 1. 安全加固服务(4次/年)：根据安全评估和测试服务的结果，提供应用安全、操作系统安全、Web服务器（中间件）、数据库安全加固辅导服务。

交付成果：《安全加固报告》4份1. 安全培训服务(1次/年)：面向全院新员工讲座开展网络安全意识培训(一节课30-60分钟)，培训内容包含不限于以下方面：安全标准、政策法规解读，信息安全意识、信息安全发展方向，周期性安全服务报告解读，可定制培训内容。

交付成果：《安全培训PPT》1份1. 应急响应服务（按需提供）：当医院网络和信息系统遇到黑客攻击或网页篡改等恶性事件，提供7\*24小时电话响应或即时通讯或邮件等方式解疑答惑；远程支持无法解决时，提供30分钟内突发安全事件现场应急响应服务。

交付成果：按需提供《应急响应报告》。1. 服务时间为1年。
 |
| 4 | 网络安全审计系统扩容升级服务 | 1项 | 对现有无线区域的网络安全审计系统提供设备扩容升级服务并完成旧设备日志、用户账号信息迁移，升级后的设备性能满足以下要求：模块化设计，提供千兆电口、千兆SFP接口、扩展槽。适用带宽不小于1000M，网络吞吐量大小于8G，最大并发连接数不少于160万，每秒最大新建连接数不低于50000。 |

1. **其他要求：**

1.按照《网络安全法》、等级保护等相关要求进行规划和建设；符合《信息安全技术网络安全等级保护基本要求》GB/T22239-2019（三级）要求（下文简称：三级等保），并在三级等保测评中协助完成测评工作。

2.项目实施应尽可能小地影响系统和网络的正常运行，不能对现有网络的运行和业务的正常提供产生显著影响(包括系统性能明显下降、网络拥塞、服务中断等)；

3.对服务过程中的过程数据和结果数据严格保密，未经授权不泄露给任何单位和个人，不利用此数据进行任何侵害用户单位的行为。

1. **调研说明**

报名参加本次调研的供应商、厂家需提供如下相关资料。

1. 报名时请携带加盖公章的项目文件回执单、营业执照复印件、公司简介（可含提供设备彩页等）。

2、参与项目调研供应商代表的个人授权函（需加盖供应商公章）和身份证复印件。

3、分别提供“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（http://www.ccgp.gov.cn/search/cr/）信用记录查询截图，无不良记录并加盖公章（截图查询日期必须在该公告日期内）。

4、提供业绩清单及近3年省内同类项目中标书

5、本调研会的报价仅做为本项目公开招标的预算限价；不做参与投标的限制条件；

6、上述各参数将做为本项目招标的主要参数，不代表本项目公开招标的最终参数；

7、参加调研会的公司应准备PPT材料（含方案介绍、服务及集成能力、应用案例、报价等）、技术参数等材料，每公司讲解时间30分钟（含答疑10分钟）；同时上述材料须交予院方留档（发送邮件到wlb@fjzlhospital.com，并提供U盘留档）。

**项目文件回执单**

请有意向参与的公司在项目公示期内携带回执单至福建省肿瘤医院网络技术中心报名。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目名称 | 数量 | 品牌及型号 |
| 1 |   |   |  |
| 2 |   |   |  |

公司名称：

联系人：

联系电话：

公司盖章：

 福建省肿瘤医院

 年 月 日