**重庆医科大学附属口腔医院**

**需求询价公告**

**一、各供应商根据询价公告要求报价。**

**二、报价需按照后附要求格式报价，对技术要求响应情况进行逐条备注，如“无差异”或“有差异，差异是”。本次询价为确定预算需要，非正式采购，技术要求为初步要求，最终以正式发布招标公告的技术要求为准。**

**三、需求公告时间2025年5月12日至2025年5月16日17:30止**

**四、报价（需盖章PDF或图片电子版，按照后附报价格式要求）发送：[sjk806@163.com](mailto:sjk806@163.com)，报价邮件名称和文件名称需写上《XXXX公司重庆医科大学附属口腔医院XXXXXX报价表》。**

**五、重庆医科大学附属口腔医院,采购联系人：陈老师023-88860001,技术联系人:李老师023-88860177。**

**网络安全等级保护测评服务采购项目**

|  |  |
| --- | --- |
| 报价单位名称： | |
| 联系人： 联系电话： | |
| 报价产品**生产商**企业性质： （大型/中型/小型/微型） | |
| 报价： 元（总价，附分项报价表），报价需含货物、人工、培训、运输、税费等全部费用。 | |
| **项目服务技术及商务要求** | 响应情况 |
| 附后 |  |

**备注：供应商还需提供投标产品成交记录:合同扫描件/中标通知书扫描件/公示结果网络链接及截图均可,能从中看出投标产品型号配置等信息。**

**附件：**

## **第一篇 项目技术/服务要求**

## 一、采购项目一览表

|  |  |  |
| --- | --- | --- |
| **序号** | **名 称** | **数量/单位** |
| 1 | 重庆医科大学附属口腔医院医院信息系统HIS（包括HIS、LIS、PACS、EMR）（三级） | 1 |
| 2 | 互联网医院（包含互联网医院、微信挂号、包含OA、科研教学等）（三级） | 1 |
| 3 | 集成平台系统（三级） | 1 |

## 二、采购项目技术/服务要求

（一）项目依据

测评指标和对象选择须符合《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》标准的相关要求。本项目测评人员应依据测评目的和测评内容，选取、实施特定测评操作的方式方法。除按照现行国家和行业信息安全相关规定进行外，主要规范性文件依据有：

《中华人民共和国网络安全法》

《信息安全等级保护管理办法》（公通字〔2007〕43号）

《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）

《信息安全等级保护备案实施细则》

GB/T 22240-2008 《信息安全技术信息系统安全保护等级定级指南》；

GB/T 17859-1999 《计算机信息系统安全等级保护划分准则》；

GB/T 25058-2019 《信息安全技术信息系统安全等级保护实施指南》；

GB/T 28448-2019《信息安全技术信息系统安全等级保护测评要求》；

GB/T 28449-2019《信息安全技术信息系统安全等级保护测评过程指南》；

GB/T 25070-2019 《信息安全技术信息系统等级保护安全设计技术要求》；

GB/T 20271-2006 《信息安全技术信息系统通用安全技术要求》；

GB/T 20270-2006 《信息安全技术网络基础安全技术要求》；

GB/T 21052-2007 《信息安全技术信息系统物理安全技术要求》；

GB/T 20274 《信息安全技术信息系统安全保障评估框架》；

GB/T 20282-2006 《信息安全技术信息系统安全工程管理要求》；

GB/T 20269-2006 《信息安全技术信息系统安全管理要求》；

GB/T 20984-2007 《信息安全技术信息安全风险评估规范》；

本次需要测评的系统包括被测系统运行密不可分的物理环境、网络区域环境、安全计算环境、安全管理中心及安全管理制度等，最终形成《网络安全等级测评报告》（含基线检查报告，可单独输出）。具体内容包括：

|  |  |
| --- | --- |
| 序号 | 工作项目 |
| 安全物理环境 | |
| 1 | 物理位置选择 |
| 2 | 物理访问控制 |
| 3 | 防盗窃和防破坏 |
| 4 | 防雷击 |
| 5 | 防火 |
| 6 | 防水和防潮 |
| 7 | 防静电 |
| 8 | 温湿度控制 |
| 9 | 电力供应 |
| 10 | 电磁防护 |
| 安全通信网络 | |
| 11 | 网络架构 |
| 12 | 通信传输 |
| 13 | 可信验证 |
| 安全区域边界 | |
| 14 | 边界防护 |
| 15 | 访问控制 |
| 16 | 入侵防范 |
| 17 | 恶意代码和垃圾邮件防范 |
| 18 | 安全审计 |
| 19 | 可信验证 |
| 安全计算环境 | |
| 20 | 身份鉴别 |
| 21 | 访问控制 |
| 22 | 安全审计 |
| 23 | 入侵防范 |
| 24 | 恶意代码防范 |
| 25 | 可信验证 |
| 26 | 数据完整性 |
| 27 | 数据保密性 |
| 28 | 数据备份与恢复 |
| 29 | 剩余信息保护 |
| 30 | 个人信息保护 |
| 安全管理中心 | |
| 31 | 系统管理 |
| 32 | 审计管理 |
| 33 | 安全管理 |
| 34 | 集中管控 |
| 安全管理制度 | |
| 35 | 安全策略 |
| 36 | 管理制度 |
| 37 | 制定和发布 |
| 38 | 评审和修订 |
| 安全管理机构 | |
| 39 | 岗位设置 |
| 40 | 人员配备 |
| 41 | 授权和审批 |
| 42 | 沟通和合作 |
| 43 | 审核和检查 |
| 安全管理人员 | |
| 44 | 人员录用 |
| 45 | 人员离岗 |
| 46 | 安全意识教育和培训 |
| 47 | 外部人员访问管理 |
| 安全建设管理 | |
| 48 | 定级和备案 |
| 49 | 安全方案设计 |
| 50 | 产品采购和使用 |
| 51 | 自行软件开 |
| 52 | 外包软件开发 |
| 53 | 工程实施 |
| 54 | 测试验收 |
| 55 | 系统交付 |
| 56 | 等级测评 |
| 57 | 服务商供应商选择 |
| 安全运维管理 | |
| 58 | 环境管理 |
| 59 | 资产管理 |
| 60 | 介质管理 |
| 61 | 设备维护管理 |
| 62 | 漏洞和风险管理 |
| 63 | 网络和系统安全管理 |
| 64 | 恶意代码防范管理 |
| 65 | 配置管理 |
| 66 | 密码管理 |
| 67 | 变更管理 |
| 68 | 备份与恢复管理 |
| 69 | 安全事件处置 |
| 70 | 应急预案管理 |
| 71 | 外包运维管理 |

**五、实施要求**

1、测评指标和测评对象确定须符合国家标准《GB/T 22239-2019信息安全技术-网络安全等级保护基本要求》等相关标准的要求。测评中应严格按照GBT28449-2018《信息系统安全等级保护测评过程指南》标准的要求实施,加强人员及项目过程管控,明确风险隐患，确保各项工作高质量推进。

2、供应商应加强本项目资料的保密管控，与采购人签订《保密协议》。

3、在项目实施过程中，投标方应根据项目内容制定技术方案和时间计划，严格按照项目方案及计划开展工作，确保项目实施不影响系统的正常运行。

4、测评过程中应结合国家法律法规和政策方针为采购人提供网络安全规划和管理制度体系咨询服务，同时对被测系统涉及的配置调整、漏洞修复、安全加固等工作提供技术指导。

5、供应商必须为本项目成立等级保护测评小组，测评人员均具有公安部认证的测评师证书，持证上岗。测评小组至少3-4人构成，为保证项目实施质量，测评服务提供方应为本项目指定一名高级测评师为该项目负责人现场主持测评工作。供应商需具有应急服务团队（团队成员必须为供应商单位正式员工并具备信息安全相关专业资质和测评师资质），当发生突发网络安全公共事件时，能在1小时内派出技术团队到达现场协助处置突发事件，事件处置要求高级测评师现场参与。

6、在项目服务周期内，为招标人提供数据安全相关咨询服务，以满足招标人下一步数据安全合规工作的开展，以及落实国家数据安全协调机制相关工作要求和招标人数据安全保护义务。投标人需要具有相关服务能力并提供相应的证明材料（国家/省级数据安全协调机制办公室认定的第三方评估机构或相关国家或部委认可的数据安全服务机构）。

六、供应商特定资格要求：

1、供应商应为国家网络安全等级测评与检测评估机构（提供网络安全服务认证证书等级保护测评服务认证），并在公安部网络安全等级保护网（www.djbh.net）最新发布的全国网络安全等级测评与检测评估机构目录中在列。

2、供应商具备中国合格评定国家认可委员会颁发的检验机构认可证书（CNAS）或具备带（CNAS）标的ISO27001 认证证书且检验项目包含网络(信息)安全等级测评，认可的检验能力范围为“网络安全等级保护测评”。

# 第二篇 项目商务要求

## 一、交货期、交货地点及验收方式

1.1交货期

中标人应在采购合同签订后，根据采购人的通知前来测评,测试工期两个月。

1.2交货地点

交货地点：采购人指定地点。

1.3验收方式

1.3.1.服务内容与采购合同一致，达到合同及招投标规定的标准。

1.3.2.在规定时间内完成交货并验收，并经采购人确认。

1.3.3.投标人提供的服务未达到招标文件规定要求，且对采购人造成损失的，由投标人承担一切责任，并赔偿所造成的损失。

## 二、报价要求

2.1.本次报价须为人民币报价，包含：产品价、运输费（含装卸费）、保险费、安装费、调试费、售后服务费、税费、培训费等货到采购人指定地点的所有费用。

## 三、质量保证及售后服务

**3.1产品质量保证期**

3.1.1.投标人应明确承诺：其投标服务质量保证期达到 一 年。

**3.2.售后服务内容**

3.2.1、支撑保障服务，在测评年度内以及下一年测评前，在项目执行期间，中标的等保测评单位须配合用户单位开展重要信息安全专项检查及网络安全保障任务，按要求提供包括远程协助和现场支援在内的专业技术支持服务。（如发生安全事故，1小时到达事故现场）。提供医院新系统上线前的安全扫描服务。提供重大节假日或重大网络安全安保工作前的系统安全检测服务。

3.2.2、安全咨询服务，在测评年度内以及下一年测评前，结合国家法律法规和政策方针为采购人提供网络安全规划和管理制度体系咨询服务，同时对被测系统涉及的配置调整、漏洞修复、安全加固等工作提供技术指导，满足GBT22239-2019《信息安全技术-信息系统安全等级保护基本要求》等标准、规范的相关要求。同时，为招标人提供数据安全相关咨询服务，以满足招标人下一步数据安全合规工作的开展，以及落实国家数据安全协调机制相关工作要求和招标人数据安全保护义务。

3.2.3、安全培训，在测评年度内以及下一年测评前，提供一次网络安全等级保护相关的安全培训，参会人数由招标方自拟。

3.2.4、安全检测，在测评年度内以及下一年测评前，除等保测评报告外，免费提供一次以上所有系统的安全检测服务出扫描报告。

3.2.5、在项目服务周期内，为招标人提供数据安全相关咨询服务，以满足招标人下一步数据安全合规工作的开展，以及落实国家数据安全协调机制相关工作要求和招标人数据安全保护义务。

**3.3.备品备件及易损件**

中标人和制造商售后服务中，维修使用的备品备件及易损件应为原厂配件，未经采购人同意不得使用非原厂配件。

## 四、付款方式

项目通过采购人验收合格，并移交最终测评报告与发票后30个工作日内，采购人支付测评合同金额的95%；剩余5%自采购人签署验收报告之日起1年内中标人完成安全监测服务后，一次性付清。