**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2023年6月30日至2023年7月6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《 公司重医口腔医院 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023-88860176。

重医附属口腔医院信息系统安全等级保护测评服务

## **一、货物一览表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目内容** | 等级要求 | 服务次数 | **备注** |
| 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）等保测评 | 三级 | 1次 |  |
| 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次 |  |
| 3 | 集成平台系统 | 三级 | 1次 |  |

## **二、技术参数要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **参数要求** | **响应情况** |
|  | 2.1信息系统概况：  本次进行等级保护测评服务的为：医院信息系统（主要指HIS,包含LIS,PACS，EMR等）（三级）、互联网医院（主要指互联网医院，微信挂号、包含OA、科研教学等）（三级）、集成平台系统（三级）。  2.2 测评依据:  本项目信息安全等级保护测评目的和测评内容，必须与信息安全等级保护要求的基本安全控制要求相一致。内容按照GB/T 22239-2019《信息安全技术 信息系统安全等级保护基本要求》等国家相关标准进行测评，确保测评结论真实性。其他测评规范性文件还需参照：  《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》；  2.3测评内容:  安全保护等级为三级的，测评指标应包括GB/T 22239-2019“技术要求”中的3级通用指标类（G3），3级业务信息安全指标类（S3），3级系统服务安全指标类（A3），以及第3级“管理要求”中的全部指标类。从安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个技术层面和安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个管理层面，对重庆医科大学附属口腔医院HIS系统（主要指HIS,包含LIS,PACS，EMR等）、互联网医院（主要指互联网医院，微信挂号，包含OA、科研教学等）、集成平台系统行等级测评，找出系统安全保护现状与所定等级的保护要求之间的差距，分析差距可能导致的系统风险，给出等级测评结论并形成系统测评报告。  本次测评的详细测评指标情况，如下表1所示： |  |
|  | |  |  |  |  | | --- | --- | --- | --- | | 安全类别 | 安全层面 | 序号 | 测评指标 | | **技术安全** | **8.1.1 安全物理环境** | 1 | 8.1.1.1 物理位置选择 | | 2 | 8.1.1.2 物理访问控制 | | 3 | 8.1.1.3 防盗窃和防破坏 | | 4 | 8.1.1.4 防雷击 | | 5 | 8.1.1.5 防火 | | 6 | 8.1.1.6 防水和防潮 | | 7 | 8.1.1.7 防静电 | | 8 | 8.1.1.8 温湿度控制 | | 9 | 8.1.1.9 电力供应 | | 10 | 8.1.1.10 电磁防护 | | **8.1.2 安全通信网络** | 11 | 8.1.2.1 网络架构 | | 12 | 8.1.2.2 通信传输 | | 13 | 8.1.2.3 可信验证 | | **8.1.3 安全区域边界** | 14 | 8.1.3.1 边界防护 | | 15 | 8.1.3.2 访问控制 | | 16 | 8.1.3.3入侵防范 | | 17 | 8.1.3.4 恶意代码和垃圾邮件防范 | | 18 | 8.1.3.5 安全审计 | | 19 | 8.1.3.6 可信验证 | | **8.1.4 安全计算环境** | 20 | 8.1.4.1 身份鉴别 | | 21 | 8.1.4.2 访问控制 | | 22 | 8.1.4.3 安全审计 | | 23 | 8.1.4.4 入侵防范 | | 24 | 8.1.4.5 恶意代码防范 | | 25 | 8.1.4.6 可信验证 | | 26 | 8.1.4.7 数据完整性 | | 27 | 8.1.4.8 数据保密性 | | 28 | 8.1.4.9 数据备份与恢复 | | 29 | 8.1.4.10 剩余信息保护 | | 30 | 8.1.4.11 个人信息保护 | | **8.1.5 安全管理中心** | 31 | 8.1.5.1 系统管理 | | 32 | 8.1.5.2 审计管理 | | 33 | 8.1.5.3 安全管理 | | 34 | 8.1.5.4 集中管控 | | **管理安全** | **8.1.6 安全管理制度** | 35 | 8.1.6.1 安全策略 | | 36 | 8.1.6.2 管理制度 | | 37 | 8.1.6.3 制定和发布 | | 38 | 8.1.6.4 评审和修订 | | **8.1.7 安全管理机构** | 39 | 8.1.7.1 岗位设置 | | 40 | 8.1.7.2 人员配备 | | 41 | 8.1.7.3 授权和审批 | | 42 | 8.1.7.4 沟通和合作 | | 43 | 8.1.7.5 审核和检查 | | **8.1.8 安全管理人员** | 44 | 8.1.8.1 人员录用 | | 45 | 8.1.8.2 人员离岗 | | 46 | 8.1.8.3 安全意识教育和培训 | | 47 | 8.1.8.4 外部人员访问管理 | | **8.1.9 安全建设管理** | 48 | 8.1.9.1 定级和备案 | | 49 | 8.1.9.2 安全方案设计 | | 50 | 8.1.9.3 产品采购和使用 | | 51 | 8.1.9.4 自行软件开 | | 52 | 8.1.9.5 外包软件开发 | | 53 | 8.1.9.6 工程实施 | | 54 | 8.1.9.7 测试验收 | | 55 | 8.1.9.8 系统交付 | | 56 | 8.1.9.9 等级测评 | | 57 | 8.1.9.10 服务商供应商选择 | | **8.1.10 安全运维管理** | 58 | 8.1.10.1 环境管理 | | 59 | 8.1.10.2 资产管理 | | 60 | 8.1.10.3 介质管理 | | 61 | 8.1.10.4 设备维护管理 | | 62 | 8.1.10.5 漏洞和风险管理 | | 63 | 8.1.10.6 网络和系统安全管理 | | 64 | 8.1.10.7 恶意代码防范管理 | | 65 | 8.1.10.8 配置管理 | | 66 | 8.1.10.9 密码管理 | | 67 | 8.1.10.10 变更管理 | | 68 | 8.1.10.11 备份与恢复管理 | | 69 | 8.1.10.12 安全事件处置 | | 70 | 8.1.10.13 应急预案管理 | | 71 | 8.1.10.14外包运维管理 | |  |
|  | 2.4工具测试:  使用专业的安全分析工具对待测系统进行安全分析,最终形成扫描、渗透报告。  2.5信息系统安全保护等级测评工作要求:  在投标方的技术应标书中，提供针对本项目建设的详细实施计划，提供本项目详细工作实施组织方案，包括(但不限于)以下内容：组织机构、工作时间进度表、工作程序和步骤、管理和协调方法、关键步骤的思路和要点。在项目实施过程中，中标的等保测评机构应成立相应的项目组，并指定一名专职的项目经理，主要负责人力资源调度、项目的总体计划、与采购人协调和项目调度等工作。  2.6信息系统安全保护整改:  根据测评结果和风险分析结果，提供详细的整改建议指导服务，其内容包含技术和管理两大方面。技术方面应包含：物理安全、网络安全、主机安全、应用安全、工具扫描和数据安全及备份恢复。管理方面应包含：安全管理制度、安全管理机构、人员安全管理、系统建设安全管理和系统运维安全管理。  2.7质量保证及售后服务：  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。测评过程和结论需执行《 GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》和《 GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》的相关要求。中标单位应提供相关的安全咨询技术服务。提供的整改建议要有高度的性价比并且符合等保测评的相关规定。  2、中标的等保测评机构应为我院提供提供完善信息安全管理体系、信息安全目标战、IT安全基础、安全防护措施，为被测信息系统建立风险评估和整改机制，确保安全防护体系的有效性，符合信息安全等级保护要求。  3、中标的等保测评单位应按照等级保护测评要求制定测评详细计划和方案。测评过程中，应针对重要的主机操作系统、数据库系统、信息系统、网络设备等进行渗透测试,形成安全检测报告和整改建议方案，并指导完成高风险漏洞的安全整改，并具有较强的安全服务能力，能够利用测评、评估、漏洞扫描等方法发现系统安全隐患并提出合理的整改建议；对系统漏洞能够及时定位，并对后续修复的情况进行验证。  4、支撑保障服务，在测评年度内以及下一年测评前，协助在重大信息安全检查工作或重大网络安全安保工作中提供远程或现场相关的技术支撑服务。（如发生安全事故，3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。  5、安全咨询服务，在测评年度内以及下一年测评前，提供相关的安全咨询服务。提供的安全咨询建议、策略、规范和整改建议要切合招标单位实际情况，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。  6、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。  7、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。  2.8项目成果：  项目成果应包含：系统测评记录、工具扫描报告、系统风险分析、系统等级测评报告、系统整改加固方案等。  测评方应按照等级保护测评要求制定测评详细计划和方案。在项目实施过程中能够严格遵循等级测评流程规范、质量保证和过程管理规范，形成规范、详尽、统一的过程文档、工作记录、进度报告等。  交付物：  1、《医院信息系统等级保护测评进度计划表》纸质版、电子版  2、《医院信息系统等级保护测评实施方案》纸质版、电子版  3、《医院信息系统等级保护测评差距分析报告》纸质版、电子版  4、《互联网医院等级保护测评进度计划表》纸质版、电子版  5、《互联网医院等级保护测评实施方案》纸质版、电子版  6、《互联网医院等级保护测评差距分析报告》纸质版、电子版  7、《集成平台系统等级保护测评进度计划表》纸质版、电子版  8、《集成平台系统等级保护测评实施方案》纸质版、电子版  9、《集成平台系统等级保护测评差距分析报告》纸质版、电子版  10、《医院信息系统等级保护测评差距分析报告》纸质版、电子版  11、《互联网医院等级保护测评最终测评报告》纸质版、电子版  12、《集成平台系统等级保护测评最终测评报告》纸质版、电子版  13、《LIS、PACS、EMR、手麻、合理用药、供应室追溯、院感及传染病上报、移动医护、微信挂号、互联网医院随访、OA、HRP、科研教学扫描报告、人事管理系统、电子发票、不良事件上报、心电管理、病理系统、影像云、输血管理、电子签名扫描报告》纸质版、电子版。  2.9人员保障要求：  投标方拟投入本项目的等级保护测评小组至少由5名测评人员构成（其中，中、高级测评师至少分别1人），且测评人员均具有公安部认证的测评师证书，为保证项目实施质量，要求项目骨干人员具有3年及以上相关工作经验。  2.10保密要求：  中标方要保守测评中所有涉及招标方的数据、安全问题、测评报告等结果与数据、资料的秘密，并与招标方签订保密协议。若因中标方原因，泄露招标方测评结果，安全漏洞、数据、资料等的，将承担由此产生的一切责任。 |  |

## **三、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。

## **四、报价要求**

报价包括完成本项目所需的本项目报价总价，本次报价须为人民币报价，包含：人工、保险费、安装费、调试费、售后服务费、税费、培训费等所有费用，因成交供应商自身原因造成漏报、少报皆由其自行承担责任，采购人不再补偿。

## **五、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%自采购方签署验收报告之日起1年后一次性付清。

**六、特定资格条件**

1、投标方须为国家网络安全等级测评与检测评估机构（提供公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》），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；投标方应具备中国合格评定国家认可委员会（CNAS）检验机构认可证书且检验项目包含网络（信息）安全等级测评，提供网站有效证明截图并加盖供应商鲜章。注册地在重庆市外的投标方应在重庆市相关主管部门完成相关备案手续；同时投标方经营范围不得涉及网络安全产品开发、销售或信息系统集成等可能影响测评结果公正性的业务。投标方需要有本地服务团队，当发生突发网络安全公共事件时，能在第一时间派出技术团队协助处置突发事件，技术人员须具有中级及以上测评师资质且在本次项目现场测评人员名单内。

2、依照渝网通[2016]11号文《重庆市网络与信息安全信息通报工作规范》要求，投标人需协助招标人进行网络安全事件应急处置机制建设工作，落实招标人的网络安全应急处置通报工作。投标人需为重庆市网络与信息安全信息通报机制成员单位或重庆市网络与信息安全信息通报中心支撑单位，按渝网通[2016]11号文开展相关通报工作。