大庆市人民医院采购信息系统安全保护等级评测项目

一、**采购单位**：大庆市人民医院

二、**项目名称**：大庆市人民医院信息系统安全保护等级评测项目(项目编号:XXZXPC006）

三、**采购方式**：竞争性谈判

四、**采购预算**：110,000.00元（报价超出采购预算为无效报价）。

五、**采购内容及技术要求：**

为切实提升我院信息系统的安全防护能力，根据《网络安全法》相关规定，开展对我院信息系统的等保测评工作。本次测评须按照信息系统网络安全等级保护三级系统相关要求，对我院的系统信息出具公安部认可的的《网络安全等级保护等级测评报告》，结合我院现有网络安全措施参照《GB/T28448-2019 信息安全技术 网络安全等级保护测评要求》优化安全策略、提出安全整改建议，进一步提升我院信息安全防护水平，保障信息系统的正常稳定运行，支撑我院信息化建设的正常开展。

根据《网络安全法》、GBT/T 22239-2019《信息安全技术网络安全等级保护基本要求》、GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》对我院系统三级信息系统等级保护测评服务。服务期限一年，并出具《网络安全等级保护等级测评报告》并加盖等级保护测评机构测评章。

1、服务要求

对我院现有信息系统的安全物理环境、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、安全管理机构、安全管理人员、安全建设管理、安全运维管理层面进行等级保护安全测评服务。

2、技术要求

（1）依据

根据GBT/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》、GB/T 28449-2018《信息安全技术 信息系统安全等级保护测评过程指南》、《中华人民共和国信息安全等级保护管理办法》等相关政策和技术标准，对我院“医院信息系统”提供三级等级保护测评服务。

（2）服务要求

1)在确保信息系统正常运行的前提下，根据国家等级保护相关标准对各系统进行等级保护测评。测评工作需由测评师根据GB/T 28449-2018《信息安全技术 信息系统安全等级保护测评过程指南》进行前期信息系统的调研，并编写针对信息系统等级保护合规性的实施方案。

2)信息安全等级保护检测工作完成后，报告中应包含单项测评结果、单元测评结果、层面间分析、区域间分析等内容，并结合我院网络信息系统的实际情况，指出信息系统中存在的安全薄弱环节，提出安全整改建议。

3)测评项目组至少包含1名高级测评师组成参与现场测评工作。

4)采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件。

5)采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品。

（3）指标

1)等级保护测评安全要求从整体上分为技术和管理两大类，其中，管理类和技术类安全要求按其保护的侧重点不同，根据GBT/T 22239-2019《信息安全技术 网络安全等级保护基本要求》将所有的控制点分为以下三类：

* 业务信息安全类：关注的是保护数据在存储、传输、处理过程中不被泄露、破坏和免受未授权的修改。
* 系统服务安全类：关注的是保护系统连续正常的运行，避免因对系统的未授权修改、破坏而导致的系统不可用。
* 通用安全保护类：既关注保护业务信息的安全性，同时也关注系统的连续可用性。

2)信息系统控制点指标，根据GBT/T 22239-2019《信息安全技术 网络安全等级保护基本要求》对信息系统的控制点测评指标的要求，控制点测评指标见下表：

测评指标须包含下表测评指标。

| **序号** | **安全要求类别** | **层面** | **控制点** |
| --- | --- | --- | --- |
| 1 | 技术要求 | 安全物理环境 | 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 |
| 11 | 安全通信网络 | 网络架构 |
| 12 | 通信传输 |
| 13 | 可信验证 |
| 14 | 安全区域边界 | 边界防护 |
| 15 | 访问控制 |
| 16 | 入侵防范 |
| 17 | 恶意代码防范 |
| 18 | 安全审计 |
| 19 | 可信验证 |
| 20 | 安全计算环境 | 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 | 数据备份恢复 |
| 29 | 剩余信息保护 |
| 30 | 个人信息保护 |
| 31 | 安全管理中心 | 系统管理 |
| 32 | 审计管理 |
| 33 | 安全管理 |
| 34 | 集中管控 |
| 35 | 管理要求 | 安全管理制度 | 安全策略 |
| 36 | 管理制度 |
| 37 | 制定和发布 |
| 38 | 评审和修订 |
| 39 | 安全管理机构 | 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 |
| 44 | 安全管理人员 | 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 |
| 48 | 安全建设管理 | 定级和备案 |
| 49 | 安全方案设计 |
| 50 | 产品采购和使用 |
| 51 | 自行软件开发 |
| 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 | 服务供应商选择 |
| 58 | 安全运维管理 | 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 |

（4）服务工具技术要求

（1）服务过程中所需要的服务工具由投标人自行负责，并保证其所使用的服务相关工具不会产生因第三方提出侵犯其专利权或其它知识产权而引起的法律和经济纠纷，招标人不另行支付任何费用。

（2）服务工具应采用成熟、业界著名的商业化的安全服务工具进行安全检査，保证对目标系统无大的影响以及扫描结果的准确性和可信度。投标人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，并保证工具和软件可用性和可靠性。由此产生的一切责任由投标人负完全责任。

（3）安全服务工具在检查过程中起到良好的辅助作用，检查时使用的工具的种类包括但不限于：Windows主机安全配置检查工具、主机病毒检查工具、主机木马检查工具、网站恶意代码检查工具、Linux主机安全配置检查工具、网络及安全设备配置检查工具、弱口令检查工具、数据库安全检查工具、网站安全检查工具、系统漏洞检查工具、邮件漏洞检测工具等。

（4）安全服务工具支持对误报的漏洞进行修正，避免将误报结果导出。（提供相关证材料）

（5）安全服务工具支持端口探测方式包括但不限于TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin等。（提供相关证材料）

（6）安全服务工具的弱口令扫描功能，支持弱口令扫描协议数量，包括但不限于FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典等。（提供相关证材料）

**六、供应商资格条件：**

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.未被信用中国网站（www.creditchina.gov.cn）列入失信被执行人、重大税收违法案件当事人名单；未被中国政府采购网（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单。

3、本项目参与评测供应商必须是由网络安全等级保护网公布的《全国网络安全等级测评与检测评估机构目录》名单内的机构（提供证明截图）

4、本项目参与评测供应商等级保护测评机构必须具有《网络安全等级测评与检测评估机构服务认证证书》（提供证书复印件）

5、本项目不接受联合体投标。

**七、质量及服务要求：**

1.服务方提供周一至周日7×24小时的电话支持和现场响应服务，针对所升级设备发生的宕机等重大故障，服务方要在接到甲方报修电话后30分钟内响应，并在1小时内到达现场。

2.安全服务要求：

服务方必须按照大庆市人民医院要求提供相应的维护方案，提交服务方案经甲方审阅通过后才能执行。在整个服务过程中，服务方要服从甲方的管理，严格遵守保密规定，不得向无关人员透露买方设备、数据信息。

**八、验收标准：**

《网络安全等级保护测评报告》

**九、交付使用期及合同履行期：**

合同签订之日起60日内交付使用并完成验收。合同履行期为验收合格之日起1年。

**十、付款方式及履约保证金：**

1.验收合格后90日内一次性支付项目合同款100%。

2.成交后履约保证金按合同总价的5%，由成交供应商交给采购单位账户。

3.采购单位验收合格且质保期满后，无质量问题无息退还给供应商。

户名：大庆市人民医院

地址：大庆市开发区建设路213号

电话：0459-6612123

开户行：龙江银行大庆市开发区支行

账号：04010120002000734

履约保证金交纳方式：转帐汇款

十一、投标文件格式：

1.有意投标者请将投标资料密封在信封或档案袋内（投标书封面，要求写明文件名称、投标单位名称（盖章）、地址、投标单位法定代表人（签字或盖章），投标单位联系人，联系电话），提供原件的需单独密封。

2.标书要求：一本正本、三本副本均加盖公章，装订方式为胶装。

3.标书封面须有以下内容（1）投标公司全称及正本或副本标识

（2）投标公司联系人及联系方式

4.投标文件包含项目：

（1）提供有效的营业执照副本（加盖公章）

（2）法定代表人身份证（法定代表人参会时提供）。如参会代表不是法定代表人的，须附有授权委托书及授权代表社保证明。法定代表人身份证及授权代表身份证。否则投标无效。（加盖公章）

（3）报价明细单（加盖公章）

（4）提供投标截止日前6个月内任意1个月依法缴纳税收和社会保障资金的相关材料。或不需要缴纳社会保障资金的，提供相应证明材料（加盖公章）

（5）诚信竞争承诺书。（加盖公章，格式自定）

（6）提供本单位的参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（加盖公章，格式自定）。

（7）响应资料无弄虚作假声明。如发现资料为虚假资料，将取消响应资格，且供应商自行承担法律责任（加盖公章，格式自定）。

（8）未被信用中国网站（www.creditchina.gov.cn）列入失信被执行人、重大税收违法案件当事人名单；未被中国政府采购网（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单。提供网站查询截图。（加盖公章，格式自定）

（9）参与本项目供应商需提供测评人员由公安部信息安全等级保护评估中心或中关村信息安全测评联盟颁发《信息安全等级测评师证书》或《网络安全等级测评师证书》复印件，其中，高级、中级和初级测评师须与投标文件中提供的信息或网络安全等级测评师证书人员为同一人，须提供测评人员社保证明及公司承诺函。（加盖公章，格式自定）

（10）参与本项目供应商必须是网络安全等级保护网公布的《全国网络安全等级测评与检测评估机构目录》名单内的机构（提供证明截图，加盖公章）

（11）参与本项目供应商必须具有《网络安全等级测评与检测评估机构服务认证证书》（提供证书复印件，加盖公章）

十二、报名须知：

1.本项目采购公告发出后，如有变更（如：变更通知、有关问题答复、质疑答复等相关文件），将在“大庆市人民医院网站”告知，转载无效，所有参与本项目投标的供应商，供应商应主动查看。

2.本项目不设资格预审，供应商应详细阅读本公告，符合条件即可参与。参标供应商按照要求将所有资质证明资料提供到开标会现场，由评委小组审查，经评审不符合条件者投标无效。

3.如有质疑，请以书面形式提出并附营业执照复印件及法人身份证复印件，其它形式采购方均不受理。

4.招标谈判价格及中标价格都为税后价格。

5、报名时间：公告之日起至2022年 7月25 日16时00分。超过报名期限，报名无效。

报名方式：邮箱报名：rmyyxxzx@126.com，需要填写附件报名表（本公告最后一页），填写完整并加盖公章后上传PDF版至此邮箱。

咨询电话： 6612123

开 标 地 址：大庆市人民医院（如遇特殊情况另行通知）

开 标 时 间： 2022年 7 月 26日 ( 如有变化另行通知)

1. 投标代表（法人或法人授权人）请在开标时间前20分钟携带身份证到达会场签到（签到时查验身份证件）未按开标时间参加开标会议的将视为自动弃权。具体事项工作人员将通过报名表中移动电话进行告知。如现场开标，需提供行程码、健康码和24小时核酸截图的纸质材料。

附件

xx项目投标报名表

项目名称：

项目编号：

联系人： 移动电话：

电子邮件：

我公司已阅读该项目招标文件及公告，并按照要求提供资料报名参加投标。

投标单位（公章）：

报名代表签字：

报名日期： 年 月 日

**注：如放弃此项目，请在开标前电话告知。**