**昌吉回族自治州阜康市人民医院信息系统网络安全等级保护测评服务的需求说明**

**一、项目背景及详细要求**

**1.1 项目背景**

为进一步加强昌吉回族自治州阜康市人民医院信息系统网络安全防护能力，切实做好2024年度昌吉回族自治州阜康市人民医院信息系统安全等级保护测评工作，根据《中华人民共和国网络安全法》、《新疆维吾尔自治区贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的实施意见》等相关规定，为认真贯彻和执行网信办和网安等监管单位的网络安全等级保护需求，切实做好我单位等级保护测评和安全防护评估工作，结合单位业务系统实际情况建设本项目。

**1.2 项目目的**

通过等级保护测评工作发现信息系统在安全方面的不足之处，找出昌吉回族自治州阜康市人民医院各信息系统与国家和行业等级保护标准要求和之间的差距，可以有效地提高昌吉回族自治州阜康市人民医院网络安全建设的整体水平，并且指明方向，有利于在信息化建设过程中同步建设网络安全设施，保障网络安全与信息化建设相协调；有利于加强对涉及国家安全、经济秩序、社会稳定和公共利益的信息系统的安全保护和管理监督；有利于明确国家、法人和其他组织、公民的安全责任，强化政府监管职能，共同落实各项安全建设和安全管理措施。为信息系统的安全提供合理化建议，并协助昌吉回族自治州阜康市人民医院设计详细和合理的等级保护测评方案，通过安全等级保护测评使各信息系统达到相应安全保护等级的能力要求。具体如下：

（1）通过等级保护测评，对昌吉回族自治州阜康市人民医院信息系统安全防护体系能力的分析与确认，发现存在的安全隐患，协助进行整改，全面达到国家网络安全等级保护相关要求；

（2）对昌吉回族自治州阜康市人民医院信息系统的安全状态做出判断，验证其是否符合等级保护要求，提出安全防护相关合理化建议，提升安全防护水平。同时，将测评结论作为进一步完善系统安全防护措施的依据。

（3）提升昌吉回族自治州阜康市人民医院网络安全事件应急响应及安全事件分析，使技术人员更全面掌握了解信息系统安全状况，提升人员安全威胁处置能力。

（4）遵循国家等级保护有关规定的要求，对信息系统安全建设进行符合性测评，出具网络安全等级保护测评报告。

**1.3 采购产品及预算金额**

阜康市人民医院三级等级保护测评服务

预算金额：24万元

**1.4 资格要求**

（1）符合《中华人民共和国政府采购法》第二十二条规定的合格投标供应商。

（2）具有独立法人资格，具有有效的营业执照。

（3）具有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》。

（4）投标人不踏勘看现场的，视为对现场了解，中标后不得在此方面提出增加费用的请求。

（5）报价单位需提供一名网络安全等级保护测评师（中级）驻场12个月的履约保证书（加盖公章及附人员证书）。

（6）报价单位至少拥有网络安全等级保护测评师（高级）1名、网络安全等级保护测评师（中级）2名，网络安全等级保护测评师（初级）3名。

**1.5商务要求**

（1）报价时上传报价详细清单签字并加盖公章。

（2）交货期:中标后20天内完成相关服务。

（3）供应商中标后2个工作日内提供所竞价材料文件纸质版(原件及加盖公章的复印件一份)及电子版递交至采购单位，并全部完成合同签订的必要流程。供应商存在不按参数要求报价、低价低质恶性竟争、中标后无故放弃、不按合同执行等违约行为的，采购人将根据在线询价、反向竟价违约处理规则，依法依规提请政采云平台进行处罚并记入政府采购诚信档案。供货实物与乙方提供交付项目产品真实图片不一致的，或商品性能及功能不能达到采购要求的,视为虚假响应采购要求，将列入虚假响应采购要,将列入政府采购黑名单，需赔付我单位总金额30%的违约金。

（4）报价明细要求:报价单要求涵盖服务名称等简要内容。

（5）响应文件需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》，有违反市场价格规律超低价恶意谋取中标后，又不能按竞价要求提供合格产品者，将做无效标处理。

（6）服务需求响应要求:供应商须逐条响应采购需求，提供采购人需求的服务需求参数中如存在矛盾表述之处，以有利于采购人表述的要求为准；如投标单位对采购需求有不响应之处作无效标处理，供应商必须满足本项资格要求并提供相应材料，如不满足或未提供将做无效标处理。

（7）报价人需现场踏勘。以便测评单位充分了解系统及机房的实际情况，确保报价准确并有效识别潜在风险。

(8)所有复印件需注明与原件一致字样。

**1.6 响应附件**

（1）报价人需踏勘的需在2024年9月27日进行现场踏勘。

（2）报价人需满足一名网络安全等级保护测评师（中级）驻场12个月，并出具保证书（格式自拟、加盖公章、附人员相关证书）

**1.7测评依据**

 《中华人民共和国网络安全法》

 《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）

 《计算机信息系统 安全保护等级划分准则》（GB 17859-1999）

 《信息系统安全等级保护实施指南》 (GB/T25058-2010)

 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

 《信息安全技术 网络安全等级保护测评过程指南》（GBT 28449-2018）

 《网络安全等级保护测评报告模板（2021 版）》

 委托测评协议书等

**1.8项目要求**

（1）自项目合同签订之日起，昌吉回族自治州阜康市人民医院20个工作日内完成系统梳理和测评工作并出具测评相关报告。

（2）现场测评活动中，必须使用漏洞扫描、渗透测试等验证性测试方法， 对昌吉回族自治州阜康市人民医院的信息系统进行全面的工具测试，确保全面的找出系统的漏洞薄弱点，并协助甲方完成漏洞修复或风险降低工作。

（3）在合同服务期内，中标方须提供应急事件处理及应急响应服务。一旦被测系统出现安全事件，驻场测评师应在收到单位服务请求30分钟内到达现场提供服务。

**二、等级保护测评工作内容**

**2.1 等级测评内容**

测评的内容包括但不限于以下内容：

(1)安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；

(2)安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

(3)安全物理环境

根据昌吉回族自治州阜康市人民医院信息系统机房和现场安全测评记录，针对机房和现场在 “物理位置选择”、“物理访问控制”、“防盗窃和防破坏”、“防雷击”、“防火”、“防水和防潮”、“防静电”、“温湿度控制”、“电力供应”和“电磁防护”等物理安全方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

(4)安全通信网络

安全通信网络现场测评主要针对系统网络架构方面，在“网络架构”、“通信传输”、“可信验证”等网络安全方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

(5)安全区域边界

安全区域边界现场测评主要针对网络安全区域边界进行测评，测评内容包括“边界防护”、“访问控制”、“入侵防范”、“恶意代码防范和垃圾邮件防范”、“安全审计”、“可信验证”等。

(6)安全计算环境

安全计算环境现场测评主要针对系统网络设备、安全设备、服务器、数据库、 应用系统等资产进行现场测评，测评内容包括“身份鉴别”、“访问控制”、“安全审计”、“入侵防范”、“恶意代码防范”、“可信验证”、“数据完整性”、 “数据备份和恢复”、“剩余信息保护”、“个人信息保护”等方面。

(7)安全管理中心

安全管理中心现场测评包括“系统管理”、“审计管理”等方面的测评。

(8)安全管理制度

根据现场安全测评记录，针对昌吉回族自治州阜康市人民医院信息系统在安全管理制度方面的 “安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

(9)安全管理机构

根据现场安全测评记录，针对昌吉回族自治州阜康市人民医院信息系统在安全管理机构方面的 “岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

(10)安全管理人员

根据现场安全测评记录，针对昌吉回族自治州阜康市人民医院信息系统在人员安全管理方面的 “人员录用”、“人员离岗”、 “安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

(11)安全建设管理

根据现场安全测评记录，针对昌吉回族自治州阜康市人民医院信息系统在系统建设管理方面的 “定级和备案”、“安全方案设计”、“产品采购和使用”、“自行软件开发”、 “外包软件开发”、“工程实施”、“测试验收”、“系统交付”、“等级测评” 以及“服务供应商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

(12)安全运维管理

根据现场安全测评记录，针对昌吉回族自治州阜康市人民医院信息系统在系统运维管理方面的 “环境管理”、“资产管理”、“介质管理”、“设备维护管理”、 “漏洞和风险管理”、“网络和系统安全管理”、“恶意代码防范管理”、“配置管理”、“密码管理”、“变更管理”、“备份和恢复管理”、“安全事件处置”、 “应急预案管理”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。

**2.2 项目实施要求**

（一）保密要求

投标方对项目实施过程中所获得数据及文档等保密信息，承担以下保密义务：

1.中标方应按要求与昌吉回族自治州阜康市人民医院签署保密协议。

2.主动采取加密措施对上述所列及之保密信息进行保护，防止不承担同等保密义务的任何第三者知悉及使用。

3.不得刺探或者以其他不正当手段（包括利用计算机进行检索、浏览、复制等）获取与本职工作或本身业务无关的甲方关于该项目的商业秘密。

4.不得向不承担同等保密义务的任何第三人披露甲方关于该项目的商业秘密。

5.不得允许（包括出借、赠与、出租、转让等行为）或协助不承担同等保密义务的任何第三人使用甲方关于该项目的商业秘密。

6.不论何种原因终止参与甲方关于该项目的工作后，都不得利用该项目之商业秘密为其他与甲方有竞争关系的企业（包括自办企业）服务。

7.该项目的商业秘密所有权始终全部归属甲方，乙方不得利用自身对项目不同程度的了解申请对于该项目的商业秘密所有权，在本协议签订前乙方已依法具有某些所有权者除外。

8.如发现甲方关于该项目的商业秘密被泄露或者自己过失泄露秘密，应当采取有效措施防止泄密进一步扩大，并及时向甲方报告。

**2.3 交付物**

根据《网络安全等级保护测评机构管理办法》要求，成果交付物为：

1、所有登记备案的信息系统出具由测评机构法人审签的正式纸质测评报告2 套。

2、测评活动原始记录材料1份。

**2.4 质量保证**

1、为保证网络安全等级测评项目质量，要求在测评过程中就等级保护测评过程控制、等级保护测评过程监督、等级保护测评结果的验证等方面严格按照国家相关标准要求执行。

2、等级保护测评结果必须通过昌吉回族自治州阜康市人民医院组织的评审和审批。

**三、等级保护测评培训**

3.1测评机构必须提供本项目所需的现场培训。

3.2培训目的：使招标人人员熟悉国家对信息安全等级保护相应法律法规；使甲方人员熟悉信息安全等级保护测评的方法。

3.3培训内容：信息安全等级保护法律法规；信息安全等级保护测评方法。

3.4培训对象：招标人信息系统使用及安全管理人员。

3.5培训教师：培训教师须具备相关专业认证资质与丰富经验。

3.6培训人数：现场培训人数根据甲方需求确定。

3.7培训次数：根据招标人需求确定。