附件1：

遂宁市民康医院2023年信息系统安全等级保护

测评服务实施方案

遂宁市民康医院按照国家、行业相关的安全要求，需要对其信息系统进行安全等级保护测评。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、安全计算环境和安全管理中心等五个方面的安全测评。安全管理测评：包括安全管理制度、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等五个方面的安全测评。依据相关的测评准则，结合系统的构成特点，确定具体的测评对象，制定测评方案，通过访谈、检查、测评和系统分析等方式判断其安全技术和安全管理的各方面是否达到了相应等级的国家信息系统等级保护要求，找出信息系统中存在的安全隐患，对安全性进行整体评估，制定相关的信息安全整体安全策略和中长期的安全规划，以便对被测系统进行安全方面的调整和改进，确保其安全防护水平达到信息系统安全等级保护相应能力的要求。

一、采购需求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评系统 | 级别 | 预算价 |
| 1 | 医院HIS系统 | 三级 | 7.36万 |
| 2 | 医院LIS系统 | 三级 | 7.36万 |
| 3 | 医院OA系统 | 二级 | 3.68万 |

二、项目要求

1.项目检测依据

《中华人民共和国网络安全法》

《信息安全技术 信息安全风险评估规范（GB/T 20984-2007）》；

《网络安全等级保护基本要求（GB/T 22239-2019）》

《信息安全等级保护管理办法（公通字﹝2007﹞43 号）》；

《信息安全技术网络安全等级保护定级指南（GBT 22240—2020）》；

《网络安全等级保护设计技术要求（GB/T25070-2019）》；

《网络安全等级保护测评要求（GB/T28448-2019）》；

《信息系统安全等级保护基本要求（GB/T 22239-2019）》；

《信息安全技术 网络安全等级保护实施指南（GB/T 25058-2019）》；

《信息安全技术信息安全风险评估规范（GB/T 20984-2007）》

2.项目测评内容

2.1 信息系统技术安全性测评

2.1.1 安全物理环境

安全物理环境针对物理机房提出了安全控制要求，主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、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、安全等级保和电磁防护。

2.1.2 安全通信网络

安全通信网络针对网络架构和通信传输提岀了安全控制要求。主要对象为广域网、城域网、局域网的通信传输以及网络架构等；涉及的安全控制点包括网络架构、通信传输和可信验证。

2.1.3 安全区域边界

安全区域边界针对网络边界提出了安全控制要求，主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

2.1.4 安全计算环境

安全计算环境针对边界内部提出了安全控制要求，主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证。

2.1.5 安全管理中心

安全管理中心针对整个系统提出了安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集全等级。

2.1.6 安全管理制度

安全管理制度测评是对信息系统的安全管理制度体系和制度内容、制定和发布流程、评审和修订机制等情况进行测评。

2.1.7 安全管理机构

安全管理机构测评是对信息系统的安全管理组织和岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

2.1.8 安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗、人员考核、安全意识教育和培训，以及外部人员访问管理等情况进行测评。

2.1.9 安全建设管理

系统建设管理测评是对信息系统建设过程中的系统定级、安全方案设计、产品采购和使用、自主软件开发、外包软件开发、工程实施、测试验收、系统交付、系统定级备案、等级测评、安全服务商选择等情况进行测评。

2.1.10 安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等情况进行测评。

2.2 等级保护要求的相关内容

3.项目测评要求

3.1 按照国家相关标准要求，完成在公安局完成信息安全等级保护定级备案所有工作。

3.2 对遂宁市民康医院信息系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理共 10 个层面通过访谈、检查、测评等方法进行初测评，找出差距、安全漏洞和隐患并分析其风险，制订出整改建议报告。

3.3 根据相关要求及测评的整改意见，协助被测信息系统的安全修复、系统加固等工作。

4.项目测评交付资料

项目测评后需提交《遂宁市民康医院HIS应用等级测评报告》、《遂宁市民康医院LIS应用等级测评报告》、《遂宁市民康医院OA应用等级测评报告》《系统整改建议报告》、HIS应用系统信息安全等级保护备案证明、LIS应用系统信息安全等级保护备案证明、OA应用系统信息安全等级保护备案证明等资料。

三、商务要求

1.服务要求

1.1.项目现场实施配备人员不得少于 5 名，其中信息安全等级测评师（高级）不少于 1 名，信息安全等级测评师（中级）不少于 2 名，信息安全等级测评师（初级）不少于 2 名，提供上述人员的近一年社保证明材料加盖公章，要求上述人员在项目过程中务必到场实施。

1.2.服务期限：1 年

1.3.服务地点：遂宁市民康医院指定地点

1.4.免费提供一次全院级别的信息安全培训会议。

2．服务保障与承诺

2.1.服务提供商应严格按照测评人员执业守则，按照国家相关法规、规范、标准及制定的测评方案、项目计划书、实施细则进行测评，在保证质量、安全的前提下，确保在项目规定的期限内按期完成。

2.2.服务提供商应协助、配合与上级监管部门、公安机关的沟通协调。在测评过程中和测评完成后，协助、配合进行相关的信息系统安全整改。

2.3.服务提供商应在项目期内向提供 7\*24 小时电话咨询服务，必要时上门服务。跟踪信息安全等级保护的最新发展情况，及时告之，提供相应解决方案及建议，协助其持续符合信息系统信息安全等级保护工作的要求。

2.4.服务提供商应在项目实施过程中，对相关人员进行安全方面的技术培训，明确项目实施的思路、方案、技术路线，提升技术人员的安全意识，可以独立的对信息安全等级保护的国家安全政策和法规进行把握，了解测评整改手段，掌握测评整改方法。

2.5.服务提供商应在项目开始前，与签订保密协议，严格遵守法律法规，对商业秘密、系统风险信息、项目实施内容及成果信息进行严格保密，未经同意，严禁将上述内容与任何第三方透露或用于其他商业用途，并承担由此产生的一切损失。

四、供应商邀请方式

公告方式：本次邀请在遂宁市民康医院官网上以公告形式发布。

附件2：

评分细则

|  |  |  |  |
| --- | --- | --- | --- |
| **评分因素** | **分值** | **评分标准** | **备注** |
| 价格  （30%） | 30分 | 以本次有效投标的最低投标报价为基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算价格得分=（基准价/投标报价）×30。 |  |
| 履约能力20% | 20分 | 供应商提供类似项目业绩一个得5分，本项最高得20分。 | 提供合同复印件及验收单加盖供应商单位鲜章。 |
| 服务方案（30%） | 30分 | 对提供的测评服务方案进行评审，包括但不限于以下内容：①具有完整的物理安全方案、②网络安全方案、③主机系统安全方案、④应用安全方案、⑤数据安全方案，方案完整包含以上内容，详细、切实可行、满足采购需求的，得30分。存在缺陷（缺陷是指：分析内容与实际情况不符或内容前后不一致或前后逻辑错误或过于简略或存在不足或不符合采购实施方案等）的得3c分，未提供不得分，本项满分30分。 |  |
| 实施保障20% | 20分 | 1.项目组负责人具有以下资格的：①项目负责人具有信息安全等级测评师高级证书的得1分，此项最多得1分，未提供不得分；②项目负责人同时具有互联网安全评估师高级证书（CIISA）、计算机技术与软件专业资格信息安全工程师（软考类）、国家重要信息系统保护人员证书的（CIIP-A）、商用密码应用安全性评估人员能力合格证书、系统架构师（高级）、实验室质量管理师证书全部满足得9分，缺少一项扣1.5分。  2.拟派的测评人员在具有信息安全等级测评师证书的同时具有以下证书：①具有互联网安全评估师证书（CIISA）的得2分；②具有商用密码应用安全性评估人员能力合格证书的得2分；③具有国家重要信息系统保护人员证书（CIIP-A）得2分；④具有信息安全保障人员认证证书（CISAW）得2分；⑤具有国家网络安全应用检测专业测评人员证书（NSATP-A）得2分；全部满足得10分。 | 提供相关人员证书证明材料和复印件，加盖投标人公章 |