一、采购项目概况

根据《中华人民共和国网络安全法》、《成都市卫生健康委员会、成都市公安局关于印发<成都市卫生健康行业网络安全等级保护工作实施方案〉的通知》要求:三级医疗卫生机构建设和运营的重要信息系统应定级为信息安全等级保护三级;面向患者提供服务的系统，如HIS、LIS、 PACS、 EMR及门户网站等，原则上不低于第三级。通过等级保护测评工作可发现医院信息系统与国家安全标准之间存在的差距，查明目前信息系统中存在的安全隐患和不足之处，通过安全整改之后，进而提高信息系统的安全防护能力，降低系统被攻击的风险。

二、采购标的汇总表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 包号 | 序号 | 标的名称 | 品目分类编码 | 计量单位 | 数量 | 是否进口 |
| **1** | **1** | 彭州市妇幼保健院信息安全等级保护测评服务采购项目 | **C0205**  | **项** | **1** | 否 |

 三、技术要求和商务要求

（一）**技术参数条款**

1.采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范。

下列文件中的条款通过本规范的引用而成为本规范的条款，除本技术规范书特别规定外，所提供的测评标准均应遵循公安部相关文件要求和的相关文件要求，所用的标准必须是其最新版本；如果这些标准内容矛盾时，应按最高标准的条款执行或按双方商定的标准执行。

(1)《中华人民共和国网络安全法》；

(2)《信息安全等级保护管理办法》（公通字[2007]43号）；

(3)《GB/T22239-2019信息安全技术 网络安全等级保护基本要求》；

(4)《GB/T22240-2020信息安全技术 网络安全等级保护定级指南》；

(5)《GB/T25058-2010信息安全技术 信息系统安全等级保护实施指南》；

(6)《GB/T28448-2019信息安全技术 网络安全等级保护测评要求》；

(7)《GB/T28449-2018信息安全技术 网络安全等级保护测评过程指南》。

2.测评范围

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 级别 |
| 1 | 核心业务系统 | 三 |
| 2 | 门户网站系统 | 三 |
| 3 | 集成平台系统 | 三 |
| 4 | 金蝶HRP系统 | 二 |

3.技术服务要求

3.1测评及评估原则

3.1.1保密性原则：项目实施方应与签订保密协议，对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据侵害的权益，否则有权追究的责任。

3.1.2标准性原则：测评及评估方案的设计与实施应依据国家的相关标准进行。

3.1.3规范性原则：项目实施方工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

3.1.4可控性原则：项目的进度应符合进度安排，保证对测评工作的可控性。

3.1.5整体性原则：测评及评估的范围和内容应系统、全面、规范，满足等级保护的相关基本要求。

3.1.6最小影响原则：技术测评及评估工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评及评估应在许可的条件下进行。

3.2咨询服务要求：

3.2.1提供7\*24响应服务，负责解决出现的任何问题，确保不影响正常业务运行；提供7×24小时的在线技术支持。

3.2.2供应商提供现场服务，供应商接到采购人现场服务通知后，须在2小时内到达采购人现场。

3.3测评及评估方法

测评及评估方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地察看等多种方法。

如需对系统安全等级保护测评实施过程中采用在线测评工具，各种工具软件由项目实施方推荐，经确认后由项目实施方提供并在工作中使用。

安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由项目实施方推荐，经采购人确认后由项目实施方提供并在测评中使用。

3.4等级保护测评内容

根据国家等级保护相关标准，本次项目的安全等级保护测评应包括以下内容：

3.4.1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、安全计算环境和安全管理中心等五个方面的安全测评；

3.4.2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。

3.5互联网资产服务要求：

3.5.1互联网资产风险检测服务

基于梳理好的互联网资产，提供一年不少于12次的检测服务，包含WEB漏洞、主机漏洞、安全事件、文件泄露、可用性、弱口令、高危服务等。供应商将检测结果形成纸质的检测报告，加盖供应商公章后递交给采购人。同时将梳理好的互联网资产根据算法自动评估出互联网资产风险值，在每次检测服务完成后，通过平台展示资产风险情况，提供风险值变化趋势分析及资产风险值TOP排名，服务单位可通过微信公众号进行安全事件、域名有效期、证书有效期的推送。供应商提供推送服务的功能截图，加盖供应商公章。

检测服务需采用验证式漏洞检测技术，对web站点和主机进行漏洞扫描发现和验证，通过模拟真实攻击行为，根据上下文智能判断漏洞是否真实存在。支持对用户进行多种协议的弱口令爆破（可自定义弱口令库），检测出攻击者能够爆破利用的弱口令。

支持展示当前最新的检测结果中新增WEB/主机漏洞和本次被修复的WEB/主机漏洞、新增弱口令和本次被修复的弱口令；支持展示客户当前环境的主机中存在的高危端口服务的检测结果；支持展示用户安全事件发现的变化趋势。（提供此项功能性截图证明文件并加盖供应商公章）

3.5.2互联网资产梳理、管理服务

供应商须对采购人在互联网上的资产进行梳理和排查，通过关联主体发现、域名探测、主机IP探测、站点探测、组件探测、端口服务探测等方式快速发现客户全网的域名、站点、IP、服务、数字证书、等资产信息，找出已知和未知资产。

提供资产管理服务平台，结合资产的信息、业务属性进行动态的安全标记，形成资产台账进行管理，全方面识别用户数字资产暴露面。提供自定义资产和人工添加资产能力。对具备有效期的资产如域名、证书等需做到实时数据查询和到期提醒。

3.6其他要求

3.6.1供应商应与合同签订后10个工作日内向采购提交《信息系统安全等级保护测评方案》经采购人审核同意后方可实施。

3.6.2本次信息安全等级保护测评需按照“成都市网络安全大队”和“信息安全等级保护测评”相关政策要求进行测评。测评过程中提供《信息系统安全等级保护测评现场测评结果记录表》

3.6.3测评完成之后, 供应商须协助本中心完成信息系统整改,供应商所提供的整改建议科学、合理、有效、并及时跟进整改情况；

3.6.4供应商在测评完成之后，出具符合标准要求的系统安全等级保护测评报告；

3.6.5供应商在测评完成之后，供应商根据采购人系统现状与标准的差距情况提供整改建议方案。

**（二）商务要求：**

1.付款方式

合同签订后采购人收到供应商提供的发票资料后10个工作日内向供应商预付40%的合同金额。

测评工作完成，供应商出具测评报告经采购人确认后，供应商向采购人开具发票，采购收到响应票据资料后10个工作日内，支付合同总金额30%。

项目实施完毕经采购人验收合格后供应商开具发票，采购人收到相应票据资料后10个工作日内，支付合同总金额剩余30%。

2.测评时间：接采购人测评通知后45个工作日完成并出具测评报告。

3.咨询服务期限：一年（合同签订之日起）

4.服务地点：彭州市妇幼保健院

5.验收时间及内容：

5.1供应商需在项目工期内按要求完成项目。如供应商逾期未完成合同约定事项，每逾期一日，应按合同总金额的0.1％向甲方支付违约金，最高不超过本合同金额的10％，逾期超过30日的，甲方有权解除本合同，乙方应当支付甲方逾期时间范围内所产生的违约金。

5.2供应商在完成测评和取得成都市公安局信息系统安全等级保护备案证明后，采购人在10个工作日内组织有关单位或人员进行验收，验收合格后出具验收报告，若验收不合格供应商应在约定时间内完成整改后重新申请验收。

5.3若采购人无故不予验收，在供应商提出验收申请并提交相关验收资料的30个工作日后，视为验收合格。