瑞安市妇幼保健院等保测评招标技术要求

**一、供应商资格要求：**

1、符合《中华人民共和国政府采购法》第二十二条对供应商的资格要求；

2. 供应商具有网络安全等级测评与检测评估机构服务认证证书且近五年没有被主管部门处罚；

3. 不接受联合体投标；

4、法律、行政法规规定的其他条件。

**二、招标内容**：

**本次测评的信息系统清单如下表：**

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 级别 |
| 1 | 基础支撑系统 | 三级 |
| 2 | 面向患者的业务系统 | 三级 |

等级保护测评内容：在服务期限内，完成2个信息系统等级保护测评工作，具体测评内容包括物理安全、网络安全、主机系统安全、应用安全和数据安全、安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等十个方面的安全测评，提交系统安全保护等级测评报告，并协助做好现场测评完成后的整改工作。

信息系统安全检查：瑞安市妇幼保健医院目前运行的信息系统众多，根据等级保护测评结果、整改建议，结合信息系统实际情况，通过安全扫描、渗透检测、应急响应、安全巡查等专业服务，对主要信息系统开展安全检查，保障网络和重要信息系统安全、稳定、高效运行。

等级保护测评内容：在服务期限内，完成2个信息系统等级保护测评工作，2个系统分别为（1）基础支撑系统（三级）、（2）面向患者服务系统（三级），具体测评内容包括物理安全、网络安全、主机系统安全、应用安全和数据安全、安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等十个方面的安全测评，提交系统安全保护等级测评报告，并协助做好现场测评完成后的整改工作。

协助加固：在服务期内根据用户需要不限次数，针对安全漏洞和安全配置评估中发现的安全漏洞和配置缺陷，提供加固意见和方案，配合客户完成配置修复。

1. **实施要求：**

**（一）测评应满足的原则**

本次安全保护等级保护测评实施方案设计与具体实施应满足以下原则：

a、保密原则：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，不得利用此数据进行任何侵害采购人的行为，否则采购人有权追究投标供应商的责任。

b、标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

c、规范性原则：投标供应商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

d、可控性原则：测评服务的进度要跟上进度表的安排，保证采购人对于测评工作的可控性。

e、整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

f、最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

**（二）安全测评报告**

a、投标供应商应对采购人的信息系统进行等级保护测评，形成相应的报告。

b、投标供应商在测评后出具符合公安局要求的系统安全保护等级测评报告；

c、对上述系统不符合信息安全等级保护有关管理规范和技术标准的，投标供应商出具可行整改方案并协助采购人整改服务。

d、投标供应商协助采购人办理信息系统安全保护等级测评备案手续。

**（三）本次等级保护测评的整体要求**

A、投标供应商应详细描述本次等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

B、投标供应商应详细描述测评人员的组成、资质及各自职责的划分。投标供应商应配置有经验的测评人员进行本次等级保护测评工作。

C、本次等级保护测评实施过程中所使用到的各种工具软件由投标供应商推荐，经采购人确认后由投标供应商提供并在测评中使用。在报价文件中应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

D、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投标供应商推荐，经采购人确认后由投标供应商提供并在测评中使用。

E、安全测评需要的运行环境（如场地、网络环境等）由采购人提供，投标供应商应详细描述需要的运行环境的具体要求。

F:本次项目实施骨干人员至少包含1名高级测评师（提供证书复印件）。本项目负责人必须具有5年以上的测评工作经验，并参与过具有大型复杂测评项目的实施经验，项目团队成员具有高级测评师且同时具有公安部科学技术奖证书、实施团队人员具有高级测评师且同时具有全国信息安全标准化技术委员会颁发的信息安全标准优秀应用案例奖证书；承担本次项目的项目经理必须同时具有高级测评师证书、国家重要信息系统保护人员培训证书（CIIPT）、信息安全管理系统审计认证（DNV）、信息安全保障人员认证证书(CISAW)、渗透测试认证证书（NSCP)、国家级优秀科技成果完成者证书、商用密码应用安全性评估人员测评能力证书，确保项目的顺利实施。

**(四)项目验收**

（1）本项目的目标是输出等级保护测评报告，并配合办理信息系统安全保护测评评备案手续，该项目将产生一定数量的文档。

（2）投标供应商应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责。

（3）投标供应商应提交验收方案，供采购人参考。

（4）采购人将依据本项目的要求，组织相关部门或单位的技术专家对投标供应商提交的项目成果进行验收。

**（五）项目承诺**

（1）投标供应商应满足采购人提出的标准性、规范性、可控性、整体性、最小影响性及保密性原则，做到守时、保质。

（2）保密性要求：投标供应商必须和采购人签订保密协议和非侵害性协议，投标供应商必须要与参加此次测评项目的所有项目组成员签订保密协议和非侵害性协议，在合同签定时一并提供给采购人。

（3）投标供应商具体测评工作和等级保护测评报告的编写，必须在采购人的指定地点进行。对于测评中的重要资料和结果，在测评期间和测评结束后，投标供应商不得带离该地点。

（4）投标供应商对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论投标供应商中标与否，其对上述内容的保密责任将长期存在。

（5）等级保护测评的品质保证：投标供应商应承诺指派工作经验丰富、技术实力雄厚的安全顾问，结合技术领先、结论可靠的测评工具为客户作全面等级保护测评。承诺测评过程按照国家标准进行，并保证对客户的资料严格保密。

**（六）其它要求**

（1）投标供应商在测评方案书中，对能提供的信息系统安全等级保护测评进行详细说明，可根据具体情况在项目方案中提出建议，并附详细资料和说明。

（2）投标供应商应对提供测评服务时所使用的设备及软件保证拥有设备软硬件的知识产权和所有权，并对所涉及的专利、知识产权等法律条款承担义务，采购人以上问题不承担任何法律责任。

（3）若投标供应商的设备和系统包含自己的专用标准，应在建议书中具体说明，并附上相应的详细技术资料。

**（七）项目成果**

提交包括且不仅仅包括以下成果：

《信息系统安全整改规划》

《信息系统等级保护测评报告》

**（八）、服务要求**

（1）本项目服务要求提供本地化服务人员，提供7×24小时本地响应服务。协助招标人处理重大突发信息安全事件。

（2）中标人对本次安全服务项目实施过程产生的数据严格保密，未经招标人授权，不得以任何方式将有关系统数据信息披露、发表或传播。中标人需与招标人签订相关保密协议。

（3）在2022年12月中旬，完成2个系统的测评工作，本次安全服务采购项目的服务期为一年。