附件：

第一部分 供应商资格要求

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）具有依法缴纳税收和社会保障资金的良好记录；

（五）参加本次政府采购活动前三年内，在经营活动中没有重大违法违规记录；

（六）法律、行政法规规定的其他条件；

（七）采购项目的特定条件：具有信息安全等级保护测评资质。

**注：供应商应对相关资料的真实性、合法性、完整性负责，现场审查过程对资料不真实、不合法或不完整的，将不给予参选资格。**

第二部分 项目内容及要求

### **项目概述**

 **本项目最高预算价45000元，超过最高预算价为无效报价。**

依照国家《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统安全保护等级定级指南》等标准，对照信息系统等级保护工作的有关规定和要求，对网络和信息系统进行等级保护定级，按信息系统编制定级报告和定级备案表，并指导信息化人员将定级材料提交当地公安机关备案。通过物理安全、网络安全、主机安全、应用安全、数据安全五个方面基本技术要求进行测评；为满足安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理五个方面基本管理要求进行管理体系建设。使得网络系统的等级保护建设方案最终既可以满足等级保护的相关要求，又能够全方面为业务系统提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

### **二、采购项目技术、服务要求**

（一）采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 系统名称 | 服务要求 | 采购数量 | 计量单位 |
| 1 | 血站管理信息系统 | 等级保护二级测评服务 | 1 | 项 |

**（二）服务内容**

依据国家等级保护相关政策、标准以及其它相关要求，并结合血站管理信息系统具体情况，对该信息系统进行等级保护测评，内容包括：

1、完成上表中信息系统的网络安全等级定级和备案工作，必须保证每项信息系统定级、备案通过市级及以上公安机关的备案手续，取得相应等级保护证书。

2、按照信息系统安全等级保护要求，对上表中各信息系统完成系统拓扑结构及说明；完成广安市公安部门认可的系统等级测评报告。

3、现状测评，至少包括：

（1）安全技术测评。包括物理环境安全，网络通信安全、安全区域边界、安全计算环境、安全管理中心五个方面的安全测评。

（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、安全运维管理等五个方面的安全测评。

（3）形成差距分析报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出差距测评结论（结论为达标、基本达标、不达标）。根据测评结果制定《血站管理信息系统测评差距分析报告》，列出被测信息系统中存在的主要问题以及可能造成的后果。

4、编制系统安全整改方案。依据差距分析报告结果，编制针对各信息系统的安全整改建设方案，方案要具有可行性；。

5、协助完成管理制度的修制定：根据广安市中心血站单位血站管理系统的具体情况，制定有效的信息管理制度。

6、协助完成整改工作。依据整改方案，为血站管理系统安全整改的各项工作提供技术咨询服务，并协助制定整改计划和确定网络安全整改标准和整改结果达标确认。

7、等级测评，至少包括：

（1）按照等级保护相关标准对系统从技术、管理等方面进行安全等级测评工作。

（2）编制测评报告。制定并提交《血站管理信息系统测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求，备案证明作为验收材料之一。

8、对信息系统进行技术测试和安全扫描，测试各系统的可用性、可靠性、安全漏洞、系统后门、病毒木马、受攻击情况、网页篡改情况、系统防篡改能力等，测评报告内容、格式、规范和结果必须符合市级以上公安机关相关要求和认可。

 **(三)测评依据：**

此次测评依据的标准包括但不限于以下规范性文件：

基础类标准

《计算机信息系统安全保护等级划分准则》GB 17859-1999

应用类标准

网络定级：

《信息安全技术 信息系统安全等级保护定级指南》GB/T 22240-2008

《网络安全等级保护定级指南》GA/T 1389-2017

等级保护实施：

《信息安全技术 信息系统安全等级保护实施指南》GB/T 25058-2010

网络安全建设：

《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 网络安全等级保护设计技术要求》GB/T 25070-2019

《信息安全技术 信息系统通用安全技术要求》GB/T 20271-2006

《信息安全技术 信息系统等级保护安全设计技术要求》GB/T 24856-2009

《信息安全技术 信息系统安全管理要求》GB/T 20269-2006

《信息安全技术 信息系统安全工程管理要求》GB/T 20282-2006

《信息安全技术 信息系统安全物理环境技术要求》GB/T 21052-2007

《信息安全技术 网络基础安全技术要求》GB/T 20270-2006

《信息系统安全等级保护体系框架》GA/T 708-2007

《信息系统安全等级保护基本模型》GA/T 709-2007

《信息系统安全等级保护基本配置》GA/T 710-2007

管理：

《信息系统安全管理要求》GB/T 20269-2006

《信息系统安全工程管理要求》GB/T 20282-2006

等级测评：

《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 网络安全等级保护测评过程指南》GB/T 28449-2018

《信息系统安全管理测评》GA/T 713-2007

其他类标准：

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

《信息安全事件管理指南》GB/Z 20985-2007

《信息安全事件分类指南》GB/Z 20986-2007

《信息系统灾难恢复规范》GB/T 20988-2007

 **(四)测评应满足的原则**

本次信息系统安全等级保护测评服务方案设计，以及具体实施内容应满足以下原则：

（1）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人的责任。

（2）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。

（3）规范性原则：投标人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。

（4）可控性原则：等保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。

**(五)本次网络安全等级保护测评的整体要求。**

（1）投标人应详细描述本次项目整体实施方案，包括项目概述、等保测评服务方案、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。

（2）投标人应详细描述服务人员的组成、资质及各自职责的划分。投标人应配置有经验的测评人员进行本次等级保护测评工作。

（3）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人推荐，经采购人确认后由投标人提供并在测评中使用。

（4）投标人根据采购人现有场地和网络环境提出相应的运行环境的具体要求。

（5）本次测评，因问题整改有可能涉及多次测评，相关费用均已包含在本次投标报价中，采购人不再支付费用。

**（六）本次等级测评内容**

测评服务内容包括但不仅限于以下内容：

1.安全技术测评：包括物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复五个方面的安全测评；

（1）物理安全测评

物理安全检测应当包含：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、电磁防护等十个单元。

（2）网络安全测评

网路安全测评应当包含：结构安全、访问控制、网络安全审计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备防护等。

（3）主机安全测评

主机安全测评应当包含：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制等。

（4）应用安全测评

应用安全测评应当包含：身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制。

（5）数据安全及备份恢复测评

数据安全及备份恢复测评应当包含：数据完整性、数据保密性、备份和恢复。

2.安全管理测评：安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

（1）安全管理制度测评

安全管理制度测评应当包含：管理制度、制定与发布、审批和修订。

（2）安全管理机构测评

安全管理机构测评应当包含：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

（3）人员安全管理测评

人员安全管理测评应当包含：人员录用、人员离岗、人员考核、安全意识教育和培训、第三方人员访问管理。

（4）系统建设管理测评

系统建设管理测评应当包含：系统定级、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、系统备案、测评、安全服务商选择。

（5）系统运维管理测评

系统运维管理测评应当包含：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。

3.安全漏洞扫描

安全漏洞扫描应当依据GB/T 18336-2015《信息技术 安全技术 信息技术安全性评估准则》、GB/T 20274-2008《信息系统安全保障评估框架》对被测评单位被测信息系统的应用安全漏洞、主机安全漏洞、数据库安全漏洞三个内容进行测评。

**（七）实施和保障方案**

1.项目进度要求

本项目测评实施要求同步实施、重点先行、阶段性成果展现相结合。

具体实现进度要求如下：

本次信息系统安全等级保护测评服务工作分为：测评准备、方案编制、现场测评、问题整改、回归测评、报告编制等几个阶段。

（1）第一阶段：

组建项目组，制定信息安全等级保护测评项目计划书、测评实施方案以及人员安全培训计划，并提交被测评单位审核。

（2）第二阶段：

进行现场测评，同时对被测评单位信息安全相关管理和技术人员进行安全技术培训。初次测评完成后，提交初评的整改意见报告。

（3）第三阶段：

协助被测评单位针对测评过程中发现的安全问题进行技术整改加固工作，并进行整改后的回归测评。

（4）第四阶段：

整理测评结果，向被测评单位提交被测信息系统安全等级保护测评报告、定级备案证书、以及相应文档。

2.项目实施要求

依据国家各项相关标准法规和被测评单位现有的规范、制度，同时结合项目实际需要，对信息安全等级保护项目工作中的定级、备案、测评（包括测评范围、测评方法等）、整改（包括整改方法、范围等）过程中，所需的产品、技术、制度、流程、建设要求和实施规范等方面，提供咨询、测评、整改建议以及整个建设过程的监督和管理等服务。所提供的整体方案需包括技术方案和实施方案。技术方案包括整体流程、技术方法和服务方案设计等，需要对每项技术方法的应用位置进行详细描述，对系统进行详细的测评，发现系统不足，明确安全风险隐患和差距，提出整改意见，协助被测评单位信息安全管理人员进行整改；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等，需要明确每项工作的时间安排、操作时间和操作人员。投标人负责提供的服务内容至少应包括，但不限于以下各项：

（1）服务提供商在信息安全等级保护测评前应制定详细的技术方案，包括信息安全等级保护测评项目计划书、测评实施方案以及人员安全培训计划等，并提交被测评单位审核。

（2）信息安全等级保护测评包括但不限于以下对象：网络结构、网络服务、主机系统、存储备份系统、数据库、中间件、应用系统、数据安全、安全系统、系统安全策略等。

（3）服务提供商应描述测评服务的技术方案，包括准备工作、技术措施、人员安排、时间进度、可能对系统造成的影响等。

（4）安全测评工作应尽量选择在非业务繁忙时段进行，将对被测系统可能带来的影响减至最小。

（5）信息安全等级保护测评完后，协助被测评单位整理备案材料和进行安全主管部门备案工作。

（6）服务提供商应书面承诺能够积极与被测评单位协作，共同完成本项目的测评工作，项目实施过程中出现问题不得互相推诿，双方应主动进行沟通，并及时解决问题，确保项目顺利实施。

3.项目管理要求

对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，投标人必须提供完整的项目管理方案，项目的方案设计与具体实施应满足以下原则：

（1）最小影响原则：工作应尽可能小的影响系统和网络的正常运行，不能对网络的运行和业务的正常运行产生显著影响（包括系统性能明显下降、网络拥塞、服务中断）；

（2）标准性原则：服务方案的设计与实施应依据国家相关标准进行，包括但不限于《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019，符合《信息安全等级保护管理办法（公通字[2007]43号）》、《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/T 25058-2010）》等国家标准；

（3）规范性原则：服务提供商工作中的过程和文档，应具有较好的规范性，便于项目的跟踪和控制；

（4）可控性原则：方法和过程要在双方认可的范围之内，安全服务的进度要按照进度表安排实施，保证被测评单位对于服务工作的可控性；

（5）整体性原则：评估内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患；

（6）保密原则：对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招标人的行为，否则被测评单位有权追究服务提供商的责任。

服务提供商需根据上述要求，提供项目详细的项目管理方案，并予以详细解释。

**三、商务要求**

|  |  |  |
| --- | --- | --- |
| 序号 | 内容 | 采购要求 |
| 1 | 服务期限 | 合同签订后60个工作日内。 |
| 2 | 履约、验收要求与标准 | 按照《四川省政府采购项目需求论证和履约验收管理办法》（川财采〔2015〕32号）的要求进行验收，采购人可以委托专业人员验收，必要时可以邀请相关监督部门现场监督。 |
| 3 | 付款方式 | 甲方在乙方协助下取得公安机关出具的等级保护备案证明及乙方开具的发票后10个工作日内，甲方向乙方支付合同价款总额100%的款项。 |
| 4 | 交货地点 | 广安市中心血站 |
| 5 | 分包履约 | 本项目不允许成交方将合同内容分包履约。 |

### **四、售后服务**

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.服务提供商应协助、配合被测评单位与上级监管部门、公安机关的沟通协调。在测评过程中和测评完成后，协助、配合被测评单位进行相关的信息系统安全整改，确保已定级系统达到等级保护的相关要求，并通过上级监管部门和公安机关的审核验收。

3.服务提供商应在项目期内向被测评单位提供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，及时告之被测评单位，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。

4.服务提供商应在项目实施过程中，对被测评单位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。

5.服务提供商应在项目开始前，与被测评单位签订保密协议，严格遵守法律法规，对被测评单位商业秘密、系统风险信息、项目实施内容及成果信息进行严格保密，未经被测评单位同意，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。

说明：

1、响应文件报价表将按采购清单中产品名称顺序报价。

2、以上技术服务要求、商务要求及售后服务为本次采购活动满足采购产品质量和服务的最低要求，要求必须完全满足。

四、验收及其他要求

严格参照《四川省政府采购项目需求论证和履约验收管理办法》（川财采〔2015〕32号）的要求进行验收。

验收以交付物作为主要验收依据，包括但不限于：

|  |  |  |
| --- | --- | --- |
| 序号 | 文档类型 | 文档名称 |
| 1 | 项目实施过程文档 | 测评方案、计划 |
| 3 | 项目实施过程文档 | 安全整改建议方案 |
| 4 | 项目成果文档 | 信息系统安全等级测评报告 |
| 5 | 项目成果文档 | 安全优化建议方案 |
| 6 | 其他要求的文档 | 根据采购人、公安等主管部门要求 |

第三部分 投标文件的组成

**一、资格部分**

1、营业执照（供应商是社会团体、事业单位的提供法人证书，供应商是非企业专业服务机构的提供执业许可，供应商是自然人的提供自然人身份证明）复印件；

2、法定代表人授权委托书原件（注：①授权委托书按邀请文件第五部分中“法定代表人授权委托书”格式提供；②如参选申请文件均由供应商法定代表人签字的，则可不提供）；

3、法定代表人身份证复印件及代理人身份证复印件（注：如参选申请文件均由供应商法定代表人签字的，则只需提供法定代表人身份证复印件）；

4、《网络安全等级保护评测机构推荐证书》

**注：以上要求提供的资格证明文件如不是原件请加盖公章（是原件的按照邀请文件要求格式提供）。**

**二、技术、服务部分**

1、供应商基本情况表。

2、项目服务内容；

3、项目实施方案；

**三、报价部分**

1、供应商的报价是供应商响应本项目要求的全部工作内容的价格体现，包括供应商完成本项目所需的一切费用以及邀请文件规定的其他费用。

2、以人民币报价。

3、其他需要澄清、补充或更正的事项。

4、供应商只允许有一个报价，任何有选择或可调整的报价将不予接受。