**四川省政府政务服务和公共资源交易服务中心 系统安全等级保护测评和12345政务服务热线及网络理政平台等级保护项目**

**比**

**选**

**文**

**件**

**四川省政府政务服务和公共资源交易服务中心**

**2025年6月**

# **第一章** **采购邀请函**

本项目为四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评和12345政务 服务热线及网络理政平台等级保护项目，采购单位为四川省政府政务服务和公共资源交易服务中心。本项目采购内容在规定的集中采购目录之外，且在省直部门分散采购限额标准以下，因此我中心拟用比选方式进行自行采购。

**1、项目概况：**

1.1采购项目：四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评和12345政务服务热线及网络理政平台等级保护项目。

1.2项目资金：预算内资金。

1.3项目实施方式：内部采购。

1.4质量效果要求：符合国家相关要求。

1.5采购内容：

采购包1：2025年交易系统、专家库系统、服务平台、OA系统、内控系统网络安全等级保护。

#### 采购包2：2025年12345政务服务热线及网络理政平台网络安全等级保护。

1.6项目预算：

采购包1：人民币 32 万元整（叁拾贰万圆整）

采购包2：人民币 8 万元整（捌万圆整）

1.7中选原则：**根据综合评分法按排名由高到低推荐第一名为中标候选人。**

**2、资格审查方式及供应商资格要求**

本项目采用资格预审，采购评审小组根据采购文件的规定对供应商进行资格审查，若资格审查不合格其响应文件将被否决，采购申请人资格要求如下：

2.1具有独立承担民事责任的能力。

2.2证明材料：提供营业执照复印件。

2.3具有良好的商业信誉和健全的财务会计制度。

2.4具有履行合同所必需的设备和专业技术能力。

2.5有依法缴纳税收和社会保障资金的良好记录。

2.6参加政府采购活动近三年内，在经营活动中没有重大违法记录。

2.7法律、行政法规规定的其他条件。

#### 2.8根据项目特殊要求设置的特定条件（不得以不合理的条件对供应商实行差别待遇或歧视待遇）：无

**3、报名方式**

供应商通过省中心门户网站采购公告自行下载比选文件。获取文件时间为2025年6月4日至6月8日17:00（北京时间）。

**4、响应文件的递交**

比选文件提交的截止时间为2025年6月9日上午10：00（北京时间），提交地点：四川省成都市青羊区鼓楼南街101号丰德成达中心10楼1005。逾期送达的比选文件将被拒绝。

本次采购项目将于2025年6月9日在四川省成都市青羊区鼓楼南街101号丰德成达中心10楼进行评审。无需采购申请人的法定代表人或其委托的授权代表参加。

**5、联系方式**

四川省政府政务服务和公共资源交易服务中心

联 系 人：郭老师 联系电话：86953169

# 第二章 技术规范要求

## **一、项目概述**

采购包1：

为了保障四川省公共资源交易服务平台、四川省综合评标专家库系统、四川省公共资源交易电子招投标系统、OA系统、内控系统安全、稳定、可靠、高效的运行，按照国家网络安全等级保护系列标准要求，需要对其进行安全等级保护三级测评。测评内容包括：信息系统技术安全性测评及信息系统管理安全性测评；信息系统技术安全性测评包括但不限于：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；信息系统管理安全测评包括但不限于：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；安全漏洞扫描包括但不限于：应用系统漏洞扫描、应用服务器漏洞扫描、数据库服务器漏洞扫描。通过测评，对照相应安全等级保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，制订出整改措施，出具测评报告，并按照公安部制定的要求完成信息系统安全等级保护定级备案工作。

采购包2：

为了保障12345政务服务热线及网络理政平台安全、稳定、可靠、高效的运行，按照国家网络安全等级保护系列标准要求，需要对其进行安全等级保护三级测评。测评内容包括：信息系统技术安全性测评及信息系统管理安全性测评；信息系统技术安全性测评包括但不限于：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；信息系统管理安全测评包括但不限于：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；安全漏洞扫描包括但不限于：应用系统漏洞扫描、应用服务器漏洞扫描、数据库服务器漏洞扫描。通过测评，对照相应安全等级保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，制订出整改措施，出具测评报告，并按照公安部制定的要求完成信息系统安全等级保护定级备案工作。

## **二、服务内容技术、服务要求**

### （一）服务目标

采购包1：

依据国家和行业信息安全的相关标准，全面了解和掌握企业为系统现有安全状况，找出其与《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）对应级别的差距，及时发现系统存在的安全问题，针对等级保护测评中发现的各种安全风险，测评项目组提出适宜的安全整改建议，最终提交该系统等级保护测评报告。

采购包2：

依据国家和行业信息安全的相关标准，全面了解和掌握企业为系统现有安全状况，找出其与《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）对应级别的差距，及时发现系统存在的安全问题，针对等级保护测评中发现的各种安全风险，测评项目组提出适宜的安全整改建议，最终提交该系统等级保护测评报告。

★（二）工作内容及要求

采购包1：

**2.1测评对象**

|  |  |
| --- | --- |
| 系统名称 | 安全等级 |
| 四川省公共资源交易服务平台 | 第三级 |
| 四川省综合评标专家库系统 | 第三级 |
| 四川省公共资源交易电子招投标系统 | 第三级 |
| OA系统 | 第三级 |
| 内控系统 | 第三级 |

具体服务内容包括：

1、协助四川省政府政务服务和公共资源交易服务中心需要进行测评的信息系统进行定级、备案材料的编写，协助采购方到公安监管等部门办理备案手续，确保信息系统安全保护等级定级准确、备案完整。

2、按照《信息安全技术网络安全等级保护基本要求》对系统从技术、安全管理等方面进行安全等级测评工作。

3、形成问题汇总及整改意见报告。根据测评结果，对等级测评结果进行汇总统计，并编制系统等级保护测评问题汇总及整改意见报告，列出被测系统中存在的主要问题和整改意见。

4、协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询与支撑服务。

5、编制并提交等级保护测评报告，报告需提交公安机关有关部门备案，且能满足合规性要求。

**2.2测评要求**

根据项目需求，为保障信息安全现场测评过程安全可控，明确测评人员职责分配、规范测评人员操作，保障测评结果有效，至少包括以下几个流程：

| 序号 | 关键实施阶段 | 工作要求 |
| --- | --- | --- |
| 1 | 确定测评范围 | 明确本次被测评信息系统的范围，包括每个信息系统的范围、信息系统的边界等。 |
| 2 | 获得信息系统的信息 | 通过调查或查阅资料的方式，了解被测评信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等。 |
| 3 | 确定具体的测评对象 | 初步确定每个信息系统的被测评对象，包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。 |
| 4 | 确定测评工作的方法 | 根据信息系统安全等级情况、系统规模大小等，明确本次测评的方法。 |
| 5 | 制定测评工作计划 | 制定测评工作计划或方案，说明测评范围、测评对象、工作方法、人员组成、角色职责、时间计划等。 |
| 6 | 实施等级保护测评 | 实施测评，包括人工检查、工具扫描等方式。 |
| 7 | 项目总结 | 对测评结果进行总结、汇报。 |

**2.3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供应商的责任。

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：供应商工作中的过程和文档，具有很好的规范性，以便于项目的跟踪和控制。

4、可控性原则：等级保护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。

5、整体性原则：等级保护测评服务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。

6、最小影响原则：等级保护测评服务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。供应商应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

**2.4测评依据**

供应商应按照下面所列出的标准、规程和规定进行设备的设计、制造和试验，本设备技术规范中所使用的标准或规程应是最新版，本技术条款提出了最低限度的技术要求，并未规定所有的技术要求和适用的标准，对国家有关的强制性标准，必须满足其要求。

* 《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》 （国务院令第147号）
* 《信息安全等级保护管理办法》（公通字[2007]43号）
* GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》
* GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》
* GB 17859-1999：《计算机信息系统安全保护等级划分准则》
* GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》
* GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》
* T/ISEAA 001-2020：《网络安全等级保护测评高风险判定指引》

**2.5 服务内容**

按照网络安全等级保护测评依据开展测评工作（包括不限于以下内容）：

（一）安全物理环境

安全物理环境等级测评将通过访谈和检查的方式评测该信息系统的物理环境安全保障情况，主要涉及对象为机房。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 物理位置选择 | 通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
| 2 | 物理访问控制 | 通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
| 3 | 防盗窃和防破坏 | 通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
| 4 | 防雷击 | 通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
| 5 | 防火 | 通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
| 6 | 防水和防潮 | 通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。 |
| 8 | 温湿度控制 | 通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。 |
| 9 | 电力供应 | 通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。 |
| 10 | 电磁防护 | 通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |

（二）安全通信网络

安全通信网络测评将通过访谈、检查和测试的方式评测该信息系统的通信网络安全保障情况。主要涉及对象为网络拓扑结构。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 网络架构 | 测评分析网络架构与网段划分、隔离等情况的合理性和有效性。 |
| 2 | 通信传输 | 测评通信过程中的完整性、保密性等。 |
| 3 | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |

（三）安全区域边界

安全区域边界安全测评将通过访谈、检查和测试的方式评测该信息系统的区域边界安全保障情况。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 边界防护 | 测评分析信息系统网络边界安全防护的状况。 |
| 2 | 访问控制 | 测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。 |
| 3 | 入侵防范 | 测评分析信息系统对攻击行为的识别和处理情况。 |
| 4 | 恶意代码和垃圾邮件防范 | 测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮件的防护情况。 |
| 5 | 安全审计 | 测评分析信息系统审计配置和审计记录保护情况。 |
| 6 | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |

（四）安全计算环境

安全计算环境测评将通过访谈、检查和测试的方式评测该信息系统的各类计算环境，包括网络互联设备、安全设备、服务器、数据库、终端、应用软件等的安全保障情况。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 身份鉴别 | 检查服务器的身份标识与鉴别和用户登录的配置情况。 |
| 2 | 访问控制 | 检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。 |
| 3 | 安全审计 | 检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。 |
| 4 | 入侵防范 | 检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 |
| 5 | 恶意代码防范 | 检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。 |
| 6 | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |
| 7 | 数据完整性 | 测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。 |
| 8 | 数据保密性 | 测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。 |
| 9 | 数据备份恢复 | 测评信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。 |
| 10 | 剩余信息保护 | 测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。 |
| 11 | 个人信息保护 | 测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。 |

（五）安全管理中心

安全管理中心测评将通过访谈和检查的方式评测该信息系统的安全管理保障情况。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 系统管理 | 测评信息系统的系统管理员对系统的管理情况。 |
| 2 | 审计管理 | 测评信息系统的安全审计员对系统的审计情况。 |
| 3 | 安全管理 | 测评信息系统的安全管理员对系统的安全策略的配置情况。 |
| 4 | 集中管控 | 测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。 |

（六）安全管理制度

安全管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 安全策略 | 测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。 |
| 2 | 管理制度 | 测评信息系统管理制度在内容覆盖上是否全面、完善。 |
| 3 | 制定和发布 | 测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 |
| 4 | 评审和修订 | 测评信息系统管理制度定期评审和修订情况。 |

（七）安全管理机构

安全管理机构测评将通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 岗位设置 | 测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。 |
| 2 | 人员配备 | 测评信息系统各个岗位人员配备情况。 |
| 3 | 授权和审批 | 测评信息系统对关键活动的授权和审批情况。 |
| 4 | 沟通与合作 | 测评信息系统内部部门间、与外部单位间的沟通与合作情况。 |
| 5 | 审核和检查 | 检查信息系统安全工作的审核和测评情况。 |

（八）安全管理人员

安全管理人员测评将通过访谈和检查的形式评测机构人员安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 人员录用 | 测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
| 2 | 人员离岗 | 测评信息系统人员离岗时是否按照一定的手续办理。 |
| 3 | 安全意识教育和培训 | 测评是否对人员进行安全方面的教育和培训。 |
| 4 | 外部人员访问管理 | 测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |

（九）安全建设管理

安全建设管理测评将通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 定级和备案 | 测评是否按照一定要求确定系统的安全等级并完成备案工作。 |
| 2 | 安全方案设计 | 测评系统整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购和使用 | 测评是否按照一定的要求进行系统的产品采购。 |
| 4 | 自行软件开发 | 测评自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
| 5 | 外包软件开发 | 测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。 |
| 6 | 工程实施 | 测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
| 7 | 测试验收 | 测评系统运行前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 测评是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 等级测评 | 测评是否依据国家要求完成等级测评和整改工作。 |
| 10 | 服务供应商选择 | 测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

（十）安全运维管理

安全运维管理测评将通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 环境管理 | 测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。 |
| 2 | 资产管理 | 测评是否采取必要的措施对系统的资产进行分类标识管理。 |
| 3 | 介质管理 | 测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
| 4 | 设备维护管理 | 测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
| 5 | 漏洞和风险管理 | 测评是否采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补。测评是否定期开展安全测评。 |
| 6 | 网络和系统安全管理 | 测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。 |
| 7 | 恶意代码防范管理 | 测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。 |
| 8 | 配置管理 | 测评是否记录和保存系统的基本配置信息 |
| 9 | 密码管理 | 测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
| 10 | 变更管理 | 测评是否采取必要的措施对系统发生的变更进行有效管理。 |
| 11 | 备份与恢复管理 | 测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
| 12 | 安全事件处置 | 测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。 |
| 13 | 应急预案管理 | 测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |
| 14 | 外包运维管理 | 测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。 |

**2.6项目管理**

供应商必须提供完整的项目管理方案，供应商需要针对以下项目管理要求进行项目管理服务要求进行承诺，未提供项目管理服务承诺为无效供应商。

（1）供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任；

（2）应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力；

（3）供应商在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留；

（4）供应商的岗位配置要至少配置测评师、项目经理、渗透工程师、质量主管等并明确各个岗位的相关职责。

（5）测评工具要求

①采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件；

②采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品；
 ③采用的测评工具的生产商应为正规厂商，能够对产品进行持续更新并提供质量和安全保障；
 ④测评机构所使用的测评工具不会对单位系统产生破坏或负面影响以及不影响医院业务正常开展。

**2.7交付产物**

包括但不仅限于以下资料：

|  |  |
| --- | --- |
| 1 | 网络安全等级保护测评报告（包含整改建议） |
| 2 | 其他未列入的应交资料 |

采购包2：

**2.1测评对象**

|  |  |
| --- | --- |
| 系统名称 | 安全等级 |
| 12345政务服务热线及网络理政平台 | 第三级 |

具体服务内容包括：

1、协助四川省政府政务服务和公共资源交易服务中心需要进行测评的信息系统进行定级、备案材料的编写，协助采购方到公安监管等部门办理备案手续，确保信息系统安全保护等级定级准确、备案完整。

2、按照《信息安全技术网络安全等级保护基本要求》对系统从技术、安全管理等方面进行安全等级测评工作。

3、形成问题汇总及整改意见报告。根据测评结果，对等级测评结果进行汇总统计，并编制系统等级保护测评问题汇总及整改意见报告，列出被测系统中存在的主要问题和整改意见。

4、协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询与支撑服务。

5、编制并提交等级保护测评报告，报告需提交公安机关有关部门备案，且能满足合规性要求。

**2.2测评要求**

根据项目需求，为保障信息安全现场测评过程安全可控，明确测评人员职责分配、规范测评人员操作，保障测评结果有效，至少包括以下几个流程：

| 序号 | 关键实施阶段 | 工作要求 |
| --- | --- | --- |
| 1 | 确定测评范围 | 明确本次被测评信息系统的范围，包括每个信息系统的范围、信息系统的边界等。 |
| 2 | 获得信息系统的信息 | 通过调查或查阅资料的方式，了解被测评信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等。 |
| 3 | 确定具体的测评对象 | 初步确定每个信息系统的被测评对象，包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。 |
| 4 | 确定测评工作的方法 | 根据信息系统安全等级情况、系统规模大小等，明确本次测评的方法。 |
| 5 | 制定测评工作计划 | 制定测评工作计划或方案，说明测评范围、测评对象、工作方法、人员组成、角色职责、时间计划等。 |
| 6 | 实施等级保护测评 | 实施测评，包括人工检查、工具扫描等方式。 |
| 7 | 项目总结 | 对测评结果进行总结、汇报。 |

**2.3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供应商的责任。

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：供应商工作中的过程和文档，具有很好的规范性，以便于项目的跟踪和控制。

4、可控性原则：等级保护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。

5、整体性原则：等级保护测评服务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。

6、最小影响原则：等级保护测评服务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。供应商应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

**2.4测评依据**

供应商应按照下面所列出的标准、规程和规定进行设备的设计、制造和试验，本设备技术规范中所使用的标准或规程应是最新版，本技术条款提出了最低限度的技术要求，并未规定所有的技术要求和适用的标准，对国家有关的强制性标准，必须满足其要求。

* 《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》 （国务院令第147号）
* 《信息安全等级保护管理办法》（公通字[2007]43号）
* GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》
* GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》
* GB 17859-1999：《计算机信息系统安全保护等级划分准则》
* GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》
* GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》
* T/ISEAA 001-2020：《网络安全等级保护测评高风险判定指引》

**2.5 服务内容**

按照网络安全等级保护测评依据开展测评工作（包括不限于以下内容）：

（一）安全物理环境

安全物理环境等级测评将通过访谈和检查的方式评测该信息系统的物理环境安全保障情况，主要涉及对象为机房。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 物理位置选择 | 通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
| 2 | 物理访问控制 | 通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
| 3 | 防盗窃和防破坏 | 通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
| 4 | 防雷击 | 通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
| 5 | 防火 | 通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
| 6 | 防水和防潮 | 通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。 |
| 8 | 温湿度控制 | 通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。 |
| 9 | 电力供应 | 通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。 |
| 10 | 电磁防护 | 通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |

（二）安全通信网络

安全通信网络测评将通过访谈、检查和测试的方式评测该信息系统的通信网络安全保障情况。主要涉及对象为网络拓扑结构。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 网络架构 | 测评分析网络架构与网段划分、隔离等情况的合理性和有效性。 |
| 2 | 通信传输 | 测评通信过程中的完整性、保密性等。 |
| 3 | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |

（三）安全区域边界

安全区域边界安全测评将通过访谈、检查和测试的方式评测该信息系统的区域边界安全保障情况。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 边界防护 | 测评分析信息系统网络边界安全防护的状况。 |
| 2 | 访问控制 | 测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。 |
| 3 | 入侵防范 | 测评分析信息系统对攻击行为的识别和处理情况。 |
| 4 | 恶意代码和垃圾邮件防范 | 测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮件的防护情况。 |
| 5 | 安全审计 | 测评分析信息系统审计配置和审计记录保护情况。 |
| 6 | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |

（四）安全计算环境

安全计算环境测评将通过访谈、检查和测试的方式评测该信息系统的各类计算环境，包括网络互联设备、安全设备、服务器、数据库、终端、应用软件等的安全保障情况。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 身份鉴别 | 检查服务器的身份标识与鉴别和用户登录的配置情况。 |
| 2 | 访问控制 | 检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。 |
| 3 | 安全审计 | 检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。 |
| 4 | 入侵防范 | 检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 |
| 5 | 恶意代码防范 | 检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。 |
| 6 | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |
| 7 | 数据完整性 | 测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。 |
| 8 | 数据保密性 | 测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。 |
| 9 | 数据备份恢复 | 测评信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。 |
| 10 | 剩余信息保护 | 测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。 |
| 11 | 个人信息保护 | 测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。 |

（五）安全管理中心

安全管理中心测评将通过访谈和检查的方式评测该信息系统的安全管理保障情况。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 系统管理 | 测评信息系统的系统管理员对系统的管理情况。 |
| 2 | 审计管理 | 测评信息系统的安全审计员对系统的审计情况。 |
| 3 | 安全管理 | 测评信息系统的安全管理员对系统的安全策略的配置情况。 |
| 4 | 集中管控 | 测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。 |

（六）安全管理制度

安全管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 安全策略 | 测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。 |
| 2 | 管理制度 | 测评信息系统管理制度在内容覆盖上是否全面、完善。 |
| 3 | 制定和发布 | 测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 |
| 4 | 评审和修订 | 测评信息系统管理制度定期评审和修订情况。 |

（七）安全管理机构

安全管理机构测评将通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 岗位设置 | 测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。 |
| 2 | 人员配备 | 测评信息系统各个岗位人员配备情况。 |
| 3 | 授权和审批 | 测评信息系统对关键活动的授权和审批情况。 |
| 4 | 沟通与合作 | 测评信息系统内部部门间、与外部单位间的沟通与合作情况。 |
| 5 | 审核和检查 | 检查信息系统安全工作的审核和测评情况。 |

（八）安全管理人员

安全管理人员测评将通过访谈和检查的形式评测机构人员安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 人员录用 | 测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
| 2 | 人员离岗 | 测评信息系统人员离岗时是否按照一定的手续办理。 |
| 3 | 安全意识教育和培训 | 测评是否对人员进行安全方面的教育和培训。 |
| 4 | 外部人员访问管理 | 测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |

（九）安全建设管理

安全建设管理测评将通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 定级和备案 | 测评是否按照一定要求确定系统的安全等级并完成备案工作。 |
| 2 | 安全方案设计 | 测评系统整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购和使用 | 测评是否按照一定的要求进行系统的产品采购。 |
| 4 | 自行软件开发 | 测评自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
| 5 | 外包软件开发 | 测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。 |
| 6 | 工程实施 | 测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
| 7 | 测试验收 | 测评系统运行前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 测评是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 等级测评 | 测评是否依据国家要求完成等级测评和整改工作。 |
| 10 | 服务供应商选择 | 测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

（十）安全运维管理

安全运维管理测评将通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 环境管理 | 测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。 |
| 2 | 资产管理 | 测评是否采取必要的措施对系统的资产进行分类标识管理。 |
| 3 | 介质管理 | 测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
| 4 | 设备维护管理 | 测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
| 5 | 漏洞和风险管理 | 测评是否采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补。测评是否定期开展安全测评。 |
| 6 | 网络和系统安全管理 | 测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。 |
| 7 | 恶意代码防范管理 | 测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。 |
| 8 | 配置管理 | 测评是否记录和保存系统的基本配置信息 |
| 9 | 密码管理 | 测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
| 10 | 变更管理 | 测评是否采取必要的措施对系统发生的变更进行有效管理。 |
| 11 | 备份与恢复管理 | 测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
| 12 | 安全事件处置 | 测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。 |
| 13 | 应急预案管理 | 测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |
| 14 | 外包运维管理 | 测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。 |

**2.6项目管理**

供应商必须提供完整的项目管理方案，供应商需要针对以下项目管理要求进行项目管理服务要求进行承诺，未提供项目管理服务承诺为无效供应商。

（1）供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任；

（2）应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力；

（3）供应商在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留；

（4）供应商的岗位配置要至少配置测评师、项目经理、渗透工程师、质量主管等并明确各个岗位的相关职责。

（5）测评工具要求

①采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件；

②采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品；
 ③采用的测评工具的生产商应为正规厂商，能够对产品进行持续更新并提供质量和安全保障；
 ④测评机构所使用的测评工具不会对单位系统产生破坏或负面影响以及不影响医院业务正常开展。

**2.7交付产物**

包括但不仅限于以下资料：

|  |  |
| --- | --- |
| 1 | 网络安全等级保护测评报告（包含整改建议） |
| 2 | 其他未列入的应交资料 |

## ★三、商务要求

采购包1：

1、服务期限：自合同签订之日起365日。

2、项目地点：四川省政府政务服务和公共资源交易服务中心。

3、项目预算：32万

4、**供应商所提供的报价须包含实施服务过程中和采购文件规定的所有费用。**

5、支付方式：

签订合同后且采购人收到成交供应商开具的正规等额增值税发票后10个工作日内支付合同金额的60%；测评工作完成，成交供应商出具测评报告，经采购人认可且采购人收到成交供应商开具的正规等额增值税发票后10个工作日内，付合同金额的40%。

6、验收标准和方法：

本项目采购人或委托的采购代理机构将严格按照政府采购相关法律法规、《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）、《关于印发〈政府采购需求管理办法〉的通知》（财库（2021）22号）及国家现行有关标准及比选文件、响应文件和采购人要求进行验收。

采购包2：

1、服务期限：自合同签订之日起365日。

2、项目地点：四川省政府政务服务和公共资源交易服务中心。

3、项目预算：8万

4、**供应商所提供的报价须包含实施服务过程中和采购文件规定的所有费用。**

5、支付方式：

签订合同后且采购人收到成交供应商开具的正规等额增值税发票后10个工作日内支付合同金额的60%；测评工作完成，成交供应商出具测评报告，经采购人认可且采购人收到成交供应商开具的正规等额增值税发票后10个工作日内，付合同金额的40%。

6、验收标准和方法：

# 本项目采购人或委托的采购代理机构将严格按照政府采购相关法律法规、《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）、《关于印发〈政府采购需求管理办法〉的通知》（财库（2021）22号）及国家现行有关标准及比选文件、响应文件和采购人要求进行验收。

# **第三章 评审办法（综合评分法）**

##

## **3.1评审的量化因素及权重比值**

## 详见评分标准

## **3.2** **评审方法**

综合评分法

**3.2.1比选响应文件的初步评审**

如发现下列情况之一的，将被评审小组否决：

（1）响应文件未按比选文件要求进行签署、盖章的；

（2）资格证明文件不全的；

（3）同一供应商提交两个以上不同的响应文件或者报价，以及响应文件没有提交报价的；

（4）响应文件载明的招标项目完成期限超过比选文件规定的期限；

（5）经评审小组认定供应商的报价低于成本价形成恶性竞争的；

（6）明显不符合比选文件服务标准的要求；

（7）响应文件附有采购人不能接受的条件；

（8）报价超过比选文件规定的限价；

（9）其他不符合比选文件实质性要求及法律、法规规定的其他情形。

**3.2.2 报价计算错误的修正原则**

评审小组将对确定为实质上响应比选文件要求的响应文件进行校核，看其是否有计算上或汇总上的算术错误，修正错误的原则如下：

响应文件中的大写金额与小写金额不一致的，以大写金额为准。

**3.2.3 详细评审**

# （一）评选办法

本项目采用综合评分法，是指参选文件满足比选文件全部实质性要求且按评审因素的量化指标评审得分最高的比选申请人为中标候选人的评审方法。比选文件中“★”条款为实质性要求项，比选申请人必须满足，否则为无效投标

评审时，委员会各成员应当独立对每个有效参选的文件进行评价、打分，然后汇总每个比选申请人每项评分因素的得分。最终得分最高者即为中标人。

（二）评分标准

#### 采购包1：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分因素及权重 | 分值 | 评分标准 | 评分因素类别 |
| 1 | 报价 | 10分 | 满足比选文件要求且最后报价最低的投标人的价格为投标基准价，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：投标报价得分=（投标基准价/最后投标报价）×10 | 共同评分因素 |
| 2 | 技术方案 | 25分 | 根据投标人针对本项目的技术方案进行综合评分：①项目实施流程、②项目管理、③测评风险控制、④项目实施时间计划、⑤项目组织架构，上述内容均符合实际情况、内容完善详细、描述准确、分析内容齐全、条理结构清晰、层次细化完善完全响应项目要求的得25分；每有一项缺项的扣5分，每有一处内容存在内容不足的扣2.5分，扣完为止。 | 技术类评分因素 |
| 3 | 投标人项目人员配置情况 | 12分 | **拟派项目经理1名：**1、信息（网络）安全等级评测师（高级）证书；2、注册信息安全专业人员（CISP）证书；3、注册信息系统审计师（CISA）证书；4、重要信息系统安全等级保护培训证书（CIIP-T）；5、软件性能测试高级工程师；6、信息系统安全专业认证（CISSP）证书。以上证书每提供一个得2分，最多得12分，未提供不得分。注：提供人员证书复印件和在投标单位就职的证明材料，并加盖供应商公章。 | 共同评分因素 |
| 4 | 投标人项目人员配置情况 | 16分 | **拟派技术负责人1名：**1、信息（网络）安全等级测评师（高级）证书；2、商用密码应用安全性评估从业人员考核合格证书；3、注册信息安全专业人员（CISP）证书；4、注册网络安全渗透评估专业人员（NSATP-A）证书；5、信息安全保障人员认证证书（CISAW）；6、工业和信息化部教育与考试中心颁发的网络信息安全工程师证书；7、信息技术应用创新考试评价证书--信息安全工程师；8、软件性能测试高级工程师。以上证书每提供一个得2分，最多得16分，未提供不得分。注：提供人员证书复印件和在投标单位就职的证明材料，并加盖供应商公章。 | 共同评分因素 |
| 5 | 投标人项目人员配置情况 | 16分 | **拟派项目团队**：所有人员具有信息安全等级测评师证书或网络安全等级测评师证书且获得该证书，满足要求后以下证书每提供一个得2分，最多得16分，此项一人多证可重复得分，未提供不得分。1、注册信息安全专业人员（CISP）证书；2、信息技术应用创新考试评价证书--信息安全工程师；3、信息安全保障人员认证(CISAW)证书；4、网络安全能力认证（CCSC）证书；5、软件测试工程师。注：①项目经理、技术负责人应分别由不同人员构成，不得计入项目组成员。②提供人员证书复印件和在投标单位就职的证明材料，并加盖供应商公章。 | 共同评分因素 |
| 6 | 投标人机构情况 | 11分 | 1、投标人具有检验检测机构资质认定证书(CMA)，检验检测能力范围具有①网络安全等级保护测评、②信息系统风险评估③软件产品，具有一项得2分，全部满足得6分。(提供证书复印件和检测能力附表复印件加盖公章)。2、投标人具有信息安全服务资质证书(风险评估)的得1分(提供证书复印件加盖公章)3、投标人具有信息安全风险评估辅助分析软件具有软件著作权得2分，最多得2分。（需提供著作权证书复印件加盖公章）；4、投标人具信息安全风险评估系统具有软件著作权得2分，最多得2分。（需提供著作权证书复印件加盖公章） | 共同评分因素 |
| 7 | 业绩 | 10分 | 2022年1月1日以来，具有信息安全测评项目案例，每具有一个案例得2分，最多得10分，不提供不得分；（需提供证明材料，以合同签订时间或中标（成交）通知书发放时间为准；提供合同或中标（成交）通知书复印件并加盖供应商公章（鲜章）） | 共同评分因素 |

注：评分的取值按四舍五入法，保留小数点后两位。

采购包2：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分因素及权重 | 分值 | 评分标准 | 评分因素类别 |
| 1 | 报价 | 10分 | 满足比选文件要求且最后报价最低的投标人的价格为投标基准价，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：投标报价得分=（投标基准价/最后投标报价）×10 | 共同评分因素 |
| 2 | 技术方案 | 25分 | 根据投标人针对本项目的技术方案进行综合评分：①项目实施流程、②项目管理、③测评风险控制、④项目实施时间计划、⑤项目组织架构，上述内容均符合实际情况、内容完善详细、描述准确、分析内容齐全、条理结构清晰、层次细化完善完全响应项目要求的得25分；每有一项缺项的扣5分，每有一处内容存在内容不足的扣2.5分，扣完为止。 | 技术类评分因素 |
| 3 | 投标人项目人员配置情况 | 12分 | **拟派项目经理1名：**1、信息（网络）安全等级评测师（高级）证书；2、注册信息安全专业人员（CISP）证书；3、注册信息系统审计师（CISA）证书；4、重要信息系统安全等级保护培训证书（CIIP-T）；5、软件性能测试高级工程师；6、信息系统安全专业认证（CISSP）证书。以上证书每提供一个得2分，最多得12分，未提供不得分。注：提供人员证书复印件和在投标单位就职的证明材料，并加盖供应商公章。 | 共同评分因素 |
| 4 | 投标人项目人员配置情况 | 16分 | **拟派技术负责人1名：**1、信息（网络）安全等级测评师（高级）证书；2、商用密码应用安全性评估从业人员考核合格证书；3、注册信息安全专业人员（CISP）证书；4、注册网络安全渗透评估专业人员（NSATP-A）证书；5、信息安全保障人员认证证书（CISAW）；6、工业和信息化部教育与考试中心颁发的网络信息安全工程师证书；7、信息技术应用创新考试评价证书--信息安全工程师；8、软件性能测试高级工程师。以上证书每提供一个得2分，最多得16分，未提供不得分。注：提供人员证书复印件和在投标单位就职的证明材料，并加盖供应商公章。 | 共同评分因素 |
| 5 | 投标人项目人员配置情况 | 16分 | **拟派项目团队**：所有人员具有信息安全等级测评师证书或网络安全等级测评师证书且获得该证书，满足要求后以下证书每提供一个得2分，最多得16分，此项一人多证可重复得分，未提供不得分。1、注册信息安全专业人员（CISP）证书；2、信息技术应用创新考试评价证书--信息安全工程师；3、信息安全保障人员认证(CISAW)证书；4、网络安全能力认证（CCSC）证书；5、软件测试工程师。注：①项目经理、技术负责人应分别由不同人员构成，不得计入项目组成员。②提供人员证书复印件和在投标单位就职的证明材料，并加盖供应商公章。 | 共同评分因素 |
| 6 | 投标人机构情况 | 11分 | 1、投标人具有检验检测机构资质认定证书(CMA)，检验检测能力范围具有①网络安全等级保护测评、②信息系统风险评估③软件产品，具有一项得2分，全部满足得6分。(提供证书复印件和检测能力附表复印件加盖公章)。2、投标人具有信息安全服务资质证书(风险评估)的得1分(提供证书复印件加盖公章)3、投标人具有信息安全风险评估辅助分析软件具有软件著作权得2分，最多得2分。（需提供著作权证书复印件加盖公章）；4、投标人具信息安全风险评估系统具有软件著作权得2分，最多得2分。（需提供著作权证书复印件加盖公章） | 共同评分因素 |
| 7 | 业绩 | 10分 | 2022年1月1日以来，具有信息安全测评项目案例，每具有一个案例得2分，最多得10分，不提供不得分；（需提供证明材料，以合同签订时间或中标（成交）通知书发放时间为准；提供合同或中标（成交）通知书复印件并加盖供应商公章（鲜章）） | 共同评分因素 |

注：评分的取值按四舍五入法，保留小数点后两位。

## **3.3** **报价表（格式）**

**报价表**

**项目名称：**四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评和12345政务服务热线及网络理政平台等级保护项目

#### **采购包1：**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务内容** | **报价（元）** |
| 1 |  |  |
| 2 |  |  |
| .... |  |  |
| 合计 | 小写： 大写： |

报价（大写人民币）：

供应商名称：　　 　　　　　　(加盖公章)

法定代表人或代理人：　　 　　　　　　（签字）

日期：

**说明：报价应是包括邀请文件中规定的全部响应内容的报价（包含中标供应商应承担的物耗、人工、税费等）。**

**报价表**

**项目名称：**四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评和12345政务服务热线及网络理政平台等级保护项目

#### **采购包2：**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务内容** | **报价（元）** |
| 1 |  |  |
| 2 |  |  |
| .... |  |  |
| 合计 | 小写： 大写： |

报价（大写人民币）：

供应商名称：　　 　　　　　　(加盖公章)

法定代表人或代理人：　　 　　　　　　（签字）

日期：

**说明：报价应是包括邀请文件中规定的全部响应内容的报价（包含中标供应商应承担的物耗、人工、税费等）。**

## **3.4声明（格式）**

**声 明**

**致：四川省政府政务服务和公共资源交易服务中心**

我单位作为四川省政府政务服务和公共资源交易服务中心2024年四川省12345政务服务热线及网络理政平台网络安全等级保护的供应商，在此郑重声明：

一、我单位参加采购活动前三年内，在经营活动中**（说明：填写“无”或“有”**）重大违法记录。

二、我单位**（说明：填写“具有”或“不具有”**）良好的商业信誉。

三、与我单位存在直接控股、管理关系的相关供应商：**（说明：填写“无”或“（一）供应商名称１；（二）供应商名称２ ；（三）……”）。**

四、在行贿犯罪信息查询期限内，我公司及我公司现任法定代表人、主要负责人**（说明：填写“没有”或“有”）**行贿犯罪记录。

五、我公司**（说明：填写“未列入”或“被列入”**）失信被执行人、重大税收违法案件当事人名单。

我公司**（说明：填写“未列入”或“被列入”**）采购严重违法失信行为记录名单。

我公司**（说明：填写“没有”或“有”**）未依法缴纳税收和社会保障资金的不良记录。

特此声明。

供应商名称：　　 (加盖公章)

日 期：　　年　　月　　日