**四川省政府政务服务和公共资源交易服务中心 网络安全监测服务采购项目**

**比**

**选**

**文**

**件**

**四川省政府政务服务和公共资源交易服务中心**

**2023年3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网络安全监测服务采购项目，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网络安全监测服务采购项目。

1.2项目资金：自筹资金。

1.3项目实施方式：在合同约定时间范围内为四川省政府政务服务和公共资源交易服务中心提供网络安全监测服务。

1.4质量效果要求：符合国家相关要求。

1.5采购内容：四川省政府政务服务和公共资源交易服务中心网络安全监测服务项目。

1.6项目总预算：人民币 45 万元整（肆拾伍万元整）

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前三年内，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。

**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2023年3月24日至3月28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2023年3月29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2023年3月29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：18200305935

地址：四川省成都市青羊区鼓楼南街101号

2023年3月23日

# **技术规范要求**

# 一、项目主要工作内容及要求

 **1．安全建设规划更新**

为基础信息网络和重要信息系统提供合规性管理咨询服务，从信息安全战略、安全策略规范等角度，根据省中心网络和数据安全实际，协助省中心开展安全保障的各项指导工作。

（1）安全技术体系规划：依据国家网络安全相关要求、标准、规范，结合单位现状，分析风险漏洞，以安全策略为指导，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、数据安全、终端安全、安全管理中心等方面出发，立足于现有成熟的安全技术和安全机制，根据省中心当前实际，规划完善网络安全体系。

（2）安全管理体系规划：依据国家网络安全相关要求、标准、规范，结合省中心现状，分析安全风险和漏洞，从安全管理制度、安全组织机构、安全管理人员、安全建设管理、安全运维管理等方面出发，细化网络安全管理，将每项安全管理类分解为多个安全目标和安全控制进行规划建设，最终达成相应安全目标的管理工作和要求。

（3）安全运维保障体系规划：进一步完善当前安全运维保障体系，紧密结合安全技术和安全管理，优化系统可靠性、系统数据备份和安全、安全事件的应急响应计划、安全审计、灾难恢复计划等。

**2．安全制度建设**

根据省中心实现，协助修订完善网络和数据安全相关的制度、规范、网络安全规程等，推进省中心网络安全制度体系和网络数据安全工作机制不断完善，按服务内容配合安全制度落实执行。

**3．安全监测审核**

通过人工结合技术手段，对网络、系统、终端等运行状态进行安全监测，及时发现病毒传播、黑客攻击、数据泄露等安全事件，对于已经发生的网络安全事件，查找源头，发现问题，举一反三，落实整改，逐一销号，总结提高。

**4．安全咨询服务**

参考国内外信息安全标准，结合省中心IT业务实际情况，充分考虑行业在信息安全方面的特有属性，调查分析省中心已有的安全策略，从管理、制度、落实情况、物理安全、人员安全、第三方安全等各方面进行评估分析，提供完整的风险处置和控制建议，帮助省中心进行信息安全合规性检查以及标准的贯彻。具体包括：

4.1信息安全等级保护建设咨询：遵循国家等级保护要求，协助省中心进行定级、备案、差距评估、整改方案设计、安全加固、整理测评资料和协助通过测评，最终帮助省中心完成信息系统达标建设，高分通过测评机构的测评。

4.2信息安全管理体系建设咨询：为基础信息网络和重要信息系统提供合规性管理咨询服务，从信息安全战略、安全策略规范等角度协助省中心开展安全保障的各项指导工作。

4.3安防系统规划、建设及运维管理咨询：提供高质量方法建议，协助省中心准确了解本部门的信息安全现状，指导省中心信息安全建设和投入，建立信息安全管理和技术体系。

4.4商用密码咨询：按照商用密码管理要求，在系统规划、建设以及运行阶段，对省中心商用密码进行应用安全性评估。针对省中心商密应用，需要提供系统密码应用建设、改造规划设计服务，包括信息系统建设初期密码应用设计，密码技术、密码产品、密码服务相关评估，并提供正确有效地密码设备配置策略以及日常系统运维过程中密钥地安全生命周期管理设计。

**5.代码审计服务**

为了消除代码中的漏洞，减少不必要的补丁升级，从根源上解决源代码导致的安全问题，对业务核心系统的升级改造及新上线重要系统的源代码和程序进行白盒+黑盒测试。

通过实施代码安全审计服务，快速发现项目中的代码安全漏洞、快速评估系统代码安全风险、增强系统安全性，抵御黑客恶意攻击，最大程度保护省中心信息系统资产。

**6．漏洞扫描**

通过对信息系统定期检测（工具扫描及安全专家人工检测），及时发现信息系统（网络架构、网络设备、服务器主机、操作系统、数据库和用户账号、口令等安全对象）存在的各种安全漏洞、隐患，以及系统运行状态，漏洞扫描完毕后提供检测报告，提出系统加固建议以及相关的处置措施，并在完成整改后进行复扫，直至整改完成。

**7．WEB安全扫描**

不定期（每月不少于1次），针对WEB应用系统漏洞进行定期检测（工具扫描及安全专家人工检测），及时发现WEB应用层存在的各种安全漏洞、隐患，以及系统运行状态，安全扫描完毕后提供检测报告，提出系统加固建议以及相关的处置措施，并在完成整改后进行复扫，直至整改完成。

**8.渗透检测**

不定期（每年至少6次），利用网络安全测试工具，对省中心网络设备和信息系统进行非破坏性模拟黑客攻击，入侵目标系统过程和细节，以书面报告呈现，真实、深入地找出省中心当前信息安全问题和隐患，提出解决和处理方案，并配合省中心进行逐一整改，并在完成整改后进行复扫，直至整改完成。

**9．数据流向梳理**

通过工具对网络结构、路由配置、网络数据包进行分析，梳理网络数据通信情况，提出链路调整、路由优化建议，提高网络通信效率。

**10．安全策略完善和安全配置核查**

从管理、技术两个维度完善网络安全策略，并进行定期修订。依据网络安全策略、网络安全预警信息和国家、行业相关标准，核查路由交换设备、网络安全设备、服务器、数据库、用户终端、应用系统等的安全配置，及时发现配置错误、缺失，并进行修正完善。

**11．安全应急处理**

在省中心发生确切的安全事件时，应急响应实施人员及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，实施人员协助省中心检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件整体安全解决方案，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。

**12．安全日常管理**

对网络安全保障工作进行日常管理，提高单位网络安全保障水平。

**13.安全意识教育和培训**

全年至少2次，按照相关要求，针对不同人员，对省中心各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；定期对不同岗位的人员进行技能考核。供应商按照省中心邀请的专家进行内容培训，省中心不再支付培训及专家费用。

**14.参与公共资源交易安全攻防演练**

全年1次，派一支攻击队伍参与配合省中心开展全省公共资源交易体系网络安全攻防演练。在涉及省中心的网络安全攻防演练中做好防守工作。

 **15．协助处理其他安全任务**

# 根据省中心要求，协助处理其他安全任务，包括对本系统内市县部门的安全技术支持，完成包括护网以及重大活动期间的保障。需要固定派驻至少一名较强业务素质的工作人员长期在省中心现场。

# **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谈判申请文件的初步评审**

3.2.1.1在初步评审中，评审小组将首先审定每份谈判申请文件是否响应了比选文件的下述要求。

3.2.1.2如发现下列情况之一的，其谈判将被评审小组否决：

（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**

3.2.2.1 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 谈判申请文件的详细评审**

综合评审包括：报价+技术服务方案+供应商综合实力+售后服务+履约能力。评委将根据评分标准，依据综合评分结果排名。

评分标准

| **序号** | **评分因素及权重** | **分值** | **评分标准** | **说明** |
| --- | --- | --- | --- | --- |
| 1 | 报价 | 10分 | 以本项目有效参选报价的最低价为基准价，参选报价得分=(基准价／投标报价)×10。 |  |
| 2 | 技术服务方案 | 39分 | 1．供应商的技术方案能按照整体等级保护、风险评估体系，有针对性地设计、选择合适的技术方案作为整体安全解决方案。对项目实际情况和需求描述最好、无漏项的得6分，对项目实际情况和需求描述基本完整、细微不足的得4分，部分满足的得2分，不满足的不得分。2．供应商的渗透服务方案能够结合采购人的核心业务系统，通过数据说明该业务系统当前的主要风险和威胁，制定科学合理的渗透测试方案，并对发现的安全风险进行整改。对采购人核心业务系统当前的安全风险了解并有详细数据说明，且能够进行安全整改的得6分，对采购人核心业务系统当前的安全风险了解程度一般的，且能够进行安全整改的，得4分，描述笼统且有能力做整改的得2分，其他不得分。3.供应商提供的业务安全运维方案，需要梳理采购人的的核心业务系统的实际业务安全事件，并详细介绍如何通过该平台解决此类事情发生。梳理的安全事件完全结合实际，贴合采购人安全痛点的，并解决方案能落地的得6分，梳理的安全事件部分贴合实际，并解决方案能落地的得4分，方案笼统的得2分，其他不得分。4.根据供应商的整体项目实施方案进行对比，方案详细完整的体现供应商设置的实施组织、实施进度安排、实施进度保障措施、实施质量保障措施等、风险控制等关键因素进行详细阐述，横向综合对比供应商实施方案后，完全满足并优于采购人实际需要的得6分，能够基本满足采购人实际需要的得4分，部分满足采购人实际需要的得2分；不满足的不得分。5供应商提供服务时使用的安全扫描工具为公安部认可的等级保护检查工具箱，提供该等级保护检查工具箱具有《等级保护检查工具箱国家信息安全漏洞库兼容性资质证书》证明的得6分，未提供或提供证书无效不得分。6、根据供应商提供的技术方案：整体流程、技术方法、服务方案设计、人员组织、时间安排、阶段性文档提交、验收标准、风险规避、响应能力。方案包含以上内容且无内容错误的得9分，每缺少一项内容或每有一项内容错误（内容错误是指：不可实现的夸大情形或涉及的规范、标准与本项目要求不一致的情形）的扣1分。 |  |
| 3 | 供应商综合实力 | 31分 |  1.供应商具有信息系统建设和服务能力等级证书CS4级别的得4分；2.供应商具有中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书，包括应急处理证书、风险评估证书、安全运维证书，每提供1个得2分，不提供不得分，共6分；3.供应商具有中国信息安全测评中心颁发的安全工程证书的得3分；4.供应商具有公安部颁发的信息安全等级保护安全建设服务机构能力评估合格证书的得3分；5.供应商具有中国电子工业标准化技术委员会颁发的信息技术服务标准符合性证书-运行维护（ITSS）得3分；6、供应商具有中国网络安全审查技术与认证中心（原中国信息安全认证中心）颁发的信息安全服务资质认证证书，提供证书复印件得4分；7、供应商具有有效的质量管理体系认证证书、环境管理体系认证证书、职业健康安全管理体系认证证书，每提供一个以上证书复印件得2分，最多得6分。8.供应商拟派负责本项目的项目组技术人员，除派遣驻场工程师外，项目组其他应急人员具有CISP安全工程师证书，每提供一人得1分，此项最高2分（涉及人员的需提供投标单位劳动关系证明加盖公章） | 提供相关有效期内的证书复印件加盖供应商鲜章，未提供不得分。 |
| 4 | 售后服务 | 10分 | 1.根据供应商提供的售后服务方案进行对比，方案详细完整的体现售后服务组织、售后服务机构、售后服务人员、售后服务流程、售后服务响应时间、售后服务方式、售后服务内容、售后服务质量保障措施等关键因素。供应商售后服务方案完全包含以上几点要求且切实可行的得8分，每缺少一项或每有一项不切实可行扣1分，扣完为止。2.根据供应商售后服务方案中质保期内的应急响应时间进行评价，应急响应时间≤2小时得2分，2小时＜应急响应时间≤4 小时得1分，其余的不得分； | 共同评分因素 |
| 5 | 履约能力 | 10分 | 供应商提供近三年（2020年1月1日至本项目开标之日）安全服务类项目履约证明材料，每提供1个证明材料得2分，最多得10分。未提供不得分；（须提供合同复印件关键页加盖供应商公章作为履约证明材料） | 共同评分因素 |

**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网络安全监测服务采购项目报价表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务内容** | **报价（元）** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| .... |  |  |
| 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）。**

**3.5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网络安全监测服务采购项目的供应商，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