2022年淮北市政府网站集约化平台

系统代码审计和安全扫描项目

竞争性磋商文件

淮北市人民政府办公室

2022年7月26日

# 供应商须知前附表

|  |  |  |
| --- | --- | --- |
| **序号** | **条款名称** | **编 列 内 容** |
| 1 | 采购人 | 淮北市人民政府办公室 |
| 2 | 采购项目名称 | 2022年淮北市政府网站集约化平台系统代码审计和安全扫描项目 |
| 3 | 标段（包别）划分 | 本项目共分为 1 个标包 |
| 4 | 采购预算 | 见竞争性磋商公告 |
| 5 | 资金落实情况 | 已落实 |
| 6 | 采购需求 | 具体采购需求详见第三章采购需求。 |
| 7 | 服务期限 | 见竞争性磋商公告。 |
| 8 | 性能要求 | 是否允许负偏离：☑不允许 □允许 |
| 9 | 付款方式 | 付款方式：服务完成并经甲方审核通过后5个工作日内支付全部费用。 |
| 10 | 性能响应 | 是否允许负偏离：☑不允许 □允许 |
| 11 | 供应商资格条件能力和信誉 | 见竞争性磋商公告 |
| 12 | 是否接受联合体响应 | ☑不接受 □接受 |
| 13 | 竞争性磋商文件澄清发出的形式 | 发出时间：如澄清或修改的内容可能影响响应文件编制的，应当在提交响应文件截止之日至少5日前发布澄清或修改 |
| 14 | 分包 | ☑不允许 □允许 |
| 15 | 供应商要求澄清竞争性磋商文件 | 时间：在提交响应文件截止之日至少5 前（以收到时间为准），逾期提出采购人可不予受理。 |
| 16 | 响应报价包括的内容 | 响应报价包括提供服务的一切成本和费用、管理费、利润和税金，以及采购合同中明示或暗示的所有责任、义务和风险。 |
| 17 | 最高限价 | 见竞争性磋商公告 |
| 18 | 提交响应文件截止时间 | 见竞争性磋商公告 |
| 19 | 是否退还响应文件 | ☑否 |
| 20 | 响应文件开启时间和地点 | 开启时间：同提交响应文件截止时间开启地点：同响应文件提交地点 |
| 21 | 响应文件开启程序 | 采购人根据有关规定在开标截止时间内组织评标专家到达开标地点。 |
| 22 | 磋商小组的组建 | 磋商小组的组成：由采购人代表选择专家组成。磋商小组的人数：3 人或 3 人以上单数组成。 |
| 23 | 供应商家数 | 参与竞争性磋商的供应商不得少于 3 家。 |
| 24 | 确定提交最后报价的供应商 | 竞争性磋商文件能够详细列明采购标的的技术、服务要求，磋商结束后，磋商小组将要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商家数不得少于 3 家。 |
| 25 | 报价轮次 | 一轮，各供应商首轮报价即最终报价。 |
| 26 | 磋商小组推荐成交候选人的人数 | 磋商小组推荐的成交候选人数量：3 名 |
| 27 | 合同形式 | 固定总价合同 |

# 第一章 采购需求

# **一、项目背景**

为深入贯彻落实习近平总书记关于网络安全工作的重要指示精神，根据《中华人民共和国网络安全法》、《网络安全等级保护条例（征求意见稿）》以及《关于开展全国重要信息系统安全等级保护定级工作的通知》等文件要求，须对淮北市政府网站集约化平台网络安全开展安全扫描和代码审计工作。

**二、项目目的**

依据《中华人民共和国网络安全法》《信息安全等级保护管理办法》的相关要求，为进一步加强淮北市政府网站集约化平台信息系统的整体安全防护能力，确保政府网站集约化平台系统在使用过程中的安全稳定，拟通过竞争性磋商方式采购政府网站集约化平台系统代码审计和安全扫描服务。根据审计和扫描结果持续推进政府网站集约化平台的安全建设，不断提高政府网站集约化平台系统的安全防护能力。

**参考标准**

* 《中华人民共和国网络安全法》
* 《信息安全等级保护管理办法》
* 《信息技术-安全技术-信息技术安全性评估准则》（ GB/T 18336-2015）
* 《信息安全技术代码安全审计规范》（GB/T 39412-2020）
* OWASP TOP 10
* CWE/SANS TOP 25
* ASP/ASP.NET/PHP/JSP安全编码规范
* 代码审计实施规范

**三、项目内容**

本次采购服务内容：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务名称 | 期限（次数） | 备注 |
| 1 | 淮北市政府网站集约化平台-代码审计服务 | 1次 | 按采购人相关要求进行安全代码审计工作 |
| 2 | 淮北市政府网站集约化平台系统-安全扫描服务 | 1次 | 按采购人相关要求进行安全扫描工作 |

**1、代码审计服务内容：**

依据GBT39412-2020《代码安全审计》采用代码安全审计工具和人工排查的方式对代码中存在的编码漏洞和缺陷等进行检查分析，发现当前应用程序存在的漏洞，如跨站脚本漏洞、SQL注入漏洞、命令执行漏洞、日志伪造漏洞、参数篡改等，并针对检测发现的问题协助进行问题修复。

**整体代码审计：**

代码审计服务人员对被审计系统的所有源代码进行整体的安全审计，代码覆盖率为100%，整体代码审计采用源代码扫描和人工分析确认相结合的方式进行分析，发现源代码存在的安全漏洞。

整体代码审计属于白盒静态分析，仅能发现代码编写存在的安全漏洞，无法发现业务功能存在的缺陷。

**功能点人工代码审计**

对某个或某几个重要的功能点的源代码进行人工代码审计，发现功能点存在的代码安全问题。功能点人工代码审计需要收集系统的设计文档、系统开发说明书等技术资料，以便代码审计服务人员能够更好的了解系统业务功能。由于人工代码审计工作量极大，所以需要分析并选择重要的功能点，有针对性的进行人工代码审计。

**2、安全扫描服务内容**

**梳理资产**

通过现场调研和网络扫描的方式梳理设备资产、识别开放端口/服务。

**发现漏洞**

通过内网检查发现内部设备脆弱性（如弱口令、系统漏洞、非授权访问等高危漏洞）。

**排除隐患**

通过外网测试全面检测重要信息系统及相关信息系统直接暴露在互联网上的安全隐患，并提供实际可行的安全修复建议。

1. **服务要求**

**1.服务原则**

本次代码审计和安全扫描实施方案设计与具体实施应满足以下原则：

（1）标准性原则：代码审计和安全扫描工作方案的设计与实施应依据国家相关标准进行。

（2）规范性原则：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。

（3）可控性原则：代码审计和安全扫描工作服务的进度要跟上进度表的安排，保证测评对于工作进度的可控性。

（4）整体性原则：代码审计和安全扫描工作的范围和内容应当整体全面，包括国家相关要求涉及的各个层面。

（5）最小影响原则：代码审计和安全扫描工作应尽可能小的影响系统和网络，并在可控范围内；代码审计和安全扫描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。

**2.质量要求**

服务方应提前制定详细的服务方案，明确本次服务所遵循的标准、服务计划安排、使用的工具以及执行方式。

**3.代码审计和安全扫描报告交付**

（1）供应商应对采购人的信息系统进行代码审计和安全扫描，提供符合要求的测评报告，出具《淮北市政府网站集约化平台系统代码审计安全评估报告》以及《淮北市政府网站集约化平台系统安全扫描报告》一式三份。

（2）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。

**4.保密要求**

（1）供应商必须和采购人签订保密协议和非侵害性协议，供应商必须要与参加此次代码审计和安全扫描项目的所有项目组成员签订保密协议和非侵害性协议，在合同签订时一并提供给采购人。

（2）供应商具体代码审计和安全扫描工作报告的编写，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，在代码审计期间和代码审计结束后，供应商不得带离该地点。

（3）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。无论供应商中标与否，其对上述内容的保密责任将长期存在。

**5.人员要求**

供应商拟派的安全服务团队不得少于4人，成交供应商需保证在项目实施阶段主要技术人员必须是全职。

注：以上人员须提供证书复印件加盖供应商单位公章，以及自2022年1月起近三个月个人社保缴纳证明。

**6、报价要求**

本项目报总价，报价包含完成本项目服务期间所产生的一切费用，采购人后期不再另行追加费用。

**7、项目实施时间及地点**

合同签订后10个工作日内完成2022年淮北市政府网站集约化平台系统代码审计和安全扫描报告等系统环境调研工作，完成代码审计和安全扫描工作方案实施计划编制，项目进场实施后30个工作日内完成所有系统代码审计和安全扫描工作，服务地点为淮北市政府办公室指定地点。

# 第二章 磋商和评审办法

# 评审办法前附表

以下涉及初步评审及详细评审的资料均须提供复印件并加盖供应商单位公章放入响应文件（供应商提供的资料须清晰、明确、可辨认，否则磋商小组可作出不利于供应商的决定）。

**1、符合性审查标准**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **评审项** | **评审因素** | **评审标准** | **备注** |
| 1 | 形式评审 | 供应商名称 | 与营业执照一致 |  |
| 法定代表人身份证明及授权委托书 | 法定代表人身份证明及授权委托书符合竞争性磋商文件规定的格式，按规定格式签字盖章 |  |
| 联合体响应 | 本项目不接受联合体响应 |  |
| 书面承诺函格式及内容 | 应符合磋商文件的要求 |  |
| 其他要求 | 应符合磋商文件的要求 |  |
| 2 | 资格评审 | 资格要求 | 具有独立法人资格，提供有效营业执照。 |  |
| 信用要求 | 供应商（含其不具有独立法人资格的分支机构）不得存在下列不良信用记录情形之一：1、被人民法院列入失信被执行人的；2、被税务部门列入重大税收违法案件当事人名单的；备注：是否有不良信用记录，仅以评审当日查询的结果为准。 |  |
| 其他要求 | 磋商文件其他实质性要求 |  |
| 3 | 响应性评审 | 响应报价 | 响应报价不得超过采购预算（最高限价），只能有一个有效报价，不得提交选择性报价。 |  |
| 响应文件有效期 | 应符合磋商文件的要求 |  |
| 服务期 | 应符合磋商文件的要求 |  |
| 付款方式 | 应符合磋商文件的要求 |  |
| 服务质量 | 应符合磋商文件的要求 |  |
| 其他要求 | 磋商文件其他实质性要求 |  |

**2、磋商程序及要求**

2.1初步评审合格的供应商进入两阶段磋商程序。

|  |  |  |
| --- | --- | --- |
| **序号** | **类别** | **磋商程序（两阶段磋商）** |
| 第一阶段 | 技术、服务要求方面磋商 | 本项目竞争性磋商文件已详细列明采购标的的技术、服务要求，磋商小组原则上不再与各供应商就采购标的的技术、服务要求及拟签订的合同内容进行一对一磋商。 |
| 第二阶段 | 价格方面磋商 | 由于本项目竞争性磋商文件已能够较详细的列明采购标的的服务方案、内容以及合同条款，在服务方案、内容以及合同条款不变的情况下，各供应商响应文件中的首轮报价即作为最终报价。 |

2.2两阶段磋商程序后，磋商小组采用综合评分法对响应文件进行综合评分。

**3、详细评审标准**

分值构成：总分 100 分，商务报价部分：10 分，商务技术部分：90 分。

**商务报价得分计算方法：**

满足磋商文件要求且各家报价的最低价为响应基准价，其价格分为满分，其他响应报价得分统一按照下列公式计算：响应报价得分=（基准价/响应报价）×10。

**商务技术得分计算方法：**

先由磋商小组对每个供应商独立打分，然后取所有磋商小组评分的算术平均值。磋商小组根据供应商最终综合得分（商务技术得分+报价得分，取小数点后两位，第三位四舍五入） 由高到低推荐 3 名有排序的成交候选供应商。若出现综合得分相同的情况，则按报价低的列前；最后报价也相等的，则采取供应商抽签方式确定成交候选人排序。

**评分细则：**

| **类别** | **评分内容** | **评分标准** | **分值范围** |
| --- | --- | --- | --- |
| 技术分（35分） | 服务方案 | 1、服务方案工作范围清晰，具有完整的服务方案。评委对各家服务方案进行横向比较：方案全面、合理、准确，完全符合竞争性磋商文件要求，得11-15分；较合理、准确，基本符合竞争性磋商文件要求，得6-10分；基本合理、准确，部分符合竞争性磋商文件要求，得1-5分；差或未提供不得分。2、项目管理方案：工作范围清晰，具有完整的项目管理方法论和内容。评委对各家项目管理方案进行横向比较：方案全面、合理、准确，完全符合竞争性磋商文件要求，得4-5分；较合理、准确，基本符合竞争性磋商文件要求，得2-3分；基本合理、准确，部分符合竞争性磋商文件要求，得0-1分；差或未提供不得分。 | 0-20分 |
| 项目人员 | 供应商针对本项目需求拟配备的项目团队应设置质量经理、项目经理等，具体评审指标如下：1、质量经理（1人，本小项满分4分）：具有中级（含）以上等级测评师证书，得1分；（2）具有软件性能测试高级工程师证书，得1分；（3）具有注册信息安全专业人员（CISP）证书，得1分；（4）具有重要信息系统保护人员（证书类别：CIIP-T）证书，得1分；满分4分。2、项目经理（1人，本小项满分4分）：（1）具有高级测评师证书，得1分；（2）具有软件性能测试高级工程师证书，得1分；（3）具有注册信息安全认证讲师（CISI）证书，得1分；（4）具有信息安全保障人员认证（CISAW）证书，且认证方向为风险管理和安全运维方向的，得1分。3、渗透测试工程师（1人，本小项满分2分）：（1）具有中级（含）以上等级测评师证书，得1分；（2）具有国家网络安全应用检测专业测评人员（NSATP-A），得1分；4、团队成员（最少2人，本小项满分5分）：项目组其他成员（不包括质量经理、项目经理）全部具有初级（含）以上等级测评师证书及工业和信息化人才专业知识测评证书（软件测试科目），满足得3分，否则本小项不得分；在满足上述条件基础上，每提供1名具有CISP证书或CCSC证书或CISAW证书或软件测试工程师证书的，得1分。注：以上证书须提供证书扫描件或复印件，且提供持证人员近三个月在投标单位的社保证明。 | 0-15分 |
| 资信分（55分） | 供应商业绩 | 1、供应商提供自2019年01月01日以来等保测评服务业绩合同（以合同签订日期为准）：每提供一个得3分；最高得9分。2、供应商提供自2019年01月01日以来软件测试（代码审计、安全扫描、安全测试、漏洞扫描、渗透测试等）业绩合同（以合同签订日期为准）：每提供一个得3分；最高得6分。注：响应文件中须提供业绩合同的扫描件/复印件,合同扫描件至少提供封面、服务内容和签字盖章页。 | 0-15分 |
| 供应商实力 | 1、供应商具有ISO9001质量管理体系认证证书、ISO/IEC 27001信息安全管理体系认证证书、ISO/IEC20000信息技术服务管理体系认证证书、ISO14001环境管理体系认证证书和ISO45001职业健康安全管理体系认证证书的，每提供一个证书得1分，本小项最多得5分。2、供应商具有ISO 22301业务连续性管理体系认证证书，得5分，否则不得分。3、投标人具有检验检测机构资质认定证书（CMA）证书且检验检测的能力范围包括就绪可用软件产品、信息安全风险评估的，得5分，否则不得分。4、供应商具有信息技术服务标准符合性证书（ITSS）的，得5分，否则不得分。5、自2019年1月1日以来，供应商获得过国家网络安全等级保护协调小组办公室颁发的“全国网络安全等级保护测评机构先进单位”荣誉证书的，得5分，否则不得分。6、供应商具有自主研发的网络安全等级保护助手软件、智能测评服务软件、网络流量分析工具、网络安全漏洞扫描工具和关键信息基础设施安全检查工具的，得5分，否则不得分。注： （1）第1、2两项须提供证书扫描件或复印件及全国认证认可信息公共服务平台（http://cx.cnca.cn/）查询结果截图。（2）第3项须提供证书扫描件或复印件及市场监督管理部门证书公示查询系统查询结果截图。（3）第4项须提供证书扫描件或复印件及中国电子工业标准化技术协会信息技术服务分会工作网站（www.itss.cn）查询结果。（4）第5项须提供荣誉证书扫描件或复印件及省级（含）以上等保办出具的证明文件。（5）第6项须提供自主研发工具的软著登记证书扫描件或复印件。 | 0-30分 |
| 售后服务能力 | 1、供应商在完成测评工作后应为甲方提供常态化的安全技术支撑，提供售后服务承诺书，评委对各家售后服务内容进行横向比较：详实得5分、良好得3分、一般得1分、较差得0分。注：响应文件中须提供售后服务承诺书。2、供应商具有国家互联网应急中心颁发的“网络安全能力认证”培训机构（CCSC）证书的，得5分。注：响应文件中须提供证书扫描件/复印件。 | 0-10分 |
| 价格分（10分） | 投标报价 | 价格采用有效报价平均值为评审基准价，报价等于评审基准价时得满分，在此基础上每高于评审基准价1个百分点扣0.2分，扣完为止，不得负分；每低于评审基准价1个百分点扣0.2分，扣完为止，不得负分。 | 0-10分 |
| 供应商得分计算方法 | 各供应商的技术标得分为各评委所评技术标合计分值的算术平均值（取小数点后两位，第三位的数字四舍五入）。供应商总得分=技术分得分+资信分得分+价格分得分 |

**服务响应表**

|  |  |
| --- | --- |
| 按招标文件规定填写 | 按供应商所投内容填写 |
| 序号 | 品名 | 服务内容 | 偏离说明 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |

投标供应商签章：

年 月 日

**注：1、供应商必须逐项对应描述服务要求，如不进行描述，仅在响应栏填“响应”或未填写或复制（包括全部复制或部分复制）招标文件采购需求的，包括有选择性的技术响应（例如在某一分项中出现两个及以上的或两种及两种以上的技术规格），均可能导致响应无效；**

**2、偏离说明项需注明：完全响应或正偏离或负偏离（满足用户需求）。正偏离或负偏离还需详细描述偏离情况；**

**3、响应部分可后附详细说明及技术资料。**

**投标企业符合《政府采购法》第二十二条规定声明函**

根据《财政部关于促进政府采购公平竞争优化营商环境的通知》（财库〔2019〕38号）的规定，本公司郑重声明,本公司同时满足以下条件：

1.符合《中华人民共和国政府采购法》第二十二条规定。

2.本公司参加本项目采购活动由本企业提供服务。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标供应商签章：

日 期：

### **无不良信用记录声明函**

本公司郑重声明，我公司无以下不良信用记录情形：

1、公司被人民法院列入失信被执行人；

2、公司、法定代表人或拟派项目经理（项目负责人）被人民检察院列入行贿犯罪档案；

3、公司被工商行政管理部门列入企业经营异常名录；

4、公司被税务部门列入重大税收违法案件当事人名单；

5、公司被政府采购监管部门列入政府采购严重违法失信行为记录名单。

**我公司已就上述不良信用行为按照招标文件中投标供应商须知前附表规定进行了查询。**我公司承诺：合同签订前，若我公司具有不良信用记录情形，贵方可取消我公司中标资格或者不授予合同，所有责任由我公司自行承担。同时，我公司愿意无条件接受监管部门的调查处理。

投标供应商签章：

日 期：

### **无重大违法记录声明函**

本公司郑重声明，根据《中华人民共和国政府采购法》及《中华人民共和国政府采购法实施条例》的规定，参加政府采购活动前三年内，本公司在经营活动中没有重大违法记录，没有因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标供应商签章：

日 期：