遂宁市财政局三级等保测评技术服务项目

采

购

文

件

遂宁市财政局　编制

2023 年 7 月

目 录

第一章 采购邀请

根据工作安排， 遂宁市财政局拟对 遂宁市财政局三级等保测评技术服务项目 通过竞争性方式择优采购供应商，兹邀请符合本次采购要求的供应商参与，有关要求具体如下。

一、采购项目

项目名称：遂宁市财政局三级等保测评技术服务项目；

二、采购预算

本项目最高限价：8 万元（人民币），超过最高限价的做无效报价处理。

三、成交原则

本次采用为综合评分法，符合采购需求且综合得分最高供应商作为本次成交供应商。若明显低于市场价又不能作出合理说明的视为恶意报价，做无效处理。

四、项目简介

本项目为 1 个包，遂宁市财政局三级等保测评技术服务采购，具体采购要求详见采购文件。

五、供应商参加本次采购活动，须具备以下条件

1. 具有独立承担民事责任的能力；

2. 具有良好的商业信誉和健全的财务会计制度；

3. 具有履行合同所必须的设备和专业技术能力；

4. 有依法缴纳税收和社会保障资金的良好记录；

5. 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记录；

6. 法律、行政法规规定的其他条件；

7. 采购人根据采购项目提出的特殊条件：

7.1 参加本项目政府采购活动的供应商及其现任法定代表人、主要负责人在前三

年内不具有行贿犯罪记录。

7.2 本项目不接受联合体参与竞标。

六、供应商邀请方式

本项目供应商邀请在遂宁市财政局门户网站（https://sczj.suining.gov.cn/）上以公告形式发布。

七、响应文件提交

截止时间：2023 年 8 月 7 日（星期一）上午 9：50。

地点：遂宁市船山区燕山街 86 号，遂宁市财政局 306 室。响应文件必须在响应文件递交截止时间前送达采购地点。逾期送达的响应文件恕不接收。

八、开标时间和地点

时间：2023 年 8 月 7 日（星期一）上午 10：00。

地点：遂宁市财政局三楼会议室。

九、其他要求

1. 成交供应商收到成交通知书后 10 个工作日内签订采购合同；

2. 报价时各供应商应提供采购文件中提及的资格证明材料；

3. 成交供应商禁止采取分包或转包方式履行合同，一旦发现取消其成交资格，并追究相关当事人责任。

4. 凡递交了响应文件供应商均视为理解和承认采购文件的所有内容。

5. 协助采购人完成网络安全等级保护建设相关工作。

6. 其他未尽事宜，由遂宁市财政局负责解释。

十、报名咨询及投诉受理单位

报名咨询电话：0825-2314666。

投诉受理单位：遂宁市财政局党办或遂宁市纪委监委驻市国资委纪检监察组。

投诉受理电话：0825-2316754。

第二章 采购项目技术、服务及其他商务要求

一、采购清单

序号	系统名称	安全保护等级	采购数量	最高限价（元）	合计金额（元）
1	遂宁市财政局财政身份认证与授权管理系统	第三级	1	80000	80000

二、项目概况

（一）项目概述

本次测评的主要是按照《中华人民共和国网络安全法》、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全等级保护管理办法》（公通字[2007]43 号）等相关标准，对我单位一个三级系统，在技术和管理两方面 10 大项内容进行逐一的检查和测试。主要包括但不限于：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、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理。通过测评来发现问题、解决问题，从而帮助系统的使用者规避信息安全风险。中标人将在采购人指定地点完成所有信息系统的测评服务，并提出整改建议，最终提交该系统等级保护测评报告。

（二）测评依据

《中华人民共和国网络安全法》

GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

GB/T 22240-2020：《信息安全技术 网络安全等级保护定级指南》

GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》

GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》

GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》

《信息安全等级保护管理办法》（公通字[2007]43 号）

《网络安全等级保护测评机构管理办法》（公信安[2018]765 号）

（三）测评要求

根据项目需求，为保障信息安全现场测评过程的安全可控，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

（四）测评内容

按照信息系统等级保护测评依据开展测评工作（包括不限于以下项目）

1. 安全物理环境

序号	工作单元名称	工作单元描述
1	物理位置选择	对机房进行检查，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	对机房出入口等过程进行检查，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	对机房内的主要设备、介质和防盗报警设施等过程进行检查，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	对机房设计/验收文档进行检查，测评信息系统是否采取相应的措施预防雷击。
5	防火	对机房防火方面的安全管理制度、防火设备等进行检查，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	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	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	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	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	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。

2. 安全通信网络

序号	工作单元名称	工作单元描述
1	网络架构	通过检查、测试、访谈等方式查看网络拓扑情况及网络互联设备，检查核心设备的 CPU 和内存使用率，整个网络带宽是否满足现状，VLAN 划分是否合理，网络架构是否做到设备冗余、链路。
2	通信传输	检查数据在传输过程中的的完整性和保密性措施。
3	可信计算	检查设备是否进行可信验证。

3. 安全区域边界

序号	工作单元名称	工作单元描述
1	边界防护	检查网络边界是否有访问控制设备，访问控制策略是否合理，是否关闭了闲置端口等。
2	访问控制	检查网络中的访问控制策略是否合理、有效。

3	入侵防范	检查网络中是否采用了入侵防范措施，验证该措施是否有效。
4	恶意代码和垃圾邮件防范	检查网络中是否有恶意代码和垃圾邮件防范措施。
5	安全审计	检查网络中是否有综合安全审计措施。
6	可信验证	检查设备是否进行可信验证。

4. 安全计算环境

序号	工作单元名称	工作单元描述
1	身份鉴别	检查所有设备的登录用户是否有身份鉴别措施，是否有复杂度、唯一性等检查。
2	访问控制	检查用户的权限分配情况，默认用户和默认口令使用情况等。
3	安全审计	检查是否开启安全审计功能，是否能审计到每个用户，审计记录是否有保护措施。
4	入侵防范	检查设备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	检查设备的恶意代码防范情况。
6	可信验证	检查设备是否进行可信验证。
7	数据完整性	检查系统数据的传输完整性和存储完整性措施。
8	数据保密性	检查系统数据的传输保密性和存储保密性措施。
9	数据备份恢复	检查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	检查系统的剩余信息保护情况，如将用户鉴别信息以及文件、目录和数据库记录等资源所在的存储空间再分配时的处理情况。
11	个人信息保护	检查系统对个人信息的采集和使用情况。

5. 安全管理中心

序号	工作单元名称	工作单元描述
1	系统管理	检查是否对系统管理员进行统一的身份鉴别，操作审计等。
2	审计管理	检查是否对审计管理员进行统一的身份鉴别，操作审计等。

3	安全管理	检查是否对安全管理员进行统一的身份鉴别，操作审计等。
4	集中管控	检查是否划分独立的安全管理区域，是否对网络中运行的设备进行状态监测、日志审计、安全审计等，是否对补丁、恶意代代码进行统一管理。

6. 安全管理制度

序号	工作单元名称	工作单元描述
1	安全策略	核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目 标、范围、原则和各类安全策略
2	管理制度	检查有关管理制度文档和重要操作规程等过程，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	检查有关制度制定要求文档等过程，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	检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。

7. 安全管理机构

序号	工作单元名称	工作单元描述
1	岗位设置	检查部门/岗位职责文件，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	检查人员名单等文档，测评信息系统各个岗位人员配备情况。
3	授权和审批	检查相关文档，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	检查相关文档，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	审核与检查	检查记录文档等过程，测评信息系统安全工作的审核和检查情况。

8. 安全管理人员

序号	工作单元名称	工作单元描述
1	人员录用	检查人员录用文档等过程，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	检查人员离岗安全处理记录等过程，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	检查培训计划和执行记录等文档，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	检查有关文档等过程，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。

9. 安全建设管理

序号	工作单元名称	工作单元描述
1	定级和备案	检查系统定级相关文档等过程，测评是否按照一定要求确定系统的安全等级。
2	安全方案设计	检查系统安全建设方案等文档，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	检查相关软件开发文档等，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	检查相关文档，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	检查相关文档，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	检查测试验收等相关文档，测评系统运行前是否对其进行测试验收工作。
8	系统交付	检查系统交付清单等过程，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	检查系统之前等级测评的情况，以及之前测评机构的资质等。
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。

10. 安全运维管理

序号	工作单元名称	工作单元描述
1	环境管理	检查机房安全管理制度，机房和办公环境等过程，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	检查资产清单，检查系统、网络设备等过程，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	检查介质管理记录和各类介质等过程，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	检查设备使用管理文档和设备操作规程等过程，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	检查系统对于漏洞和安全隐患风险的管理，是否有报告、记录等文档，是否定期开展安全测评等。
6	网络和系统安全管理	检查系统和网络的安全管理文档，是否明确了角色划分、权限划分，是否覆盖安全策略、账户管理、配置文件的生成及备份、变更审批等内容；检查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修 改等内容；核查是否具有对日志、监测和报警数据等进行分析统计的报告；核查开通远程运维的审批记录，核查针对远程运维的审计日志是否不可以更改等。
7	恶意代码防范管理	检查恶意代码防范管理文档和恶意代码检测记录等过程，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	检查是否对基本配置信息进行记录和保存，基本配置信息改变后是否及时更新基本配置信息库等。
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	检查变更方案和变更管理制度等过程，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	检查系统备份管理文档和记录等过程，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	资产管理	检查是否有资产清单，清单是否包括资产类别、资产责任部门、 重要程度和所处位置等内容；是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施 的选取上是否不同；核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求。
13	应急预案管理	检查应急响应预案文档等过程，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	检查外包运维服务情况，单位是否符合国家有关规定，协议是否明确约定外包运维的范围和工作内容等。

（五）交付产物

包括但不限于以下资料:

1	信息系统安全等级测评报告方案
2	信息系统安全等级保护测评现场测评结构记录表
3	信息系统等级保护定级报告

4	差距分析及整改建议
5	信息系统安全等级保护测评报告
6	其他未列入的应交资料

三、服务保障与承诺

（一）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。

（二）服务提供商应协助、配合采购人与管理部门、公安机关的沟通协调。在测评过程中和测评完成后，协助、配合采购人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，并通过管理部门和公安机关的审核验收。

（三）服务提供商应在项目期内向采购方提供 7*24 小时电话咨询服务，按采购方通知要求提供 2 小时内上门服务。跟踪信息安全等级保护的最新发展情况，及时告之采购人，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。

（四）服务提供商应在项目实施过程中，对采购方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。

（五）服务提供商应在项目开始前，与采购方签订保密协议，严格遵守法律法规，对采购方商业秘密、系统风险信息、项目实施内容及成果信息进行严格保密，未经采购人同意，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。

四、商务要求

（一）服务及合同期限

本次采购项目服务期限为一年，一个服务期满后，可根据服务考评结果确定是否续签，一次续签一年，累计续签不超过两次。

（二）付款方式

合同签订后，首付合同金额 80%，剩余 20%为绩效服务费用。合同金额分两期支付。上述款项由采购人收到供应商出具的等额且合法有效发票后 30 个工作日内支付。

（三）完成期限

合同签订后，5 个月内完成等保测评服务工作，并向采购人提供本合同约定的交付产物。因采购人原因导致供应商测评工期延误，完成期限按延误日期顺延。

（四）服务要求

★1. 供应商要求（实质性要求）投标人提供公安部认可的测评服务单位资质认证（提供相关证明材料复印件或扫描件）。

2. 提供相关的信息安排培训。根据采购人要求组织一次全员网络安全培训，两次网络安全管理人员技术培训。

3. 服务期内提供测评相关仪器设备的共享服务。

4. 提供 7×24 小时电话咨询服务，2 小时内上门服务。

5. 本测评年度内根据采购人要求对单位进行 4 次网络安全分析，包含物理环境，安全管理制度，漏洞扫描等内容，并出具相应分析报告。

6. 本测评年度内根据采购人要求对单位开展 2 次网络安全渗透测试并出具相应测试报告。

7. 本测评年度内根据采购人要求协助查询最近三个月的数据库的审计记录和安全分析报告，协助单位完成安全管理制度制定和应急预案制定。

（五）履约验收

供应商提出验收申请后 5 个工作日内，采购人严格按照《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）、《政府采购需求管理办法》（财库〔2021〕22 号）文件及采购文件要求，结合项目实际，对本项目服务商履约情况与政府采购合同、采购文件及投标文件响应承诺等相关资料进行查验。

第三章 评审方法

由遂宁市财政局组建评审小组，其中评审人员 3 人，监督人员 1 人。通过资格性审查的供应商不足 3 家的，终止本次采购活动，并发布终止采购活动公告。

一、评审

1. 评审小组所有成员集中与单一供应商分别进行一轮或多轮沟通，并给予所有参加采购的供应商平等的机会。沟通顺序以报名顺序为准。评审过程中，评审小组可视情况调整沟通轮次。

2. 在评审过程中，评审小组可以根据采购文件和沟通情况实质性变动采购文件的技术、服务要求以及合同事项等条款，但不得变动采购文件中实质性内容，实质性变动的内容，须经采购人代表书面确认。

3. 对采购文件作出的实质性变动是采购文件的有效组成部分，评审小组应当及时以书面形式同时通知所有参加评审的供应商。

4. 评审过程中，评审的任何一方不得透露与评审有关的其他供应商的技术资料、价格和其他信息。

5. 评审过程中，评审小组发现或者知晓供应商存在违法、违纪行为的，评审小组应当将该供应商响应文件作无效处理，不允许其提交最后报价。

6. 评审完成后，评审小组应出具评审情况记录表，评审情况记录表需包含评审内容、沟通意见、实质性变动内容等。

7. 本项目为一次性报价（即响应文件中报价），现场不再进行二次报价。

8. 推荐成交候选供应商。评审小组应当根据综合评分情况，按照评审得分由高到低顺序推荐 2 家以上成交候选供应商，并编写评审报告。评审得分相同的，按照技术指标优劣顺序推荐。评审得分且技术指标分相同的，按照报价由低到高的顺序推荐。评审得分且技术指标分且报价项得分均相同的，通过抽签确定成交供应商。

9. 评审结果发布。（1）评审小组推荐成交候选供应商后，应第一时间向采购人报告评审结果。（2）采购人同意评审小组评审意见后，及时告知供应商采购结果，并于评审结束后 5 个工作日内，向中标人发布《中标通知书》。

10. 其他事项，评审小组应做好评审情况记录和说明，包括对供应商的资格审查情况、供应商响应文件审查情况、沟通情况、报价情况等，并做好纸质资料的整理归档。

11. 评审过程中未明确事宜，由评审小组负责解释。

二、综合评分

1. 本次综合评分的因素是：报价、运维服务方案、人员综合素质、运维服务应急保障方案、履约考核等。

2. 评审小组成员应当根据响应文件对评分事项进行独立评分。

3. 综合评分明细表

（1）综合评分明细表的制定以科学合理、降低评委会自由裁量权为原则。

（2）综合评分明细表（总分值 100 分）：

序号	评分因素	分值	评分标准
1	报价 30%	30 分	满足采购文件要求且响应价格最低价格为响应基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：报价得分=(基准价 / 报价)×30%×100。 【评分的取值按四舍五入法，保留小数点后两位。】
2	企业综合实力 20%	20 分	1. 具有质量管理体系认证证书、信息安全管理体系认证证书，每有一个得 2 分，最多不超过 4 分，没提供不得分。 2. 具有中国网络安全审查技术与认证中心颁发的信息安全（CCRC）风险评估服务资质、信息安全（CCRC）安全集成服务资质、信息安全（CCRC）灾难备份与恢复服务资质、信息安全（CCRC）应急处理服务资质，每有一个得 2 分，最多不超过 8 分，没提供不得分。 3. 具有数据安全服务能力评定资格证书 （数据安全评估）得 4 分，没提供不得分。 4. 具有中国合格评定国家认可委员会（CNAS）证书的得 2 分，没提供不得分。 5. 具有信息安全服务资质证书-安全工程类证书（二级及以上）得 2 分，没提供不得分。 【注：资质证书复印件须盖投标人公章。招标完成后，采购人有权对中标人提供的相关证书原件进行审查，如中标人不能提供或提供不符，将认定中标人虚假应标。】

3	项目人员配备 20%	20 分	1.拟任本项目的项目负责人（1 人）若具有以下资质或资格的，每有一个得 2.5 分，最多得 10 分，不提供不得分： ①具有信息安全等级测评师（高级）证书；②具有 PMP 证书； ③具有信息安全管理员（CIIP-A）证书； ④注册信息安全专业人员（CISP）。 2.项目团队人员（除项目负责人），具有以下资质或资格的，每有一个证书得 2 分，最多得 10 分，不提供不得分。①具有信息安全等级测评师（中级及以上）证书 ②网络安全保障人员（CISAW）； ③注册信息安全专业人员（CISP）；④CCSS-M 认证证书；⑤DSMM 测评师。 【需提供项目负责人及团队成员社保缴费证明，社保缴费证明以社保局书面证明材料或社保局官方网站查询的缴费记录截图为准;需提供在有效期内的证书复印件并加盖投标人公章，未提供的不得分】
4	实施方案 20%	20 分	等保测评方案从测评需求理解、测评依据、测评流程、测评方法和采用技术、进度保障、质量管理、风险规避措施、人员管理、保密措施、售后服务 10 个方面有单独的文字和章节来表述。每缺少一个章节扣 2 分，每有一个缺陷的扣 1 分。 【备注：缺陷是指方案不适用项目实际情况、凭空编造与项目无关的方案、项目实施时间地点有误、技术引用错误以及不可能实现的夸大情形】
5	类似业绩 10%	10 分	具有等级保护测评案例每个得 1 分，最多 10 分。 【注：应提供自 2020 年 1 月 1 日以来开展的信息系统第三级测评案例，相同案例不重复计分，案例需提供合同复印件或用户证明（加盖用户单位公章）等相关证明材料，以上证明材料均需加盖投标人公章，未提供不得分。】
注：评分的取值按四舍五入法，小数点后保留两位。			

第四章 成交事项

一、确定成交供应商

采购人将按评审小组推荐的成交候选供应商顺序确定成交供应商。

1. 采购人收到评审结果及有关资料后，将在 2 个工作日内按照评审结果中推荐的成交候选供应商顺序确定成交供应商。成交候选供应商并列的，采购人自主采取公平、择优的方式选择成交供应商。采购人逾期未确定成交供应商且不提出异议的，视为确定评审结果提出的排序第一的供应商为成交供应商。

2. 采购人确定成交供应商过程中，发现成交候选供应商有下列情形之一的，应当不予确定其为成交供应商：

（1）发现成交候选供应商存在禁止参加本项目采购活动的违法行为的；

（2）成交候选供应商因不可抗力，不能继续参加政府采购活动；

（3）成交候选供应商无偿赠与或者低于成本价竞争；

（4）成交候选供应商提供虚假材料；

（5）成交候选供应商恶意串通。

成交候选供应商有本条情形之一的，采购人可以确定后一位成交候选供应商为成交供应商，依次类推。无法确定成交供应商的，应当重新组织采购。

二、成交结果

采购人确定成交供应商后，成交供应商不能及时领取成交通知书的，可由采购人按照成交供应商提供的收件信息通过邮寄、快递等方式将项目成交通知书送达成交供应商。

三、成交通知书

1. 成交通知书为签订采购合同的依据之一，是合同的有效组成部分。

2. 成交通知书对采购人和成交供应商均具有法律效力。成交通知书发出后，采购人无正当理由改变成交结果，或者成交供应商无正当理由放弃成交的，将承担相应的

法律责任。

3. 成交供应商的响应文件作为无效响应文件处理，采购人在取得有权主体的认定以后，有权宣布发出的成交通知书无效，并收回发出的成交通知书，依法重新确定成交供应商或者重新开展采购活动。

第五章 合同事项

一、签订合同

1. 成交供应商应在成交通知书发出之日起10个工作日内与采购人签订采购合同。由于成交供应商的原因逾期未与采购人签订采购合同的，将视为放弃成交，取消其成交资格并将按相关规定进行处理。

2. 采购文件、成交供应商的响应文件及双方确认的澄清文件等，均为有法律约束力的合同组成部分。

3. 采购人不得向成交供应商提出任何不合理的要求，作为签订采购合同的条件，不得与成交供应商私下订立背离合同实质性内容的任何协议，所签订的采购合同不得对采购文件和成交供应商响应文件确定的事项进行修改。

4. 成交供应商因不可抗力原因不能履行政府采购合同或放弃成交的，采购人可以与排在成交供应商之后第一位的成交候选人签订采购合同，以此类推。

5. 采购文件、成交供应商提交的响应文件、采购商中的报价、成交供应商承诺书、成交通知书等均称为有法律约束力的合同组成内容。

二、合同分包、转包

本采购项目禁止成交供应商采取分包、转包方式履行合同。

三、履约保证金（实质性要求）

本项目不收取履约保证金。

四、履行合同

1. 成交供应商与采购人签订合同后，合同双方应严格执行合同条款，履行合同规定的义务，保证合同的顺利完成。

2. 在合同履行过程中，如发生合同纠纷，合同双方应按照《合同法》的有关规定进行处理。

五、验收

本项目采购人将严格按照有关要求及采购需求组织验收。

六、资金支付

1. 采购人将按照采购合同规定，及时向成交供应商支付采购资金。

2. 采购项目资金支付程序，按照国家有关财政资金支付管理的规定执行。