第三章 技术、服务及其他要求

（注：本章的技术、服务及其他要求中，带“★”的要求为实质性要求。采购人、代理机构应当根据项目实际要求合理设定，并在第五章符合性审查中明确响应要求。）

3.1.采购内容

采购包1：

采购包预算金额（元）：610,000.00

采购包最高限价（元）：608,700.00

序号	采购品目名称	标的名称	数量(计量单位)	标的金额（元）	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及强制采购节能产品	是否涉及优先采购节能产品	是否涉及优先采购环境标志产品
1	C16070400 安全运维服务	政务外网安全服务	1.00（项）	608,700.00	软件和信息技术服务业	否	否	否	否	否

报价要求

采购包1：

序号	报价内容	数量（计量单位）	最高限价	价款形式	报价说明
1	政务外网安全服务	1.00（项）	608,700.00	总价	本项目预算金额：610,000.00元/年；最高限价：608,700.00元/年；服务期限：三年（合同一年一签）。

★注：本采购包涉及采购货物的，供应商响应产品应当明确品牌和规格型号并指向唯一产品，不能指向唯一产品的，应通过报价表唯一产品说明栏补充说明。

本项目涉及核心产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：涉及核心产品的，具体评审规定见第五章。

本项目涉及采购进口产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：不涉及采购进口产品时，供应商不得提供进口产品进行响应；涉及采购进口产品时，如国产产品满足采购需求，也

可提供国产产品进行响应。

本项目涉及强制采购节能产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：响应产品属于《节能产品政府采购品目清单》中政府强制采购的产品，供应商应当提供由国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，否则作无效响应处理。具体要求详见第五章符合性审查表。

本项目涉及优先采购节能产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《节能产品政府采购品目清单》中优先采购的产品，供应商提供由国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

本项目涉及优先采购环境标志产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《环境标志产品政府采购品目清单》中的产品，供应商提供由国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

3.2.技术要求

采购包1：

标的名称：政务外网安全服务

序号	符号标识	技术要求名称	技术参数与性能指标
			一、项目背景与目标 为深入贯彻落实《网络安全法》《关键信息基础设施安全保护条例》《数据安全法》《密码法》等法律法规要求，全面提升新津区智慧蓉城运行中心电子政务外网的安全防护能力、应急响应水平和持续运营保障能力，特实施本项目。 以“体系化建设、常态化运营、实战化保障”为原则，聚焦“基础设施巡检、人员驻场、重保支撑、漏洞治理、渗透验证、终端安全、意识提升”七大核心能力模块，构建覆盖“云-网-边-端-数-人”的全栈式安全运营体系，实现“监测-预警-处置-加固-培训-合规”闭环管理，确保政务外网业务连续、数据安全、风险可控。 **二、服务范围与依据**

2.1政务基础设施现状

覆盖新津区智慧蓉城运行中心所辖电子政务外网全网信息系统，具体包括：

序号	项目名称	具体对象	数量	状态	部署位置
1	网络设备	核心路由器	2台	良好	新津区人民政府2F机房
2		核心交换机	2台	良好	新津区人民政府2F机房
3		局办汇聚交换机	6台	良好	新津区人民政府2F机房
4	网络安全设备	互联网出口防火墙	2台	良好	新津区人民政府2F机房
5		DMZ区域防火墙	1台	良好	新津区人民政府2F机房
6		内网区域防火墙	1台	良好	新津区人民政府2F机房
7		云边界防火墙	1台	良好	新津区人民政府2F机房
8		外联区域防火墙	3台	良好	新津区人民政府2F机房
9		入侵防御系统（IPS）	1台	良好	新津区人民政府2F机房
10		SSLVPN	1套	良好	新津区人民政府2F机房
11		运维堡垒机	1套	良好	新津区人民政府2F机房
12		日志审计系统	1套	良好	新津区人民政府2F机房
13		全流量网络安全分析系统	1套	良好	新津区人民政府2F机房
14		网络安全事件验证系统	1套	良好	新津区人民政府2F机房
15		流量采集交换机	1套	良好	新津区人民政府2F机房
16		漏洞扫描系统	1套	良好	新津区人民政府2F机房
17	服务器资源	政务云服务器（含云主机、云数据库等）	300台	良好	成都市政务云环境
18	终端设备	各局办单位终端（PC/笔记本）	3965台	良好	局办单位机房
19	核心业务系统	政务云和本地的核心业务系统	46套	良好	政务云环境

基于基础设施的完备，以 “一朵政务云”和“一张网” 为核心的集约化架构基本成型。这不仅实现了跨部门、跨层级的信息共享与业务协同，同时，高速网络覆盖

纵深推进，为政务服务直达基层提供了“高速公路”。

三、服务内容

3.1服务内容

新津区政务外网安全服务，具体包括：

序号	服务名称	服务子项	内容概述
1	安全基础设施巡检	网络与安全设备日常巡检	面向电子政务外网骨干网络核心节点（含核心/汇聚交换机、边界路由器等）及全域安全防护体系（涵盖出口防火墙、区域隔离防火墙、全流量安全分析系统、网络安全事件验证平台、统一运维监控中心、日志审计系统、堡垒机、SSL VPN等），实施7×24小时全时域、全要素、全链路的安全运维保障。通过策略动态调优、健康状态智能巡检、多源日志关联分析与自动化应急响应机制，构建“可视、可管、可控、可溯”的一体化安全基础设施运营体系。
		本地与政务云服务器安全监测	针对部署于新津区本地机房的物理/虚拟化服务器集群及政务云平台中的云主机、云数据库等关键计算资源，开展常态化安全基线核查、自动化漏洞探测、异常行为智能监测与精细化访问控制审计，实现“云-边-端”协同的纵深防御与持续合规保障。
2	人员驻场服务	日常安全运营支持	驻场工程师提供工作日5×8小时现场值守，非工作时段远程应急待命，深度参与安全运营全生命周期管理。依托多维安全数据（日志、流量、威胁情报、资产画像），开展高级威胁研判、攻击链还原、事件协同响应与闭环治理，并支撑安全制度落地执行，同步输出结构化运营报告（日报/月报/巡检报告），赋能决策层精准掌握安全态势。
		安全文档编制	体系化输出《网络安全运营日报》《月度安全态势分析报告》《年度安全工作总结》《重大安全事件应急响应报告》《关键设备健康巡检报告》《高危漏洞预警函》等标准化、可审计、可追溯的安全运营交付物，全面支撑监管合规与内部治理需求。
		重保前准备	围绕重大活动保障目标，定制专项安全保障方案与多场景应急预案，系统性开展漏洞清零、访问权限收敛、安全策略加固、关键数据备份验证及攻击面收敛等前置防御动作，筑牢“事前预防”防线。
	网络		

			3	安全重保服务	重保中值守与响应	实施“专家5×12小时现场坐镇 + 7×24小时远程协同”双轨保障机制，依托实时威胁监测平台，对APT攻击、DDoS、0day利用等高危行为实现秒级发现、分钟级封控、小时级溯源，每日输出《重保安全日报》，确保保障期间“零重大事件、零数据泄露、零业务中断”。
					重保后总结提升	基于实战攻防数据，深度复盘攻击手法、防御短板与响应效能，输出《重保总结与能力提升报告》，提出体系化加固建议，推动“以战促防、以战促改、以战促建”的安全能力螺旋式上升。
			4	网络安全漏洞扫描与闭环治理服务	月度自动化扫描	每月对本地及政务云环境中的操作系统（Windows/Linux）、Web应用、数据库、中间件等资产开展全覆盖、高频次自动化漏洞扫描，并在重大活动前实施增强型专项检测，确保攻击面持续收敛。
					人工验证与闭环治理	结合人工渗透验证手段有效降低误报率，精准识别真实风险，输出《漏洞风险评估报告》与《高危漏洞预警函》，建立“发现-通报-整改-复测-归档”五步闭环管理机制，实现漏洞全生命周期可控、可管、可验。
			5	网络安全渗透测试服务	年度手工渗透测试	面向政务云及本地机房承载的核心业务系统（含物联网感知平台、事件中枢平台、数据中台等），开展年度深度红队式渗透测试。严格遵循 MITRE ATT&CK® 攻击框架，模拟高级持续性威胁（APT）攻击者的战术、技术与过程（TTPs），完整复现从初始入侵、权限提升、横向移动到数据窃取的攻击链。重点聚焦身份认证绕过、会话劫持、API滥用、水平/垂直越权、任意文件上传及业务逻辑缺陷等高危场景，全面检验现有防御体系在真实对抗环境下的有效性、韧性与检测盲区。
					修复指导与复测	提供可落地的漏洞修复方案与安全编码建议，并在修复完成后开展回归性复测验证，确保风险彻底消除，最终交付《渗透测试报告》与《复测验证报告》，形成“攻-防-验”闭环。
			6	终端与接入安全监测	局办单位终端安全监测	基于政务外网流量镜像或轻量化探针部署，对全区各局办单位接入终端（PC/笔记本等）实施无感化、非侵入式远程安全监测。依托网络流量深度检测（NDR）与行为基线建模技术，实时识别木马回连、异常远程控制（RDP/VNC/TeamViewer）、挖矿外联、C2通信、暴力破解及违规访问境外高危地址等失陷指标（IOCs），精准定位已失陷或高风险终端，自动生成《终端安全风险预警单》，支撑快速隔离与应急处置。

		年度线下安全巡检	每年对不少于32家区属局办单位开展现场安全合规巡检，重点核查终端安全策略执行、网络结构、外设管控、账户权限等基线符合性，出具《网络安全巡检问题清单》，推动问题整改与安全能力标准化提升。
7	网络安全技术培训服务	网络安全培训	面向“管理层-技术人员-普通员工”三类角色，分层设计课程体系：为管理层强化合规责任与风险治理意识，为技术人员提升实战攻防与应急处置能力，为普通员工普及基础安全素养。采用“线上直播+录播回看+线下小班实训”混合式教学模式，确保培训覆盖率、参与度与实效性。
		培训支撑与内容更新 应急演练	全流程支撑培训组织工作（通知发布、签到管理、在线考试、证书生成、档案归集），并建立课程动态更新机制——每季度结合最新攻防趋势、监管要求及本地典型安全事件，迭代优化课件内容，确保培训内容“紧贴实战、紧跟政策、紧随威胁”。 负责组织1场大型应急演练

3.2安全基础设施巡检要求

服务目标：保障政务外网骨干网络与全域安全设备7×24小时稳定、高效、合规运行。

服务要求：

(1)对核心/汇聚交换机、边界路由器、各类防火墙、IPS、堡垒机、日志审计、全流量分析系统等实施策略动态调优、健康状态智能巡检；

(2)对政务云及本地服务器开展安全基线核查、异常行为监测、访问控制审计；

(3)构建“可视、可管、可控、可溯”的一体化基础设施运营体系。

交付成果：

(1)《机房巡检报告》

(2)《策略变更记录》

3.3人员驻场服务要求

服务目标：配置1名专职安全工程师常驻运行中心，提供“贴身式”安全运营支持。

服务要求：

(1)工作日5×8小时现场值守，非工作时间远程待命，重大时期7×24小时响应；

(2)每日开展多源日志关联分析、威胁告警初判与高级威胁研判；

(3)协助应急响应、溯源分析、制度执行（如变更审批、机房出入、密码管理）；

(4)作为安全服务接口人，推动问题闭环。

交付成果：

(1)《网络安全运营日报》

(2)《网络安全运营月报》

			(3)《网络安全运营季报》 (4)《年度安全工作总结报告》 (5)《重大安全事件应急响应报告》 (6)《网络安全事件预警函》 (7)《高危漏洞预警函》 **3.4网络安全重保要求** 服务目标：在国家重要保障时期，构建战时防御体系，实现“零事故、零泄露、零中断”。 服务要求： (1)重保前：制定保障方案与应急预案，开展漏洞扫描与修复，完成策略加固、权限收敛、备份验证； (2)重保中：专家5×12小时现场值守加7×24小时远程响应，实时监测攻击行为，快速封禁与响应，每日提交专报； (3)重保后：总结攻击类型与处置效率，输出改进报告，推动长效加固。 交付成果： (1)《网络安全重保专项保障方案》 (2)《重保前资产与漏洞梳理报告》 (3)《重保安全日报》 (4)《重保总结与能力提升报告》 **3.5网络安全漏洞扫描与闭环治理服务要求** 服务目标：通过月度自动化扫描+人工验证，主动发现并推动修复主机、应用、数据库等层面漏洞，降低被攻击风险。 服务要求： (1)每月1次全面扫描，重大活动前加测； (2)覆盖主机系统（Windows/Linux/网络设备）、Web应用（OWASP Top 10）、数据库、中间件； (3)使用网络安全漏扫工具等合规工具，结合人工验证降低误报； (4)输出报告→派发整改→限期修复→复扫验证→闭环归档。 交付成果： (1)《月度信息资产漏洞扫描报告》（含漏洞清单、风险等级、影响描述） (2)《漏洞风险评估报告》 (3)《高危漏洞预警函》 (4)《漏洞闭环治理台账》
1		服务内容及要求	**★3.6网络安全渗透测试服务要求** 服务目标：模拟红队真实攻击，深度挖掘自动化工具无法发现的逻辑漏洞、权限绕过等高风险问题，验证防御体系有效性。 服务要求： (1)年度1次对核心业务系统（如物联网感知平台、事件中枢平台、数据中台等）开展手工渗透测试；

(2)采用黑盒/灰盒测试，覆盖身份认证、会话管理、API安全、文件上传、越权等；

(3)输出报告→修复指导→复测验证；

(4)全程授权、录像、避开业务高峰。

交付成果：

(1)《渗透测试报告》（含攻击路径、漏洞详情、风险等级、修复建议）

(2)《渗透复测报告》

3.7终端与接入安全监测要求

服务目标：实现对全区3965台终端的无感化、非侵入式安全监测与风险闭环。

服务要求：

(1)基于流量镜像或轻量探针，实时识别木马回连、C2通信、挖矿外联、暴力破解等失陷行为；

(2)每年对不少于32家局办单位开展线下安全合规巡检；

(3)自动输出风险预警单，支撑快速隔离处置。

交付成果：

(1)《网络安全事件预警函》

(2)《局委办网络安全巡检报告》

3.8网络安全技术培训服务要求

服务目标：协助新津区智慧蓉城运行中心构建分层、分类、灵活的网络安全培训体系，提升管理人员合规意识、技术人员实战能力、普通员工安全素养，降低因人为操作或意识不足引发的安全风险。

服务要求：

(1)培训形式灵活适配：支持“线上直播+录播回看+线下小班”多种方式，根据运行中心实际工作安排协商确定培训时间与形式，不强制集中参训；

(2)分层课程设计：

管理层：聚焦《网络安全法》《关基条例》《数据安全法》责任解读、安全事件追责案例、应急指挥流程；

技术岗位：涵盖安全设备调测（防火墙/WAF/SIEM）、漏洞修复实操、日志分析、应急响应流程演练；

普通员工：普及钓鱼邮件识别、社交工程防范、密码安全、终端合规操作、数据防泄露常识；

(3)内容持续更新：每季度更新1次课件内容，结合最新攻防趋势、本地安全事件、制度修订动态；

(4)培训组织协助：协助运行中心发布培训通知、收集反馈、需求组织考试、归档材料等。

（5）应急演练：组织一次应急演练。

交付成果：

(1)《网络安全培训课件PPT》

(2)《网络安全培训记录表》

(3)《网络安全应急演练方案》

(4)《网络安全应急演练记录》

四、考核办法

本项目采用“过程+结果+服务+协同”四维联动的综合考核机制，总分100分。考核旨在客观评价供应商在安全运营中的专业能力、响应效率、管理规范与协同效果，不仅关注“做了什么”，更关注“做得好不好”、“有没有价值”。

4.1考核维度与权重分配

考核维度	权重	核心关注点
结果成效	30%	安全风险是否有效控制，重大事故是否为零，核心指标是否达成。
过程质量	30%	服务流程是否规范，交付物是否及时、完整、准确、可审计。
服务质量	25%	响应时效、沟通态度、问题解决能力、客户满意度。
管理协同	15%	对运行中心及各委办局的支撑力度、制度落地配合度、整改督办执行力。

4.2具体考核指标与评分细则

4.2.1、结果成效考核（30分）

本部分聚焦安全运营的核心目标达成情况，是“硬性底线”。

指标名称	分值	考核标准	评分说明
重大安全事故发生率	5分	服务期内发生1起及以上重大网络安全责任事故（如数据泄露、业务中断超过2小时），此项得0分。	以采购人出具的《安全事件认定书》为准。
漏洞闭环治理率	10分	高危/严重级别漏洞整改完成率≥95%，每低于1%扣1分；整改超期未闭环，每项扣0.5分。	以《漏洞预警函》签收记录和复测报告为准。
告警研判准确率	10分	经人工复核，真实威胁识别率≥95%，误报率≤5%。每低于1%扣1分。	由运行中心随机抽样100条告警进行人工复核。
终端风险处置率	5分	对发出的《终端安全风险预警单》，相关单位在3个工作日内完成隔离或修复的比例≥90%。每低于5%扣1分。	以预警单回执及复测记录为准。

补充：**重大安全事件**指造成严重后果的安全事故，包括但不限于：发生数据泄露（涉及敏感信息或影响用户1万人以上）、核心业务系统中断持续2小时及以上、遭受勒索软件或APT攻击导致系统失陷、或被监管机构通报/处罚等情形；**一般安全事件**指未造成重大影响但需处置的安全异常，如低风险漏洞被利用、短暂服务抖动、少量非敏感数据误发、终端感染未扩散等。

4.2.2、过程质量考核（30分）

本部分考核服务执行的规范性、严谨性和可追溯性，是“工作痕迹”，本模块的分数等于本模块实际得分（总分100分）x30%

模块	权重	交付成果名称	量化考核指标	分值	评分标准
人员驻场服务	50%	《网络安全运营日报》	每工作日交付1份	10	每缺1份扣0.5分，扣完为止
		《网络安全运营月报》	每月交付1份	10	每缺1份扣4分，扣完为止
		《网络安全运营季报》	季度交付≥1份	10	不提供不得分
		《网络安全事件预警函》	季度交付≥5份	10	每缺1份扣2分；应发未发致事故，本项0分
		《高危漏洞预警函》	按实际发生情况提供	10	应发未发致事故，本项0分
网络安全重保	10%	《网络安全重保专项保障方案》	每次重保前交付	3	每缺1次扣1.5分，未交付0分；每季度无重保则此项满分
		《重保安全日报》	重保期间每日提交	4	每缺1日扣1分；每季度无重保则此项满分
		《重保总结与能力提升报告》	每次重保结束后5个工作日内交付	3	每延迟1次扣1.5分，未交付0分，无重保此项满分
网络安全漏洞扫描与闭环治理服务	30%	《月度信息资产漏洞扫描报告》	每月交付1份	15	每缺1份扣5分，扣完为止
		《高危漏洞预警函》	按实际发生情况提供	15	应发未发致事故，本项0分
终端与接入安全监测	5%	《网络安全事件预警函》	季度交付≥5份	5	每缺1份扣1分；应发未发致事故，本项0分
网络安全技术培训服务	5%	《网络安全培训课件PPT》	季度交付≥1套	2.5	每缺1套扣2.5分，最低0分
		《网络安全培训记录表》	季度交付≥1份	2.5	每缺1份扣2.5分，最低0分

4.2.3、服务质量考核（25分）

本部分考核供应商的服务意识、响应速度和问题解决能力，是“用户体验”。

指标名称	分值	考核标准	评分说明
响应时效	8分	一般事件：30分钟内响应并提供初步处置建议。 重大事件：15分钟内响应，2小时内专家到场。	每超时1次扣2分，扣完为止。以系统日志、电话录音、微信记录等为证。
沟通协作	7分	与运行中心、各委办局沟通顺畅、态度积极、解答清晰。	由运行中心组织季度满意度调查，平均分低于85分，扣3分；低于80分，扣5分。
问题解决能力	6分	对复杂安全事件（如APT、勒索病毒）能独立提出有效解决方案，无需反复请示。	由运行中心专家团根据事件处理报告打分，优秀得6分，良好得4分，一般得2分，差得0分。
服务主动性	4分	能主动发现潜在风险（如策略配置错误、资产遗漏）、提出优化建议并推动落实。	每季度至少提交1份《安全优化建议书》，未提交扣2分；建议被采纳并实施，每条加1分（上限2分）。

4.2.4、管理协同考核（15分）

本部分考核供应商对全区安全治理体系的支撑作用，是“大局观”。

指标名称	分值	考核标准	评分说明
制度落地支持	5分	积极协助运行中心推动《网络安全管理制度》《终端安全管理规范》等文件的宣贯与执行。	由运行中心信息安全科打分，优秀得5分，良好得3分，一般得1分。
跨部门协调能力	5分	在漏洞整改、事件处置中，能有效协调各委办局，确保任务按时完成。	由运行中心根据《整改督办单》完成情况打分，完成率≥95%得5分，每低5%扣1分。
数据与平台对接	5分	所有安全数据（日志、报告、告警）均按要求接入“墨攻平台”，确保数据实时、准确、完整。	由运行中心技术团队核查，数据缺失或延迟，每次扣1分；数据格式错误，每次扣0.5分。

4.3考核周期与方式

4.3.1、考核周期

考核类型	时间节点	考核内容
月度抽查	每月第5个工作日前	抽查上月关键交付物（日报、预警函、扫描报告）的质量与及时性。

季度评估	每季度末月第10个工作日前	综合评估四大维度表现，形成季度考核报告，作为支付进度款依据。
年度总评	每年12月20日前	全年综合评分，结合满意度调查、整改成效、重大事件复盘，确定最终等级。

4.3.2、考核方式

文档审查：对所有交付物进行完整性、规范性、实用性评审。

系统核查：通过“墨攻平台”、堡垒机日志、邮件系统等，核查响应时效、操作留痕、数据上报情况。

现场抽查：每季度随机抽取1-2次驻场工作记录、巡检过程、培训组织情况，进行现场或视频复核。

满意度调查：每季度向运行中心及各委办局发放匿名问卷，收集对供应商服务态度、响应速度、专业能力的评价。

专家评议：对于重大事件处置、渗透测试报告等复杂事项，由运行中心组织专家团进行独立打分。

4.4考核等级与奖惩措施

考核得分	等级	结果与奖惩措施
95-100分	优秀	全额支付服务费；优先续约；通报表扬。
90-94分	合格	全额支付服务费；并在下一季度完成整改。
<90分	不合格	扣减当期服务费的5%；限期1个月整改，整改后复评；若连续两次不合格，启动退出机制。

五、项目管理与运行管理

(1)项目组织架构：设立项目经理+技术组长+驻场工程师三级管理机制。

(2)沟通机制：周例会+月度汇报+紧急事件即时响应通道。

(3)质量保障：所有交付物需经内部QA审核+采购人确认签字。

(4)保密机制：签署保密协议，数据不出本地，操作留痕审计。

(5)应急机制：建立7×24小时专家支持热线，重大事件2小时内到场。

六、其他要求

供应商须在响应文件中提供实施方案：①安全基础设施巡检方案；②人员驻场服务方案；③网络安全重保服务方案；④网络安全漏洞扫描与闭环治理服务方案；⑤网络安全渗透测试服务方案；⑥终端与接入安全监测方案；⑦网络安全技术培训服务方案。服务方案：①服务机构设置；②项目质量保障措施；③响应措施。

注：1、以上带★号条款为实质性要求。

2、本项目所涉及的所有国家标准、地方标准、行业标准等如有最新的标准以最新标准为准。

3.3.服务要求

3.3.1服务内容要求

采购包1：

序号	符号标识	服务要求名称	服务要求内容
1	★	付款进度安排（以此为准）	因系统固化原因，3.3.2商务要求中付款进度安排不适用于本项目，付款进度安排以此为准：按季度支付，每个季度服务结束后供应商向采购人提供服务报告且完成当季度考评后，采购人收到供应商提供的等额有效增值税发票，10个工作日内支付上一个季度的服务费，以此类推。（如季度考核中有服务费扣除的，则按扣除服务费用后的金额支付；若供应商未及时提交增值税发票，采购人付款时间顺延且对此不承担任何责任）

3.3.2.商务要求

采购包1：

序号	符号标识	商务要求名称	商务要求内容
1	★	服务期限	三年（合同一年一签）
2	★	服务地点	成都市新津区，具体地点由采购人指定。
3		验收、交付标准和方法	严格按照政府采购相关法律法规以及《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)、采购文件要求、成交供应商的响应文件及承诺、签订的合同、验收所必须具备的其他材料以及主管部门的相关要求进行验收。采购人与供应商双方如对质量要求和技术指标的约定标准有 相互抵触或异议的事项，由采购人在采购文件及投标文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。
4		支付方式	分期付款

5		付款进度安排	1、按季度支付，每个季度服务结束后供应商向采购人提供服务报告且完成当季度考评后，采购人收到供应商提供的等额有效增值税发票，10个工作日内支付上一个季度的服务费，以此类推。（如季度考核中有服务费扣除的，则按扣除服务费用后的金额支付；若供应商未及时提交增值税发票，采购人付款时间顺延且对此不承担任何责任），达到付款条件起10日内，支付合同总金额的25.00% 2、按季度支付，每个季度服务结束后供应商向采购人提供服务报告且完成当季度考评后，采购人收到供应商提供的等额有效增值税发票，10个工作日内支付上一个季度的服务费，以此类推。（如季度考核中有服务费扣除的，则按扣除服务费用后的金额支付；若供应商未及时提交增值税发票，采购人付款时间顺延且对此不承担任何责任），达到付款条件起10日内，支付合同总金额的25.00% 3、按季度支付，每个季度服务结束后供应商向采购人提供服务报告且完成当季度考评后，采购人收到供应商提供的等额有效增值税发票，10个工作日内支付上一个季度的服务费，以此类推。（如季度考核中有服务费扣除的，则按扣除服务费用后的金额支付；若供应商未及时提交增值税发票，采购人付款时间顺延且对此不承担任何责任），达到付款条件起10日内，支付合同总金额的25.00% 4、按季度支付，每个季度服务结束后供应商向采购人提供服务报告且完成当季度考评后，采购人收到供应商提供的等额有效增值税发票，10个工作日内支付上一个季度的服务费，以此类推。（如季度考核中有服务费扣除的，则按扣除服务费用后的金额支付；若供应商未及时提交增值税发票，采购人付款时间顺延且对此不承担任何责任），达到付款条件起10日内，支付合同总金额的25.00%
6		违约责任与解决争议的方法	1、违约责任：（1）因成交供应商不履行合同，不按规定完成任务或未按响应文件承诺投入人力、物力和设备，采购人有权要求成交供应商限期整改，逾期未整改且严重违约的，采购人有权终止合同；因此造成的经济损失由成交供应商给予采购人赔偿。（2）因成交供应商管理不善或操作不当等原因造成采购人、成交供应商或第三方人身、财产事故的，由成交供应商承担责任并负责善后处理，造成采购人经济损失的，成交供应商应给予采购人经济赔偿。产生事故的直接原因，以相关主管部门的鉴定为准。（3）成交供应商无正当理由提前解除合同的，应向采购人支付违约金（具体违约金以合同约定为准）；由于解除合同造成的经济损失超过违约金的，成交供应商还应给予采购人赔偿。（4）成交供应商若未达到规定履约能力接受该项任务，采购人有权无条件终止合同；给采购人造成经济损失的，成交供应商应做相应赔偿。 2、解决争议的方法：向项目所在地的人民法院提起诉讼。

3.4.其他要求

采购包1：

无