采购需求

（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）：1,345,300.00

采购包最高限价（元）：1,160,700.00

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	C16079900 其他运行维护服务	网络安全服务	1.00（项）	1,160,700.00	软件和信息技术服务业	否	否	否	否	否

是否适用本国产品标准：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	网络安全服务	1.00（项）	1,160,700.00	总价	无

★注：采购包涉及采购货物的，投标人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，投标人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，投标人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，否则作无效投标处理。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，投标人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，投标人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：网络安全服务

<table>
<tr><th>序号</th><th>符号标识</th><th>技术要求名称</th><th>技术参数与性能指标</th></tr>
<tr><td>1</td><td></td><td>技术参数及服务要求</td><td>1.★服务内容清单
<table><tr><th>序号</th><th>名称</th><th>数量</th></tr><tr><td>1</td><td>网络安全检测分析服务</td><td>1 项</td></tr><tr><td>2</td><td>漏洞扫描服务</td><td>1 项</td></tr><tr><td>3</td><td>安全通告服务</td><td>1 项</td></tr><tr><td>4</td><td>终端病毒统一防护服务</td><td>1 项</td></tr><tr><td>5</td><td>安全态势感知服务</td><td>1 项</td></tr><tr><td>6</td><td>网络安全管理体系建设服务</td><td>1 项</td></tr><tr><td>7</td><td>网络安全培训服务</td><td>1 项</td></tr></table></td></tr>
</table>

			8	网络安全咨询服务	1 项
			9	应急演练服务	1 项
			10	风险评估服务	1 项
			11	渗透测试服务	1 项
			12	应急响应服务	1 项
			13	重要时期保障	1 项
			14	安全巡检服务	1 项
			15	代码审计服务	1 项
			16	安全加固服务	1 项
			17	台账登记服务	1 项
			18	边界防火墙续保升级服务	1 项
			19	准入系统服务	1 项
			20	入侵防御系统服务	1 项
			21	网页防篡改防护服务	1 项
			22	USB 外设管理服务	1 项

2.技术要求

（1）网络安全检测分析服务

1.服务内容：依托专业的网站安全监测平台，对采购人网站的木马安全、网页篡改、网站可用性、网页关键字、网站安全漏洞等进行全天 24 小时不间断监测服务，从而提升网站的安全防护能力和网站服务质量。每月提供 1 次网络安全监测分析服务，并编制《网站安全监测报告》。

（2）漏洞扫描服务

1.服务内容：通过具备国有自主知识产权的漏洞扫描工具以及综合安全评估工具以本地扫描或远程扫描的方式对中心的服务器、数据库、WEB 应用和网络设备进行安全扫描，从内网和外网两个角度来查找服务器、数据库、WEB 应用和网络设备等安全对象目标存在的安全风险、漏洞和威胁。每月提供 1 次提供漏洞扫描服务，并编制《漏洞扫描报告》，如遇上级部门或网络安全主管部门通报重大漏洞时需进行专项漏洞扫描，并编制专项漏洞扫描报告。

2.▲为保障漏洞扫描工具数据存储的安全性，工具所使用的后台数据库需为国产数据库，且符合国家对软件可控的要求。**（提供承诺函并加盖供应商公章）**

3.▲由于采购人资产数量较多且业务连续性要求高、为降低扫描对业务的影响、需在业务空闲时完成扫描，脆弱性识别与分析扫描工具后台国产数据库需支持分布式大规模并行处理集群 150 个节点以上。（提供第三方机构出具的检验或检测报告复印件，并加盖供应商公章）

4.▲为保障漏洞扫描工具数据存储的安全性，漏洞扫描工具所使用的后台数据库需为国产数据库，后

			台国产数据库支持国密 SM 系列算法等、保障漏扫数据的安全。（提供第三方机构出具的检验或检测报告复印件，并加盖供应商公章） 5.▲工具后台国产数据库支持在数据库初始化时配置加密选项，支持全库加密、口令加密、指定列加密、跨网络加密等多种加密方式，以及通过 TLS 加密方式进行加密通信。**（提供功能截图并加盖供应商公章）** 6.▲工具后台国产数据库支持对同构及异构数据库互连，同时支持 DBLINK 和 FDW 功能，具备对国内外主流数据库及标准数据文件的访问能力。**（提供功能截图并加盖供应商公章）** 7.▲工具后台国产数据库支持 bytea、oid、clob、blob 等数据类型，能够存储大型非结构化数据。**（提供功能截图并加盖供应商公章）** **（3）安全通告服务** 1.服务内容：提供安全通告服务，安全通告包含最新安全漏洞、威胁（0day、系统漏洞、网络攻击）的解决办法、安全问题描述和相应的处理意见。每月提供 1 次安全通告服务，并编制《安全通告》。 **（4）终端病毒统一防护服务** 1.服务内容：提供统一的支持信创的病毒防护体系服务，在采购人单位的计算机终端上部署企业版病毒防护工具，实现全中心终端电脑统一安全管控。每月编制《终端病毒防护服务报告》。 **（5）安全态势感知服务** 1.服务内容：按照网络安全的相关要求，分别在新华三云、浪潮云提供信息安全（态势感知）监测预警服务。实时采集与分析现有成都政务云上信息系统的网络访问流量，同时收集多元、异构的海量日志，结合威胁情报、攻击行为分析、机器学习、关联分析等新一代安全技术对各类型网络攻击行为进行检测、分析，追踪和定位，以可视化手段向采购人展示，并配合采购人进行预防整改，针对系统安全进行加固。每月编制《安全态势服务报告》。 **（6）网络安全管理体系建设服务** 1.服务内容：从实际业务流程的原则出发，协助采购人开展网络安全管理体系建设，建立健全网络安全相关管理制度文件，供管理人员或操作人员执行日常操作时参考，确保所制定的文件的适用性，且满足相应保护等级的安全管理要求。每年提供 1 次网络安全管理体系建设服务，并编制《网络安全管理制度》《网络安全组织管理制度》《网络安全人员管理制度》《网络安全建设制度》。

			（7）网络安全培训服务 1.服务内容：提供覆盖信息安全意识、技术、管理等内容的信息安全培训服务，以提升信息安全认知、技术与管理能力。通过定期开展覆盖网络信息安全意识、技术、管理等内容的网络安全基础培训服务，以提升人员网络信息安全认知、大数据中心技术与管理能力。培训内容包括但不限于网络安全意识、网络安全基础知识、安全配置、安全升级、安全政策、Web安全培训、攻防演练培训等内容。每年提供2次网络安全培训服务，并编制《网络安全培训课件》。 （8）网络安全咨询服务 1.服务内容：提供信息安全等级保护咨询、信息安全管理体系咨询、信息安全规划建设咨询、信息安全考核解读咨询等咨询服务，帮助采购人建设全面、有效、合规的信息安全管理体系。每年按需提供，不少于3次网络安全咨询服务，并做好相关服务记录。 （9）应急演练服务 1.服务内容：提供应急演练服务，通过服务规范中心网络与信息安全应急响应工作内容和流程，科学应对网络与信息安全突发事件，提升对黑客入侵等安全事件的监测应急能力，提升对具有社会动员能力系统突发事件的紧急处置能力，缩短系统中断时间，降低业务损失，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，保障信息系统的实体安全、运行安全和数据安全。每年提供1次应急演练服务，并编制《网络安全应急演练报告》。 （10）风险评估服务 1.服务内容：依据GB/T 20984-2022《信息安全技术 信息安全风险评估方法》，对中心的城市桥梁水位监测系统、城市桥梁健康监测系统、城市道路桥梁管理信息系统、城市检查井盖信息化监管平台、城市道路桥梁监控中心应用平台、占用挖掘城市道路信息管理系统进行风险评估。通过风险评估项目的实施，对信息系统的重要资产、资产所面临的威胁、资产存在的脆弱性、已采取的防护措施等进行分析，对所采用的安全控制措施的有效性进行检测，综合分析、判断安全事件发生的概率以及可能造成的损失，判断信息系统面临的安全风险，提出风险管理建议，为系统安全保护措施的改进提供参考依据。每年提供1次风险评估服务，并编制《信息安全风险评估报告》。 （11）渗透测试服务 1.服务内容：参考国际公认的PTES、CPT及GB/T 28448《信息安全技术网络安全等级保护测评要求》、GB/T 36627-2018《信息安全技术网络安全等级保护测

			试评估技术指南》、GB/T 20278-2022《信息安全技术网络脆弱性扫描产品安全技术要求和测试评价方法》，通过使用各类网络黑客攻击技术对网络进行模拟渗透攻击，测试系统、网络、主机和应用服务的安全性和健壮性。通过这一系列渗透测试服务，保障城市桥梁水位监测系统、城市桥梁健康监测系统、城市道路桥梁管理信息系统、城市检查井盖信息化监管平台、城市道路桥梁监控中心应用平台、占用挖掘城市道路信息管理系统的安全、可靠地上线，让安全管理人员直观感知自身业务安全风险现状、提升关键业务系统或设备的安全性和稳定性，并为后续的安全规划提供更客观的依据，全面增强防护技术和策略。整个过程要求借助专业人员的技能与经验，挖掘传统自动化检测工具所无法识别的安全漏洞。测试内容包括敏感信息泄露、任意文件下载、暴力破解、跨站脚本攻击、弱口令、SQL 注入、后台越权等。每月提供 1 次渗透测试服务，并编制《渗透测试报告》。 **（12）应急响应服务** 1.服务内容：根据采购人故障紧急情况，提供远程协助处理、现场技术处理、电话支持服务等。每年按需提供，不少于 3 次应急响应服务，并编制《网络安全应急响应处置报告》。 2.在服务期内供应商应有专门的网络安全保障工程师，提供及时响应服务，保证采购人可以随时得到技术支持服务。如供应商在接到报修电话 2 小时内无法电话解决采购人所提出的保障要求，须在报修 4 小时内派工程师到达采购人指定的现场。 3.如遇网络安全一般风险，供应商必须保证在监测发现 48 小时内配合风险处置完成。如遇严重网络安全风险，须在监测发现 24 小时内提出解决方案和解决时间计划，并在计划时间内解决问题。如遇重大事件服务保障需求，在接到采购人通知后，供应商须在 1 个小时内响应服务保障任务，并落实网络安全保障工作。 **（13）重要时期保障** 1.服务内容：提供春节、国庆、两会、护网行动及其他重点保障时段 24 小时保障人员在中心驻场值守服务。在上述各种重要保障值守任务期间，应按照采购人要求，在任务开始前完成相关系统的全面技术检查，确保系统运行稳定可靠；同时提供任务期间现场技术保障及配合完成相关系统操作、演示材料（文档、视频等）的制作以及汇报演示工作。重要时期保障期间提供不少于 2 名驻场值守人员进行服务。每年按需提供编制《重保服务报告》。

（14）安全巡检服务

1.服务内容：对中心的机房环境、网络设备状态、安全设备状态、应用系统状态和终端设备进行检查与分析，对中心部署在云上系统的安全设备进行巡检，了解当前系统与设备的运行情况，并对发现的安全隐患提供改善建议。每月提供1次安全巡检服务。巡检清单如下：

巡检项目	类型	数量
城市桥梁水位监测系统	业务系统	1套
城市桥梁健康监测系统	业务系统	1套
城市道路桥梁管理信息系统	业务系统	1套
城市检查井盖信息化监管平台	业务系统	1套
城市道路桥梁监控中心应用平台	业务系统	1套
占用挖掘城市道路信息管理系统	业务系统	1套
计算机、手机、打印机	终端设备	按需配置

（15）代码审计服务

1.服务内容：针对本项目中心的城市桥梁水位监测系统、城市桥梁健康监测系统、城市道路桥梁管理信息系统、城市检查井盖信息化监管平台、城市道路桥梁监控中心应用平台、占用挖掘城市道路信息管理系统进行代码审计。每年提供1次代码审计服务。

（16）安全加固服务

1.服务内容：根据采购人相关工作安排不定期进行安全加固服务，针对系统的漏洞扫描、渗透测试及系统网络安全等级保护测评等相关情况，对发现的各种已存在的、潜在的风险点进行整改加固，满足和达到安全要求。每年提供4次安全加固服务，并编制《安全加固报告》。

2.▲为保障安全加固的有效性，进行服务器安全加固时需采用“人工+工具”优化方式实现。加固工具需满足《信息安全技术主机安全加固系统安全技术要求GA/T1393-2017》增强级标准，并通过国家认可的专业机构的检测。（提供第三方机构出具的检验或检测报告复印件，并加盖供应商公章）

3.▲工具支持对操作系统安全基线进行检测、加固、恢复，满足操作系统安全防护基线要求。**（提供功能截图并加盖供应商公章）**

4.▲工具支持应用程序白名单，只有属于白名单列表的可执行程序可以运行，不在列表中的所有可执行程序都不能执行。**（提供功能截图并加盖供应商公章）**

			5.▲工具支持进程保护，可以保护指定进程，如系统进程、应用进程，防止进程被非法终止等操作。**（提供功能截图并加盖供应商公章）** 6.▲工具支持文件的强访问控制权限：可以细化和严格定义用户对文件的访问权限（剥离超级用户权限），也可以结合强访问控制模型定义用户对文件的访问权限。**（提供功能截图并加盖供应商公章）** 7.▲工具支持微隔离策略配置，微隔离支持标签和标签、标签和主机、主机和主机之间的隔离策略配置。**（提供功能截图并加盖供应商公章）** **（17）台账登记服务** 1.服务内容：全面掌握运维范围内的六个信息系统的使用和操作，全面收集信息化系统及相关设备运行现状，建立系统及设备配置资料、网络拓扑结构图及端口分配表，收集系统运行健康指标、正常运行率、故障信息等各类运行数据，建立完备的系统及设备台账、维护服务档案。每年提供1次台账登记服务，根据业务需要，及时对相关设施设备建立台账，并根据实际变换情况，及时更新台账，并编制《台账登记报告》。 **（18）边界防火墙续保升级服务** 1.服务内容:对采购人现有2台USG-FW-2000DP-B边界防火墙进行续保升级，保障网络边界安全防护能力持续有效、系统版本与威胁特征库保持最新、设备运行稳定可靠。升级防火墙系统版本、升级设备特征库，防护最新安全漏洞，保证设备性能、安全能力满足安全需求，具备访问控制、入侵防御、病毒过滤、应用识别、流量统计等功能。 **（19）准入系统服务** 1.服务内容：提供1套准入系统服务，为终端用户接入内网全过程提供一套综合完整的端点安全准入控制解决方案。解决“网络接入不可知、非法外联不可控、违规行为不可管”的网络安全管理问题，减少网络事故。可以针对复杂的网络现状，提供用户多种准入模式混合应用，并根据不同的用户分配不同的网络区域和访问权限。同时，可以对入网请求用户的终端做健康评估，并根据管理员配置的评估策略，对不满足条件的终端进行隔离和提供修复向导，从而确保用户内部网络安全性，实现入网必可信。 **（20）入侵防御系统服务** 1.服务内容：提供入侵防御系统服务，为采购人的网络环境搭建一道主动、实时、高效的安全防御屏障，全方位抵御网络入侵攻击行为。在采购人网络关键节点，对数据进行2-7层的全面检查分析，提供安

			全防护，实时阻断并记录网络流量中的病毒、蠕虫、木马、间谍软件、注入攻击、跨站攻击、DDos 攻击、漏洞扫描、异常协议、网络钓鱼等威胁。有效管理 IM 聊天软件、P2P 下载软件、炒股软件、网络游戏应用、流媒体在线视频应用等，并集成带宽管理、URL 过滤、关键字过滤等，确保中心不出现违规访问境外非法网站。 **（21）网页防篡改防护服务** 1.服务内容：提供网页防篡改防护服务，防止网页被非法篡改、挂黑链、植入恶意代码或替换内容。实时监控服务器网站目录或文件，并可在网站被恶意篡改时通过备份数据恢复被篡改的文件或目录，防止网站被植入非法信息，防止黑客、病毒等对目录中的网页、电子文档、图片等任何类型的文件进行非法篡改和破坏，保障网站正常运行。 **（22）USB 外设管理服务** 1.服务内容：在运维期内提供 USB 外设管理服务，保障终端 USB 外设安全合规使用。对 USB 设备进行管控，支持对外设权限进行管理和外设接入申请管理。
2	★	商务要求	1．服务期： 1.1． 本项目一采两年，合同一年一签，每个服务期为 12 个月。 2.付款方法和条件： 2.1.1 合同签订并生效后，由供应商提出付款申请，采购人在收到供应商等额合格有效发票及付款申请资料后 10 个工作日内向供应商支付合同金额的 50%作为预付款； 2.1.2 采购人根据考核结果分期向供应商支付服务费： 2.1.2.1 供应商月基本服务费=本合同暂定总金额×50%÷12。采购人对供应商每月服务情况进行考核，供应商应将当月服务资料提供给采购人，采购人审核通过且双方完成该月考核后，由供应商提出付款申请，采购人在收到供应商等额合格有效发票资料后 10 个工作日内，根据考核结果向供应商支付该月服务费（供应商月服务费=供应商月基本服务费-月考核扣款）。 2.1.2.2 本项目财政资金下达甲方账户是本项目资金支付的前提，如遇财政资金未到位或其他不可抗力情况，支付将按财政资金到位情况进行顺延。 3.项目实施地点：成都市。 4.履约验收 供应商履行政府采购合同约定义务后，为保证采购质量，采购人将按照《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）和《成都市市级采购项目履约验收实施细则（试行）》（成财规〔2026〕1 号）和其他政府采购相关法律法规要求，以及本项目招标文件、中标供应商的投标文件及承诺、本项目采购合同约定进行验收。若国家及行业现行相关技术规范及要求有强制性规定的，按照强制性规定执行；若采购人要求高于强制性规定的，按采购人要求执行；若非强制性规定和采购人要求不一致的，以有利于采购人为原则。 （1）履约验收主体：成都市城市道路桥梁监管服务中心 （2）履约验收时间：计划于供应商提出验收申请之日起 15 日内组织验收 （3）验收组织方式：自行验收 （4）履约验收程序：一次性验收 （5）技术履约验收内容：按照本项目投标文件中“技术、服务要求”及中标人投标文件进行验收。 （6）商务履约验收内容：按照本项目投标文件中“商务要求”及中标人投标文件进行验收。 （7）履约验收标准：采购人对项目按投标文件要求、中标人投标文件内容、国家、省、行业等相关标准开展项目验收，发现不符合相关要求的采购人将拒绝验收。 5.售后服务 5.1.在运维期间，妥善保管采购人提供的相应文档、技术资料、安装介质等，不得非工作原因，查看、保存、分析系统数据。无论任何原因，服务终止后，不可保留相关数据。 5.2.提供全年 365 天，24 小时/自然日（含周末、国家法定节假日）无间断服务。根据故障紧急情况，提供远程协助处理、现场技术处理、电话支持服务等。 5.3.在运维期内应有专门的软硬件工程师，提供 7×24 时响应服务，保证可以随时得到技术支持服务。 5.4.在运维期内，如在接到报修电话 2 小时内无法电话解决所提出的维修要求，须在报修 4 小时内派工程师到达指定的现场。 5.5.在运维期内，系统一般故障必须保证在报修 48 小时内恢复系统的正常运行。如遇严重故障，须在 24 小时内提出解决方案和解决时间计划，并在计划时间内解决问题。 5.6.在运维期内，如遇重大事件运维保障需求，在接到采购人通知后，须在 1 个小时内响应运维保障任务，并落实系统软硬件运维保障工作，直至接到取消重大事件运维保障的通知止。

5.7.（1）考核采用扣分制，根据供应商的工作情况及运维报告等，每月将扣分情况通报供应商。供应商月度考核扣分不超过5分（含5分），视为合格，不扣减费用，供应商月度考核扣分6-10的，根据总扣分情况进行处罚。处罚金额=（总扣分-5）*200。

（2)供应商月度考核扣分超过10分(不含10分)，根据总扣分情况进行处罚。处罚金额=（总扣分-10）*合同金额的千分之一，一个考核期内扣分超过40分，即视为违约，采购人有权终止合同。

（3）在年度合同履行期间内，采购人根据实际情况，可适当调整工作内容及工作要求，并相应修订考核标准。

序号	考核项目	考核要求	考核标准
1	网络安全相关培训、演练	根据采购人要求定期开展网络安全相关培训、演练	未开展相关培训、演练，每次扣20分；开展的相关培训、演练未达到采购人要求，每次扣10分。
2	定期报告服务	根据采购人要求定期提交服务报告	每季度提交3次网站安全监测报告，1次漏扫报告，每4季度提交不低于2次渗透测试报告。未提交报告的每次扣2分；未按时提交的每次扣1分；报告不规范的，每次扣0.5分。
3	病毒防护服务	根据采购人要求提供终端病毒统一防护	配合采购人部署终端病毒防护软件并定期进行维护，对漏洞、系统进行修复，保证系统安全状态评分90分以上。若系统安全评分低于90分，60—90分每次扣5分，60分以下每次扣10分。
4	网络安全保障 响应服务	服务期间，应尽量避免系统出现安全问题；系统出现安全问题后应及时按照预设	重大安全事故发生时未按时响应或未按规定流程处置，造成严重舆情影响或受到市级以上通报批评、处分的，每发生一次扣40分； 较大安全事故发生时未按

					流程或应急方案进行处置，做好记录；事后应进行专题分析，提交专题报告	时响应或未按规定流程处置，造成较大舆情影响或受到上级主管行政部门通报批评、处分的每有 1 次扣 30 分； 一般安全事故发生时未按时响应，造成负面舆情影响或受到采购人通报批评的，每有 1 次扣 5 分； 系统出现安全问题后，未进行有效专题分析、未提交专题分析报告或未进行有效优化措施的，每有一项/次，扣 2.5 分； 可累计，扣完为止。	
				5	网络安全漏洞管理	根据采购人要求加强网络安全漏洞排查及管理	被上级或网络安全主管部门通报，且被通报内容涉及翻墙行为的，每次扣 20 分；所通报漏洞属于历史重复同类漏洞，每次扣 10 分；通报漏洞类型为 30 日内新增的，每次扣 5 分；通报漏洞类型为 7 日内新增的，每次扣 0.5 分。	
				6	专项保障服务	根据采购人要求进行专项保障	未响应采购人保障需求的，每次扣 10 分；因保障工作不到位，导致严重影响的，视情况扣 1—5 分。	
				7	用户满意度	用户投诉	服务机构和人员在开展工作时需保持良好的态度，提供专业和耐心的技术支持服务。收到各级用户书面投诉的，每次扣 2 分。受到用户书面表扬的每次加 2 分。	
				8	项目管理服务	按照采购人参加项目例会	未经采购人同意，项目经理或技术负责人缺席项目例会。采购人可视供应商	

						违约的严重程度进行处罚。①项目经理按3分/人·天计算； ②技术负责人按2分/人·天计算； 连续3天以上的缺岗，按上述标准的双倍扣分。
			附：信息安全分级			
				信息安全响应时间	信息安全解决时间	信息安全级别
			1	30分钟，3小时内提交故障处理方案	6小时以内	Ⅰ级：会使“特别重要信息系统”遭受“特别严重的系统损失”。产生特别重大的社会影响，也就是波及一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。
			2	30分钟，6小时内提交故障处理方案	12小时以内	Ⅱ级：会使“特别重要信息系统”遭受“严重的系统损失”，或使“重要信息系统”遭受“特别严重的系统损失”。产生重大的社会影响，即波及一个或多个地市的大部分地区，威胁国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害公众利益。
			3	30分钟，12小时内提交故障处理方案	24小时以内	Ⅲ级：会使“特别重要信息系统”遭受“较大的系统损失”或使“重要信息系统”遭受“严重的系统损失”“一般信息系统”遭受“特别严重的系统损失”。产生较大的社会影

						响，指波及一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。
			4	30分钟，24小时内提交故障处理方案	48小时以内	Ⅳ级：会使“特别重要信息系统”遭受“较小的系统损失”或使“重要信息系统”遭受“较大的系统损失”，一般信息系统遭受严重或严重以下级别的系统损失。产生一般的社会影响，是指波及一个地市的部分地区，对国家安全，社会秩序，经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

6.违约条款

本项目合同经双方正式签署后具有法律效力，如果违约，双方应按下列各条承担违约责任：

6.1.供应商未能按合同规定的时间完成任务的，采购人有权根据延迟完工时间按本合同总金额的0.5%/日要求供应商承担违约金责任，最高不超过合同总额的5%。

6.2. 如果供应商提供的服务或提交的服务成果与采购合同规定不符、无法满足承诺的技术要求，供应商应当及时查找问题原因，采取相应整改措施，以达到采购合同规定,采购人有权按照合同总金额的10%要求供应商承担违约责任且应赔偿由此给采购人造成的全部损失。若供应商整改后，仍未达到本项目合同要求，采购人有权解除本合同，供应商已收取的服务费应当全部退还。

6.3.采购人未按期付款的，供应商有权根据延付时间按合同欠款的0.1‰/日要求采购人承担违约金责任，最高不超过合同总额的5%。

6.4.若因不可抗力等因素造成无法完成项目内容，由双方共同承担风险。

6.5.供应商有下列违约情形之一的，采购人有权

			解除合同，要求供应商退还全部费用，并要求供应商按照本合同总金额的10%承担违约责任： （1）供应商除不可抗力原因未按照合同规定的时间完成工作，延迟超过10个工作日，经采购人催告后成果仍未完工的； （2）供应商派驻本项目的项目经理和技术负责人在项目验收前未经采购人同意更换的； （3）供应商违反《廉政合同》的约定的。 7.保密要求 中标供应商必须对工程技术文件以及由采购人提供的所有内部资料、技术文档和信息予以保密。未经采购人书面许可，中标供应商不得以任何形式向第三方透露本期项目的任何内容。 中标供应商中标（成交）后须与采购人签订保密协议，并在项目合同签订时一并提供给采购人。

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
无			

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	本项目一采两年，合同一年一签，每个服务期为12个月。
2		服务地点	成都市
3		验收、交付标准和方法	供应商履行政府采购合同约定义务后，为保证采购质量，采购人将按照《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）和《成都市市级采购项目履约验收

			实施细则（试行）》（成财规〔2026〕1号）和其他政府采购相关法律法规要求，以及本项目招标文件、中标供应商的投标文件及承诺、本项目采购合同约定进行验收。若国家及行业现行相关技术规范及要求有强制性规定的，按照强制性规定执行；若采购人要求高于强制性规定的，按采购人要求执行；若非强制性规定和采购人要求不一致的，以有利于采购人为原则。 （1）履约验收主体：成都市城市道路桥梁监管服务中心 （2）履约验收时间：计划于供应商提出验收申请之日起15日内组织验收 （3）验收组织方式：自行验收 （4）履约验收程序：一次性验收 （5）技术履约验收内容：按照本项目投标文件中“技术、服务要求”及中标人投标文件进行验收。 （6）商务履约验收内容：按照本项目投标文件中“商务要求”及中标人投标文件进行验收。 （7）履约验收标准：采购人对项目按投标文件要求、中标人投标文件内容、国家、省、行业等相关标准开展项目验收，发现不符合相关

			要求的采购人将拒绝验收。
4		支付方式	分期付款
5		付款进度安排	1、预付款，详见商务要求 2.付款方法和条件，达到付款条件起 10 个工作日内，支付合同总金额的 50.0% 2、进度款，详见商务要求 2.付款方法和条件，达到付款条件起 10 个工作日内，支付合同总金额的 50.0%
6		违约责任与解决争议的方法	一、违约条款：本项目合同经双方正式签署后具有法律效力，如果违约，双方应按下列各条承担违约责任： 6.1.供应商未能按合同规定的时间完成任务的，采购人有权根据延迟完工时间按本合同总金额的 0.5%/日要求供应商承担违约金责任，最高不超过合同总额的 5%。 6.2. 如果供应商提供的服务或提交的服务成果与采购合同规定不符、无法满足承诺的技术要求，供应商应当及时查找问题原因，采取相应整改措施，以达到采购合同规定，采购人有权按照合同总金额的 10%要求供应商承担违约责任且应赔偿由此给采购人造成的全部损失。若供应商整改后，仍未达到本项目合同要求，采购人有权解除本合同，

			供应商已收取的服务费应当全部退还。6.3.采购人未按期付款的，供应商有权根据延付时间按合同欠款的0.1‰/日要求采购人承担违约金责任，最高不超过合同总额的5%。 6.4.若因不可抗力等因素造成无法完成项目内容，由双方共同承担风险。 6.5.供应商有下列违约情形之一的，采购人有权解除合同，要求供应商退还全部费用，并要求供应商按照本合同总金额的10%承担违约责任： （1）供应商除不可抗力原因未按照合同规定的时间完成工作，延迟超过10个工作日，经采购人催告后成果仍未完工的； （2）供应商派驻本项目的项目经理和技术负责人在项目验收前未经采购人同意更换的； （3）供应商违反《廉政合同》的约定的。 二、合同争议解决方式 合同双方约定，如出现合同纠纷，由双方协调解决，协商不成的将依法向成都市锦江区人民法院提起法律诉讼。

3.4.其他要求

采购包1：

特别说明：因系统模板固化原因，本项目商务要求以本章3.2技术要求中序号2“商务要求”为准，原3.3.2.商务要求无须响应。