第六章　采购项目技术、服务内容及其他商务要求

一、项目概况

根据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）、《国家政务信息化项目建设管理办法》等国家相关法规、技术标准和规范的要求，成都市中级人民法院对重要信息系统开展商用密码应用安全性评估工作。

依据《政务信息系统密码应用与安全性评估工作指南》（2020版）、《GB/T 39786-2021信息安全技术 信息系统密码应用基本要求》标准的要求，对政务信息系统现状和密码应用需求进行分析，协助制定密码应用方案实施密码应用改造，开展商用密码应用安全性评估工作，切实提高重要信息系统的综合防护能力和安全保障水平，保障政务信息系统安全稳定运行。

二、项目服务内容

（一）依据标准和规范

1.《中华人民共和国网络安全法》

2.《中华人民共和国密码法》

3.《商用密码管理条例》（国务院第273号令）

4.《国家政务信息化项目建设管理办法》（国办发[2019]57号）

5.《信息安全技术 信息系统密码应用基本要求 GB/T39786-2021》

6.《政务信息系统密码应用与安全性评估工作指南（2020版）》

7.《信息系统密码应用测评要求》GM/T 0115-2021

8.《信息系统密码应用测评过程指南》GM/T 0116-2021

9.《信息系统密码应用高风险判定指引》

10.《商用密码应用安全性评估量化评估规则》

（二）技术服务要求

序号	名称	技术服务要求参数
1	**总体要求**	1.1 供应商依据《政务信息系统密码应用与安全性评估工作指南》（2020版）、《GB/T39786-2021信息安全技术信息系统密码应用基本要求》等标准，结合信息系统等保定级情况，明确密码应用需求，协助采购人编制密码应用方案；对密码应用方案进行审核，出具密码应用方案评审报告，协助采购人到密码局进行

		方案审批备案；依据评估通过的密码应用方案，协助采购人从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等层面采用密码技术措施，并采取有效的安全管理措施，对政务信息系统进行保护；政务信息系统改造完成后，对政务信息系统进行密码应用安全性评估，出具信息系统密码应用安全性评估报告。
2	**密码应用方案评审服务**	2.1 明确密码应用需求。协助采购人和建设单位依据《政务信息系统密码应用与安全性评估工作指南》（2020 版）、《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》等标准对重要信息系统面临的安全风险和风险控制需求进行分析，根据各信息系统的网络安全保护等级，协助采购人设计编制《政务信息系统密码应用方案》。
		2.2 编制政务信息系统密码应用方案应遵循以下原则： **总体性原则**。密码应用方案应做好顶层设计，明确应用需求和预期目标，与政务信息系统整体网络安全保护等级相结合，通过体系化的设计形成涵盖技术、管理、实施保障的整体方案，有效落实密码应用相关要求。 **完备性原则**。密码应用方案需紧密结合信息系统业务应用实际与安全保护等级，站在整体角度，通过自上而下的体系化设计，综合考虑物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等层面密码应用需求。 **适用性原则**。依据《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》，通过体系化、分层次的设计，形成包括密码支撑总体架构、密码基础设施建设部署、密钥管理体系构建、密码产品部署及管理等的总体方案。
		2.3 依据《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》、《政务信息系统密码应用与安全性评估工作指南》（2020 版）标准要求，成交供应商对采购人编制的《政务信息系统密码应用方案》进行方案评审，需分析密码应用方案是否对信息系统中需要保护的资产、数据提供了体系化、完备、适用、合规、有效的密码保障措施。对不适用指标及其论证材料进行评估，并审核是否存在可满足安全要求并达到等效控制的其他替代性风险控制措施。提交符合密码局格式要求的《密码应用方案评审报告》。
		2.4 依照密码局评审备案工作相关要求，按照格式协助采购人提交评审材料到密码局审批；审批结果作为履行服务证明文件。
3	**安全建设咨询服务**	3.1 依据评审通过的密码应用方案，按照《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》、《政务信息系统密码应用与安全性评估工作指南》（2020 版）等标准，指导采购人的项目承建方对被测信息系统存在的问题进行整改，提供整改咨询服务，协助完成被测信息系统的安全整改，完善安全防护措施，规划整体安全架构，完善安全管理相关制度，直至符合对应级别密码保护的要求。
4	**商用密码应**	4.1 依据《GB/T39786-2021 信息安全技术信息系统密码应用基本

	用安全性评估服务	要求》标准，对被测信息系统进行密码应用安全性评估，按照《商用密码应用安全性评估报告模板（2021 年版）》格式要求出具《密码应用安全性评估报告》，协助采购人提交到密码局完成备案工作。
		4.2 主要评估内容如下： （1）物理和环境安全应包括：身份鉴别、电子门禁记录数据完整性、视频记录数据完整性、硬件密码模块实现等工作单元。 （2）网络和通信安全应包括：身份鉴别、访问控制信息完整性、通信数据完整性、通信数据机密性、集中管理通道安全、硬件密码模块实现等工作单元。 （3）设备和计算安全应包括：身份鉴别、远程管理身份鉴别信息机密性、访问控制信息完整性、敏感标记完整性、重要程序文件完整性、日志记录完整性、硬件密码模块实现等工作单元。 （4）应用和数据安全应包括身份鉴别、访问控制、数据传输安全、数据存储安全、日志记录完整性、重要应用程序的加载和卸载、抗抵赖、硬件密码模块实现等工作单元。 （5）安全管理应包括管理制度、人员管理、建设运行、应急处置等工作单元。
5	**实施要求**	5.1 评估实施原则 （1）保密原则：对评估的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购人的行为。 （2）标准性原则：评估方案的设计与实施应依据国家相关标准进行。 （3）规范性原则：供应商工作中产生的过程文档，应具有很好的规范性，便于对项目进行跟踪和控制。 （4）可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。 （5）最小影响原则：评估工作应尽可能小的影响系统和网络，并在可控范围内；评估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。 （6）整体性原则：评估的范围和内容应当整体全面，包括密码应用与安全性评估等相关要求涉及的各个层面。
		5.2 专用工具要求 本项目涉及测试所需的工具由供应商负责提供，包括但不限于以下工具： 供应商具备专用密码应用安全性评估工具，包含国密协议分析工具、国外算法检测工具、签名验签工具、CA 管理工具、随机数检测工具等。
		5.3 安全保密管理 提供保密管理方案，对测评人员进行资格审查，并制定人员奖惩措施。为做好全过程的安全保密工作，在商用密码应用安全性评估前、中、后三个阶段都要做好安全保密工作。 5.3.1 评估前

		（1）对实施人员要进行安全保密教育，制定安全保密措施； (2）签订安全保密协议。 5.3.2 评估中 （1）对被评估单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理； （2）评估工具应经过严格测试和检验，确保不对被评估系统造成损失，工作结束后不驻留任何程序； （3）对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围； （4）对评估设备、介质进行严格的保密管理； （5）工作过程中对人员要实施集中管理； （6）对进场人员要求遵守被测单位的相关管理规定。 5.3.3 评估后 （1）认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏； （2）现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序； （3)在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感信息。
		5.4 风险规避要求 项目开展工作涉及到单位重要信息系统和数据，在评估过程中必须加强安全保密管理与风险控制。 指定项目经理为专人负责商用密码应用安全性评估过程中的安全保密管理工作，对评估活动、评估人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。 项目组人员对评估工作中可能出现的安全风险点，按照检测对象制定评估方法，根据被评估对象的不同采取相应的风险控制手段。包括但不限于以下方法： （1）操作的申请和监护 在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。 （2）操作时间控制 对评估直接影响系统工作时，尽可能避开敏感时期。 （3）人员与数据管理 必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。评估与被评估单位之间应签署保密协议，按国家有关要求做好保密工作。 （4）制定应急预案 根据评估范围界定的系统情况，在实施前制定应急预案。 （5）关键业务系统风险控制 对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用评估工具，采用访谈、测评和简单测试的方式进行。

		（6）数据备份与恢复 对业务系统和数据库主机，应对其上数据进行备份，防止评估过程中对设备与主机的损伤影响业务系统的正常运行。 （7）厂商协作 项目建设或使用管理单位要协调被测信息系统软件开发商或运维单位提供测评所需基本信息，在评估之前，由三方共同分析评估对业务可能造成的风险，分析可能存在的问题，制定应急处置方案，协助被测信息系统建设单位及时处置。
6	**综合要求**	6.1 供应商应详细描述本次商用密码应用安全性评估整体实施方案，包括项目概述、密评工作方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。
		6.2 供应商应详细描述测评人员的组成、资质及各自职责的划分。
		6.3 商用密码应用安全性评估需要的运行环境（如场地、网络环境等）由采购人提供，供应商应详细描述需要的运行环境的具体要求。
		6.4进度保证。有工作流程，有计划、按步骤地开展测评工作，保证测评活动的每个环节都得到有效的控制。若进度计划目标延迟，应有相应的后续计划承诺及惩罚措施。
		6.5项目质量管理。有项目质量控制及保证措施，供应商要提出质量控制及保证措施方案并提供承诺函。
		6.6项目风险管理。结合项目建设内容，提出项目风险规避措施，制定项目风险管理方案。
		6.7安全培训方案。供应商制定安全培训方案及计划。
		6.8 售后服务承诺：供应商提供完整售后服务措施、技术支持、服务承诺、售后服务保障体系等。

三、商务要求（实质性要求）

1.工期时间：签订合同之日起1年，若服务的目标项目未验收，则合同服务时间顺延至服务的所有目标项目终验完成。

2.实施要求：①合同签订后，以合同时间节点按照年度开展服务，按照每个项目成交单价据实结算具体服务费用，全年上限预算48万，超出预算部分双方均可不履行合同。②根据采购人每个项目的报审时间，于报审前10个日历日内完成信息系统的密码应用方案评审工作（方案编制、修改和整改等周期不含在内，评审期间提供咨询和技术支持服务，确保评审通过）；③根据采购人每个项目的结项时间，于终验前60个日历日内完成信息系统的密码应用安全性评估工作（至少应包含初测1次，复测2次）。④合同期内和项目实施周期内，提供商用密码应用安全建设咨询和技术支持服务，若涉及与承建方协调的应支持驻场开展服务。

3.付款方式：

序号	投资总额（万元）	单项服务费（万元）
1	经评估可达到等保二级要求的网络安全标准的信息系统项目（不限预算额度）	上限为 6 万元，实际以中标价为准
2	经评估可达到等保三级要求的网络安全标准的信息系统项目（预算额度≤400）	上限为 8 万元，实际以中标价为准
3	经评估可达到等保三级要求的网络安全标准的信息系统项目（预算额度＞400 且≤700）	上限为 10 万元，实际以中标价为准
4	经评估可达到等保三级要求的网络安全标准的信息系统项目（预算额度＞700）	上限为 12 万元，实际以中标价为准

（1）乙方提供咨询和评审服务，所服务的甲方目标项目通过密码局评审获得批复后，甲方支付目标项目投资总额对应单项服务费的 10%；

（2）乙方提供咨询和协助服务，所服务的甲方目标项目通过采购完成确定承建商后，甲方支付目标项目投资总额对应单项服务费的 70%；

（3）乙方提供咨询和评估服务，所服务的甲方目标项目完成评估测评并通过终验后，甲方支付目标项目投资总额对应单项服务费的 20%；

4.报价要求：①供应商的报价应包含为完成本采购文件提出的要求对信息系统进行密码应用方案评审和密码应用安全性评估，分别出具密码应用方案评审报告和密码应用安全性评估报告，并提供系统安全建设咨询服务以及售后服务等全部相关工作所有可能发生的费用，即所需的一切人工、物耗、工具、设备、用水、用电、保险和调研、咨询、测试、验收、评审、培训、税金等所有可能发生的一切费用，即投标总报价为“交钥匙”价。对在合同实施过程中可能发生的其他费用（如：增加耗材、材料涨价、人工、运输成本增加等因素），采购人概不负责。本文件所要求内容应视为保证项目完成所需最低要求，如有遗漏，供应商应予补充。否则，将不予以付款。②对本文件未列明，而供应商认为必需的费用也需列入磋商报价。在合同实施时，采购人将不予支付成交供应商没有列入的项目费用，并认为此项目的费用已包含在磋商总报价中。

5.验收要求：

（1）主体：采购人组织

（2）时间：每个服务的目标项目终验同时即视同验收单项评估服务

（3）方式：采购人自行组织验收

（4）程序：一次性验收

（5）内容和验收标准：

本项目参照《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）的相关规定、采购文件的质量要求和成交供应商的响应文件应答及承诺进行验收。

6.质量要求：

6.1本次采购项目的服务必须完全满足中华人民共和国国家质量标准及现行规范要求，供应商应根据企业实际能力在响应文件中对项目质量予以承诺，成交供应商后在合同中加以确认。

6.2供应商在采购过程及成交供应商后，发生侵犯专利权的行为时，其侵权责任与采购人无关，应由供应商承担相应的责任，并不得影响采购人的利益。

6.3当国家关于密码应用安全性评估方面的政策或技术标准发生变化，须按照新的政策和技术标准执行，所产生的评估费用由成交供应商承担。

7.违约责任：成交供应商在评估过程中如故意歪曲事实、未经采购人确认擅自进行高风险的操作，经采购人三次书面通知无法改进的，采购人有权解除合同，并追究成交供应商责任，本合同因此被解除的，成交供应商承担的违约金为本项目金额的10%。

8.其他要求：

8.1严禁借用资质，发现借用或假冒资质投标的，采购人有权随时取消或终止合同，并按照有关法律法规规定处理。

8.2如成交供应商发生兼并、重组等，由新组建的公司按响应文件承担相应义务和责任

8.3 本项目的合同年度周期结束时，若评审、咨询和评估的目标项目已确立项且正在实施中，服务工作时间顺延，仍在本项合同中继续执行，费用一经立项即确认本合同中支付，不产生任何额外费用。