## 一、项目基本情况：

为认真贯彻落实《中华人民共和国网络安全法》、《中华人民共和国密码法》、《计算机信息系统安全保护条例》、《国家政务信息化项目建设管理办法》等法律法规精神，按照《信息安全等级保护管理办法》、《商用密码应用安全性评估管理办法（试行）》等有关要求，进一步增强网络安全防护能力，确保网络安全稳定运行，防止因网络安全事件引发安全事故，全面提升省人大机关信息系统整体安全防范能力，省人大常委会办公厅计划通过购买服务方式确定一名比选申请人，对省人大机关信息系统进行网络安全等级保护测评和商用密码应用安全性评估，并协助采购人完成相应备案，服务期限三年，即2025年至2027年。

（一）测评内容。省人大机关信息系统经整合，有三套应用系统，均已备案，具体情况如下：

1.四川省人大内部应用系统部署在省人大机关机房内，属于等保二级；

2.四川省人大对外服务应用系统部署在省人大机关机房内，属于等保三级；

3.四川省“数字人大”融合平台部署在政务云上，属于等保三级。

## ★二、测评范围：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 系统名称 | 安全保护等级 | 等保测评年度 | 商用密码应用安全性评估年度 |
| 1 | 四川省人大内部应用系统 | 二级 | 2025年、2027年 |  |
| 2 | 四川省人大对外服务应用系统 | 三级 | 2025年、2026年、2027年 | 2025年、2026年、2027年 |
| 3 | 四川省“数字人大”融合平台 | 三级 | 2025年、2026年、2027年 | 2025年、2026年、2027年 |

## 三、技术标准和规范：

《中华人民共和国计算机信息系统安全保护条例》（国务院令147号）

《信息安全等级保护管理办法》公通字〔2007〕43号

《计算机信息系统·安全保护等级划分准则》（GB17859-1999）

《信息安全技术·网络安全等级保护定级指南》（GB/T22240-2020）

《信息安全技术·网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术·网络安全等级保护测评要求》（GB/T28448-2019）

《信息安全技术·网络安全等级保护测评过程指南》（GB/T28449-2018）

《信息安全技术·信息安全风险评估方法》（GB/T20984-2022）

《中华人民共和国密码法》

《商用密码管理条例》

《信息系统密码应用基本要求》（GM/T0054）

《信息系统密码测评要求（试行）》

《商用密码应用安全性评估测评过程指南（试行）》

《商用密码应用安全性评估测评作业指导书（试行）》

《商用密码应用安全性评估测评工作使用需求说明（试行）》

相关国家标准和密码行业标准。  
注：**以上标准若有更新，以最新标准文件中的规定执行。**

## ★四、服务内容及要求：

**（一）等级保护测评服务**

1. 测评范围。

根据等级保护测评的工作要求，测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度，以及云计算安全、移动互联安全、物联网安全、工控制系统安全等方面。

2.测评服务内容

2.1协助业主单位进行信息系统的信息安全等级定级和备案工作。

2.2差距测评，至少包括安全技术测评和安全管理测评，并形成问题汇总及整改意见报告。

2.2.1安全技术测评。包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的安全测评。

2.2.1.1安全物理环境

安全物理环境针对物理机房提出了安全控制要求，主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

2.2.1.2安全通信网络

安全通信网络针对网络架构和通信传输提岀安全控制要求。主要对象为广域网、城域网、局域网的通信传输以及网络架构等；涉及的安全控制点包括网络架构、通信传输和可信验证。

2.2.1.3安全区域边界

安全区域边界针对网络边界提出了安全控制要求，主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、邮件防范、安全审计和可信验证。

2.2.1.4安全计算环境

安全计算环境针对边界内部提出了安全控制要求，主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护。

2.2.1.5安全管理中心

安全管理中心针对整个系统提出了安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

2.2.2安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。

2.2.2.1安全管理制度

安全管理制度测评是对信息系统的安全策略、安全管理制度体系和制度内容、制定和发布流程、评审和修订机制等情况进行测评。

2.2.2.2安全管理机构

安全管理机构测评是对信息系统的安全管理组织和岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

2.2.2.3安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗、人员考核、安全意识教育和培训，以及外部人员访问管理等情况进行测评。

2.2.2.4安全建设管理

系统建设管理测评是对信息系统建设过程中的系统定级、安全方案设计、产品采购和使用、自主软件开发、外包软件开发、工程实施、测试验收、系统交付、系统定级备案、等级测评、安全比选申请人选择等情况进行测评。

2.2.2.5安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、资产管理、介质管理、设备管理、漏洞和风险管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等情况进行测评。

2.2.3形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题及整改意见。

2.3协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

2.4等级测评，至少包括：按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。

**（二）商用密码应用安全性评估**

服务总体目标：严格按照《中华人民共和国密码法》、《商用密码管理条例》、GM/T0054《信息系统密码应用基本要求》、《信息系统密码测评要求（试行）》、《商用密码应用安全性评估测评过程指南（试行）》、《商用密码应用安全性评估测评作业指导书（试行）》、《商用密码应用安全性评估测评工作使用需求说明（试行）》和相关国家标准和密码行业标准，高质量完成信息系统的密码应用安全性评估工作。

被评估对象的商用密码应用安全性评估服务内容如下:

1．密码应用总体要求测评

1.1密码算法合规性测评

系统中使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。

1.2密码技术合规性测评

系统中使用的密码技术是否遵循密码相关国家标准和行业标准。

1.3密码产品合规性测评

系统中使用的密码产品与密码模块是否通过国家密码管理部门核准。

1.4密码服务合规性测评

系统中使用的密码服务是否通过国家密码管理部门许可。

2．密码应用技术要求测评

2.1 物理和环境安全测评

2.1.1 是否使用密码技术的真实性服务来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性；

2.1.2 是否使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性；

2.1.3 是否使用密码技术的完整性服务来保证视频监控音像记录的完整性。

2.2 网络和通信安全测评

2.2.1是否在通信前基于密码技术对通信双方进行身份认证,使用密码技术的机密性和真实性服务来实现防截获、防假冒和防重用,保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；

2.2.2是否使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性；

2.2.3 是否采用密码技术保证通信过程中数据的完整性；

2.2.4 是否采用密码技术保证通信过程中敏感信息字段或整个报文的机密性；

2.2.5 是否釆用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。

2.3 设备和计算安全测评

2.3.1 是否使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

2.3.2 在远程管理时，是否使用密码技术的机密性服务来实现鉴别信息的防窃听；

2.3.3 是否使用密码技术的完整性服务来保证系统资源访问控制信息的完整性；

2.3.4 是否使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性；

2.3.5 是否采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护；

2.3.6 是否使用密码技术的完整性服务来对日志记录进行完整性保护。

2.4 应用和数据安全测评

2.4.1 是否使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；

2.4.2 是否使用密码技术的完整性服务来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；

2.4.3 是否采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

2.4.4 是否采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

2.4.5 是否采用密码技术保证重要数据在传输过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；

2.4.6 是否采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；

2.4.7 是否使用密码技术的完整性服务来实现对日志记录完整性的保护；

2.4.8 是否采用密码技术对重要应用程序的加载和卸载进行安全控制。

**3．密钥管理测评**

对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程进行测评：

3.1 密钥生成测评

密钥生成使用的随机数是否符合《GM/T 0005-2012 随机性监测规范》的要求，密钥是否在符合《GM/T 0028-2014 密码模块安全技术要求》的密码模块中产生；密钥是否在密码模块内部产生，不得以明文方式出现在密码模块之外；是否具备检查和剔除弱密钥的能力。

3.2 密钥存储测评

密钥是否加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥是否存储在符合《GM/T 0028-2014 密码模块安全技术要求》的二级及以上密码模块中。

3.3 密钥分发测评

密钥分发是否采取身份鉴别、数据完整性、数据机密性等安全措施，是否能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

3.4 密钥导入与导出测评

是否采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

3.5 密钥使用测评

密钥是否明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前是否对其进行验证；是否有安全措施防止密钥的泄露和替换；密钥泄露时，是否停止使用，并启动相应的应急处理和响应措施。是否按照密钥更换周期要求更换密钥；是否采取有效的安全措施，保证密钥更换时的安全性。

3.6 密钥备份与恢复测评

是否制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复是否进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

3.7 密钥归档测评

是否采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档是否进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥是否进行数据备份，并采用有效的安全保护措施。

3.8 密钥销毁测评

是否具有在紧急情况下销毁密钥的措施。

**4．安全管理测评**

4.1 制度测评

4.1.1 是否制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度是否包括密码建设、运维、人员、设备、密钥等密码管理相关内容；

4.1.2 是否定期对密码安全管理制度的合理性和适用性进行论证和审定,对存在不足或需要改进的安全管理制度进行修订；

4.1.3 是否明确相关管理制度发布流程。

4.2 人员测评

4.2.1 是否了解并遵守密码相关法律法规；

4.2.2 是否能够正确使用商用密码产品；

4.2.3 是否根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用；

4.2.4 是否建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度；

4.2.5 是否建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训；

4.2.6 是否建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

4.3 实施测评

4.3.1 规划测评

系统规划阶段，责任单位是否依据密码相关标准，制定密码应用方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。

4.3.2 建设测评

是否按照国家相关标准，制定实施方案，方案内容是否包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等；是否选用的经国家密码管理部门核准的密码产品、许可的密码服务。

4.3.3 运行测评

系统投入运行前，是否经密码测评机构进行安全性评估，评估通过方可投入正式运行；信息系统投入运行后，责任单位每年是否委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，是否停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。

4.4 应急测评

4.4.1 是否制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置；

4.4.2 事件发生后，是否及时向信息系统的上级主管部门进行报告；

4.4.3 事件处置完成后，是否及时向同级的密码主管部门报告事件发生情况及处置情况。

**（三）测评原则**

在项目实施过程中，必须遵守以下技术原则：

1.保密原则：对测评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方的行为，否则采购方有权追究中选对象的责任。

2.标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

3.规范性原则：中选对象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，测评出具的报告须符合公安部颁布的《信息系统安全等级测评报告模板》。

4.可控性原则：等保测评服务的进度要按照比选文件的要求，保证采购方对于测评工作的可控性。

5.整体性原则：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。

6.安全性原则：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得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。

7.测评机构资质及人员要求：

（1）从事信息系统检测评估相关工作人员无违法记录。

（2）工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。

（3）测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。

（4）按照采购人要求开展测评工作，听从采购人安排，合理安排调度人员，满足采购人实际工作需求。

**（四）文档资料要求**

在本项目完成后，中选对象须提供以下文档资料：

1.《信息系统安全问题汇总及整改建议》

2.《网络安全等级保护等级测评报告》（至少2份）及过程资料

3.《商用密码应用安全性评估基本情况调查表》

4.《商用密码应用安全性评估基本情况调查表》

5.《商用密码应用安全性评估报告》（至少2份）及过程资料

6.采购人要求的其他相关内容。

**（五）保密要求**

1.比选申请人应当严格执行有关管理规范和技术标准，开展客观、公正、安全的测评服务，应制定保证其公正性、客观性、诚实性的制度、程序或行为规范，并向采购人和社会作出公正性声明或承诺，接受行为监督。

2.比选申请人应重视安全保密工作，指派安全保密工作的责任人。比选申请人应依据保密管理制度，定期对工作人员进行保密教育，比选申请人和测评人员应当保守在测评活动中知悉的国家秘密、商业秘密、敏感信息和个人隐私等，应制定保密管理制度，明确保密范围、各岗位的保密职责和保密要求。

3.比选申请人应采取技术和管理措施来确保等保测评相关信息的安全、保密和可控，这些信息包括但不限于：

（1）被测单位提供的资料；

（2）等保测评活动生成的数据和记录；

（3）依据上述信息做出的分析与专业判断。

4.比选申请人应着重对被测单位的技术资料、测评数据、评估数据、测评报告等信息进行保护。对上述信息资料应专门保管，对数据信息存储和借阅应严格控制。

5.比选申请人应借助有效的技术手段，确保等保测评相关信息的整个数据生命周期的安全和保密，如数据加密存储、传输、处理方式，保证数据的安全。同时防止存储测评数据信息的计算机非法外联、非受控移动存储设备接入、重要信息的互联网传输等问题的发生。

6.比选申请人应严格执行被测单位的保密要求，比选申请人以及测评人员均需和被测单位签订保密协议。在项目实施过程中，采购人有权根据项目进展情况，对相关要求进行调整。

## ★五、项目相关商务要求：

★（一）服务地点和期限

服务地点：成都市中南大街1号；

服务期限：服务期三年（2025年、2026年、2027年）。

★（二）付款方式

每年度，采购人收到比选申请人出具的纸质版盖章的《网络安全等级保护等级测评报告》和《商用密码应用安全性评估报告》后，采购人组织人员对比选申请人的测评和评估服务进行验收，在验收合格且采购人资金到位后15个工作日内，一次性支付年度合同价款的100%。

（三）验收办法

本项目完成测评任务并出具相关测评报告后，采购人将在10日内组织验收，其余事项参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）的要求执行。

（四）方案编制要求

比选申请人应针对本项目制定测评服务方案，至少包含1.实施计划；2.测评实施流程；3.测评原则；4.测评指标；5.测评标准及规范；6.测评方法；7.质量保障措施；8.测评风险及规避对策；9.项目组织与管理；10.人员安排及分工等内容。