四川省生态环境信息安全等级保护测评服务项目技术方案

1、总体需求

为了保障四川省环境工程专业职称评审管理信息系统、四川省环境信息化三级统筹建设基础支撑系统（4A 系统）、四川省环境保护厅公众门户网站系统、四川省生态环境监测业务管理系统、四川省机动车排污监控信息系统（二期）、国控污染源自动监控系统安全、稳定、可靠、高效的运行，按照国家网络安全等级保护 2.0 系列标准要求，需要对其进行安全等级保护三级测评。

测评内容包括：信息系统技术安全性测评及信息系统管理安全性测评。信息系统技术安全性测评包括但不限于：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；信息系统管理安全测评包括但不限于：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理；安全漏洞扫描包括但不限于：应用系统漏洞扫描、应用服务器漏洞扫描、数据库服务器漏洞扫描。通过测评，对照相应安全等级保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，制订出整改措施，出具测评报告，并按照公安部制定的要求完成信息系统安全等级保护定级和备案工作。具体内容包括：

（1）按照国家等级保护相关标准要求，协助被测评单位完成被测信息系统在当地公安机关的网络安全等级保护定级和备案工作。

（2）对被测评单位被测信息系统的安全物理环境、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、安全运维管理共 10 个层面通过访谈、检查、测评等方法进行初测评，找出差距、安全漏洞和隐患并分析其风险，制订出整改建议报告。

（3）按照国家网络安全等级保护 2.0 系列标准，以及初测评的整改意见协助被测评单位完成被测信息系统技术方面的安全修复、系统加固等工作。

（4）对经过整改后的信息系统进行回归测评，正式形成《信息系统安全等级保护测评报告》，确保已定级系统达到网络安全等级保护 2.0 的相关要求，通过公安机关的审核认可并提供证明材料。

2、服务内容及要求

按照国家网络安全等级保护 2.0 系列标准要求，对 6 个信息系统进行安全等级保护三级测评。

（1）信息系统技术安全测评

1) 安全物理环境测评

安全物理环境测评应当包含：物理位置选择、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、电磁防护等方面。

2) 安全通信网络测评

安全通信网络测评应当包含：网络架构、通信传输、可信验证等方面。

3) 安全区域边界测评

安全区域边界测评应当包含：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面。

4) 安全计算环境测评

安全计算环境测评应当包含：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、个人信息保护等方面。

5) 安全管理中心测评

安全管理中心测评应当包含：安全管理中心测评：系统管理、审计管理、安全管理、集中管控等方面。

6) 安全扩展要求

按照所测评系统的具体情况选用云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求。

（2）信息系统管理安全测评

1) 安全管理制度测评

安全管理制度测评应当包含：安全策略、管理制度、制定和发布、评审和修订等方面。

2)安全管理机构测评

安全管理机构测评应当包含：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等方面。

3)安全管理人员测评

安全管理人员测评应当包含：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等方面。

4)安全建设管理测评

安全建设管理测评应当包含：系统定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面。

5)安全运维管理测评

安全运维管理测评应当包含：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、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、外包运维管理等方面。

（3）验证测试要求

按照等级保护测评要求，测评过程中应配备必要的工具、仪器/设备对信息系统进行验证测试，采用的测评工具的生产商应为正规厂商，具有一定的研发和服务能力，能够对产品进行持续更新并提供质量和安全保障。

1)渗透测试

验证安全策略正确性；保证用户登录窗体身份验证的安全性；非授权用户不能浏览到未授权内容；不存在跨站点脚本攻击漏洞；脚本不存在SQL、Cookie注入漏洞；安全的处理异常，没有出错页面泄露系统信息；应用和系统漏洞及其他，并提出整改建议。验证内容包括（但不限于）以下几个方面：

注入	失效的身份认证
敏感信息泄露	XML外部实体（XXE）
失效的访问控制	安全配置错误
跨站脚本（XSS）	不安全的反序列化
使用含有已知漏洞的组件	不足的日志记录和监控

2) 漏洞扫描

据相关标准、规范要求对重要信息系统的安全漏洞进行测评，安全漏洞扫描包括但不限于：应用系统漏洞扫描、应用服务器漏洞扫描、数据库服务器漏洞扫描。分析总结系统中存在的主要安全漏洞，指出系统中可能被利用的安全漏洞、系统配置错误等缺陷以及相应的安全加固意见、建议。

3) 风险分析和评价

依据信息安全技术、信息安全风险评估规范，针对被测系统采用风险分析方法，分析信息系统测评结果中存在的安全问题可能对信息系统安全造成的影响，并给出发现的安全问题以及风险分析及评价情况。

（四）实施和保障要求

1）项目进度要求

本项目测评实施要求同步实施、重点先行、阶段性成果展现相结合。

具体实现进度要求如下：

本次信息系统安全等级保护测评服务工作分为：定级、备案、测评准备、方案编制、现场测评、问题整改、回归测评、报告编制等几个阶段。

①第一阶段：

组建项目组，制定信息安全等级保护测评项目计划书、测评实施方案以及人员安全培训计划，并提交被测评单位审核。

②第二阶段：

进行现场测评，同时对被测评单位信息安全相关管理和技术人员进行安全技术培训。初次测评完成后，提交初评的整改意见报告。

③第三阶段：

协助被测评单位针对测评过程中发现的安全问题进行技术整改加固工作，并进行整改后的回归测评。

④第四阶段：

整理测评结果，向被测评单位提交被测信息系统安全等级保护测评报告、定级备案证书、以及相应文档。

2）项目实施要求

依据国家各项相关标准法规和被测评单位现有的规范、制度，同时结合项目实际需要，对信息安全等级保护工作所涉及的定级、备案、测评（包括测评范围、测评方法等）、整改（包括整改方法、范围等）过程中，所需的产品、技术、制度、流程、建设要求和实施规范等方面，提供组织定级评审、报告编制、咨询、测评、整改建议以及整个建设过程的监督和管理等服务。所提供的整体方案需包括技术方案和实施方案，技术方案包括整体流程、技术方法和服务方案设计等，需要对每项技术方法的应用位置进行详细描述，对系统进行详细的测评，发现系统不足，明确安全风险隐患和差距，提出整改意见，协助被测评单位信息安全管理人员进行整改；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等，需要明确每项工作的时间安排、操作时间和操作人员。供应商负责提供的服务内容至少应包括但不限于以下各项:

①供应商在信息安全等级保护测评前应制定详细的技术方案，包括信息安全等级保护测评项目计划书、测评实施方案以及人员安全培训计划等，并提交被测评单位审核。

②信息安全等级保护测评包括但不限于以下对象：网络结构、网络服务、主机系统、存储备份系统、数据库、中间件、应用系统、数据安全、安全系统、系统安全策略等。

③供应商应描述测评服务的技术方案，包括准备工作、技术措施、人员安排、时间进度、可能对系统造成的影响等。

④安全测评工作应尽量选择在非业务繁忙时段进行，将对被测系统可能带来的影响减至最小。

⑤提供系统及系统整合定级咨询建议并组织定级评审等。协助被测评单位整理定级备案材料和进行安全主管部门定级备案工作。

⑥供应商应书面承诺能够积极与被测评单位协作，共同完成本项目的测评工作，项目实施过程中出现问题不得互相推诿，双方应主动进行沟通，并及时解决问题，确保项目顺利实施。

3）项目实施团队

供应商的岗位配置要至少配置项目经理 1 名、总测评师 1 名、测试工程师 4 名，且各个岗位应独立配置，不能有兼任的情况。

4）测评工具要求

①采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件。

②采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品。

③采用的测评工具的生产商应为正规厂商，具有一定的研发和服务能力，能够对产品进行持续更新并提供质量和安全保障。

④测评机构所使用的测评工具不会对系统产生破坏或负面影响。

5）项目管理要求

对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，供应商必须提供完整的项目管理方案，项目的方案设计与具体实施应满足以下原则：

①最小影响原则：工作应尽可能小的影响系统和网络的正常运行，不能对网络的运行和业务的正常运行产生显著影响（包括系统性能明显下降、网络拥塞、服务中断）;

②标准性原则：服务方案的设计与实施应依据国家网络安全等级保护 2.0 系列标准进行;

③规范性原则：供应商工作中的过程和文档，应具有较好的规范性，便于项目的跟踪和控制;

④可控性原则：方法和过程要在双方认可的范围之内，安全服务的进度要按照进度表安排实施，保证被测评单位对于服务工作的可控性;

⑤整体性原则：评估内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患;

⑥保密原则：对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招标人的行为，否则被测评单位有权追

究供应商的责任。

6）服务保障与承诺

①供应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。

②供应商应协助、配合被测评单位与上级监管部门、公安机关的沟通协调。在测评过程中和测评完成后，根据被测评单位要求及时派遣测评工程师对在测评过程中出现的风险问题进行现场技术整改指导，协助、配合被测评单位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，并通过上级监管部门和公安机关的审核验收。

③供应商应在项目期内向被测评单位提供 7*24 小时电话咨询服务，咨询服务内容包括但不限于等级保护测评、商用密码应用、网络安全建设合规等方面，必要时上门服务。根据甲方需求提供重大活动、节假日的安全保障服务。跟踪信息安全等级保护的最新发展情况，及时告知被测评单位，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。

④供应商应在项目实施过程中，对被测评单位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。

⑤供应商应在项目开始前，与被测评单位签订保密协议，严格遵守法律法规，对被测评单位商业秘密、系统风险信息、项目实施内容及成果信息进行严格保密，未经被测评单位同意，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。