四川泸州川南发电有限责任公司2×600MW机组

2025年DCS网络安全等级保护测评

技术规范书

**四川泸州川南发电有限责任公司**

**二〇二五年五月 四川·泸州**

目录

1． 总则 1

2． 工程概况 1

3． 标准规范及原则 2

4． 测评及服务内容 3

5． 技术要求 4

6． 服务时间 6

7． 项目验收 6

8． 双方责任 7

9． 考核细则 7

附件一 、差异表（投标方填写） 8

1. 总则

1.1 本技术规范适用于四川泸州川南发电有限责任公司2×600MW机组2025年度DCS网络安全等级保护测评，本规范书提出了本次测评的标准、内容、要求及验收等方面的技术规范。

1.2比选申请人必须具备合法的企业资质，具有《网络安全服务认证证书》和《等级保护测评服务认证证书》，具有中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质证书；具有市场监督管理局颁发的检验检测机构资质认定证书（CMA），须提供相关证明材料。至少具有一个发电机组电力监控系统等保测评业绩，须提供相关证明材料。

1.3 本技术规范提出的要求为最低限度要求，并未对一切细节作出详细规定，也未充分引述有关标准和规范的条文，投标方应提供符合本技术规范和有关标准规程的技术服务，并满足有关强制性标准要求。

1.4比选申请人如对本规范书有偏差(仅允许正偏差、无论多么微小)都必须清楚地表示在本规范书的“差异表”中，否则比选人将认为投标方完全接受和同意本规范书的要求。若本技术规范书前后有不一致的地方，投标方应提前提出澄清，未提出澄清的则以比选人的解释为准。若本技术规范书书与合同有差异，应按照有利于比选人的原则处理。

1.5 工程使用国际计量单位（SI）制，招、投标双方均需遵循。工作语言为中文，所有的文件、报告、图纸均用为中文编写。

1.6 在签订合同之后，比选人保留对本技术规范书提出补充要求和修改的权利，投标方应承诺予以配合行业要求及规范变化。本技术规范书解释权归比选人。

1. 工程概况

2.1 地理位置

电厂厂址位于泸州市江阳区江北镇，西北距江北镇约600m，东北距泸州市区直线距离约15km，公路距离约30km，东面距纳溪区约7.5km，南面距长江北岸约2km，北面距泸州机场跑道轴线延长方向约2km。

2.2 系统概述

 电厂#1、#2机DCS分散控制系统ovation公司产品，布置在独立的电子间，系统配备了PWCS网络安全柜，安装有安全交换机、工业防火墙、入侵检测装置、网络审计等设备。

1. 标准规范及原则

3.1比选申请人须执行本技术规范所列标准。本技术规范与现行规程规范有矛盾时，按较高标准执行。投标方应在投标阶段提交所采用的全部标准与规范清单，且至少是下列规范、规程和标准的最新版本。在合同执行过程中，投标方采用的其他标准需经比选人确认。

《中华人民共和国网络安全法》

GB17859-1999：《计算机信息系统安全保护等级划分准则》

GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

GB/T 22240-2020：《信息安全技术 网络安全等级保护定级指南》

GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》

GB/T 25070-2019：《信息安全技术 网络安全等级保护安全设计技术要求》

GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》

GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》

GB/T 31509-2015：《信息安全技术 信息安全风险评估实施指南》

GB/T 20984-2022：《信息安全技术 信息安全风险评估方法》

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 36959-2018：《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》

DLT 2614-2023：《电力行业网络安全等级保护基本要求》

DLT 2613-2023：《电力行业网络安全等级保护测评指南》

《电力监控系统安全防护规定》 （国家发展改革委员会[2014年]第14号令）

《电力监控系统安全防护评估规范》 国能安全[2015]36号

《电力行业网络安全等级保护管理办法》（国能发安全规〔2022〕101号）

3.2 测评原则

网络等级保护测评方案设计与实施应满足以下原则：

（1）符合性原则：应符合国家网络安全等级保护制度及相关法律法规，指出防范的方针和保护的原则。

（2）标准性原则：方案设计、实施与网络安全体系的构建应依据国内、国际的相关标准进行。

（3）规范性原则：项目实施应由专业的等级测评师依照规范的操作流程进行，在实施之前将详细量化出每项测评内容，对操作过程和结果提供规范的记录，以便于项目的跟踪和控制。

（4）可控性原则：项目实施的方法和过程要在双方认可的范围之内，实施进度要按照进度表进度的安排，保证项目实施的可控性。

（5）整体性原则：安全体系设计的范围和内容应当整体全面，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）最小影响原则：项目实施工作应尽可能小的影响网络和信息系统的正常运行，不能对信息系统的运行和业务的正常提供产生显著影响。

（7）保密原则：对项目实施过程获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害测评委托单位利益的行为。

1. 测评及服务内容

4.1测评对象

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务内容 | 系统名称 | 安全等级 | 备注 |
| 1 | 等级保护测评服务 | #1、#2机组DCS分散控制系统 | 三级 |  |
| 2 | 风险评估服务 | #1、#2机组DCS分散控制系统 | 三级 |  |

4.2测评内容

4.2.1 网络安全等级保护测评要求由安全测评通用要求和安全测评扩展要求两部分组成。安全测评通用要求具体分为安全物理环境、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、安全运维管理等十个方面。安全测评扩展要求具体分为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、工业控制系统安全测评扩展要求等四个方面。在具体测评实施过程中根据不同的等级保护对象组成，选择安全测评通用要求以及合适的安全测评扩展要求进行测评。

4.2.2 根据国家及电力行业监控系统安全防护评估规范，在系统网络安全等级保护测评的基础上，增加如下测评项：电力监控系统风险评估服务，内容包含：

（1）技术要求：包括物理环境测评、网络系统测评、主机安全测评、应用安全测评。物理环境测评主要包括位置、访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电磁防护等内容。网络系统测评主要包括网络架构、网络访问控制、网络安全审计、边界完整性检查、网络入侵防范、网络恶意代码防范、网络设备防护等内容。主机安全测评主要包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制等内容。应用安全测评主要包括应用系统身份鉴别、应用系统访问控制、应用系统安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等内容。数据及备份恢复测评主要包括数据完整性、数据保密性、备份和恢复等内容。

（2）管理要求：涵盖安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面。安全管理制度主要包括管理制度、制定和发布、评审和修订。安全管理机构主要包括岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。人员安全管理主要包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理。系统建设管理主要包括系统定级、安全方案设计、产品采购和使用、自行软件开发、外部软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择。系统运维管理主要包括环境管理、资产管理、介质管理、设备管理、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。

4.3 服务内容

4.3.1 信息系统备案。完成定级、备案材料的整理及在公安机关网安部门备案工作，并取得公安相关部门出具的信息系统安全等级保护备案证明。

4.3.2 初次测评。检查系统安全现状，从物理安全、网络安全、主机安全、应用安全、数据安全和安全管理等层面进行差距分析，对系统进行初次安全防护评估。通过对系统现状的分析和梳理，发现系统现有安全措施与等级保护基本要求的差距，提出安全整改建议，以指导后续安全整改工作。

4.3.3 DCS系统网络等保整改方案及建议。制定安全管理制度、落实安全责任，建议安全技术设施，落实安全技术措施。通过安全建设整改，确保DCS系统通过三级网络安全等级评测。

4.3.4 二次测评。对整改后的系统及网络再次实施等级测评，提出安全整改建议，协助比选人完成整改工作。

4.3.5 对测评结果记录进行分类统计、风险计算、综合分析与评估，编写《等级测评报告》及《风险评估报告》。

4.3.6 咨询服务。提供信息系统的安全咨询和整改建议等技术支持服务，涵盖系统建设、运维、管理、技术等相关安全问题；协助开展单位内部网络与信息安全检查工作。

4.3.7 安全意识和技能培训。针对技术人员、管理层提供不同类型的信息安全培训，包括管理培训和网络安全技术培训。

1. 技术要求

5.1 人员配置要求

为本项目的顺利、有序实施和质量保证，为本项目配置项目负责人、项目经理、质量主管和一定数量的系统测评工程师人、渗透工程师，具体如下：

5.1.1 项目经理是本项目的总协调人，负责领导、指挥、协调项目负责人、测评实施员等开展测评工作，负责项目人员安排，制定项目计划，对整个项目的质量、进度进行把控，负责项目总协调工作。项目经理应具有信息（或网络）安全等级测评师（中级及以上）证书，除此之外还应具有包含但不限于：COBIT信息系统审计认证证书、重要信息系统保护人员CIIP-A(可信计算）证书、注册密码安全专业人员（NSATP-CSP)证书等安全服务能力证书。（投标方提供承诺函，承诺合同签订时需提供证书复印件并加盖单位公章）

5.1.2 项目负责人是具体系统现场测评工作的现场负责人，负责组织、协调现场测评实施员开展具体的测试工作，制定具体系统的测评进度计划，负责具体系统的现场测评交流、沟通和组织协调，向招标人汇报系统测评进度。项目负责人应具有信息（或网络）安全等级测评师（中级及以上）证书，除此之外还应具有包含但不限于：信息技术应用创新考试评价证书（信息安全工程师）、CCSC网络安全能力认证（网络安全管理2级）等安全服务能力证书。投标方提供承诺函，承诺合同签订时需提供证书复印件并加盖单位公章）。

5.1.3质量主管对项目实施全过程的质量监控，动态监控质量体系执行情况，对违反质量管理规范的情况提出改进或否决意见，及时出具质量监控报告或意见。质量主管应具有信息（或网络）安全等级测评师（中级及以上）证书，除此之外还应具有包含但不限于：高级软件测评工程师证书、注册密码安全专业人员（NSATP-CSP）证书等安全服务能力证书。（投标方提供承诺函，承诺合同签订时需提供证书复印件并加盖单位公章）。

5.1.4 测评实施人员、渗透工程师在项目经理和项目负责人的领导下展开具体的系统测评工作。测评实施人员应具有信息（或网络）安全等级测评师（中级）证书，除此之外还应具有包含但不限于：CCSS-M网络安全服务能力评价证书（安全管理能力认证）、高级软件测评工程师证书、注册密码安全专业人员（NSATP-CSP）证书。项目渗透测试人员应具有信息（或网络）安全等级测评师（中级及以上）证书，除此之外还应具有包含但不限于：信息技术应用创新考试评价证书（数据库工程师）、CCSS-R网络安全服务能力评价证书（应急响应能力认证）等安全服务能力证书。

人员配置表（投标方填写）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 岗位 | 姓名 | 具备资质 |
| 1 |  |  |  |
| 2 |  |  |  |
| ... | ... | ... | ... |

5.2 管理要求

5.2.1比选申请人必须提供完整的项目管理方案，投标方需要针对本次项目管理服务要求进行承诺，未提供项目管理服务承诺为无效。

5.2.2比选申请人及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任；

5.2.3比选申请人在开展等级保护测评服务之前需与比选人签订保密协议，测评过程中向比选人借阅的文档资料应在测评工作结束后全部归还，未经比选人允许，不得擅自复制、保留；

5.2.4 岗位配置要至少配置项目负责人、测评师、项目经理、渗透工程师、质量主管等并明确各个岗位的相关职。

5.3 测评工具要求

5.3.1 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；

5.3.2 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；

5.3.3 采用的测评工具的生产商应为正规厂商，能够对产品进行持续更新并提供质量和安全保障；

5.3.4 测评机构所使用的测评工具不会对单位系统产生破坏或负面影响。

1. 服务时间

本服务计划于合同签订之日开始，至2025年12月31日结束。

1. 项目验收

7.1比选申请人应按相关的国家标准和行业规范要求，采用先进的技术措施和手段，完成项目内容，保证项目质量，确保成果真实可靠。

7.2比选申请人所提供的项目基础资料应完整、真实、可靠，成果报告文字简洁、表达准确，图像清晰无误，附件齐全。

7.3 本项目所有技术成果属于比选人所有。项目完成后，投标方按要求应将形成的过程资料、相关文件全部移交给比选人，相关文件应包含以下几项：

（1）《网络安全等级保护测评方案》

（2）《网络安全等级保护测评报告》（包含整改建议）

（3）《网络安全系统渗透报告》

（4）《电力监控系统风险评估报告》（包含整改建议）

（5）其他未列入的应交资料

1. 双方责任

为切实保障本项目的工作质量，确保测评工作达到预期目标，对双方技术工作责任约定如下：

8.1 比选人责任：

8.1.1 负责测评过程中相关单位和部门的协调。

8.1.2 为投标方提供良好的工作场地和环境。

8.1.3 按工作要求提供相关的资料和信息。

8.1.4 准备应急措施，负责实施过程中的紧急情况的处理。

8.1.5 明确专人全程配合投标方开展现场测评。

8.2比选申请人责任：

8.2.1 协助比选人根据等保2.0要求完成定级备案、专家评审等工作，取得备案证明。

8.2.2 完成公安机关的项目登记流程，测评实施得到批准后才能实施。

8.2.3 按照测评方案开展工作。

8.2.4 项目内容的变更及时与比选人代表沟通。

8.2.5 依据国家和行业相关标准开展测评（评估）工作，确保测评工作质量。

8.2.6 按照协议要求提供技术服务和成果。

8.2.7 配合比选人准备应急预案和实施过程中的紧急情况处理。

8.2.8 按照等级保护2.0要求完成测评后，针对比选人存在的问题给出有效、可行的解决建议。

1. 考核细则

投标方应认真按照有关标准、规范要求开展测评工作，随时接受比选人代表的检查、整改，并根据实际情况，作好安全、质量、环境和进度管理，若有违反，比选人将根据公司管理规定进行考核，包含但不仅限于：

（1）未按时完成测评方案，处罚责任单位500元/天。

（2）未按时完成前期准备工作，处罚责任单位1000元/天。

（3）未按时完成测评，处罚责任单位1000元/项/天。

（4）未按时提交测评结果、测评报告，处罚责任单位1000元/项/天。

（5）投标方工作严格按照比选人规定履行职责，其余考核实施。

# 附件一 、差异表（仅允许正偏差、投标方填写）

|  |  |  |
| --- | --- | --- |
| **序号** | **询价文件** | **应价文件** |
| **条目** | **简要内容** | **条目** | **简要内容** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| .. | ... |  |  |  |