

四川泸州川南发电有限责任公司
管理信息系统网络安全改造

技术规范书

四川泸州川南发电有限责任公司
二〇二四年六月 四川·泸州

一、总则

1. 本技术规范书针对四川泸州川南发电有限责任公司（以下简称招标方）的管理信息系统网络安全改造项目提出了详细的技术要求及有关方面标准。改造范围涵盖了管理信息系统网络安全改造项目的设备提供、方案设计、安装实施、系统配置、调试测试、运行验证等多个环节。

2. 本技术规范书列出了基本且必要的技术要求，并未详尽列出所有技术细节或完整引用相关行业标准和规范条款。

3. 投标方应确保提供的网络安全解决方案成熟稳定、技术领先、易于维护，完全符合本规范书、最新的网络安全工业标准以及国家关于信息安全、法律法规等强制性规定的要求。当本规范书所采用的标准与投标方遵循的标准存在冲突时，应执行更为严格的标准。

4. 鉴于本次改造是在既有管理信息系统的架构基础上进行，投标方应在保留原有系统核心功能的基础上，安全、高效地完成网络安全改造工作。

5. 投标方须具备在项目中成功实施类似网络安全改造的经验，案例不得少于两个，且每个项目稳定运行时间不少于一年。招标方不接受未经实践检验的试制型网络安全解决方案。

6. 投标方必须是所提供网络安全系统的制造商或授权经销商（并提供相应授权证明文件），且所提供的硬件设备须为信创版，并对所提供的业绩资料的真实性负责。

7. 投标方提交的所有文档、图纸、计算报告、使用手册等资料，均应采用国际单位制(SI)。所有文件、图纸以及双方通讯，均应使用中文。

8. 投标方应建立完善的质量管理及质量保证体系，在网络安全改造的全过程（包括设计、生产、安装、调试、运行阶段）中，具备详细的质量记录和质量保证文件。

9. 技术规范书中提供的设备清单为最低配置要求，投标方需根据项目实际功能需求提供全套所需的网络安全设备和材料。

10. 投标方应按分项报价，各分项之间相互独立，招标方在签订合同时可根

据实际需求减少某一单项并相应降低合同金额。

11. 投标方应确保其提供的网络安全设备或系统涉及的专利费用已包含在报价中，并保证招标方不会因此承担任何有关专利的法律责任。

12. 投标方需根据投标书编制详细的网络安全改造实施方案，并提交招标方审核通过。

13. 作为一项升级改造项目，投标方在制定实施方案前应对招标方现有的管理信息系统进行全面调研（充分理解原系统的功能并按照招标书要求实现全部功能），相关费用由投标方自理。投标方应对拟利旧设备的安全性能进行评估，确认各项设备性能参数能满足改造后的安全要求，否则应选择全新采购替代。投标文件中未明确说明需要利旧的设备，视为全新供应。

14. 签订合同后，投标方应按照招标方规定的时间、内容、深度要求提供所需的设计资料，并按施工进度和设计变更随时调整，确保提供的资料及时且满足工程需要。

15. 签订合同后，招标方保留在项目实施过程中对本技术规范书提出补充要求和修改的权利，投标方应承诺配合因行业要求、规范、标准和规程变化而产生的补充要求，合同价格保持不变。

16. 签订合同后，投标方参与项目实施的人员应签订保密协议，详见附件。

17. 本技术规范书与合同正文具有同等法律效力，最终解释权归招标方所有。

二、工程概况

1. 地理位置

招标方地址位于四川省泸州市江阳区江北镇境内，距泸州市区边缘直线距离约 15km。距江北镇约 600m，交通较为方便。

2. 环境条件

多年平均大气压力： 973.2 hPa

多年平均环境温度： 17.6℃

多年极端最高温度： 40.2℃

多年极端最低温度： -1.6℃

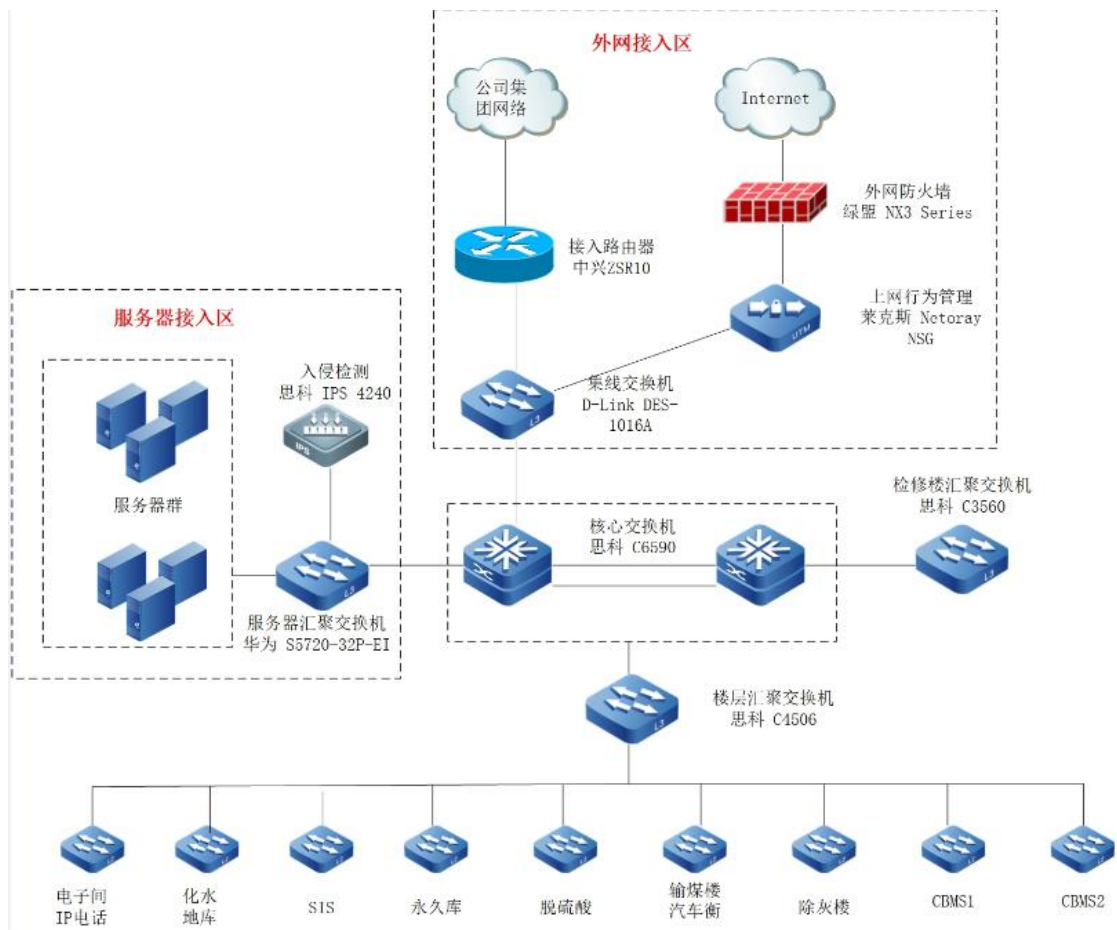
多年平均相对湿度： 84%

多年最小相对湿度： 21%

3. 管理信息系统

招标方已严格按照《电力监控系统安全防护规定》相关要求，将公司基于计算机和网络技术的业务系统划分为生产控制大区和管理信息大区，此次改造仅针对管理信息大区。具体的分区内容，请投标方自行查阅《电力监控系统安全防护规定》，也可现场调研。

4. 管理信息系统网络拓扑图



三、改造范围

针对管理信息大区所有网络情况进行梳理，排查可能存在的网络安全隐患并改造。投标方应该具备基本的网络配置能力，可以根据实际情况对招标方的网络

结构进行改善和调整，下面所列的设备清单仅为此次必须更换的设备。投标方如要新增设备需要详细说明原因。

1. 入侵检测设备 思科 IPS4240 MARS
2. 外网防火墙 绿盟 NX3
3. 上网行为管理设备 NSG
4. 在与集团网络连接处新增防火墙

四、标准与规范

投标方提供的设备及服务应符合下列标准或与之相当的其他国际标准（包括但不限于此），投标方的替代标准须经招标方认可：

《中华人民共和国网络安全法》

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

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

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

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

《信息安全技术 关键信息基础设施安全控制指南》（征求意见稿）

《信息安全技术 关键信息基础设施网络安全保护基本要求》（征求意见稿）

《信息安全技术 个人信息安全规范》（GB/T 35273-2017）

《信息安全技术 信息安全风险评估实施指南》（GB/T 31509-2015）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

《关键信息基础设施安全保护条例》（征求意见稿）

ISO/IEC17799:2005/27001

IATF 《信息保障技术框架》

国家发展改革委[2014]第 14 号令：《电力监控系统安全防护规定》

上述规范、标准是招标方要求的最低标准，如在设计过程中，国家、行业颁布了新标准、规范，则相应执行最新版本的有关规定。

五、供货范围

1. 硬件设备供货

网络安全防护设备：提供**国产**一线品牌防火墙，需满足 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》等相关标准，具备高性能、高可靠性和深度防御能力。

入侵检测与防御系统：提供**国产**一线品牌的入侵检测系统（IDS）和入侵防御系统（IPS），实现对网络流量的实时监控、分析及异常行为的预警和阻断功能。

安全审计系统：需提供**国产**一线品牌的安全审计系统，覆盖网络访问、操作行为、数据流转等多个维度，确保所有网络活动可追溯、可审计。

终端安全管理：提供**国产**一线品牌的终端安全管理软件及配套硬件，如统一终端管理平台、防病毒软件等，确保各类终端设备的安全运行。

2. 软件系统供货

网络安全管理系统：提供**国产**一线品牌的网络安全管理平台，实现对全网安全状态的集中监控、管理和运维。

恶意代码防护软件：提供**国产**一线品牌的恶意代码防护软件，具备最新威胁情报库，能有效防范和清除各类恶意软件。

六、技术资料

投标方提供全套系统设备的技术资料，包括系统设计说明、维护说明、操作说明，以及硬件配置图等技术资料，应随设备提供产品合格证书、产品说明书、测试报告以及装箱单等，进口产品应同时提供报关单和原产地证明，包括但不限于：

1. 系统设计说明书
2. 产品检验合格证书
3. 设备运行维护说明书
4. 设备简要操作说明书
5. 硬件配置图

其中纸质版三套，电子版（U盘存储）2套。验收通过后，两周内提供相关竣工文件和竣工图二套原件，二套复印件及一式三套电子版（不可擦除光盘），其中纸质档案归档质量要求按《科学技术档案案卷构成的一般要求

（GB/T 11822-2008）》和《国家重大建设项目文件归档要求与档案整理规范（DA/T 28-2002）》执行，电子档案按《电子文件归档与管理规范（GB/T 18894-2002）》执行。

七、工程进度

设备交货时间为合同签订后 7 天。项目实际开工时间由招标方提前通知，现场施工工期不超过 5 天；投标方必须配合招标方工程进度合理安排施工，按时保质完成上述工作内容。

八、运输及开箱验收

1. 投标方负责将设备运输至招标方所在地，并按招标方要求搬运至指定地点。

2. 设备运抵现场后，招标方通知投标方在一定时间内到达现场进行开箱检验。

3. 如果投标方在规定的时间内未能到达现场，又未同招标方协商到达工地时间，则招标方可根据工程需要自行开箱检验，如发现设备、部件与装箱单不符等情况，投标方将承担责任。

4. 所供设备必须与合同清单中的型号、数量一致，并提供所供产品的原产地证明、报关单、出厂检验报告。

5. 开箱检验后设备应妥善保管，避免零部件遗失和设备的损坏。

九、技术服务

1. 投标方须派出技术服务人员现场负责安装调试和试运行，直至通过验收。现场服务人员的工作时间应与现场要求相一致，以满足现场的要求。

2. 未经招标方同意，投标方不得随意更换现场服务人员。同时，投标方须及时更换招标方认为不合格的投标方现场服务人员。

3. 合同签订后 3 天，投标方技术服务人员应向招标方进行技术交底，讲解和示范将要进行的程序和方法。

4. 投标方应对其所供设备提供安装和调试监督的重要工序表，交由招标方对施工情况进行确认和签证，否则不能进行下一道工序。如因投标方技术服务人员

失误而发生问题，投标方负全部责任。

十、双方责任

1. 投标方响应招标方工作安排，按招标方要求及时到达现场负责安装调试等工作，并确保安装调试后设备各项性能指标满足要求。
2. 投标方技术服务人员的安全、差旅、住宿、餐饮等均由投标方自行负责。
3. 投标方负责对招标方技术人员的培训指导工作，针对本次改造项目的细节、设备操作、运行和维护提供培训课程。
4. 投标方无偿提供软件的备份和所有密码、操作说明等技术资料。
5. 投标方负责改造项目结束后的运维工作，并将运维方案在项目结束后提交给招标方。
6. 招标方应积极协调、配合投标方设备的安装调试工作。

十一、质保及售后服务

1. 投标方应保证所提供的硬件设备自验收合格之日起至少提供三年原厂质保服务，软件产品需提供至少一年的免费升级和技术支持服务。
2. 在质保期内，若出现因产品质量问题导致的功能异常或故障，投标方应在接到异常或故障通知后，在合同约定的时间内（例如：24小时内响应，72小时内现场处理）提供免费维修或更换服务。
3. 技术咨询服务： 投标方应设立 7×24 小时全天候的技术咨询热线，并配备专业的技术支持团队，为招标方提供及时有效的远程或现场技术指导。
4. 培训服务： 投标方需在项目实施过程中为招标方相关人员提供全面的产品操作、维护、故障排查等方面的培训，确保招标方人员能够独立进行日常运维工作。
5. 维护保养服务： 在质保期结束后，投标方应提供可选的维护保养服务合同，包括定期巡检、预防性维护以及必要的软件更新升级等服务内容。
6. 应急响应服务： 对于可能影响招标方正常运行的重大网络安全事件，投标方应具备应急响应机制，按照事先制定的服务级别协议（SLA），在最短时间内协助招标方解决问题并恢复正常运行状态。

7. 软件升级保障： 投标方须承诺在产品生命周期内持续提供软件版本更新和漏洞补丁，以应对不断变化的网络安全威胁环境。

8. 配件供应保障： 对于可能出现的硬件配件需求，投标方应保证长期稳定的配件供应，且配件价格合理透明。

十二、验收标准

1. 投标方所有提供的硬件和软件设备与合同中规定的型号、规格和性能参数一致。确认所有系统功能按照改造方案要求实现，并且运行稳定。

2. 验证网络安全措施的有效性，包括防火墙、入侵检测系统、上网行为管理系统等的配置和运行状态。确认数据保护和隐私措施得到妥善实施，确保信息安全。

3. 系统经过一段时间的试运行（一周以上），未出现重大故障或性能问题。确认系统具备良好的负载能力和故障恢复能力。

4. 投标方提供的所有文档，包括设计说明、操作手册、维护指南等，均应完整、准确，并符合招标方归档要求。

5. 招标方的操作和维护人员已经接受了充分的培训，能够熟练操作和维护系统。确认投标方提供了必要的技术支持和售后服务。

十三、考核细则

投标方应根据实际情况，做好安全、质量和进度管理，若有违反，招标方将根据公司管理规定进行考核，包含但不限于：

1. 未按时供货的，处罚责任单位 1000 元/天。
2. 未按时提供设计安装图纸资料，处罚责任单位 500 元/天。
3. 未按时完成改造方案，处罚责任单位 500 元/天。
4. 未按时完成改造工作，处罚责任单位 1000 元/天。
5. 未按时竣工，处罚责任单位 2000 元/天。
6. 未按时提交竣工资料，处罚责任单位 500 元/天。
7. 未按要求完成质保工作，处罚责任单位 1000 元/天。

附件：

信息保密承诺书

因本人在四川泸州川南发电有限责任工作过程中，可能涉及需要保密的信息，包括但不限于任何非公开的、专有的和具有保密性质的资料及信息（涉及企业秘密的会议并印发的密级文件、通过内网平台发文、公文交换、事务信息、单位通讯录电话、传真、电子文档等信息、领导指定需要保密的信息）以及在工作时得到的所有信息系统信息。

为此本人承诺：

（1）除因工作需要并得到明确书面指示外，不得使他人获得、使用或计划使用这些信息。

（2）不得为自己利益使用或计划使用这些信息。

（3）不得窃取、复制或公开包含这些信息的文件或拷贝。

（4）不得直接或间接地向外部无关人员泄露这些信息。

（5）除因工作需要外，不得向其他职工打听这些信息，不得以不正当方式窃取这些信息，指使或暗示或诱导他人以不正当方式窃取这些信息，以不正当方式包括但不限于偷拍照片、偷偷复制材料或文件，引诱或胁迫他人披露信息等。

（6）对因工作需要而保管、接触或使用的有关包含有关信息的文件、数据，应妥善对待及采取合理加密措施，未经书面许可不得超出工作范围使用。

（7）在工作结束之后仍需对以上保密信息保密。

承诺人：

年 月 日