

江西赣能股份有限公司丰城发电厂

7、8 号机组 SIS 系统商用密码应用安全性评估

技术说明

一、项目目的

为落实 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、宜密办字〔2025〕9 号《关于做好我市重要网络与信息系统商用密码应用和安全性评估工作的通知》及其他相关法律法规要求，提高网络与信息系统安全性，需对 7、8 号机组 SIS 系统开展商用密码应用安全性评估。

二、现场设备状况

江西赣能股份有限公司丰城发电厂（以下简称采购人）的 7、8 号机组 SIS 系统为江西省宜春市密码工作领导小组备案的三级信息系统，目前未开展过商用密码应用安全性评估。

三、项目内容及要求

本项目为技术服务项目，报价人应对采购人的 7、8 号机组 SIS 系统区域的主要网络设备、安全设备和服务器开展商用密码应用安全性评估，评估依据《信息系统密码应用基本要求》、《信息系统密码应用评估要求》、《信息系统密码应用评估过程指南》等技术标准，从物理和环境评估、网络和通信评估、设备和计算评估、应用和数据评估、管理制度评估、人员管控评估、建设运行评估、应急处置评估 8 个层面开展评估。

3.1 总的要求

3.1.1 本技术要求提出了最低的有关要求，报价人可以提供满足本项目的更高标准要求；报价人的所有服务内容必须满足国家、行业有关电力监控、信息系统安全强制性标准。

3.1.2 报价人禁止对项目进行外包或分包，否则视为违反合同，采购人有权终止合同。

3.1.3 报价人必须执行国家和行业相关的标准、规范，同时严格执行采购人的各项管理制度。

3.1.4 采购人有权对报价人在违反标准、规范、管理制度时进行经济考核。

3.1.5 本项目所有与相关系统的分界点上工作均在报价人负责的范围之内。

3.1.6 报价人在事前必须到现场进行勘查了解，详细了解本项目系统目前的布置状况和

运行状况，报价人事前没有进行现场勘查了解的，视为进行过现场勘查了解。

3.1.7 报价人在服务有效期内，技术有问题、人员力量不够或不服从管理，将严重影响采购人信息安全及设备的安全、稳定、经济运行且无法克服时，采购人有权单方面解除合同。或采购人有权另行委托施工队伍进行紧急处理，报价人应担负全部委托费用及由此造成的损失。

3.1.8 本文件所使用的标准如遇与报价人所执行的标准发生矛盾时，按较高标准执行。

3.1.9 本文件经双方确认后作为订货合同的技术附件，与合同正文具有同等效力。

3.1.10 报价人在提供技术服务时，不能影响现有应用系统正常运行；报价人在项目实施前需给出详细的方案，对可能影响现有应用系统正常运行的操作提出可靠的解决方案或制定应急预案等防范措施并报采购人审核。

3.1.11 技术服务所必须使用的软、硬件测试工具由报价人提供，但必须有相应检测机构出具的合格证书。

3.2 测评要求

3.2.1 商用密码应用安全性评估具体实现应满足以下原则：

1) 保密性原则：报价人应与采购人签订评估保密协议，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，不得利用此数据侵害采购人的权益，否则采购人有权追究报价人的责任。

2) 标准性原则：商用密码应用安全性评估实施应依据国家相关标准进行。

3) 规范性原则：报价人工作中的过程和文档，应具有规范性，便于项目跟踪和控制。
可控性原则：评估服务的进度应符合进度安排，保证采购人对评估工作的可控性。

4) 整体性原则：评估的范围和内容应系统、全面、规范，满足国家信息安全相关基本要求。

5) 最小影响原则：技术评估工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响，在线评估应在需方许可的条件下进行。

3.2.2 商用密码应用安全性评估服务应综合运用各种技术和工具，进行系统工具测试、验证分析。评估人员实施现场评估至少应开展访谈、核查和测试验证三种方式评估相关加密措施是否正确有效。

3.2.3 在评估实施过程中采用评估工具的，各种工具软件由报价人推荐，经采购人确认后由报价人提供并在评估中使用。应详细描述所使用的安全评估工具（软硬件型号、功



能和性能描述)、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

3.2.4 安全评估应有详细的实施方案和严格的操作步骤,采取的措施应是经过测试、稳定可靠的。

3.2.5 安全评估工具软件运行可能需要的硬件平台(如笔记本电脑、PC、工作站等)和操作系统软件等由报价人推荐,经确认后由报价人提供并在评估中使用。安全评估需要的运行环境(如场地、网络环境等)由采购人提供,报价人应详细描述需要的运行环境的具体要求。

3.2.6 测评过程应包括4项基本测评活动:测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评方与被测单位之间的沟通与洽谈应贯穿整个测评过程。

3.2.7 密码技术应用测评应包括物理和环境安全密码测评、网络和通信安全密码测评、设备和计算安全密码测评、应用和数据安全密码测评。测评验证被测系统的商用密码应用是否达到具有对应安全等级的安全保护能力,是否满足对应安全等级的保护要求。

3.2.8 密钥管理测评应包括检测被测系统密钥管理各环节,包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。

3.2.9 安全管理测评应从制度、人员、实施和应急四个方面,对被测系统的密码安全管理进行商用密码应用安全性管理测评。

3.2.10 评估完成后,应出具正式版测评报告,报告应按照国家密码管理局要求包含的内容编制或参考模板编制,报告以纸质版和电子版形式递交采购人,并协助采购人向宜春市密码管理局进行报告备案。

3.2.11 若本次评估不能达到相应符合要求,报价人应在采购人整改期间提供整改意见,在出具报告之日起一年内,报价人完成整改后免费提供一次复测评估服务。

3.3 工期要求

本期项目计划工期为:2025年08月01日-2025年08月31日。全部现场测试工作任务应在计划工期内完成。本期项目的所有工作任务应在2025年08月31日前完成,通过验收,并满足宜春市密码管理局工作要求。如时间有变动,采购人另行通知,报价人无条件服从。

3.4 资质要求

3.4.1 报价人应提供工商行政管理局登记注册并经年检（审）合格的营业执照或法人证书（复印件加盖公章）。

3.4.2 报价人必须具有国家密码管理局颁发的《商用密码检测机构资质证书》证书（复印件加盖公章）和供应商必须提供具有中国通信工业协会颁发的信息系统业务安全服务资质证书或中国电子工业标准化技术协会颁发的（ITSS）运维服务资质证书扫描件或复印件并加盖供应商公章。

3.4.3 报价人必须具有中国网络安全审查技术与认证中心颁发信息安全应急处理资质证书。

3.4.4 报价人具有公安部认可的2名及以上DJCP高级评估师证书且相关证书加盖公章、提供用人合同、社保证明（复印件加盖公章）。

3.4.5 报价人具有近两年（合同签订日期自2023年1月1日起）电力行业信息安全商用密码应用安全性评估服务工作经验并有测评案例（提供合同复印件加盖公章）。

四、考核

4.1 考核包括安健环考核、质量考核、进度考核和管理考核四个方面。

4.2 采购人严格按相关管理制度进行考核，报价人必须无条件接受。

4.3 同一事件造成多种后果，分别进行考核。同一事件适用于二种及以上考核条款，按最高考核条款执行。重复发生的事件招标方有权进行加倍考核。

4.4 项目施工过程中考核采取考核通知单形式下发。

4.5 涉及安健环的违章考核每次不低于1000元，严重违章按采购人要求从重进行考核。

4.6 采购人现场管理考核条款内没有涉及到的考核内容，采购人有权参照相关考核条款执行，从严从重部分考核以合同条款和采购人管理制度为准。

4.7 考核费用按采购人要求进行上交或扣除。

五、验收条件

5.1 本技术文件所规定的所有测评项目均已完工，并通过三级验收、完成质检点签字。

5.2 施工现场无遗留物件，现场文明生产需达到采购人验收标准。

5.3 报价人出具正式版《商用密码应用安全性评估报告》，并经过采购人相关部门审核通过。

5.4 报价人提出验收申请，采购人相关部门验收完成。

5.5 验收完成后方可付清全款。

