附件

《大模型服务与应用安全评测技术规范》团体标准立项计划

项目计划号	标准名称	主要内容	计划完成时间	牵头单位
184-T/ISC-26	《大模型服务与应用安全评测技术规范》	本文件规定了大模型服务与应用安全评测的评测对象、评测环境与测试准备、安全风险类型、安全检测方法、评价指标、评估结果判定规则以及测试报告要求。 本文件适用于对大语言模型服务平台、大模型应用系统、智能体系统以及集成大模型能力的应用程序接口（API）服务开展安全评测；重点适用于文本交互、代码生成、多轮对话、检索增强生成以及工具调用等场景的安全评测，涉及图文等多模态场景时可参照执行，音频、视频等其他模态场景可参照执行。	2026.12	广州市云山人工智能安全研究院、联通（广东）网络信息安全科技有限公司、广州亚信安全智能科技有限公司