**互联网新技术新应用安全评估专项**

**项目需求书**

**一、各类互联网信息服务的安全评估服务**

一是各类互联网信息服务的安全评估服务。

1.1针对商业平台申请上线新应用、新功能的安全评估的情况，需要在上海网信办的授权下，针对《中华人民共和国网络安全法》《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》中规定的互联网新闻信息服务；针对《中华人民共和国网络安全法》《未成年人网络保护条例》、《网络信息内容生态治理规定》、《互联网用户账号信息管理规定》中规定的具有舆 论属性或社会动员能力的新应用新功能申请上线、重大变更等需安全评估的情形，选择两种及以上方法开展安全评估 。

针对《互联网信息服务深度合成管理规定》、《互联网信息服务算法推荐管理规定》、《区块链信息服务管理规定》、《生成式人工智能服务管理暂行办法》等法律法规，开展生成式人工智能服务的安全评估。同时，根据生成式人工智能独特业态，服务期内需要供应商提供“大模型远程测评工具”使用及技术支撑服务不少于20次。

1.2需要在上海网信办授权下，开展对属地涉及上百家互联网企业的网站、APP进行摸排，并根据《中华人民共和国网络安全法》,《未成年人网络保护条例》、《互联网新闻信息服务管理规定》、《网络信息内容生态治理规定》、《互联网用户账号信息管理规定》、《网络暴力信息治理规定》等法律法规等互联网法律法规中的相关要求，对摸排到的平台开展前台巡查，选择一种及以上方法开展安全评估，需要供应商提供“内容安全审核工具”使用及技术支撑服务不少于12次。

1.3是针对上级部门下发的业务、上海网信办监管需要，根据《中华人民共和国网络安全法》《未成年人网络保护条例》、《互联网新闻信息服务管理规定》、《网络信息内容生态治理规定》、《互联网用户账号信息管理规定》、《网络暴力信息治理规定》等法律法规，开展的技术类专项任务，服务期内不少于2次。

**二、安全评估支撑服务**

一是保持对国际以及国内新技术新应用的前瞻研究，并给上海网信办提供专业研报。服务期内需要对新技术（如深度伪造、推荐算法、生成式人工智能）、强舆 论属性的新应用（社交语音、视频直播等）、新业态（元宇宙、NFT等）的关键技术进行风险评估，以研报的形式不定期上报研究成果。服务期内需要开展新技术、新应用研究报告辅助编制。服务期内不少于4次。

二是供应商需提供人员驻场服务。

2.1提供不少于10个人月的驻场服务。

2.2驻场期间需要对已上线的生成式人工智能、深度合成、区块链信息等服务开展监测、对属地重点新应用开展排查测试等支撑服务。

2.3需要支撑上海网信办开展生成式人工智能服务备案电话咨询、指导服务。

三是培训支撑服务。

3.1需要对互联网新技术、新应用、新业态研究与网信办开展相关交流培训工作。

3.2需要对互联网新技术新应用安全评估的实操规范与网信办开展相关交流培训工作。

3.3需要对生成式人工智能服务合规宣贯支撑开展安全评估与网信办开展相关实操培训或学习沙龙等。

服务期内完成相关服务数量不少于2次。

**三、供应商能力要求**

(1)供应商应具备专业的互联网信息服务、新技术新应用安全评估的能力，具有类似项目服务经验；具有ISO/IEC27001信息安全管理体系认证证书、中国合格评定国家认可委员会实验室认可证书、国家认可委员会检验检测机构认可证书等相关证书。

(2)供应商应具备针对生成式人工智能服务的安全评估，具有可定制化的“大模型远程测评工具”及技术支撑服务，实现对大模型安全风险的自动检测和结果辅助评判；对重点互联网信息服务的安全评估，具有可定制化的“内容安全评估工具”使用及技术支撑服务。

(3)供应商应有稳定的技术服务团队，成交后能够提供可靠的本地技术支撑能力，需专门为本项目成立专门的服务团队。其中项目负责人应当具有硕士学位和高级工程师证书，具有不少于5年服务网络信息安全工作的经验，具有区块链、推荐算法、生成式人工智能新技术新应用等相关项目案例经验。另提供不少于10人团队成员，其中高级工程师不少于2名，中级工程师不少于3名，驻场服务人员不少于4人。

(4)采购单位拟委托第三方机构开展该服务项目的履约评估，供应商需承担相关委托费用并配合做好评估工作。