

数字化项目等级保护测评服务项目需求

一、项目背景

网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法，是维护国家信息安全的根本保障。为进一步保障中国（上海）自由贸易试验区临港新片区管理委员会数字化项目信息系统的合规性，落实《中华人民共和国网络安全法》以及监管机构的相关要求，对临港新片区管委会信息系统开展网络安全等级保护测评和 AI 智能体专项安全测评，提升信息系统整体的安全防护能力，进一步保障临港新片区管委会数字化项目安全可靠。

随着国家越来越多重要业务工作通过信息化的平台开展，国家越来越重视重要的行业、政府机关的信息安全工作。国家相关信息安全主管机关对等级保护工作已上升为国家的政策法规的高度，要求重要信息系统的安全建设需要达到相应的安全要求，并通过测评机构的测评、公安机关监督等行政法规督促等级保护工作的开展。

二、项目目标

依据信息安全等级保护管理办法、信息系统安全等级保护测评准则和 GB/T22239-2019《信息安全技术信息系统安全等级保护基本要求》标准，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面，以等级保护 2.0 标准要求为依据，对中国（上海）

自由贸易试验区临港新片区数字化发展项目进行定级备案、差距分析、正式测评，出具《网络安全等级保护等级测评报告》，并取得“信息系统安全等级保护备案证明”。通过采用人工访谈、工具检测、文档分析的方式，分析信息系统与等级保护标准要求的差距，形成差距分析报告；并为制定安全规划、开展安全建设提供建议；完成本次项目信息系统的网络安全等级保护测评，使落实网络安全等级保护工作后的信息系统安全防御能力得到提升并且符合最新国家网络安全等级保护相关要求。由于本次测评项目中涉及 AI 智能体应用，除法定等保合规外，需依赖人工智能大模型系列国标（GB/T 45288）同步开展 AI 智能体专项安全测评，专项测评结果不替代等保测评，双方结果互为补充。

通过服务赋能，提高运维单位自主整改及持续合规能力，确保所有被测系统最终符合等保测评要求。

服务基本要求

（1）测评前准备（风险识别与防控）：开展系统调研，梳理系统信息及架构，识别潜在风险。输出《系统安全风险评估报告》《系统安全风险整改建议》，明确合规差距。

（2）测评中支持（动态管控与技术支持）：实时监测测评进展，针对发现的问题，提供整改方案及技术指导。

（3）初测未通过整改（应急响应与赋能）：提供定制化整改方案，并协助实施，确保复测通过。

（4）深度摸排与知识沉淀：对系统安全状况进行全面摸排，构建系统台账。

三、项目内容

本项目主要涉及中国（上海）自由贸易试验区临港新片区管理委员会出资建设的城市治理、智慧交通、经济、政务等领域的 13 个信息系统，依据最新国家相关法律法规、标准要求对被测信息系统进行网络安全等级保护测评和对所涉及 AI 智能体进行专项安全测评。

服务周期内，采购人如需增加系统等保测评，项目承接方须提供测评服务，且费用不再增加。投标人须充分考虑此风险，中标后不得以此为理由提出任何形式的索赔和造价调整。

四、付款方式

分期付款:第一笔-首付款(30%):合同签订, 乙方按履约验收方案的要求提交规定的成果交付物后 10 个工作日内支付 30%;第二笔-进度款(40%):在 2026 年 12 月 31 日前, 乙方按履约验收方案的要求提交规定的成果交付物后, 收到有效发票后 10 个工作日内支付 40%;第三笔尾款(30%):完成服务内容, 且验收合格, 甲方收到有效发票后 10 个工作日内支付剩余款项。

五、服务周期

自合同签订之日起一年内完成服务内容。

六、技术要求

1、测评依据

本次测评过程中主要依据的标准包括但不限于：

(1) GB/T 20984-2022:《信息安全技术 信息安全风险评估规范》

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

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

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

(5) GB/T 45288-2025:《人工智能 大模型》

(6) 《政务领域人工智能大模型部署应用指引》

2、网络安全等级保护测评内容

(1) 安全物理环境测评包括：物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等。

(2) 安全通信网络测评包括：网络架构、通信传输、可信验证。

(3) 安全区域边界测评包括：边界防护、访问控制、入侵检测、恶意代码防范和垃圾邮件防范、安全审计、可信验证。

(4) 安全计算环境测评包括：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据备份恢复、剩余

信息保护、个人信息保护。

(5) 安全管理中心测评包括：系统管理、审计管理、安全管理、集中管控。

(6) 安全管理制度测评包括：安全策略、管理制度、制定和发布、评审和修订；对涉及安全管理差距部分的整改，协助制定和完善各项安全管理制度。

(7) 安全管理机构测评包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

(8) 安全管理人员包括：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理。

(9) 安全建设管理测评包括：定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择。

(10) 安全运维管理测评包括：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、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、外包运维管理。

3、其他服务内容

(1) 风险评估及差距分析：对信息系统面临的安全风险进行总结分析，提供可行的整改建议或方案。

(2) 协助等级保护整改：根据整改建议书中的建议，指导用户进行相应的加固工作，协助完成测评整改工作。

(3) AI 智能体专项安全测评：对信息系统中涉及到的 AI 智能体，评估提示词、函数调用等特有风险，识别注入、越权、泄露等问题，提出整改并协助加固复测，确保风险闭环。

七、其他服务要求

1、项目人员配置要求

(1) 服务团队至少应配置 1 名项目负责人，项目负责人具有 5 年以上测评实施经验，全面负责本项目合同的履行、统筹项目全过程工作。

项目经理具有网络安全等级测评师高级资质证书及高级职称、具备中国信息安全测评中心颁发的注册信息安全专业人员（CISP）证书为优。

(2) 团队人员不少于 12 名（含项目经理）且不少于 5 人具有网络安全等级测评师高级（技术）资质证书；2.团队人员具有数据安全工程师证书不少于 3 人；3.团队人员具有高级职称的，不少于 2 人；4.团队人员具有注册信息安全专业人员（CISAW）证书的不少于 2 人。

(3) 项目团队应具有同类型项目经验，提供相关项目案例证明。项目团队需配备至少 1 名参与过大模型/智能体系统安全研究的人员，提供相关项目案例证明。

(4) 未经书面同意，项目参与人员不得随意更换。

(5) 供应商具有与网络安全测评有关的检测工具的，提供相应工具的计算机软件著作权登记证书或专利专有技术证明材料。

(6) 供应商具有 CCRC 信息安全服务资质认证证书（风险评估服务资质认证、网络安全审计服务资质认证或信息安全应急处理服务资质认

证) 为优

2、时间要求

(1) 项目承接方应制定清晰的项目进度计划。划分工作阶段, 明确每个工作阶段工作内容, 所需时间, 所安排的人员, 以及关键环节检查点或阶段性结案的标志性事件。

(2) 项目服务周期内, 针对采购人提出的本项目范围内的工作任务, 中标单位的响应不得超过 5 个工作日。

3、服务实施要求

(1) 在网络安全等级保护测评工作中发现相关安全风险问题应及时汇总并向用户反馈, 同时结合 GB/T-《信息系统等级保护基本要求》《人工智能 大模型》等技术标准, 提出信息系统问题整改意见, 督促和指导实施问题整改。

(2) 待相关问题整改完成后, 对整改情况进行复测, 确保满足相应安全标准要求。

(3) 承诺承接方应协助采购人起草《定级报告》《备案表》等备案材料, 并完成相关系统在公安机关的备案工作。

4、项目验收条件

(1) 提交信息系统等级保护测评报告和 AI 智能体专项安全测评报告, 该项目过程中产生的数据资产成果、文档等, 归采购人所有。

(2) 提交信息系统整改建议, 对涉及本项目测评的系统不符合有关管理规范和技术标准的, 投标方出具行之有效的整改方案并协助进行整改, 直至达到有关管理规范和技术标准, 并取得信息系统等级保护测评

报告和 AI 智能体专项安全测评报告。

5、项目风控要求

(1) 项目承接方应充分调研，确保项目实施安全，保障被测信息系统安全稳定运行。

(2) 项目承接方应严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，服从采购方的管理，严格遵守采购方的保密规定和工作制度，并承担相应的保密责任。所有参与本项目的服务人员，都必须签订保密承诺书。

(3) 项目承接方自觉接受采购方的安全保密监督和管理，项目承接方如违反安全保密条款，采购方将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任。

八、项目服务报价要求

(1) 报价依据：本项目采购需求明确的工作内容、工作范围和要求。

(2) 项目报价要求：投标人必须对以上全部采购内容及相关服务进行报价。根据相关收费标准以及市场行情并结合自身实力报出自身能够承受的闭口报价，请各投标人充分考虑今后工作中所包含的风险、责任后进行报价，报价必须是闭口包干，中标后不再调整。

(3) 投标人提供的服务，应当符合国家有关法律法规和标准规范，满足招标文件约定的服务内容和质量等要求。投标人不得违反标准规范规定或招标文件约定，通过降低服务质量、减少服务内容等手段进行恶

性低价竞争，扰乱正常市场秩序。

（4）中标单位有义务参与并协助采购人完成本项目验收，提供相关技术资料、合格证明等文件或材料，对服务过程中产出结果负责。

（5）如中标供应商实际提供服务与投标承诺的服务不一致，项目实施服务承诺无法完成，服务被使用方有效投诉，经查实中标供应商要承担相应违约责任。