公文系统安全等级保护测评、渗透测试项目

服务质量要求

1、等级保护测评

（1）信息系统备案

协助采购人按照《信息安全等级保护备案实施细则》（公信安[2007]1360号）文件要求，完成定级、备案材料的整理及在公安机关相关部门备案工作。

（2）初次测评

检查被测系统现状，参照《网络安全等级保护基本要求》（GB/T 22239-2019）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、安全管理中心和安全管理等层面对系统进行初次安全评估，通过对系统现状的分析和梳理，发现系统现有安全措施与等级保护基本要求的差距，形成差距分析；基于差距提出安全整改建议，以指导后续安全整改工作。

该阶段的测评内容包括：

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、电磁防护等内容。

安全通信网络测评：包括网络架构、通信传输、可信验证等内容。

安全区域边界测评：包括边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等内容。

安全计算环境测评：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、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等内容。

安全管理中心测评：系统管理、审计管理、安全管理、集中管控等内容。

安全管理制度测评：涵盖安全策略、管理制度、制定和发布、评审和修订。安全管理机构测评：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

安全管理人员测评：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。

安全建设管理测评：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。

安全运维管理测评：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）信息系统等保整改方案及建议

现场协助采购人按照《信息安全等级保护管理办法》（公通字[2007]43号）、《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）等有关管理规范和技术标准，制定安全管理制度、落实安全责任，建设安全技术设施，更改安全配置,增加安全策略,落实安全技术措施等。

通过安全建设整改，确保信息系统通过相应级别的安全等级评测。

（4）二次测评

此阶段是等级测评完整实施阶段，通过对整改后的系统进行分析和梳理，再次实施等级测评，记录访谈核查结果，进行综合分析，梳理安全风险，提出安全整改建议，测评结束后，按照《网络安全等级保护测评报告模板（2021版）》编写等级测评报告。

2、渗透测试

根据《中华人名共和国网络安全法》和《关键信息基础设施安全保护条例》中的要求，开展渗透测试，原则上立足于黑盒方式，模拟黑客的攻击思路与技术手段，从攻击者角度发现应用系统存在的安全隐患，检测相关系统的威胁防御能力，深度挖掘应用系统的安全漏洞，为采购人指定的应用系统提供渗透测试服务。

渗透测试工程师模拟黑客攻击，对网络系统信息系统进行渗透攻击尝试并验证相关漏洞，最终出具渗透测试服务报告，并指导采购人相关维护人员进行有针对性的安全加固。渗透服务包含但不限于：

（1）端口扫描、信息收集

对所要测试的服务器进行全端口扫描了解其开放的服务，对服务进行分析发现潜在的安全漏洞，对整体网络进行分析发现网络设计上存在的安全漏洞，对系统所暴漏的可用信息进行分析。分析、辨别网络结构查找入侵点。

（2）扫描、信息收集结果分析

分析扫描结果，对一些敏感信息进行整合，对网络拓扑情况进行分析，对所开放的服务进行排查，发现服务存在的安全漏洞，分析网络结构对可利用主机进行渗透，进一步提升权限，以达到控制网络目的。

（3）针对web服务器，分析网络结构设计是否合理

可以利用跳板对web服务器进行攻击；分析服务的版本，查找服务可能存在的漏洞；对web服务器存在的管理端口进行分析，查看是否有存在弱口令的可能性；分析web目录结构是否合理，是否存在漏洞；对web脚本进行分析查看是否存在sql注入漏洞、跨站脚本漏洞、会话管理漏洞、不安全的对象引用以及跨站请求伪造漏洞等。

供应商须配合采购人检验当前安全控制措施的有效性，针对发现的安全风险及时进行整改，增强系统自身防御能力，提升安全保障体系的整体健壮性。

供应商在渗透测试前必须提交《渗透测试方案》，并经采购人确认与授权。渗透测试后必须对每个系统编制《渗透测试报告》。在完成复测后，由供应商出具《渗透测试复测报告》，并经过采购人签字确认。