

高明区数字档案馆系统网络安全等级保护 测评服务需求

1. 项目概况

依据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》的相关要求，对高明区数字档案馆系统进行网络安全等级保护测评，包括：安全技术测评，安全管理测评，工具测试，编制系统安全整改方案，编制测评报告等。

2. 项目实施范围

本次实施网络安全等级保护测评的系统如下：

序号	待测系统名称	安全保护等级
1	高明区数字档案馆系统	三级

3. 指导思想和基本准则

根据公安部、国家保密局、国家密码管理局、国信办联合印发的《信息系统安全等级保护管理办法》（公通字〔2007〕43号）、《关于信息系统安全等级保护工作的实施意见》（公通字〔2004〕66号）、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861号）、公安部《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429号）等文件精神，结合高明区信息系统安全工作实际，现拟对高明区数字档案馆系统实施网络安全等级保护测评，以进一步完善信息系统安全管理体系和技术防护体系，切实提高系统信息安全防护能力。

4. 等级保护测评主要包括以下几个方面：

等保测评：完成包括安全物理环境、安全计算环境、安全区域边界、安全通信网络、安全管理中心和安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理方面的测评工作；

工具测试：针对重要信息系统进行漏洞扫描、渗透测试等安全服务工作；

整改建议：投标人应根据现场测评中发现的问题，分析与 GB/T 22239-2019、ISO/IEC 27001、ISO/IEC 20000、ISO 22301、ITIL 和 ITSS 等行业最佳实践之间的差距，按照网络安全等级保护标准要求提出安全整改建议；

编制测评报告：完成上述测评工作和整改加固实施后，投标人最后出具符合标准要求的信息系统网络安全等级保护测评报告。

5. 工作要求：

(1) 实施原则

规范性原则：成交供应商工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制；

标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

可控性原则：测评的工具、方法和过程需在双方认可的范围之内并符合进度表的安排，保证采购人对服务工作的可控性；

整体性原则：测评和分析的范围和内容应当整体全面，包括安全涉及各个层面，避免由于遗漏造成未来的安全隐患；

最小影响原则：测评工作应尽可能小的影响系统和网络的正常运行，不能对现网的运行和业务的正常提供产生显著影响(包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况应在应答

书上详细描述)；

保密原则：对测评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，不得利用此数据进行任何侵害采购人网络的行为，否则采购人有权追究责任。

(2) 测评依据

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

《信息安全技术 网络安全等级保护定级指南》(GB/T 22240-2020)

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

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

(3) 等级保护测评内容

根据国家等级保护相关标准，本次项目的网络安全等级保护测评应包括以下内容：

安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；

安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。

a) 安全物理环境

安全物理环境是对机房和办公场所的物理环境安全防护情况进行测评，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、电力供应和电磁防护等方面的安全状况。

b) 安全通信网络

安全通信网络测评是对网络系统安全防护情况进行测评，包括网

络架构、通信传输、可信验证等方面的安全状况。

c) 安全区域边界

安全区域边界是对边界防护、访问控制、入侵防范、恶意代码防范、安全审计、可信验证等方面的测评。

d) 安全计算环境

安全计算环境是对身份鉴别、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、个人信息保护等方面的测评。

e) 安全管理中心

安全管理中心是对系统管理、审计管理、安全管理、集中管控等方面的测评。

f) 安全管理制度

安全管理制度测评是对安全策略、管理制度、制定和发布、评审和修订进行测评。

g) 安全管理机构

安全管理机构测评是对岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

h) 安全管理人员

安全管理人员测评是对人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等情况进行测评。

i) 安全建设管理

安全建设管理测评是对建设过程中安全方案设计、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、服务供应商选择等情况进行测评。

j) 安全运维管理

安全运维管理测评是对环境管理、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、外包运维管理等情况进行测评。

6. 验收标准

本项目服务的验收将以成交供应商提交《测评报告》并在公安部登记管理系统填报结果为准。

7. 报价要求和付款说明

本项目报总价，报价包含完成本项目服务期间所产生的一切费用，采购人后期不再另行追加费用；本项目属区财政支付预算，需验收完成后才走支付流程，实际付款时间以财政批复为准（估计2024年）。