**采购需求**

（一）网络安全等级保护测评

根据国家安全评估、等级保护相关标准，等级保护测评应包括以下内容：

1.安全物理环境

物理安全测评是对信息系统机房和办公场所的物理环境安全防护情况进行测评，包括机房位置选址、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。

2.安全通信网络

网络安全测评是对信息系统网络系统安全防护情况进行测评，包括网络结构安全、网络访问控制、网络安全审计、网络边界完整性检查、网络入侵防范、网络恶意代码防范、网络设备防护等方面的安全状况。

3.安全区域边界

主机安全测评是对信息系统服务器、数据库和终端主机系统的安全防护情况进行测评，包括操作系统和数据库层面的身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、主机入侵防范、主机恶意代码防范、主机资源控制等方面的安全状况。

4.安全计算环境

应用安全测评是对信息系统业务系统的安全防护情况进行测评，包括应用系统层面的身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、应用系统的资源控制等方面的安全状况。

5.安全管理中心

数据安全及备份恢复测评是对信息系统数据安全保护情况进行测评，包括数据在传输和存储过程中的完整性、保密性措施，数据备份和恢复措施。

6.安全管理机构

安全管理机构测评是对信息系统安全管理组织和岗位设置、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。

7.安全管理制度

安全管理制度测评是对信息系统安全管理制度体系和制度内容、制定和发布流程、评审和修订机制等情况进行测评。

8.人员安全管理

人员安全管理测评是对协同办公系统相关内部人员的人员录用、人员离岗、人员考核、安全意识教育和培训，以及外部人员访问管理等情况进行测评。

9.安全建设管理

系统建设管理测评是对协同办公系统建设过程中的系统定级、安全方案设计、产品采购和使用、自主软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择等情况进行测评。

10.安全运维管理

系统运维管理测评是对协同办公系统运行维护过程中的环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等情况进行测评。

根据以上10个层面的现场测评结果出具《网络安全等级测评报告》。