**附件：**

**服务需求**

**1.定级备案**

协助采购人信息系统在网安部门完成定级备案工作，交付定级报告、专家评审意见表和备案表等内容，并取得相应系统的备案证明。

**2.等级保护测评**

依据国家等级保护相关标准《GB/T 22239-2008 信息系统安全等级保护基本要求》、《GB/T 28448-2008 信息系统安全等级保护测评要求》、《GB/T 22239-2019 网络安全等级保护基本要求》、《GB/T 28448-2019 网络安全等级保护测评要求》，以《GB/T 22240 信息系统安全等级保护定级指南》、《GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》为基础，结合ISO/IEC 27001、ISO/IEC 20000、ISO 22301、ITIL和ITSS等行业最佳实践对信息系统开展等级保护二级测评，内容包括：

2.1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；

2.2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、安全运维管理等五个方面的安全测评；

2.3工具测试：针对上述信息系统进行漏洞扫描、渗透测试等安全服务工作；

2.4整改建议：根据现场测评中发现的问题，分析与等级保护基本要求、ISO/IEC 27001、ISO/IEC 20000、ISO 22301、ITIL和ITSS等行业最佳实践之间的差距，按照信息安全等级保护标准要求提出安全整改报告；

2.5编制测评报告：完成上述测评工作和整改实施后，确保采购人等级保护达到二级水平，最后出具符合公安机关要求的信息系统网络安全等级保护测评报告。

**3.实施原则：**

3.1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招标人的行为，否则采购人有权追究中标人的责任。

3.2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。

3.3规范性原则：成交人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。

3.4可控性原则：测评服务的进度要跟上进度表的安排，保证采购人对于测评工作的可控性。

3.5整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

3.6最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内，测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

成交人应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

4.项目验收

4.1提交《信息系统等级保护整改建议》，对本次测评系统不符合信息安全等级保护有关管理规范和技术标准的，成交人出具行之有效的整改方案并协助采购人进行整改，并完成整改项的再次测评服务。

4.2提交《信息系统等级保护测评报告》，成交人协助采购人办理信息系统安全保护等级备案手续，并取得备案证书。该项目过程中产生的文档，归采购人所有。
 **5.报价要求：**

本项目按总价报价，其报价应包含为完成本项目所需的人工、物耗、设备、交通、保险、税费等可能发生的一切相关费用。一旦中标，其中标价不做任何调整。