**项目需求**

**一、项目概况**

根据《中华人民共和国密码法》《国家政务信息化项目建设管理办法》《江苏省省级政务信息化项目建设管理办法》《南通市市级政务信息化项目管理办法》等要求，结合项目建设总体规划，对市国有资产智慧监管平台开展商用密码应用安全性评估及风险评估工作，深入查找网络安全的薄弱环节和安全隐患，分析面临的风险，确保系统安全性。

**二、服务内容**

本项目为市国有资产智慧监管平台提供第三方安全测评服务，主要包括提供商用密码应用安全性评估（三级）、信息安全风险评估服务各一次，并出具测评报告。

1.商用密码应用安全性评估服务从《信息安全技术 信息系统密码应用基本要求》（GM/T 39786-2021）中选择相应等级的评估指标，结合信息系统的构成特点，确定具体的评估对象，制定评估方案，通过访谈、检查和测试等方式判断其安全技术和安全管理各层面所对应评估指标的符合程度，判断被评估系统在密码应用设计和落地方面是否满足符合国家信息系统商用密码应用安全中的合规性、正确性、有效性要求，找出与国家标准要求之间的差距，根据评估结果出具商用密码应用安全性评估报告，作为后续安全整改的依据，帮助其达到信息系统商用密码应用安全的要求。

具体评估内容

（1）密码技术应用测评：主要包括物理安全密码测评、网络安全密码测评、主机安全密码测评、应用安全密码测评、数据安全及备份恢复密码测评。测评验证不同安全等级信息系统的商用密码应用是否达到具有相应安全等级的安全保护能力，是否满足相应安全等级的保护要求；

（2）密钥管理测评：检测信息系统密钥管理各环节，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求；

（3）安全管理测评：对制度、人员、实施和应急等四个方面安全管理的测评，并指导采购人完善商用密码应用安全性管理制度以及和商用密码相关的系统运维管理制度；

（4）形成密码应用安全性评估相关报告：针对每个被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参考模板编制。协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性地加强完善密码安全管理和防护建议，指导并督促采购人现场信息系统供应商按照要求改进进行整改落实。

（5）根据被评估单位商用密码应用需求，提供相关密码应用技术咨询支持服务。

2.信息安全风险评估服务，按照GB/T 20984-2022《信息安全技术 信息安全风险评估方法》《江苏省信息安全风险评估管理办法（试行）》等规范文件要求，通过风险评估项目的实施，对信息系统的重要资产、资产所面临的威胁、资产存在的脆弱性、已采取的防护措施等进行分析，对所采用的安全控制措施的有效性进行检测，综合分析、判断安全事件发生的概率以及可能造成的损失，判断信息系统面临的安全风险，提出风险管理建议，为系统安全保护措施的改进提供参考依据。

**三、测评服务单位及人员要求**

测评服务单位要求：测评服务单位在测评过程中，需严格遵循保密原则，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害采购人利益。

人员要求：项目经理及测评技术人员应为本单位正式在职员工且均具有商用密码应用安全性评估人员培训合格证书的，测评技术人员不得少于3人。

**四、服务期限、地点与付款方式**

1.合同履行期限：具备测评条件后，40个工作日内完成。

2.服务地点：南通市财政局指定地点。

3.付款方式：合同签订后15个工作日内，支付合同总额的50%，供应商出具盖章版的《市国有资产智慧监管平台商用密码应用安全性评估报告》《市国有资产智慧监管平台信息安全风险评估报告》后15个工作日内，支付合同总额的50%。

**五、验收方式**

测评机构出具盖章版的《市国有资产智慧监管平台商用密码应用安全性评估报告》《市国有资产智慧监管平台信息安全风险评估报告》，视为验收通过。