湖北省商务厅外商投资企业“一站式”

招商及惠企服务综合应用平台项目

（密码测评）采购需求

一、基本要求

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《政务信息系统密码应用与安全性评估工作指南》（2020 版）、《信息系统密码应用测评要求》（GM/T 0115-2021）和《信息系统密码应用测评过程指南》（GM/T 0116-2021）等相关技术标准要求，由具有高级测评师证书或软件测试（高级）证书的人员协助其所有被测系统整改达到相应级别的标准和要求,对被测信息系统开展商用密码应用安全性评估（项目执行期间，如国家技术标准发生变化，按照新生效的技术标准执行），为湖北省商务厅开展密码应用方案设计，提供技术咨询及评估服务。

二、特殊资格要求

报价人须具备商用密码应用安全性评估的能力（投标人需在国家密码管理局公告（第42号）发布的《商用密码应用安全性评估试点机构目录》中或在省级密码管理局发布的《商用密码应用安全性评估试点工作机构名单》中）（提供有效期相关证明复印件加盖公章）。

三、服务内容

**（一）湖北省商务厅外商投资企业“一站式”招商及惠企服务综合应用平台项目密码应用方案评估服务**

1.依据《商用密码应用安全性评估管理办法（试行）》等技术标准要求对湖北省社会信用信息服务平台项目（二期）信息系统的密码应用设计方案或系统安全设计方案中的密码应用设计部分是否涵盖了所有需采用密码保护的核心资产及敏感信息，已设计的密码保护措施是否均能达到相应等级的密码使用要求或规定，并出具《密码应用方案评估报告》。

2.密码应用方案经过评估或者整改通过后，可进入系统建设阶段。密码应用方案经过评估后，上报主管部门审核，由密码管理部门备案。

3.备案材料需包含但不限于如下材料：

（1）《网络与信息系统密评备案信息表》

（2）《商用密码应用安全性评估报告》

（3）《商用密码应用方案》

4.协助采购人完成相关系统到当地密码局进行备案工作。

**（二）湖北省商务厅外商投资企业“一站式”招商及惠企服务综合应用平台项目各系统商用密码应用安全性评估服务**

1.商用密码应用安全性评估主要内容

按照《信息系统密码应用基本要求》，结合《信息系统密码测评要求》给出每个要求条款的测评实施方法。首先给出总体要求、典型密码产品应用、密码功能的测评实施方法，然后从密码技术应用的物理和环境、网络和通信、设备和计算、应用和数据、密钥管理及安全管理六个方面进行测评。测评过程分为四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。

2.密码应用基本要求

依据政策要求、技术标准和管理规范进行商用密码应用安全性评估服务，主要包括以下内容：

技术要求：物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全。

管理要求：管理制度、人员管理、建设运行、应急处置。

3.具体测评对象主要包括以下内容

（1）物理和环境安全测评

物理和环境安全对象应至少包括：身份鉴别、电子门禁记录数据完整性、监控记录数据完整性、密码服务等控制点。

（2）网络和通信安全测评

网络和通信安全对象应至少包括：身份鉴别、通信数据完整性、通信数据机密性、访问控制信息完整性、集中管理通道身份认证、密码服务等控制点。

（3）设备和计算安全测评

设备和计算安全对象应至少包括：身份鉴别、远程管理身份鉴别信息机密性、访问控制信息完整性、敏感标记完整性、日志记录完整性、重要程序或文件完整、性密码服务等控制点。

（4）应用和数据安全测评

应用和数据安全对象应至少包括：身份鉴别、访问控制信息完整性、安全标记完整性、数据传输安全、数据存储安全、数据传输完整性、数据存储完整性、抗抵赖、密码服务等控制点。

测评内容应至少包括：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、个人信息保护等控制点。

（5）管理要求安全测评

管理要求安全对象应至少包括：制度、人员、建设运行、应急处置等控制点。

**（三）总体要求**

如国家关于商用密码应用安全性评估测评方面的政策或技术标准发生变化，将按照新的政策和技术标准执行。提供针对该项要求的服务承诺书，加盖投标人公章。

**（四）综合要求**

1.测评实施过程中遵从以下原则

符合性原则：应符合国家密码应用安全性评估制度及相关法律法规。

标准性原则：方案设计、实施与密码应用安全体系的构建应依据国内、国际的相关标准进行。

规范性原则：项目实施应由专业的密码应用评估人员依照规范的操作流程进行，在实施之前将详细量化出每项评估内容，对操作过程和结果提供规范的记录，以便于项目的跟踪和控制。

可控性原则：项目实施的方法和过程要在双方认可的范围之内，实施进度要按照进度表进度的安排，保证项目实施的可控性。

整体性原则：密码应用安全性评估与安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

最小影响原则：项目实施工作应尽可能小的影响网络和信息系统的正常运行，不能对信息系统的运行和业务的正常提供产生显著影响。

保密原则：对项目实施过程获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害客户利益的行为。

同时，在密码应用安全性评估实施的过程中遵循以下原则：

客观性和公正性原则：虽然评估工作不能完全摆脱个人主张或判断，但评估人员应当没有偏见，在最小主观判断情形下，按照评估双方相互认可的评估方案，基于明确定义的评估方式和解释，实施评估活动。

经济性和可重用性原则：基于评估成本和工作复杂性考虑，鼓励评估工作重用以前的评估结果，包括商业安全产品评估结果和信息系统先前的安全评估结果。所有重用的结果，都应基于结果适用于目前的系统，并且能够反映出目前系统的安全状态基础之上。

可重复性和可再现性原则：不论谁执行评估，依照同样的要求，使用同样的评估方式，对每个评估实施过程的重复执行应该得到同样的结果。前者与不同评估者评估结果的一致性有关，后者与同一评估者评估结果的一致性有关。

结果完善性原则：评估所产生的结果应当证明是良好的判断和对评估项的正确理解。评估过程和结果应当服从正确的评估方法以确保其满足了评估项的要求。

2.项目质量管理。有项目质量控制及保证措施。投标人要提出质量控制及保证措施方案，要提出项目实施期间的信息系统及信息资源安全保障措施方案。

3.保密管理。对商用密码应用安全性评估或技术服务过程中获取的信息严格保密，包括但不限于采购人网络拓扑结构、IP地址、业务流程、业务数据、安全隐患等，未经授权不得泄露给任何单位和个人，不得利用保密信息进行任何侵害采购人的合法权益。

4.提供服务期保障承诺，并在服务期内提供安全管理及技术支持服务。

**（五）项目组人员资格**

1.项目经理具有国家商用密码应用安全性评估人员测评能力考核小组颁发的商用密码应用安全性评估人员证书或高级测评师证书或软件测试（高级）证书。

2.项目组成员具有国家商用密码应用安全性评估人员测评能力考核小组颁发的商用密码应用安全性评估人员证书。

**（六）项目组人员要求**

★投标人必须承诺，凡要求提供身份证及证书彩色扫描件的项目组人员必须为投标人实际项目组成员，且全程参与本项目实施。

**（七）投标人综合情况**

1.投标人具有信息安全风险评估服务资质证书或具有公安机关认可的攻防演练实验室平台。

2.投标人提供本地化应急响应服务承诺及证明材料，重要信息系统如若发生安全事件到场响应服务时间为1小时。