移动应用程序技术检测技术需求

中标供应商通过人工方式检测目标应用程序的数据安全防护能力、个人信息保护能力，发现潜在威胁，评估信息系统数据安全状况、个人隐私合规状况、权限风险状况。检测内容包括：

 1.数据安全检测：数据输入是否安全；数据传输是否安全；数据输出是否安全；是否设置数据访问控制；本地敏感信息存储是否安全；数据库信息存储是否安全；是否存在SQL注入漏洞；是否存在数据跨境情况；数据处理者收集的数据是否存储在境外。

 2.个人隐私违规检测：是否以默认选择同意隐私政策等非明示方式征求用户同意；是否超范围采集个人信息；是否公开收集使用规则；是否明示收集使用个人信息的目的、方式和范围；是否以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限；是否经用户同意收集使用个人信息；是否采取相应的加密、去标识化等技术处理个人信息；是否违反必要原则收集与其提供的服务无关的个人信息；是否未经同意向境外或他人提供个人信息；是否未经用户同意向第三方应用提供个人信息；是否利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；是否向用户提供撤回同意收集个人信息的途径、方式；收集个人信息类型或打开可收集个人信息权限是否与现有业务功能无关；收集个人信息的频度是否超出业务功能实际需要；是否提供有效的更正、删除个人信息及注销账号的功能；是否为更正、删除个人信息或注销用户账号设置不必要或不合理条件；是否因用户不同意提供非必要个人信息拒绝用户使用其基本功能服务；是否明确在个人信息采集过程中告知用户可能面临的风险；是否建立健全用户信息安全保护机制。

 3.权限风险检测：是否过度、强制、频繁索取权限；是否未经用户同意更改其设置的可收集个人信息权限状态；是否要求用户一次同意打开多个可收集个人信息的权限，用户不同意则无法使用。

 4.其他检测：是否按照“后台实名，前台自愿”的原则对注册用户进行基于移动号码等真实身份信息认证；是否依法保障用户在安装或使用过程中的知情权和选择权；以及其他违反《数据安全法》《个人信息保护法》《常见类型移动互联网应用程序必要个人信息范围》《移动互联网应用程序信息服务管理规定》《App违法违规收集使用个人信息行为认定方法》等内容。