## “互联网医院系统”

## 商用密码应用与安全性评估服务需求参数

**一．项目概况**

为落实商用密码保护制度，履行信息系统安全保护义务，根据《中华人民共和国网络安全法》、《中华人民共和国密码法》等法律法规和政策文件规定，拟对某单位的“某系统”开展商用密码应用与安全性评估查找不足以及存在的安全隐患，为后续的安全建设和整改工作提供依据。

**二．服务内容**

依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、GB∕T43206-2023 《信息安全技术 信息系统密码应用测评要求》、GB∕T 43207-2023《信息安全技术 信息系统密码应用设计指南》、GM∕T 0116-2021《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等相关测评标准，拟对“某系统”开展商用密码应用与安全性评估工作，查找不足以及存在的安全隐患，为我单位重要网络和信息系统的密码安全提供科学评价，逐步规范我单位相关人员密码使用和管理行为。

**（1）商用密码评估内容：**

从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面对信息系统密码应用进行检测评估，检测评估的内容包含但不限于以下内容：

1）物理和环境测评内容：身份鉴别、电子门禁记录数据的完整性、视频记录数据完整性、密码模块实现。

2）网络和通信测评内容：身份鉴别、内部网络安全接入(第四级信息系统要求)、访问控制信息完整性、通信数据完整性、通信数据机密性、集中管理通道安全、密码模块实现。

3）设备和计算测评内容：身份鉴别、远程管理鉴别信息机密性、访问控制信息完整性、敏感标记完整性、重要程序或文件完整性、日志记录完整性、密码模块实现。

4）应用和数据测评内容：身份鉴别、访问控制信息和敏感标记完整性、数据传输机密性、数据存储机密性、数据传输完整性、数据存储完整性、日志记录完整性、重要应用程序的加载和卸载、抗抵赖。

5）密钥管理测评内容：理清密钥流转的关系，对信息系统内的密钥(尤其是进出密码产品和密码模块的密钥)进行全生命周期的安全检查，包括密钥的生成、存储、分发、导入与导出、使用、备份与恢复、归档、销毁，确认所有密钥管理操作都是由符合GM/T0005《随机性检测规范》和GM/T0028《密码模块安全技术要求》规定的密码产品或密码模块实现。

6）安全管理测评内容：包括制度管理测评、人员管理测评、建设运行测评、应急处置测评。

**（2）服务交付物**

通过系统评估，及时发现系统脆弱性，识别变化的风险，了解系统安全状况。根据被评估对象的实际情况、所属行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以评估密码保障是否安全有效，密码使用是否合规、正确、有效。并通过测评发现系统存在的安全隐患和风险，提出可行性完善建议，编制《商用密码应用与安全性评估整改建议书》、《商用密码应用与安全性评估报告》。

**三．资质要求**

1、供应商必须在国家密码管理局公告（第42号）的商用密码应用安全性评估试点机构目录中或提供国家密码管理局《国密局字[2021]183号通知》中审批通过的“可在本地区、本行业（领域）开展密码应用安全性评估业资质的密评机构名单”的相关证明材料。提供证书或证明复印件并加盖公章；

2、供应商投入本项目的评估人员必须具有合格的商用密码应用安全性评估人员测评能力考核证书。

**四．人员配置**

投标人提供不少于5名具有商用密码应用安全性评估人员专业技术人员要求设项目经理1名、质量经理1名，在本项目进行期间，未经采购人同意，测评过程中不得离场，且中途不得更换人员，也不得将检测任务分包或转包。

**五．项目实施要求**

（1）客观性和公正性要求

在最小主观判断情形下，按照评估双方相互认可的测评方案,基于明确定义的测评方式和解释，实施测评活动。

（2）保密要求

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。

（3）最小影响要求

测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响(包括系统性能明显下降、网络阻塞、服务中断等)，如无法避免,则应预先做出说明并经采购人同意后实施。

（4）规范性要求

测评服务的实施必须由专业的测评服务人员依照规范的操作流程进行,对操作过程和结果要有相应的记录,并提供完整的服务报告。

（5）质量保障要求

在整个测评过程中,须特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行,并由项目协调小组从中监督,控制项目的进度和质量。