1.密评主要内容

1.1 测评概述

1.1.1 项目背景

为全面贯彻总体国家安全观和网络强国战略，做好国产密码应用推进工作，需要加强商用密码应用的工作部署和推进普及，在保证商用密码应用大力推广和普及的同时，做好网络与信息系统的商用密码应用安全性评估，确保商用密码应用的合规、正确、有效。

1.1.2 测评目的及范围

依据《信息系统密码应用基本要求》，针对目标系统从技术要求、密钥管理、安全管理三个角度出发，围绕信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全以及密钥管理、安全管理开展密码测评工作，以期发现信息系统与其相应安全等级要求之间的差距以及存在的安全隐患，为密码应用测评标准提供工作建议，保障信息系统密码合规、正确、有效地应用。

密码测评的目的是通过对目标系统在安全技术及管理方面的测评，对目标系统的安全技术状态及安全管理状况做出初步判断，给出目标系统在安全技术及安全管理方面与其相应安全等级要求之间的差距。测评结论作为采购人进一步完善系统安全策略及安全技术防护措施依据。

此次测评范围为：西安市全民健康信息平台升级建设项目的所有建设内容、

供应商需提供整改建议咨询服务。

1.1.3 测评依据

（1）法律法规：

《中华人民共和国密码法》

《中华人民共和国电子签名法》

《中华人民共和国网络安全法》

《中华人民共和国个人信息保护法》

《中华人民共和国数据安全法》

《商用密码管理条例》

《国家政务信息化项目建设管理办法》

《电子认证服务管理办法》

《信息安全等级保护商用密码管理办法》

（2）行业标准及其他依据：

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》

《商用密码应用安全性评估管理办法》

《商用密码检测机构管理办法》

《系统密码应用方案》

密码应用管理相关制度文件

1.1.4 测评原则

（1）客观公正原则

测评人员保证在最小主观判断情形下，按照双方认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

（2）经济性和可重用性原则

测评工作采信可重用已有测评结果中相同的检测项目，包括商用密码安全产品测评结果，信息系统密码测评结果和等级保护测评结果。所有重用结果都以结果适用于待测系统为前提，并能够客观反映目前系统的安全状态。

（3）可重复性和可再现性原则

依照同样的要求，使用同样的测评方法，在同样的环境下，不同的测评机构对每个测评实施过程的重复执行应得到同样的结果。可再现性和可重复性的区别在于，前者关注不同测评者测评结果的一致性，后者则与同一测评者测评结果的一致性有关。

（4）结果完善性原则

在正确理解《信息系统密码应用基本要求》各个要求项内容的基础之上，检测所产生的结果应客观反映信息系统的运行状态。测评过程和结果应服从正确的测评方法，以确保其满足要求。

1.2 密码应用安全性评估测评实施

1.2.1 测评目标

对信息系统所使用的密码算法、密码技术、密码产品、密码服务进行合规性测评。信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业

标准的有关要求;信息系统中使用的密码技术应遵循密码相关国家标准和行业标准；信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置对其密码应用基本要求进行测评，验证信息系统的商用密码应用基本要求是否达到其所对应网络安全等级保护级别的密码应用安全保护能力，是否满足对应安全等级的保护要求。

1.2.2 测评方法

1.2.2.1 测评方式

本次密评的主要方式有：访谈、文档审查、配置审查、工具测试、实地察看。

1.2.2.2 风险分析及防范措施

供应商应制定风险防范措施，针对测评阶段可能面临的风险制定风险规避措施，应包含测评环节各类常见风险。

1.3 测评内容（包括但不限于以下内容）：

1.3.1：包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个方面的安全测评。

（1）物理和环境安全

测评类别	**测评单元**
安全技术测评-物理和环境安全	身份鉴别
	电子门禁记录数据完整性
	视频记录数据完整性
	密码产品
	密码服务

（2）网络和通信安全

测评类别	**测评单元**
安全技术测评-网络和通信安全	实体鉴别
	通信数据完整性
	敏感信息或通信报文机密性
	网络边界访问控制信息完整性

	安全接入认证
	密码产品
	密码服务

（3）设备和计算安全

测评类别	测评单元
安全技术测评-设备和计算安全	实体鉴别
	安全的信息传输通道
	系统资源访问控制信息完整性
	重要信息资源安全标记完整性
	日志记录完整性
	重要程序或文件完整性
	密码产品
	密码服务

（4）应用和数据安全

测评类别	测评单元
安全技术测评-应用和数据安全	实体鉴别
	访问控制
	重要信息资源安全标记完整性
	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
	不可否认性
	密码产品
	密码服务

1.3.2.安全管理测评：包括安全管理（分为管理制度、人员管理、建设运行和应急处置四个子模块）的安全测评。

（1）管理制度

测评类别	测评单元
安全管理测评-管理制度	具备密码应用安全管理制度
	密钥管理规则
	建立操作规程
	定期修订安全管理制度
	明确管理制度发布流程
	制度执行过程记录留存

（2）人员管理

测评类别	测评单元
安全管理测评-人员管理度	了解并遵守密码相关法律法规和密码管理制度
	建立密码应用岗位责任制度
	建立上岗人员培训制度
	定期进行安全岗位人员考核
	建立关键岗位人员保密制度和调离制度

（3）建设运行

测评类别	测评单元
安全管理测评-建设运行	制定密码应用方案
	制定密钥安全管理策略
	制定实施方案
	投入运行前进行密码应用安全性评估
	定期开展密码应用安全性评估及攻防对抗演习

（4）应急处置

测评类别	测评单元
安全管理测评-应急处	应急策略

置	事件处置	
	向有关主管部门上报处置情况	

根据项目内容要求，以电子版或纸版形式按需求输出成果，并针对采购人的咨询进行及时反馈，方式不限于现场支撑、邮件、电话或报告。

密评现场工作完成后，立足于测评获取的数据记录、证据文件、信息资料等，对评估发现的问题提出整改建议，并按照国家密码管理局要求包含的内容或参考模板编制交付正式的密码应用安全性评估报告。

该项目提交的文档包括但不限于：

（1）提交相关系统的《商用密码应用安全性评估报告》；

（2）整改建议书；

（3）其他服务资料等。

提交形式：纸质资料一式三份，电子版资料一份。

服务期限内，提供密码应用安全性评估相关问题的咨询；协助采购人进行密码应用安全性评估相关备案、培训等工作。

二.密评服务要求

1.密评工作原则

遵循以下若干原则，是评估结论真实、准确、可信的基础，也是评估组在独立实施评估时，在相似的情况下得出相似结论的前提。本次商用密码应用安全性测评实施方案设计与具体实施应满足以下原则：

（1）客观公正原则：评估实施过程中评估人员应保证在最小主观判断情形下，按照评估双方认可的评估方案，基于明确定义的评估方式和解释，实施评估活动。

（2）经济性和可重用性原则：评估工作可重用已有评估结果，包括商用密码应用安全性评估结果。所有重用结果都应以结果适用于待评估系统为前提，并能够客观反映目前系统的安全状态。

（3）可重复性和可再现性原则：依照同样的要求，使用同样的评估方法，不同的评估机构对每个评估实施过程的重复执行应得到同样的结果。可再现性和

可重复性的区别在于，前者关注不同评估者评估结果的一致性，后者则与同一评估者评估结果的一致性有关。

（4）结果完善性原则：在正确理解《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》各个要求项内容的基础之上，检测所产生的结果应客观反映系统的运行状态。评估过程和结果应服从正确的评估方法，确保其满足要求。

2.密评服务总体要求

（1）供应商应详细描述本次项目的整体实施方案，包括项目概述、密评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

（2）供应商应详细描述实施人员的组成、资质及各自职责的划分。供应商应配置有经验的技术人员进行本次项目实施。

（3）本次项目实施过程中所使用到的各种工具软件由供应商推荐，经采购人确认后由供应商提供并在项目中使用。在响应文件中应详细描述所使用的安全技术工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

（4）本次项目实施过程中所使用到的测评工具，应包括自主密码专用检测工具、漏洞扫描工具等获得许可的检测工具，对系统数据进行分析，并以分析结果辅证评估报告。

（5）安全技术工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等） 和操作系统软件等由供应商推荐，经采购人确认后由供应商提供并在项目中使用。

（6）项目实施需要的运行环境（如场地、网络环境等）由采购人提供，供应商应详细描述需要的运行环境的具体要求。

3.密评服务过程及实施要求

密评服务过程包括四项基本测评活动：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。测评机构与建设单位之间的沟通与洽谈应贯穿整个测评过程。

（1）测评准备活动

本活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制密评方案做好准备。

（2）方案编制活动

本活动是开展测评工作的关键活动，主要任务是确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容等，形成详实的密评方案，为实施现场测评提供指导依据。

（3）现场测评活动

本活动是开展测评工作的核心活动，主要任务是根据密评方案分步实施所有测评项目，以了解被测信息系统真实的密码应用现状，获取足够的证据，发现其存在和潜在的密码应用安全性问题。

（4）分析与报告编制活动

本活动是给出测评工作结果的活动，主要任务是根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的有关要求，通过单元测评、整体测评、量化评估和风险分析等方法，找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统所面临的风险，从而给出各个测评对象的测评结果和被测信息系统的评估结论，形成密评报告。

密评各阶段详细的服务内容如下表：

序号	测评阶段	测评类别	服务说明
1	评估准备	准备阶段	编制项目计划书、收集被测系统基本资料并完成调查表格，分析调查结果，准备工具和评估表单
2	方案编制	评估方案编制	识别并描述被测系统基本情况、确定测评对象、资产和威胁评估、系统定级结果和测评指标、确定检查点和检查方法、确定单元测评内容，提交成果物《密评测评方案》
3	总体测评	总体要求	通过访谈、配置检查和工具测试的方式评估信息系统的密码算法、密码技

			术、密码产品和密码服务的合规性
4	安全技术测评	物理和环境安全	通过访谈、配置检查和工具测试的方式测评信息系统机房环境的安全情况。主要涉及对象为机房环境的电子门禁系统。本次评测包括电子门禁的身份鉴别和电子门禁记录的完整性保护。
		网络和通信安全	通过访谈、配置检查和工具测试的方式测评信息系统的网络和通信安全保障情况。本次重点测评包括通信对象的身份鉴别、访问控制信息完整性、通信数据完整性和通信数据机密性等
		设备和计算安全	通过访谈、配置检查和工具测试的方式测评信息系统的主机安全保障情况，本次重点测评包括本地主机和数据库服务器身份鉴别、远程管理身份鉴别身份信息机密性、访问控制信息完整性、敏感标记完整性、日志记录完整性等
		应用和数据安全	将通过访谈、配置检查的方式测评信息系统的数据安全保障情况，主要涉及对象为信息系统的管理数据及业务数据等,本次重点测评包括信息系统身份鉴别、访问控制信息完整性、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、日志记录完整性等
5	安全管理测评	安全管理	安全管理部分为全局性问题，涉及密码安全管理制度、密码安全管理人

			员、系统实施和系统应急管理等四个方面。
6	分析报告阶段	报告编制	根据测评编制《信息系统商用密码应用安全性评估报告》，包括：概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评的结果记录及结果汇总、整体测评、测评结果汇总、风险分析、评估结论等内容。提交成果物《信息系统商用密码应用安全性评估报告》

4.保密要求

供应商必须和采购人签订保密协议，供应商必须要与参加此次项目的所有项目组成员签订保密协议，在合同签订时一并提供给采购人。

供应商具体实施项目中的重要资料和结果，在项目实施期间和实施结束后，供应商不得带离该地点。

供应商对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论供应商中标与否，其对上述内容的保密责任将长期存在。