采购需求

序号	参数性质	技术参数与性能指标
1		一、服务内容 完成省级全民健康信息平台能力提升项目（一期）卫生健康智慧大脑、检查检验结果互认系统、居民电子健康档案查询系统、数字管理与决策分析系统、死亡信息管理系统5个信息系统的密码应用安全性评估工作。 二、技术部分 1、在商用密码应用安全性评估项目实施过程中，需按照国家商用密码测评的相关规范及标准进行测评，出具符合规范的《密码应用安全性评估报告》，并协助被测评单位及相关技术支撑单位落实密码应用安全整改工作。 2、密码测评服务要求 商用密码应用安全性评估（简称“密评”），即对采用商用密码技术、产品和服务所集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。本项目针对如下5个系统：卫生健康智慧大脑、检查检验结果互认系统、居民电子健康档案查询系统、数字管理与决策分析系统、死亡信息管理系统开展密评工作。 密评工作的主要目的是评估系统在密码应用和管理方面的合规性、正确性和有效性，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、管理制度、人员管理、建设运行和应急处置等方面进行密码应用安全性评估，通过测评项目的实施，根据被测信息系统安全状况，给出测评结果并提出改进建议，以确保被测信息系统达到《信息安全技术信息系统密码应用基本要求》，也为其信息资产安全和业务持续稳定运行提供保障。 2.1密评工作技术要求 商用密码应用安全性评估工作依据《信息安全技术信息系统密码应用基本要求》《信息系统密码应用测评要求》《信息系统密码应用测评过程指南》等技术要求，逐一对信息系统进行密码应用的合规性、正确性、有效性进行安全性评估，通过商用密码应用安全性评估深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全奠定基础。工作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。测评双方之间的沟通与洽谈贯穿整个测评过程。 （1）测评准备活动：本活动是开展测评工作的前提和基础，本活动的主要任务是掌握被测系统的详细情况，准备测评工具，为编制测评方案做好准备。 （2）方案编制活动：本活动是开展测评工作的关键活动，本活动的主要任务是确定与被测系统相适应的测评对象、测评指标及测评内容等，形成测评方案，为实施现场测评提供依据。 （3）现场测评活动：本活动是开展测评工作的核心活动。主要任务是按照测评方案的总体要求，分步实施所有测评项目，包括单项测评、测评单元和整体测评等方面，以了解系统的真实保护情况，获取足够证据，发现系统存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，是总结被测系统商用密码整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《信息系统密码应用基本要求》（GM/T 0054-2018）等文件

		的有关要求，通过单项测评结果判定、测评单元结果判定、整体测评和风险分析等方法，找出整个系统商用密码的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出测评结论，形成测评报告文本。 （5）整改咨询阶段：建设整改咨询工作以测评发现的问题为重点，编写信息系统密评整改建议；开展建设整改工作时，投标人提供建设整改相关的咨询服务。 2.2 密评工作测评内容 密码测评内容应至少包括《信息安全技术信息系统密码应用基本要求》《信息系统密码应用测评要求》《信息系统密码应用测评过程指南》中关于三级系统的测评内容指标。 2.3 密评工作服务总体要求 （1）投标人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）本项目要求密评人员不少于 5 人。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）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）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。 2.4 实施原则 为保障项目的顺利实施，在项目实施过程须遵循以下原则： （1）规范性原则 加强项目管理，在人员、质量和时间进度等方面进行严格管控。 （2）标准化原则 测评过程须严格遵守国家的相关法律、法规、规范、标准等相关要求。 （3）完整性原则 在测评过程中，必须确保测评数据、过程记录的完整性。评测内容要综合考虑所有评测对象的技术措施，并建立完整有效的评测流程，保证不存在影响评测结果的疏忽或遗漏。 （4）保密性原则 在测评过程中，切实加强对人员、技术等方面的组织管理；与所有相关人员签署具有法律意义的保密协议，确保在项目实施过程中涉及的所有信息，不会泄露给第三方单位或个人，不得擅自利用这些信息。供应商的任何工作人员均须与被测单位签署《保密承诺书》，对知悉的事项及信息予以保密，所有资料、技术文档应妥善保管，不得遗失、转借、复印，不得以任何形式向第三方透露；所有密码应用解决方案和采集汇总后的数据严禁通过互联网等公共信息网络、普通邮政进行传递，严禁在连接互联网计算机存储、处理。 （5）影响最小原则 在项目实施的过程中，须充分考虑到相关活动对系统正常运行的不利影响，采取必要的措施将相关风险降到最低。 2.5 密评工作交付 根据项目内容要求，以电子版或纸版形式按需求输出成果，并针对省卫生健

		康信息中心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。 主要产出交付物包括但不限于： 《商用密码应用安全性评估实施方案》； 《商用密码应用安全性评估测评方案》； 《商用密码应用安全性评估报告》； 《调研记录》（按系统提供）； 《培训计划》《培训讲义》； 《整改建议报告》； 三、售后服务 为期一年的售后服务工作中，供应商将向省卫生健康信息中心业务系统提供包括应急响应、安全监测、配合检查、电话支持、安全咨询等服务在内的安全维保服务。具体服务内容如下： （1）应急响应服务 供应商提供 7*24 小时常规应急响应及灾难恢复专家服务。在接到用户故障报修电话 10 分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。 （2）配合检查服务 供应商协助省卫生健康信息中心响应相关部门针对信息系统密评工作的检查工作。服务内容包括协助省卫生健康信息中心业务系统准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。 （3）电话支持服务 每周 7*24 小时不间断的电话支持服务，解答省卫生健康信息中心业务系统在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过 10 分钟，到达现场时间不超过 2 小时，解决问题不超过 24 小时。 （4）安全咨询服务 供应商为省卫生健康信息中心业务系统提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合省卫生健康信息中心业务系统做好业务系统安全保障工作。