**信息系统商用密码应用安全性评估服务项目技术需求**

|  |  |
| --- | --- |
| **项目名称** | 信息系统商用密码应用安全性评估服务 |
| 1. **项目概述**   按照《中华人民共和国密码法》、《商用密码管理条例》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、《信息系统密码测评要求》、《商用密码应用安全性评估管理办法》等法规和标准，委托商用密码应用安全性评估机构定期对信息系统密码应用的合规性、正确性和有效性等进行评估。其中，网络安全保护等级第三级及以上信息系统，每年至少进行一次商用密码应用安全性评估。  “HIS系统、LIS系统、PACS系统”作为重要信息系统，需要进行国产密码应用、改造工作，满足国家相关政策和标准要求。根据“同步规划、同步建设、同步运行”的原则，需对管理、运营、使用的信息系统进行商用密码应用安全评估。经研究，我单位拟通过购买测评服务方式对“HIS系统、LIS系统、PACS系统”开展密码应用安全性评估，对医院信息系统密码应用改造方案进行评审，并出具评审意见，宣传普及密码应用政策要求，掌握信息系统密码应用情况，分析研究、归纳梳理、发现密码应用存在的问题，提出下一步整改举措和推动落实，推动密码应用水平不断提升。  供应商须对我院提供的商用密码应用方案进行评估，出具符合商用密码应用安全性评估主管部门要求的方案评估报告，并通过国家密码管理部门备案。  项目建设完成，供应商须对我院系统进行商用密码应用安全性评估，并出具符合商用密码应用安全性评估主管部门要求的“商用密码应用安全性评估报告”，并通过国家密码管理部门备案并取得回执。 | |
| 1. **供应商资格条件**   （一）具有独立承担民事责任的能力；  （二）具有良好的商业信誉和健全的财务会计制度；  （三）具有履行合同所必需的设备和专业技术能力；  （四）有依法缴纳税收和社会保障资金的良好记录；  （五）参加政府采购活动前三年内，在经营活动中没有重大违法记录；  （六）法律、行政法规规定的其他条件；  （七）供应商单位及其现任法定代表人、主要负责人不得具有行贿犯罪记录的；  **（八）本项目的特定资格要求：**供应商在国家密码管理局《商用密码应用安全性评估试点机构目录》（国家密码管理局公告第42号文）内，或在国家密码管理局《可在本地区、本行业（领域）开展密评试点工作的机构名单》（国密局字[2021]183号文附件2）内。  （九）本项目不允许联合体投标； | |
| 1. **采购项目的技术需求（项目技术及规格参数）**   本采购项目的技术需求（项目技术及规格参数）详见附件一。 | |
| **4、售后服务要求**   1. 提供商用密码应用安全性评估相关的优化、整改建议方案。 2. 提供7×24小时电话咨询服务，必要时，工作日2小时内上门服务，非工作日4小时内上门服务。 | |
| **5、交货时间及地点，付款方式**  服务地点：业主指定地点。  服务时间：合同生效之日起至项目测评工作全部完成。  付款方式：  （1）双方签订合同生效后，甲方收到乙方开具合同金额30%的发票后10个工作日内，甲方向乙方支付合同价款总额30%的款项；  （2）商用密码应用方案评估完成后，甲方收到乙方出具的符合商用密码应用安全性评估主管部门要求的方案评估报告，并通过国家密码管理部门备案后，甲方收到乙方开具合同金额剩余30%的发票后10个工作日内，甲方向乙方支付合同价款总额30%的款项。  （3）项目建设完成进行系统商用密码应用安全性评估后，乙方出具符合商用密码应用安全性评估主管部门要求的“商用密码应用安全性评估报告”，协助甲方通过国家密码管理部门备案并取得回执后，甲方收到乙方开具合同金额剩余40%的发票后10个工作日内，甲方向乙方支付合同价款总额40%的款项。 | |

**附件一：商用密码应用安全性评估服务项目技术需求**

一、项目服务要求及内容

（一）总体要求

严格按照《中华人民共和国密码法》、《商用密码管理条例》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、GM/T0054《信息系统密码应用基本要求》、《信息系统密码测评要求》、《商用密码应用安全性评估测评过程指南》、《商用密码应用安全性评估测评作业指导书》、《商用密码应用安全性评估测评工作使用需求说明》和相关国家标准和密码行业标准，高质量完成被测信息系统的密码应用安全性评估工作和密码应用改造方案的评审工作。

（二）评估对象

根据相关法律法规，对表中项目进行商用密码应用安全性评估。

|  |  |  |
| --- | --- | --- |
| 序号 | 被测系统名称 | 网络安全  等级要求 |
| 1 | HIS系统 | 三级 |
| 2 | LIS系统 | 三级 |
| 3 | PACS系统 | 三级 |

（三）服务内容

* 根据密码应用与安全性评估要求，对医院信息系统密码应用改造方案进行评审，并出具评审意见
* 对被评估对象开展商用密码应用安全性评估服务，内容如下:

1、密码应用总体要求测评

（1）密码算法合规性测评

系统中使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。

（2）密码技术合规性测评

系统中使用的密码技术是否遵循密码相关国家标准和行业标准。

（3）密码产品合规性测评

系统中使用的密码产品与密码模块是否通过国家密码管理部门核准。

（4）密码服务合规性测评

系统中使用的密码服务是否通过国家密码管理部门许可。

2.密码应用技术要求测评

（1）物理和环境安全测评

是否使用密码技术的真实性服务来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性；

是否使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性；

是否使用密码技术的完整性服务来保证视频监控音像记录的完整性。

（2）网络和通信安全测评

是否在通信前基于密码技术对通信双方进行身份认证,使用密码技术的机密性和真实性服务来实现防截获、防假冒和防重用,保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；

是否使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性；

是否采用密码技术保证通信过程中数据的完整性；

是否采用密码技术保证通信过程中敏感信息字段或整个报文的机密性；

是否采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。

（3）设备和计算安全测评

是否使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

在远程管理时，是否使用密码技术的机密性服务来实现鉴别信息的防窃听；

是否使用密码技术的完整性服务来保证系统资源访问控制信息的完整性；

是否使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性；

是否采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护；

是否使用密码技术的完整性服务来对日志记录进行完整性保护。

（4）应用和数据安全测评

是否使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；

是否使用密码技术的完整性服务来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；

是否采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

是否采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

是否采用密码技术保证重要数据在传输过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；

是否采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；

是否使用密码技术的完整性服务来实现对日志记录完整性的保护；

是否采用密码技术对重要应用程序的加载和卸载进行安全控制。

3.密钥管理测评

对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程进行测评：

（1）密钥生成测评

密钥生成使用的随机数是否符合《GM/T 0005-2012 随机性监测规范》的要求，密钥是否在符合《GM/T 0028-2014 密码模块安全技术要求》的密码模块中产生；密钥是否在密码模块内部产生，不得以明文方式出现在密码模块之外；是否具备检査和剔除弱密钥的能力。

（2）密钥存储测评

密钥是否加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥是否存储在符合《GM/T 0028-2014 密码模块安全技术要求》的二级及以上密码模块中。

（3）密钥分发测评

密钥分发是否采取身份鉴别、数据完整性、数据机密性等安全措施，是否能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

（4）密钥导入与导出测评

是否采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

（5）密钥使用测评

密钥是否明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前是否对其进行验证；是否有安全措施防止密钥的泄露和替换；密钥泄露时，是否停止使用，并启动相应的应急处理和响应措施。是否按照密钥更换周期要求更换密钥；是否采取有效的安全措施，保证密钥更换时的安全性。

（6）密钥备份与恢复测评

是否制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复是否进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

（7）密钥归档测评

是否采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档是否进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥是否进行数据备份，并采用有效的安全保护措施。

（8）密钥销毁测评

是否具有在紧急情况下销毁密钥的措施。

4.安全管理测评

（1）制度测评

是否制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度是否包括密码建设、运维、人员、设备、密钥等密码管理相关内容；

是否定期对密码安全管理制度的合理性和适用性进行论证和审定,对存在不足或需要改进的安全管理制度进行修订；

是否明确相关管理制度发布流程。

（2）人员测评

是否了解并遵守密码相关法律法规；

是否能够正确使用商用密码产品；

是否根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用；

是否建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度；

是否建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训；

是否建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

（3）实施测评

规划测评

系统规划阶段，责任单位是否依据密码相关标准，制定密码应用方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。

建设测评

是否按照国家相关标准，制定实施方案，方案内容是否包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等；是否选用的经国家密码管理部门核准的密码产品、许可的密码服务。

运行测评

系统投入运行前，是否经密码测评机构进行安全性评估，评估通过方可投入正式运行；信息系统投入运行后，责任单位每年是否委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，是否停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。

（4）应急测评

是否制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置；事件发生后，是否及时向信息系统的上级主管部门进行报告；

事件处置完成后，是否及时向同级的密码主管部门报告事件发生情况及处置情况。

5.其他服务

在需评估的项目建设工作中，提供相关咨询服务。

二、项目涉及系统基本情况

|  |  |  |
| --- | --- | --- |
| 序号 | 被测系统名称 | 系统主要内容 |
| 1 | HIS系统 | HIS是一个综合性的管理系统，负责医院内部的各类信息处理，包括病人的就诊记录、预约挂号、住院管理、收费结算、药品管理、检验检查等，能够提升医院运营效率，优化资源配置，提供便捷的医疗服务和管理支持。 |
| 2 | LIS系统 | LIS专注于实验室的管理，包括检验样本的接收、处理、分析、报告生成等。它帮助实验室管理检验数据和结果，自动化生成报告，并将结果传送给HIS系统。HIS能够提高实验室检验流程的效率，确保检验结果的准确性和及时性，支持医务人员做出诊断决策。 |
| 3 | PACS系统 | PACS（图像归档和通信系统）：PACS是用于存储、管理和传输医学影像数据，如X光片、CT扫描、MRI等。医生和医疗人员可以更方便的查看和分析医学影像。它还能减少对传统影像存储介质的依赖，提高影像存取和分析的效率，支持远程诊断和协作。 |

三、验收方法和标准

1.所有系统评估完成，出具评估报告并提交相关部门通过后，供应商向采购人提交验收申请及相关资料，采购人组织相关人员进行验收。项目验收时，供应商需向采购人提供项目所有文档资料。

2.验收标准：按国家有关规定以及采购文件的质量要求和技术指标、供应商的响应文件及承诺与本合同约定标准进行验收。

3.其他未尽事宜应参照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》(财库〔2016〕205 号)、《四川省政府采购项目需求论证和履约验收管理办法》(川财采〔2015〕32 号)、《四川省省级政务信息化项目管理办法》的要求委托第三方机构进行验收。

四、安全保密要求

供应商在项目实施期间,从采购人获取的任何资料和重要信息，均有保密责任。未经采购人事先书面授权，不得以任何方式向任何其他组织或个人泄露、转让、许可使用、交换、赠与或与任何组织或个人共同使用或不正当使用。

供应商需对其所有参与人员进行保密安全审查，审查结果报采购人备案；供应商所有参与人员必须严格遵守《中华人民共和国保守国家秘密法》等一系列安全保密法规、制度和规定，必须与采购人签署《保密承诺书》，接受保密教育培训。

五、知识产权

1.供应商应保证在本项目使用的服务和产品（包括部分使用）或其任何一部分时，均不会侵犯任何第三方的专利权、商标权或著作权，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。

2.采购人享有本项目实施过程中产生的知识成果及知识产权。

3.（若有）供应商在项目实施过程中采用的自有知识成果，需承诺提供无限期技术支持，采购人享有永久使用权。

4.如采用供应商所不拥有的知识产权，则供应商必须提供合法获取该知识产权的相关证明，且所产生的相关费用由供应商承担。

|  |  |
| --- | --- |
| **厂商基本信息表** | |
| 产品相关产业发展情况（请详述全国产业情况及本公司发展情况） | 文字描述  1.全国情况：  2.本公司情况： |
| 产品市场供给情况（简述本公司年供给情况，且另附佐证材料） | 文字描述 |
| 同类产品成交情况（进三年的成交情况，且另附佐证材料） | 文字描述 |
| 公司企业类型（另附佐证材料） | 大型企业（ ） 中型企业（ ） 小型企业（ ） 微型企业（ ） 监狱企业（ ） 其他 注：“是”打√ |

**厂家（商）：盖公章**

**日期： 年 月 日**

成都市第二人民医院

信息系统商用密码应用安全性评估服务项目报价表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目 | 内容 | 用途 | 报价  （万） | 备注 |
| 信息系统商用密码应用安全性评估服务项目 | 详见系统需求。 | 供应商须对我院提供的商用密码应用方案进行评估，出具符合商用密码应用安全性评估主管部门要求的方案评估报告，并通过国家密码管理部门备案。  项目建设完成，供应商须对我院系统进行商用密码应用安全性评估，并出具符合商用密码应用安全性评估主管部门要求的“商用密码应用安全性评估报告”，并通过国家密码管理部门备案并取得回执。 |  |  |

报价公司：

联系方式：

日期：

成都市第二人民医院

信息系统商用密码应用安全性评估服务项目建设方案

（模板）

需求xxx

1．需求xxx

回复：（是/否完全响应）

具体方案：

2.需求xxx

回复：（是/否完全响应）

具体方案：

3.需求xxx

回复：（是/否完全响应）

具体方案：

二、其它