广西壮族自治区南溪山医院2024年等保密保测评项目采购需求

**一、项目概况**

 **本项目分为广西壮族自治区南溪山医院等级保护测评及咨询、商用密码安全性测评及咨询两部分。具体如下:**

第1项：等级保护测评及咨询。根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》相关规定，为了贯彻落实国家网络安全等级保护制度的要求，进一步增强系统安全防护能力，确保系统安全稳定运行。广西壮族自治区南溪山医院计划采购针对2个等级保护系统开展安全等级保护测评服务，对2个实施中的系统开展专家论证定级备案工作，衡量等级保护对象是否达到相应等级的安全保护能力，完成相关定级备案工作和出具公安机关认可的的网络安全等级保护测评报告。

第2项：商用密码安全性测评及咨询。根据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）等法律法规和政策文件规定，为落实商用密码保护制度，履行信息系统安全保护义务和系统自身的安全需求分析，拟对我院的“医院HIS信息系统（三级）、互联网医院系统（三级）”进行商用密码应用安全性评估，查找不足以及存在的安全隐患，衡量保护对象是否达到相应等级的安全保护能力，并出具密码局认可的商用密码应用安全性评估测评报告，为后续的安全建设和整改工作提供依据，逐步规范网络运营者的密码使用和管理行为。

 **以上项目涉及按必要流程组织邀请第三方组织、人员所产生的费用，由中标方承担。**

**二、采购标的清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项次 | 信息系统 | 服务内容 | 数量 | 单位 |
| 1 | 医院HIS信息系统（三级） | 等级保护测评及等级保护咨询工作 | 1 | 个 |
| 互联网医院系统（三级） | 等级保护测评及等级保护咨询工作 | 1 | 个 |
| 体检系统 | 专家论证定级备案工作 | 1 | 个 |
| 重症系统 | 专家论证定级备案工作 | 1 | 个 |
| 2 | 医院HIS信息系统（三级） | 商用密码应用安全性测评服务及咨询工作 | 1 | 个 |
| 互联网医院系统（三级） | 商用密码应用安全性测评服务及咨询工作 | 1 | 个 |

**三：第一项服务需求一览表**

|  |
| --- |
| **技术服务要求** |
| **★1、总的要求**1.1 完成2个系统（体检系统、重症系统）的定级备案包括组织专家，收集材料及专家评审意见，取得《备案证》；1.2 完成系统需求清单里面2个三级系统（医院HIS信息系统、互联网医院系统）的风险梳理，根据评估结果出具《整改问题清单》；1.3 根据安全整改结果，2个三级系统（医院HIS信息系统、互联网医院系统）完成网络安全等级测评及等级保护咨询工作，并提交符合国家信息安全等级保护主管部门要求的《网络安全等级保护测评报告》；**2、标准依据**《计算机信息系统安全保护等级划分准则》（GB 17859-1999)《网络安全等级保护基本要求》（GB/T 22239-2019）《网络安全等级保护测评要求》（GB/T 28448-2019）《网络安全等级保护测评过程指南》（GB/T 28449-2018)《网络安全等级保护设计技术要求》（GB/T 25070-2019）《网络安全等级保护测试评估技术指南》（GB/T 36627-2018）《信息系统安全等级保护定级指南》（GB T 22240-2020）《信息安全技术网络基础安全技术要求》《信息安全技术操作系统安全技术要求》《信息安全技术信息系统通用安全技术要求》《信息安全技术数据库管理系统安全技术要求》《信息安全技术服务器技术要求》《信息安全技术终端计算机系统安全等级技术要求》除上述规范以外，还遵循国家现行的相关标准和规范要求。**3、项目遵循原则：**符合性原则：符合国家信息安全等级保护制度及相关法律法规，指出防范的方针和保护的原则。标准性原则：方案设计与建议依据国内、国际的相关标准进行。整体性原则：方案中的安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。保密原则：对方案中获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害用户单位利益的行为。**★4、服务内容要求**4.1 按等保最新要求开展体检系统、重症系统的定级备案，包括组织专家，收集材料及专家评审意见，完成定级备案工作。4.2 针对医院HIS信息系统、互联网医院系统按等保最新要求开展网络安全等级保护测评工作，直到完成年度测评。4.3 针对各系统网络安全工作中所需要进行的定级备案、制度体系等开展咨询工作，建立和完善制度体系及相关记录。4.4 风险梳理要求，对我院被测信息系统所在的网络环境开展资产整理、风险评估、渗透测试等工作，以分析信息系统当前风险状况，进行差距分析，以明确等级保护整改需求和重点。风险梳理后需提交《差距分析报告》《问题整改清单》给我院。4.5等级保护测评要求：根据《信息系统安全等级保护基本要求》（GB/T22239-2019）等标准对我院被测信息系统开展等级保护符合性测评，衡量我院被测信息系统的安全保护管理措施和技术措施是否符合等级保护基本要求，是否具备相应的安全保护能力。依据被测信息系统的安全保护等级，通过人员访谈、文档查、实地察看、配置检查、工具检测等方法从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面，判断信息系统现有的安全保护水平与国家信息安全等级保护管理规范和技术标准要求项之间的符合情况。对被测信息系统进行整体、全面、公正的评估，对不符合项进行风险分析，编写《网络安全等级保护测评报告》，最终完成验收测评工作，达到国家规定的信息安全要求，并完成向桂林市公安局提交相关系统的《网络安全等级保护测评报告》。4.6信息安全咨询服务要求：在项目执行过程中及验收合格后一年内为招标方通过电话、邮件、面谈、组织会议等方式提供各类信息系统安全咨询和信息系统安全体系建设咨询服务，涵盖系统基础设计、系统建设方案、运维管理等相关的建设及安全问题，提供信息安全检查咨询和整改建议等技术支持服务。**5、测评工具要求**1.本项目在实施过程中所使用到的专业安全测评项目管理工具必须保证不会产生所有权和知识产权纠纷,并保证工具和软件的可用性和可靠性。由此产生的一切责任由投标人负完全责任。（报价文件中须提供说明函，格式自拟）。2.本项目使用的所有服务工具和软件（包括但不限于等级保护检查工具、网络边界完整性检查管理系统、网络安全事件应急处置工具、云安全检测工具（云镜））无需本项目采购方购买，均由中标方自行提供。（报价文件中须提供承诺函，格式自拟）。**6、服务成果**项目验收时乙方需要提交以下项目文档：6.1完成2个系统（体检系统、重症系统）的定级备案材料收集及专家评审意见，在桂林市公安局完成备案工作，取得《备案证》；6.2 被测信息系统完成风险梳理后提交《整改问题清单》。6.3被测信息系统完成整改后完成复测，并出具出具符合国家最新等保相关技术标准要求、国家网络安全等级保护管理部门规范要求且公安机关认可的的《网络安全等级保护测评报告》。6.4 项目验收单，按医院要求的标准格式验收。6.5 提供合同的PDF版本，合同的WORD版本。 |
| **商务要求表** |
| ★资质要求 | 测评机构必须具备公安部第三研究所认证颁发的《网络安全等级测评与检测评估机构服务认证证书》。投标人具备CCRC信息安全服务三级及以上资质认证证书。项目经理须具有网络安全等级测评师证书（高级）证书并通过商用密码应用安全性评估人员测评能力考核，具有密码安全工程师（中级）证书。同时具有以下的其中一项及以上:有CIIP-D（重要信息系统保护人员证书）、CISP-A（注册信息系统审计师证书）、NSAPT（注册网络安全测评专业人员证书）。项目组成员（不含项目经理）至少1人具有网络安全威胁分析师证书;至少1人具有网络安全能力认证数据安全（管理）证书或数据安全工程师证书；至少2人通过国家密码管理局商用密码组织的商用密码应用安全性评估人员测评能力考核和网络安全等级保护测评师；至少1人具备中国网络安全审查技术与认证中心颁发的数据安全官证书（DSO）和数据合规官证书（DCO）。拟投入本项目售后服务技术人员至少3人。（本条目描述的持证人员，投标人应提供近期3个月社保证明）。 |
| 服务期限及服务地点 | 服务期限：自进场测评之日起60个工作日内服务地点：采购人指定桂林市地点。 |
| 其他要求 | 1、投标人投入本项目的测评人员必须具有公安部信息安全等级保护评估中心或中关村信息安全测评联盟颁发的《信息/网络安全等级测评师证书》，项目组成人员至少5人，其中包括至少4名测评师（分别至少1名高级测评师、至少1名中级测评师和两名初级测评师）和至少1名质量管理人员。2、投标人如有广西壮族自治区区内项目服务案例，请提供相关证明文件。3、项目实施期间，如果采购人现有信息系统（不只限于本次测评范围内的信息系统）发生变更（或新建信息系统）需要重新定级备案，成交供应商须为采购人提供系统定级备案、备案更改等咨询服务。4、投标人必须针对本项目提供技术、实施和售后服务方案。5、投标人在中标后必须签署相关保密协议，并严格遵守协议要求。 |

**四、第二项服务需求一览表**

|  |
| --- |
| **技术参数要求** |
| **一、测评服务****1、★总体要求**为贯彻落实《中华人民共和国密码法》、《商用密码管理条例》与《商用密码应用安全性评估管理办法》中对密码应用与安全性评估要求，拟对广西壮族自治区南溪山医院医院HIS信息系统（三级）、互联网医院系统（三级）开展密码安全性评估工作，评估广西壮族自治区南溪山医院医院HIS信息系统（三级）、互联网医院系统（三级）的密码应用是否合规、正确、有效，并通过测评发现其密码保障系统存在的安全隐患和风险，编制被测评系统的密码应用安全性评估报告，并提出有针对性的加强完善密码安全管理和防护建议。根据密码管理部门审核通过的系统密码应用方案,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。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》，积极指导协助采购方项目团队进行系统商密整改，评估通过后分别出具《商用密码应用与安全性评估报告》，协助采购方报送密码管理部门备案。**2、测评依据标准**GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》GM/T0115-2021《信息系统密码应用测评要求》GM/T0116-2021《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（2021）商用密码应用安全性评估量化评估规则（2023版）《商用密码应用安全性评估测评作业指导书（试行）》1. **服务内容**

**（一）商用密码应用方案评估**依据中国密码学会密评联委会发布的《商用密码应用安全性评估报告模板》（2023版）对“医院HIS信息系统（三级）、互联网医院系统（三级）”系统商用密码应用方案开展评估工作，并出具《密码应用方案评估报告》。**方案评估要点：**1.文档结构是否完整2.系统基本情况是否梳理充分3.密码应用需求是否清晰明确4.密码应用技术框架中密码协议、防护机制、密钥管理、密码应用子系统设计是否合理，能否满足安全需求和保障要求5.密码产品应用和部署设计是否合理、正确6.安全管理方案是否覆盖密码安全相关人员、制度、实施、应急等内容7.实施保障方案中实施计划是否科学、合理，组织管理方法和保障是否合理有效**（二）商用密码应用安全性评估**依据《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）等技术标准对“医院HIS信息系统（三级）、互联网医院系统（三级）”系统进行商用密码应用安全性评估工作，并出具符合要求的《商用密码应用安全性评估报告》。**1.系统测评：**及时发现系统脆弱性，识别变化的风险，了解系统安全状况，对照密码应用方案对系统开展测评。根据被测评对象的实际情况、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，以测评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。**2.密码技术应用测评：**物理安全密码测评、网络安全密码测评、主机安全密码测评、应用安全密码测评、数据安全及备份恢复密码测评。测评验证不同安全等级信息系统的商用密码应用是否达到具有相应安全等级的安全保护能力，是否满足相应安全等级的保护要求。**3.密钥管理测评：**检测信息系统密钥管理各环节，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。**4.安全管理测评：**对制度、人员、实施和应急等四个方面安全管理的测评，并协助完善商用密码应用安全性管理制度，协助完善密码相关系统运维管理制度。**（三）测评工具要求**1.本项目在实施过程中所使用到的专业安全测评项目管理工具,必须保证不会产生所有权和知识产权纠纷,并保证工具和软件的可用性和可靠性。由此产生的一切责任由投标人负完全责任。（报价文件中须提供说明函，格式自拟）。2.本项目使用的所有服务工具和软件（包括但不限于等级保护检查工具、网络边界完整性检查管理系统、网络安全事件应急处置工具、云安全检测工具（云镜））无需本项目采购方购买，均由中标方自行提供。（报价文件中须提供承诺函，格式自拟）。**（四）其它要求：**1.测评人员必须为通过国家密码管理部门（或其授权的机构）组织的考核（即商用密码应用安全性评估人员测评能力考核证书），遵守国家有关法律法规，按照相关标准，为用户提供安全、客观、公正的评估服务，保证评估的质量和效果。2.供应商应具有完善的测评方案，有计划、按步骤地开展测评工作，且测评方案应专业性强，对系统现状及需求理解应准确，方案应科学合理，内容应完整、可靠性强，实施方法和技术措施应可操作性和有效性强，在签订密评合同后供应商应立即成立密评工作小组，并严格按照合同履行密评责任。3.为保障密评过程中可能涉及的重要数据和敏感信息的安全，供应商应配有相关能力支撑的保密办公区，并具备安全保密管理制度与数据安全能力，采取的安全管理措施应得当，且能够很好保障本项目测评数据的安全，明确对采购人的系统、信息、数据有安全保密的义务，进场测评前必须签订保密协议。4.供应商在现场测评工作中必须在不影响采购人信息系统正常运行的前提下进行。5.供应商应遵守相应的密评工作制度，包括会议制度、密评文件制度、密评记录制度、工作报告制度等，保证密评工作协调有序的进行。6.供应商应根据被测系统的具体情况，按合同约定，配备满足密评工作需要的人员、设备和工具。为保障密评实施与合同约定服务周期内的服务响应，供应商应具备一定的测评工具开发能力以及在测评服务地进行系统环境模拟实验能力。7.供应商应具有完善的应急流程，具有快速应急响应服务团队，以保证在整个项目过程中不影响委托单位信息系统的正常运行。8.供应商应配有较为完善的测评环境，并配备密评网络抓包、密码算法、协议分析工具、随机数检测工具以及常用密码设备，且应具有模拟以及验证被测评系统密码应用方案的能力。9.供应商完成商用密码应用安全性评估工作后，应协助用户在30日内将评估结果报国家密码管理部门备案。10.供应商在验收时应提交密码安全测评工作的档案。**4、服务交付**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。根据密码管理部门审核通过的系统密码应用方案,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。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》，积极指导协助采购方项目团队进行系统商密整改，评估通过后分别出具《商用密码应用与安全性评估报告》、《商用密码应用与安全性评估整改建议书》，协助采购方报送密码管理部门备案。在项目执行过程中及验收合格后一年内为招标方通过电话、邮件、面谈、组织会议等方式提供各类信息系统安全咨询和信息系统安全体系建设咨询服务，涵盖系统基础设计、系统建设方案、运维管理等相关的建设及安全问题，提供信息安全检查咨询和整改建议等技术支持服务。 |
| **商务要求表** |
| **★**资质要求 | 1、测评机构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、测评机构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。3、项目经理须具有网络安全等级测评师证书（高级）证书并通过商用密码应用安全性评估人员测评能力考核，具有密码安全工程师（中级）证书。同时具有以下的其中一项及以上:有CIIP-D（重要信息系统保护人员证书）、CISP-A（注册信息系统审计师证书）、NSAPT（注册网络安全测评专业人员证书）。项目组成员（不含项目经理）至少1人具有网络安全威胁分析师证书;至少1人具有网络安全能力认证数据安全（管理）证书或数据安全工程师证书；至少2人通过国家密码管理局商用密码组织的商用密码应用安全性评估人员测评能力考核和网络安全等级保护测评师；至少1人具备中国网络安全审查技术与认证中心颁发的数据安全官证书（DSO）和数据合规官证书（DCO）。 拟投入本项目售后服务技术人员至少3人。（本条目描述的持证人员，投标人应提供近期3个月社保证明）。 |
| 完成期限及服务地点： | 1、完成期限：本项目商用密码应用与安全性评估对象的所有现场测评并出具测评报告工作须在采购人通知进场之日起30个工作日之内完成。2、服务地点：广西区采购人指定地点。 |
| 其他要求 | 1、拟投入本项目商用密码应用安全性评估服务的测评机构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，项目组成员至少5人，要求设项目经理1名、质量经理1名。2、测评机构如在广西设有常驻的机构提供本地化服务，请提供相关证明文件。3、中标人必须签署相关保密协议，严格遵守协议要求。4、投标人必须针对本项目提供技术、实施、售后服务方案。 |
| 测评及售后服务基本要求 | 免费售后服务期限：自合同签订之日一年。 |