广西壮族自治区南溪山医院（广西壮族自治区第二人民医院）

2025年度等保密保测评服务项目采购需求

**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3个等级保护系统开展安全等级保护三级测评服务，衡量等级保护对象是否达到相应等级的安全保护能力，完成相关测评咨询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）”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 |
| 医院PACS系统（三级） | 等级保护测评及等级保护咨询及等级保护备案工作 | 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 完成系统需求清单里面3个三级系统（医院HIS信息系统、互联网医院系统、医院PACS系统）的风险梳理，根据评估结果出具《整改问题清单》；  1.2 根据安全整改结果，3个三级系统（医院HIS信息系统、互联网医院系统、医院PACS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》，并指导、配合采购人完成安全整改；  **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 针对医院HIS信息系统、互联网医院系统、医院PACS系统按三级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。  4.2 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。  4.3 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。  4.4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。  4.5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。  4.6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》。  4.7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。   1. **测评方法**   测评实施过程中，采用访谈、检查和测试、渗透测试等测评方法进行，并与国家相关规范及标准要求相符。  （1）访谈是指测评人员通过引导信息系统相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、分析或取得证据的过程；  （2）检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程；  （3）测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程；  （4）渗透测试是模拟黑客的攻击方法，对受保护对象，包括应用系统、主机、网络进行攻击，从而验证测评对象的弱点、技术缺陷或漏洞的一种评估方法。   1. **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 被测信息系统完成风险梳理后提交《整改问题清单》。  6.2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》。  6.3 项目验收单，按医院要求的标准格式验收。  6.4 提供合同的PDF版本，合同的WORD版本。 | |
| **商务要求表** | |
| ★资质要求 | 1.投标人必须具备公安部第三研究所认证颁发的《网络安全服务认证证书等级保护测评服务认证》,提供证书或证明复印件并加盖公章。 |
| 服务期限  及服务地点 | 服务期限：  1.网络安全等级保护测评：  （1）自甲方书面通知服务开始之日起10个工作日内完成差距分析工作;  （2）乙方在差距分析结束后15个工作日内提供差距分析报告;  （3）甲方根据差距分析报告进行整改，整改完成后甲方书面通知乙方开展现场测评，乙方应在10个工作日内完成现场测评工作。  (整改工作应在出具差距分析报告之日起60个工作日内完成，若逾期未能完成整改的，乙方将直接出具该项目的网络安全等级保护测评报告，项目完结)  （4）乙方完成现场测评后20个工作日内，出具该项目的网络安全等级保护测评报告。  服务地点：广西壮族自治区内采购人指定地点。 |
| 其他要求 | ★1.人员要求  投标人投入本项目的测评实施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》，项目组成人员至少五人，其中包括四名测评师（分别为一名高级测评师、一名中级测评师和两名初级测评师）和一名质量监督人员。  投标人投入本项目的商用密码应用安全性评估实施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，项目组成人员至少3人。  2.投标人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.投标人如在广西壮族自治区内有同行业项目服务案例，请提供相关证明文件。  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、**服务内容**  （一）商用密码应用方案评估  1.本项目需要对医院HIS信息系统（三级）开展系统密码应用方案安全性评估和信息系统密码应用与安全性评估，并通过测评发现应用系统存在的安全隐患和风险，出具对应的系统密码应用方案安全性评估报告和信息系统密码应用与安全性评估，并提出有针对性的加强完善密码安全管理和防护意见，对系统密码应用方案及改进后的被测系统提供咨询、评估服务，同时协助采购人完成对应的整改工作。  2.评估依据  《中华人民共和国密码法》  《中华人民共和国网络安全法》  《中华人民共和国数据安全法》  《商用密码管理条例》  《商用密码应用安全性评估管理办法》  《GB/T 39768-2021 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》  《GB/T 43207-2023 信息安全技术 信息系统密码应用设计指南》  《信息系统密码应用高风险判定指引》  如有最新规定按最新规定执行。  **3、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）。  **4、服务要求**  包含但不限于如下任务要求：  1）开展密码测评工作，并依据相关文件模板，对测评范围内的信息系统出具符合国家密码管理局和当地密码管理部门要求的密评报告；  2）根据测评结果，给出整改意见，指导建设单位对被测系统暴露出的密码应用安全问题进行整改；  3）根据国家密码管理局和当地密码管理部门关于规范商用密码应用安全性评估结果备案工作的通知，协助准备备案资料并完成密评备案工作；  4）协助采购人完成与密评相关的其他工作。  **5、评估流程**  密码应用安全性评估过程分为四个基本测评活动：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。供应商和采购人之间的沟通与洽谈贯穿整个密码应用安全性评估过程。  5.1测评准备活动  供应商通过查阅被测系统已有资料并使用调查表格的方式，了解整个系统的构成和密码保护情况，为编写密评方案和开展现场测评工作奠定基础。测评项目组成员在进行现场测评之前，熟悉与被测信息系统相关的各种组件、调试测评工具、准备各种表单等。  5.2 方案编制活动  根据已经了解到的被测信息系统情况，分析整个被测系统及其涉及的业务应用系统，以及与此相关的密码应用情况，确定出本次测评的测评对象；根据已经了解到的被测系统定级结果，确定出本次测评的测评指标；确认测评过程中需要现场检查的关键安全点，并且充分考虑到检查的可行性和风险，最大限度的避免对被测系统，尤其是在线运行业务系统的影响；确定现场测评的具体实施内容；最终完成测评方案的编制。  5.3 现场测评活动  1）现场测评准备：召开测评现场首次会，供应商介绍测评工作，交流测评信息，进一步明确测评计划和测评方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排，测评过程中可能存在的安全风险等，以便于后面的测评工作开展。供应商和采购方确认现场测评需要的各种资源，包括采购方的配合人员和需要提供的测评条件等，确认被测信息系统已备份过系统及数据。采购方签署现场测评授权书。密评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。  2）开展现场测评：测评项目组根据密评方案以及现场测评准备的结果，安排密评人员在现场完成测评工作，汇总现场测评的测评记录；召开测评现场结束会，供应商和采购方对测评过程中发现的问题进行现场确认；密评机构归还测评过程中借阅的所有文档资料，并由采购方文档资料提供者签字确认。  5.4 分析与报告编制活动  1）在现场测评工作结束后，供应商对现场测评获得的测评结果进行汇总分析，形成评估结论，并编制评估报告。  2）密评人员在初步判定各测评单元涉及的各个测评对象的测评结果后，还需进行单元测评、整体测评、量化评估和风险分析。经过整体测评后，有的测评对象的测评结果可能会有所变化，需进一步修订测评结果，而后进行量化评估和风险分析，最后形成评估结论。  **6.密评应用技术要求**  6.1 通用测评要求  核查被测系统中使用的密码算法、密码技术、密码产品和密码服务是否满足国家密码管理的相关标准或规范要求。  6.2 密码应用技术评估要求  具体包括但不限于:物理和环境安全测评、网络和通信安全测评、设备和计算安全测评、应用和数据安全测评，政务信息系统密码应用与安全性评估、制定测评工作方案等，验证不同安全等级信息系统的密码应用是否达到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。  6.3 物理和环境安全测评  物理和环境安全主要实现对被测系统所在机房等重要区域的物理防护，物理机房的进出必须严格符合相关规范，并对相关人员进出信息实时记录，防止非法人员采用非法手段进出，防止出现人为物理破坏，防止造成不可逆的重大损失。  针对“身份鉴别”、“电子门禁记录数据存储完整性”、“视频监控记录数据存储完整性”等物理和环境安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况（如访谈记录、配置截图、抓包分析截图、产品照片等），完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  物理和环境安全测评要求：  （1）需要采用密码技术进行物理访问身份鉴别,保证重要区域进入人员身份的真实性。  （2）需要采用密码技术保证电子门禁系统进出记录数据的存储完整性。  （3）需要采用密码技术保证视频监控音像记录数据的存储完整性。  5.4 网络和通信安全测评  网络和通信安全主要实现对信息系统与经由外部网络连接的实体进行网络通信时的安全防护，密码应用要求主要涉及通信过程中实体身份真实性、数据机密性和数据完整性，以及网络边界访问控制和设备接入控制。  针对“身份鉴别”、“通信数据完整性”、“通信过程中重要数据的机密性”、“网络边界访问控制信息的完整性”、“安全接入认证”等网络和通信安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况(如访谈记录、配置截图、抓包分析截图、产品照片等)，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  网络和通信安全测评要求内容：  (1)应采用密码技术对通信实体进行身份鉴别,保证通信实体身份的真实性。  (2)宜采用密码技术保证通信过程中数据的完整性。  (3)应采用密码技术保证通信过程中重要数据的机密性。  (4)宜采用密码技术保证网络边界访问控制信息的完整性。  (5)可采用密码技术对从外部连接到内部网络的设备进行接入认证,确保接入设备身份的真实性。  6.5 设备和计算安全测评  设备和计算安全主要实现对被测系统中各类设备和计算环境的安全防护,密码应用要求主要涉及对登录设备用户的身份鉴别、远程管理通道的建立、重要可执行程序来源真实性，以及系统资源访问控制信息、设备的重要信息资源安全标记、重要可执行程序、日志记录的完整性。  针对“身份鉴别”、“远程管理通道安全”、“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”、“重要可执行程序完整性、重要可执行程序来源真实性”等设备和计算安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况(如访谈记录、配置截图、抓包分析截图、产品照片等)，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  设备和计算安全测评标准要求内容：  (1)应采用密码技术对登录设备的用户进行身份鉴别,保证用户身份的真实性。  (2)远程管理设备时,应采用密码技术建立安全的信息传输通道。  (3)宜采用密码技术保证系统资源访问控制信息的完整性。  (4)宜采用密码技术保证设备中的重要信息资源安全标记的完整性。  (5)宜采用密码技术保证日志记录的完整性。  (6)宜采用密码技术对重要可执行程序进行完整性保护,并对其来源进行真实性验证。  6.6 应用和数据安全测评  实现对信息系统中应用及其数据的安全防护,密码应用主要涉及应用的用户身份鉴别、访问控制，以及应用相关重要数据的存储安全、传输安全和相关行为的不可否认性。其中，重要数据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个人信息等。  针对“身份鉴别”、“访问控制信息完整性”、“重要信息资源安全标记完整性”、“重要数据传输机密性”、“重要数据存储机密性”、“重要数据传输完整性”、“重要数据存储完整性”、“不可否认性”等应用和数据安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况(如访谈记录、配置截图、抓包分析截图、产品照片等)，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  应用和数据安全测评标准要求内容：  (1)应采用密码技术对登录用户进行身份鉴别,保证应用系统用户身份的真实性。  (2)宜采用密码技术保证信息系统应用的访问控制信息的完整性。  (3)宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。  (4)应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。  (5)应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。  (6)宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。  (7)宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。  (8)在可能涉及法律责任认定的应用中, 应采用密码技术提供数据原发证据和数据接收证据,实现数据原发行为的不可否认性和数据接收行为的不可否认性。  6.7 密码应用管理要求测评  从管理制度、人员管理、建设运行和应急处置四个方面进行安全管理测评，验证信息系统安全管理机制是否完善，是否能确保密码技术被合规、正确、有效的实施。  1）管理制度  针对“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”等制度方面采取的管理措施进行各项测评,详细记录现场测评情况，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  管理制度标准要求内容：  (1)应具备密码应用安全管理制度,包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。  (2)应根据密码应用方案建立相应密钥管理规则。  (3)应对管理人员或操作人员执行的日常管理操作建立操作规程。  (4)应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定,是否对存在不足或需要改进之处进行修订。  (5)应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制。  (6)应具有密码应用操作规程的相关执行记录并妥善保存。  2）人员管理  针对“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”等人员方面采取的管理措施进行各项测评，详细记录现场测评情况，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  人员管理标准要求内容：  (1)相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度。  (2)应建立密码应用岗位责任制度,明确各岗位在安全系统中的职责和权限。  (3)根据密码应用的实际情况,设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位;  (4)对关键岗位建立多人共管机制;  (5)密钥管理、密码安全审计、密码操作人员职责互相制约互相监督,其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任;  (6)相关设备与系统的管理和使用账号不得多人共用。  (7)应建立上岗人员培训制度,对于涉及密码的操作和管理的人员进行专门培训,确保其具备岗位所需专业技能。  (8)应定期对密码应用安全岗位人员进行考核。  (9)应建立关键人员保密制度和调离制度,签订保密合同,承担保密义务。  3）建设运行  针对“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”等建设方面采取的管理措施进行各项测评，详细记录现场测评情况，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  建设运行标准要求内容：  (1)应依据密码相关标准和密码应用需求,制定密码应用方案。  (2)应根据密码应用方案,确定系统涉及的密钥种类、体系及其生存周期环节,各环节密钥管理要求照GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》附录B。  (3)应按照应用方案实施建设。  (4)投入运行前应进行密码应用安全性评估,评估通过后系统方可正式运行。  (5)在运行过程中,应严格执行既定的密码应用安全管理制度,是否定期开展密码应用安全性评估及攻防对抗演习,并根据评估结果进行整改。  4）应急处置  针对“应急策略”、“事件处置”、“向有关主管部门上报处置情况”等应急方面采取的管理措施进行各项测评，详细记录现场测评情况，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。  应急处置标准要求内容：  (1)应制定密码应用应急策略,做好应急资源准备,当密码应用安全事件发生时,应立即启动应急处置措施,结合实际情况及时处置。  (2)事件发生后,应及时向信息系统主管部门进行报告。  (3)事件处置完成后,应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。  6.8 实施原则  为保障项目的顺利实施，在项目实施过程应遵循以下原则：  一）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。  二）标准化原则  评估过程应严格遵守国家的相关法律、法规、规范、标准等相关要求。  三）完整性原则  在评估过程中，应确保评估数据、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。  四）保密性原则  在评估过程中，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。  **7、成果提交**  针对被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参考模板编制。报告中应协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议，并出具商用密码应用安全性评估报告。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 | 2.投标人必须具备国家密码管理局颁发的《商用密码检测机构资质证书》（业务范围包含(商用密码应用安全性评估)）,提供证书或证明复印件并加盖公章。 |
| 完成期限及服务地点： | 服务期限：  1.商用密码应用安全性评估：  （1）自接到采购人通知进场之日起10个工作日内完成待测系统的商用密码应用安全性评估工作，若被测系统的测评结论为“基本符合”，投标人现场评估结束后20个工作日内提供该系统的商用密码应用安全性评估报告，投标人不提供复测服务，项目完结；  （2）若被测系统的初次测评结论为“不符合”，投标人在现场测评结束后15个工作日内提供该系统的整改建议，经过采购人整改完成后与投标人确认复测日期(整改应在出具整改建议或初测报告之日起6个月内完成，若逾期未能完成整改的，投标人不再提供复测服务，项目完结)；  （3）若如期完成整改，自采购人出具项目复测通知书之日起 10个工作日完成该项目现场复测，复测完成后20个工作日内提供该项目的最终商用密码应用安全性评估报告，项目完结。  服务地点：广西壮族自治区内采购人指定地点。 |
| 其他要求 | ★1.人员要求  投标人投入本项目的商用密码应用安全性评估实施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，项目组成人员至少3人。  2.投标人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.投标人如在广西壮族自治区内有同行业项目服务案例，请提供相关证明文件。  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。 |
| 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。 |