中南大学湘雅第二医院桂林医院2025年等保密保测评项目采购需求

**一、项目概况**

 **本项目分为为中南大学湘雅第二医院桂林医院网络安全等级保护测评及咨询、等级保护差距整改服务、商用密码安全性测评及咨询服务三部分。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。中南大学湘雅第二医院桂林医院计划采购针对“医院HIS信息系统（三级）”等级保护系统开展安全等级保护三级测评及整改服务，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。

**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 |
| 2 | 医院HIS信息系统（三级） | 等级保护差距整改服务 | 1 | 项 |
| 3 | 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（含备案） | 1 | 个 |

 **三、需求一览表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项号** | **服务名称** | **数量** | **单位** | **技术参数及服务要求** |
| 1 | 医院HIS信息系统（三级）网络安全等级保护测评服务 | 1 | 项 | 一、测评服务1、★总的要求依据《网络安全等级保护基本要求》（GB/T 22239-2019）对[中南大学湘雅二医院桂林医院](http://www.baidu.com/link?url=XbV0qPyBKGy32IEFjUPp5JwjyjZP-tGoXFPWpQ797Oy" \t "https://www.baidu.com/_blank)HIS系统（三级）开展网络安全等级保护测评工作，并出具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）3、★测评内容安全通用要求安全通用要求测评内容应包括安全技术和安全管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的测评，安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的测评。4、测评方法在测评实施过程中，应采用访谈、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的要求相符。 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； 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；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；渗透测试是模拟黑客的攻击方法，对受保护对象的应用系统、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。测评机构应具备对测评过程中发现的漏洞进行深度挖掘的能力。5、★服务成果测评完成后，出具符合等保2.0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。 |
| 2 | 医院HIS信息系统（三级）等级保护差距整改服务 | 1 | 项 | **一、安全评估服务** 包含系统详细调研、评估工作方案、识别关键信息资产、实施物理安全评估、实施网络安全评估、实施主机安全评估、实施应用安全评估、实施数据安全评估、实施管理机构评估、实施管理制度评估、实施管理人员评估、实施系统建设管理评估、实施系统运维管理评估、生成并确认评估报告。 **二、★差距分析服务** 包含依照系统准备差距分析表、安全管理差距分析（通过文档、访谈和测试等方式）、安全技术差距分析（通过文档、访谈等方式）、生成等级保护差距分析报告。 **三、安全规划服务** 包含安全需求分析 、安全建设与改建方案的制定、制作原信息系统产品加固方案、测评不符合及部分符合项整改建议、制作新的网络拓扑图、制作安全需求分析报告、编制并确认整体信息系统整改方案。 **四、整改咨询服务** 依据等级保护相关技术标准，协助采购方完成需测评信息系统的安全整改咨询服务，完善信息系统安全防护措施，以期使各信息系统达到等级保护基本符合的要求。 **五、★安全服务** 由安全服务商提供的电话、网络、现场等方式提供各类信息系统安全咨询和建议服务，重大活动、事件及攻防演练时等提供技术指导和采取必要的防控措施。（时间 1 年）**六、漏扫服务** 服务范围 提供2 次的漏洞扫描服务。 服务内容利用漏洞扫描器对基础环境进行漏洞扫描，发现操作系统、数据库、中间件、网络设备、网络安全设备中存在的安全漏洞，针对漏洞扫描系统出具的结果进行确认分析后，编写漏洞扫描分析报告，报告内容中涵盖漏洞整改建议。 交付成果 提供《业务系统漏洞扫描报告》，发现漏洞不同，报告内容可能有所不同，但至少需要包含以下内容：高危漏洞、中危漏洞、低危漏洞和修复建议。 **七、基线核查服务** 服务范围 提供2 次的基线核查服务。 服务内容 以等级保护基本要求结合业务安全规范，对中南大学湘雅第二医院桂林医院网络环境中指定的网络设备、安全设备、服务器操作系统、数据库、中间件等对象进行自动化配置核查，检测当前对象的身份鉴别、资源控制、访问控制、数据完整性、剩余信息保护、入侵防范、通信保密性、安全审计等方面的安全配置现状，找出高危风险项及策略配置问题，出具配置核查报告，并提供相应的解决方案，帮助中南大学湘雅第二医院桂林医院解决安全风险问题。交付成果 提供《业务系统基线核查安全评估报告》。**八、★网络安全整改服务**1、依据等级保护相关技术标准，协助采购方完成需测评信息系统的安全整改服务，完善信息系统安全防护措施，以期使各信息系统达到等级保护基本符合的要求。2、从管理和技术两个层面找出存在的问题并进行加固，加固的对象包括应用系统服务器、业务终端、安全设备、网络设备、审计管理等设备，加固的风险项包含并不限于：账户口令策略、三权分立、登录失败处理、访问控制、空闲会话超时处理、剩余信息保护、数据加密存储、日志审计、日志策略备份等；3、对于需要修改代码等复杂操作需协助或监督应用厂家修改，并在处理后确认修改是否完成；4、对制度缺失项进行补充，协助补充记录和证据类文档；5、协助第三方安全测评机构完成等级保护测评数据采集等工作；6、据初次等保测评出具相关风险问题列表后，针对仍然存在的高、中风险项，继续按照以上等保加固工作要求再次进行加固，直至完成等保测评。服务成果：《网络安全整改服务报告》**九、网络安全应急响应服务** 1、服务目标 确保中南大学湘雅医院第二附属医院桂林医院医院的 IT 应急事件能够快速响应和准确诊断，使信息系统迅速回复，确保桂医院信息系统事件导致的损失最小化。 2、服务范围 中南大学湘雅医院第二附属医院桂林医院医院信息系统发生的信息安全突发事件。 3、服务内容 需要处理的紧急安全事件包括： （1）网络性能严重下降，或者宕机，导致系统无法正常运行； （2）非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏； （3）信息泄密，数据在传输中因数据被截取、篡改而造成信息的更改； （4）拒绝服务，正常用户不能正常访问服务器提供的相关服务； （5）大面积感染计算机病毒或蠕虫； （6）设备故障导致网络或系统崩溃； （7）误操作导致网络或系统崩溃； （8）业务中断 （9）大规模病毒爆发 （10）网络瘫痪 （11）主机或网络异常事件 （12）数据丢失 应急响应服务主要包括以下内容： （1）排查故障，隔离关键数据； （2）攻击手段分析，提供应急方案或工具软件； （3）定位攻击来源，提出安全建议； （4）数据及网络业务恢复。 提供的应急响应服务方式： 远程响应和现场服务，在处理紧急事件时，通常先尝试通过远程接入的方式定位并解决问题，如果条件不允许或不能解决问题，将尽可能快的赶赴事件现场进行处理。 为中南大学湘雅医院第二附属医院桂林医院医院的突发安全事件提供 7×24 小时的电话技术支持，在工作时间内半小时响应，2 小时内到达现场，非工作时间内 8 小时到达现场。成交供应商须熟悉采购人信息系统和网络安全情况，发生紧急情况时，成交供应商须派出项目经理到达现场，进行资源调度和应急保障。**十、★测评整改服务期间提供服务工具一套，具体要求：**1、采用一体化安全运维平台，不接受平台+安全产品组合方式提供，机架式设备，默认配置≥4个千兆电口，≥64G内存，≥2T硬盘存储空间，冗余电源；2、平台配置扫描次数授权：无限制；扫描IP/域名范围授权：无限制；提供可管理主机资产授权数：无限制；提供可管理网站资产授权数：≥1000；提供仿真业务陷阱授权数：无限制；提供主机主动监测及漏洞屏蔽授权数：≥1000；提供出口流量监测带宽授权：≥2Gbps；提供二次开发接口授权；3、平台配置暴露面监测功能：通过单位全称、关键字、出口IP等信息，收集单位/企业信息、邮箱信息、敏感代码、敏感文档、app程序、微信小程序、微信公众号等外部/互联网攻击面信息。提供功能界面截图证明；输入IP或者网段，通过搜索互联网数据，自动获取到IP对应的域名、url链接、网站标题、返回状态码；提供功能界面截图证明。 4、平台配置资产深度管理功能：支持识别“打印机、网络摄像头、安全设备、投影仪、安全设备、路由器”等设备类型，具备4W+指纹特征库；支持自动扫描IP资产信息，包括：“存活IP、设备厂商、操作系统、端口、应用、数据库、中间件、服务版本”等资产指纹特征，形成主机资产台账；不需要联动第三方设备、不需要在主机中安装任何代理、无需主机开放任意端口，就可支持对跨网段的IP或多个网段对进行MAC地址探测识别，支持识别MAC地址的设备类型包含:“Windos、Linux、国产操作系统、交换机\路由器、安全设备、打印机等”。5、平台配置网站威胁检测功能：对网站的“漏洞、篡改、黑链、敏感文件、敏感词、网马监测、可用性、域名劫持”等8个维度开展实时监测，监测频率低至5分钟/次；支持以excel报表格式导入渗透测试报告，形成渗透测试台账。可在系统查看渗透测试结果，以图表形式可视化展现漏洞风险级别比例、风险应用比例，可对渗透报告中的漏洞进行跟踪确认，处置漏洞状态：未整改、已整改、忽略、未整改。提供功能界面截图证明。6、平台配置漏洞扫描与漏洞管理功能：漏洞库漏洞信息大于320000+条，集成4000+POC对内网资产进行自动漏洞验证与渗透，提供详细的漏洞描述和对应的解决方案描述。通过POC验证过的漏洞，扫描结果需包含漏洞利用证明，包括但不限于攻击Payload、目标响应结果、漏洞利用点、关键参数等内容。7、平台配置边界威胁监测功能：通过流量镜像对海量流量进行采集，基于80000+威胁特征库，对于捕获的流量进行存储、分析，内置多重检测引擎，包含入侵检测、web检测、威胁情报等，结合攻击源、风险等级、地理位置、攻击目标、命中规则数、告警次数等因素综合分析，精准识别攻击源头，发现不同场景下的已知威胁和未知威胁；不需要设备串联、不需要配置策略路由，就能通过监测中心流量监测告警处，对单个ip进行手工阻断。也可自动关联流量告警，根据智能研判标签，就会自动触发旁路阻断，包括但不限于非法外联-拦截域名解析的IP（高风险）、外网恶意攻击（高风险）、利用成功（高风险）、暴力破解（高风险）、外网可疑访问（中风险）等标签，可灵活针对国内/国外ip进行灵活封禁，可灵活指定封禁时间间隔。8、平台配置内网威胁诱捕扩展能力：无需在用户服务器上安装agent，可通过trunk方式将诱捕能力发布到全内网各vlan网段，实现在全内网中部署大量高交互病毒监测诱饵，无侵入式部署不影响用户业务运行；不需要联动第三方设备、不需要在主机上安装agent脚本，就能对失陷主机进行网络隔离，隔离后失陷主机无法访问同网段以及其它网段IP，提供功能界面截图证明。9、平台配置互联网威胁诱捕扩展能力：（1）蜜罐仿真：支持通过反向代理的方式，接入用户自身搭建的应用系统，从而实现完全仿真真实业务系统，生成完全仿真蜜罐，提供功能界面截图证明；可在平台中统计打开钓鱼邮件的账号、点击连接的账号、提交敏感数据的账号等数据，统计维度包括账号名称、访问ip、提交敏感数据内容、访问时间等。提供功能界面截图证明；（2）威胁感知：参考MITRE ATT&CK，形成黑客攻击链，攻击链检测包含：“针对蜜罐的探测扫描、渗透攻击、攻陷蜜罐、在蜜罐上安装后门远控程序、利用蜜罐进行跳板攻击”等入侵过程；支持还原攻击者的网络数据包，包括icmp、tcp、udp等协议的攻击包，可查看攻击者发起的具体攻击请求数据，比如SQL注入、XSS攻击的http请求头部信息。（3）攻击溯源：支持记录攻击者的“黑客社交画像”信息，包括社交账号、昵称、头像等信息，比如溯源百度等不同类型的社交账号，提供功能界面截图证明；（4）攻击反制：可灵活指定对某个攻击源IP地址发起威慑反制，比如灌输国家网络安全法、告知已获得相关溯源信息。提供功能界面截图证明。10、平台配置服务器主动监测扩展能力：在用户的服务器、业务系统上安装安全监控软件，主动监测webshell、暴力破解、异常登录成功、反弹shell、挖矿检测等，发现可疑的入侵事件，并实时将告警同步到服务平台，提供功能界面截图证明。11、平台配置AI智能研判功能：联动本地DeepSeek AI模型，联动分析“流量、蜜罐、主机”三者告警结论，关联“资产+漏洞”信息，辅助输出综合研判结果：1.给攻击源IP定性并打上攻击者标签，如：非法外联、外网恶意攻击、内网恶意攻击、漏洞利用成功等。2.输出攻击源资产画像，包括网络区域、主机名称、MAC地址等。提供功能界面截图证明。12、平台配置风险统计功能：（1）通过监测中心可统一展现蜜罐告警事件、主机威胁事件、流量检测告警，事件及告警结果自动刷新。支持蜜罐、主机威胁与流量告警的关联分析，提升告警可信度。支持根据攻击行为自动研判，对攻击IP进行自动分类并打上对应的攻击者标签。提供功能界面截图证明。；（2）支持大屏展示功能，可视化呈现监测中心的数据，包括主机资产监测概况、攻击监测诱饵监测概况，大屏界面能够自动刷新监测数据，实时展示最新监测结果。**十一、★提供差距整改服务服务团队及人员资质** 投标人获得SO/IEC27001:2022信息安全管理体系认证证书、信息系统安全运维三级以上服务资质、信息系统安全集成三级以上服务资质、CCRC信息安全网络安全审计三级以上服务资质、市级网络与信息安全信息通报中心颁发的网络安全技术支撑志愿服务单位。提供差距整改咨询服务团队人员不少于 6 名工程师。 团队人员中至少 1名服务工程师获得渗透测试专家(CISP-PTS)；至少 2 名服务工程师获得注册信息安全工程师（CISE），至少 2 名服务工程师信息安全保障人员认证(CISAW)，至少 1 名服务工程师获得云计算工程师、华为认证高级工程师、信息化项目经理认证，投标时必须提供以上人员资质证书复印件和投标人社保证明并加盖投标人公章。1. **★提供至少1次院级安全培训，协助开展网络安全应急演练**
 |
| 3 | 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（含备案） | 1 | 个 | 1.本项需要对医院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 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》《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.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。4.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。4.1 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。4.2 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。4.3 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。4.4 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。5.密评应用技术要求5.1 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。5.2 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。5.3 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。5.5 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。5.6 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。5.7 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。5.8 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。5.9 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。 |
| **★**资质要求 | 1.第一项服务产品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。2.第三项服务产品测评机构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。 |