# 采购需求

## 一、项目范围

|  |  |
| --- | --- |
| 序号 | 系统名称 |
| 1 | 湖北烟草电子公文系统 |

## 二、采购内容

|  |  |
| --- | --- |
| 序号 | 服务内容 |
| 1 | 网络安全等级保护测评三级 |
| 2 | 商用密码应用安全性评估三级 |

## 三、网络安全等级保护测评三级

1. **采购内容**

|  |  |
| --- | --- |
| 序号 | 服务内容 |
| 1 | 定级备案服务 |
| 2 | 差距分析服务 |
| 3 | 网络安全等级保护测评服务 |
| 4 | 整改咨询服务 |

1. **项目目标**

为了落实公安部、网信办和上级主管部门关于网络安全等级保护要求，进一步增强系统安全防护能力，保障系统安全稳定运行。现依据《中华人民共和国网络安全法》和《GB/T 22239-2019信息安全技术网络安全等级保护基本要求》等法律法规和国家标准开展网络安全等级保护工作。

按照《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）、《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）和有关规定及要求，协助采购方进行系统定级、备案工作。完成对平台的安全等级保护测评工作，指导采购方对系统测评中提出的不符合项进行整改，提出安全整改建议，编制整改方案。最终出具符合要求的安全等级保护测评报告，协助采购方取得公安机关颁发的备案证明。

1. **项目依据**

* 《中华人民共和国网络安全法》
* 《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）
* 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
* 《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）
* 《信息安全等级保护管理办法》（公通字[2007]66号）
* 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）
* 《信息安全等级保护备案实施细则》（公信安[2007]1360号）
* 《公安机关信息安全等级保护检查工作规范》（公信安[2008]736号）
* 《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071号）
* 《关于开展信息安全等级保护安全建设整改工作的指导意见》(公信安[2009]1429号)
* 《关于转发《网络安全等级保护测评报告模板（2021版）》的通知）
* 《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）
* 《GB/T22239-2019信息安全技术 网络安全等级保护基本要求》
* 《GB/T25070-2019信息安全技术 网络安全等级保护设计技术要求》
* 《GB/T28448-2019信息安全技术 网络安全等级保护测评要求》
* 《GB/T28449-2018信息安全技术 网络安全等级保护测评过程指南》
* 《GB/T25058-2019信息安全技术 信息系统安全等级保护实施指南》
* 《GB/T22240-2020信息安全技术 网络安全等级保护定级指南》

1. **测评内容**

依据等级保护政策要求、技术标准和管理规范以及行业要求开展测评，内容包括但不限于以下内容：

1. 安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评；
2. 安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评；
3. 系统整体测评：控制间测评、层面间测评、区域间测评、系统结构安全测评。

* 安全物理环境

针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

* 安全通信网络

针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网等；涉及的安全控制点包括网络架构、通信传输和可信验证。

* 安全区域边界

针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

* 安全计算环境

针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护。

* 安全管理中心

针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

* 安全管理制度

针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

* 安全管理机构

针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

* 安全管理人员

针对人员管理提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

* 安全建设管理

针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务投标人管理。

* 安全运维管理

针对安全运维过程提出的安全控制要求，涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理。

## 四、商用密码应用安全性评估三级

1. **采购内容**

|  |  |  |
| --- | --- | --- |
| 序号 | 服务名称 | 服务内容 |
| 1 | 密码应用方案设计咨询 | 协助用户分析密码应用中的技术难点，为用户设计商用密码应用方案提供技术咨询服务 |
| 2 | 密码应用方案评审 | 协助用户对密码应用方案进行审核，审核通过后，出具密码应用方案的评估报告，协助用户组织相关专家进行方案评审 |
| 3 | 密码建设咨询 | 密码方案通过专家评审后，为用户单位进行商用密码建设提供技术咨询，协助分析实施过程中遇到的问题并提供参考建议 |
| 4 | 信息系统密码应用安全性评估 | 密码体系建设完成后，通过技术手段抓包并验证密码算法和密码产品的正确性、有效性、合规性分析，并出具评估报告 |

1. **项目目标**

为全面贯彻总体国家安全观和网络强国战略，持续推进网络安全等级保护工作和商用密码应用工作，进一步增强系统安全防护能力和商用密码合规、正确、有效的使用。现依据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《国家政务信息化项目建设管理办法》（57号文）、《关于进一步加强全省政务信息化项目密码应用有关工作的通知》（2号文）等法律法规、制度和规范，开展商用密码应用安全性评估工作。

根据《GB/T 39786-2021信息安全技术 信息系统密码应用基本要求》，测评机构选择与之相对应的标准条款，对信息系统所涉及的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理及安全管理等方面进行测评，出具密码应用安全性评估报告。

1. **项目依据**

* 《中华人民共和国密码法》
* 《网络安全等级保护条例（征求意见稿）》
* 《商用密码应用安全性评估管理办法》
* 《政务信息系统密码应用与安全性评估工作指南》（2020版）
* 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》
* 《国家政务信息化项目建设管理办法》（57号文）
* 《关于进一步加强全省政务信息化项目密码应用有关工作的通知》（2号文）
* 《GB/T 39786-2021信息安全技术 信息系统密码应用基本要求》
* 《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量化评估规则》
* 《信息系统密码应用测评要求》
* 《信息系统密码应用高风险判定指引》

1. **评估内容**

依据信息系统确定安全保护等级，选择《GB/T 39786-2021信息安全技术 信息系统密码应用基本要求》中对应级别的安全要求作为安全测评的指标，以表格形式在下表中列出第一级～第四级密码应用基本要求，见下表，第五级略：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 商用密码应用安全性评估内容指标 | | |
| 1 | 总体要求 | 密码算法 | 成交供应商应验证被测信息系统中使用的密码算法是否当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。 |
| 密码技术 | 成交供应商应验证被测信息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。 |
| 密码产品 | 成交供应商应验证被测信息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。 |
| 密码服务 | 成交供应商应验证被测信息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 | 物理和环境安全 | 身份鉴别 | 成交供应商应验证被测信息系统在电子门禁系统中是否使用密码技术的真实性服务来保护身份鉴别信息，保证重要区域进入人员身份的真实性。 |
| 电子门禁记录数据完整性 | 成交供应商应验证被测信息系统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。 |
| 视频记录数据完整性 | 成交供应商应验证被测信息系统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。 |
| 3 | 网络和通信安全 | 身份鉴别 | 成交供应商应验证被测信息系统是否在通信前基于密码技术对通信双方进行验证或认证，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。 |
| 访问控制信息完整性 | 成交供应商应验证被测信息系统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。 |
| 通信数据完整性 | 成交供应商应验证被测信息系统是否采用密码技术保证通信过程中数据的完整性。 |
| 通信数据机密性 | 成交供应商应验证被测信息系统是否采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性。 |
| 集中管理通道安全 | 成交供应商应验证被测信息系统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。 |
| 4 | 设备和计算安全 | 身份鉴别 | 成交供应商应验证被测信息系统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。 |
| 远程管理身份鉴别信息机密性 | 成交供应商应验证被测信息系统是否远程管理时，应使用密码技术的机密性服务来实现鉴别信息的防窃听。 |
| 访问控制信息完整性 | 成交供应商应验证被测信息系统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。 |
| 敏感标记完整性 | 成交供应商应验证被测信息系统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。 |
| 重要程序或文件完整性 | 成交供应商应验证被测信息系统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。 |
| 日志记录完整性 | 成交供应商应验证被测信息系统是否使用密码技术的完整性功能来对日志记录进行完整性保护。 |
| 5 | 应用和数据安全 | 身份鉴别 | 成交供应商应验证被测信息系统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。 |
| 访问控制信息和敏感标记完整性 | 成交供应商应验证被测信息系统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。 |
| 数据传输机密性 | 成交供应商应验证被测信息系统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。 |
| 数据存储机密性 | 成交供应商应验证被测信息系统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。 |
| 数据传输完整性 | 成交供应商应验证被测信息系统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。 |
| 数据存储完整性 | 成交供应商应验证被测信息系统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。 |
| 日志记录完整性 | 成交供应商应验证被测信息系统是否使用密码技术的完整性功能来实现对日志记录完整性的保护。 |
| 重要程序的加载和卸载 | 成交供应商应验证被测信息系统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。 |
| 6 | 密钥管理 | 生成 | 成交供应商应验证被测信息系统密钥生成使用的随机数是否符合GM/T 0005-2012《随机性检测规范》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，是否以明文方式出现在密码模块之外；被测信息系统是否具备检查和剔除弱密钥的能力。 |
| 存储 | 成交供应商应验证被测信息系统密钥是否加密存储，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《密码模块安全技术要求》的二级及以上密码模块中。 |
| 使用 | 成交供应商应验证被测信息系统密钥是否明确用途，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。 |
| 分发 | 成交供应商应验证被测信息系统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。 |
| 导入与导出 | 成交供应商应验证被测信息系统是否采取安全措施，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。 |
| 备份与恢复 | 成交供应商应验证责任单位是否制定明确的密钥备份策略，被测信息系统是否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；审计信息是否包括备份或恢复的主体、备份或恢复的时间等。 |
| 归档 | 成交供应商应验证被测信息系统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；归档密钥是否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；审计信息是否包括归档的密钥、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。 |
| 销毁 | 成交供应商应验证被测信息系统是否具有在紧急情况下销毁密钥的措施。 |
| 7 | 安全管理 | 制度-制定 | 成交供应商应验证责任单位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。 |
| 制度-定期修订 | 成交供应商应验证责任单位是否定期对密码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。 |
| 制度-发布流程 | 成交供应商应验证责任单位是否明确相关管理制度发布流程。 |
| 人员-法律法规 | 成交供应商应验证责任单位系统负责人是否了解并遵守商用密码相关法律法规。 |
| 人员-密码产品 | 成交供应商应验证责任单位系统负责人是否能够正确使用商用密码产品。 |
| 人员-责任制度 | 成交供应商应验证责任单位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；是否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、密码操作人员职责是否建立多人共管制度，互相制约互相监督，相关设备与系统的管理和使用账号是否禁止多人共用。 |
| 人员-考核制度 | 成交供应商应验证责任单位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。 |
| 人员-培训制度 | 成交供应商应验证责任单位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。 |
| 人员-保密和调离制度 | 成交供应商应验证责任单位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。 |
| 实施-规划 | 成交供应商应验证规划阶段，责任单位是否依据密码有关标准，制信息系统定密码应用建设方案，组织专家进行评审，是否具有评审报告。 |
| 实施-建设-制定实施方案 | 成交供应商应验证责任单位是否按照国家相关标准制定实施方案,方案内容应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。 |
| 实施-建设-选用合规密码产品和服务 | 成交供应商应验证责任单位是否选用经国家密码管理部门核准的密码产品､许可的密码服务。 |
| 实施-运行前 | 成交供应商应验证被测信息系统投入运行前，是否经密评机构进行安全性评估，是否具有评估报告。 |
| 实施-运行后 | 成交供应商应验证被测信息系统投入运行后，责任单位是否每年委托测评机构开展密码应用安全性评估，是否具有评估报告；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投入运行。 |
| 应急-应急预案 | 成交供应商应验证责任单位是否根据安全事件等级制定了相应的应急预案及管理制度，明确了应急事件处理流程及其他管理措施，并遵照执行；如有安全事件发生，应检查是否有相应的处置记录。 |
| 8 |  | 应急-事件处置 | 成交供应商应验证责任单位在安全事件发生后，是否及时向信息系统的上级主管部门进行报告。 |
|  | 应急-上报 | 成交供应商应验证责任单位在安全事件完成后，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。 |

## 五、履约期限及履约地点

履约期限：1年

履约地点：甲方指定的地点

## 六、付款方式

合同生效且服务完成验收合格后30个工作日内甲方向乙方支付对应合同金额的全款。乙方根据甲方要求在甲方付款前向甲方开具对应订单全额与税法要求对应税率的增值税一般纳税人专用发票。

## 六、服务要求

（1）应按照国家标准和行业要求提供规范化、标准化的服务。

（2）拟参与本项目的测评人员具有信息安全等级测评师（DJCP）资质或具备高级工程师技术职称。

（3）本项目实施和验收测试所需的工具，由乙方负责提供。用于测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具等。在使用前，应对工具进行测评，如果需要则对工具进行软件或代码升级。

## 七、测评质量要求

项目管理是贯穿整个项目的一项任务。通过实施有效的项目管理，保证本项目能够按工作范围要求、按时间、按质量完成。投标人应提供质量控制及保证措施方案，包含项目质量控制及保证措施等。

## 八、测评风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

（1）操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

（2）操作时间控制

对测评直接影响系统工作时，尽可能避开敏感时期。

（3）人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

（4）制定应急预案

根据测评范围界定的系统情况，在实施前制定应急预案。

（5）关键业务系统风险控制

对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

（6）优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

（7）数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

## 九、验收要求

1.验收时间：合同生效完成测评服务，一年内完成验收。

2地点：湖北省武汉市

3验收内容：合同约定的服务事项

4项目验收标准：提交《网络安全等级保护测评报告》和《商用密码应用安全性评估报告》，中标人协助采购人办理定级备案手续，并取得备案证书。该项目过程中产生的文档，归采购人所有。乙方完全履行合同义务后，甲方按照合同文件列明的验收标准及要求进行验收，同时遵照《湖北省烟草商业系统采购履约验收管理办法》的相关约定。

5项目验收方式：一次性验收，双方依据项目内容和进度共同实施验收工作，验收结果和验收报告经双方确认后生效。

## 十、售后服务要求

乙方应提供本地化服务，具有专业化服务团队，提供1年咨询服务，服务方式包括电话技术支持、远程技术支持、现场技术支持等。