数据资源及安全管理子系统-密码测评采购需求

2025年

# 项目概况

近年来，网络和数据安全对国家安全和发展的重要性日益凸显，特别是在当前复杂多变的安全形势下，加强网络和数据安全保障工作已成为迫切需求。本项目依据《中华人民共和国密码法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《信息系统密码应用测评要求》、《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》、《商用密码应用测评量化测评规则》和系统自身的《密码应用技术方案》，对数据资源及安全管理子系统进行密码应用测评，通过密码应用测评深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全奠定基础。

本项目需采购符合条件的密码应用测评服务，在开展测评前，应安排技术人员对项目建设单位进行有效指导；在测评过程中，应积极配合项目建设单位督促项目承建公司进行问题整改，直至项目通过密码应用测评为止；在主体项目质量保证期内，应按规定期开展密码应用安全性评估工作出具符合规范的《密码应用测评报告》。

服务期限：合同签订之日起至项目验收止

服务地点：客户指定地点

采购金额（最高限价）：1,088,563元

组织形式：集中采购

采购方式：竞争性磋商

面向企业类型：大中小微

是否接受联合体响应：否

# 供应商资质要求

2.1具备政府采购法第二十二条规定的条件、未被列入信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）渠道信用记录失信被执行人。

2.2 供应商必须具有独立承担民事责任能力的在中华人民共和国境内注册的法人，具有良好的商业信誉和健全的财务会计制度，有依法缴纳税收和社会保障资金的良好记录，具有履行合同所必需的设备和专业技术能力。

2.3 供应商应是国家密码管理局下发的商用密码检测机构(商用密码应用安全性评估业务)目录中的测评机构。

# 测评服务范围

本次“数据资源及安全管理子系统-密码测评”项目针对“数据资源及安全管理子系统”项目开展密码应用测评工作，所属子系统清单如下：

|  |  |
| --- | --- |
| **序号** | **子系统名称** |
| 1 | 大数据平台（PaaS层） |
| 2 | 数据资源治理系统 |
| 3 | 数据安全管理系统 |
| 4 | 数据共享交换系统 |

# 测评工作内容

## 服务内容概述

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）、《信息系统密码应用测评过程指南》（GM/T 0116-2021）、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等技术要求，对信息系统进行密码应用的合规性、正确性、有效性进行安全性评估，通过密码应用测评深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全奠定基础。

测评的内容包括但不限于以下内容：

1、安全技术测评：包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个方面的安全测评。

（1）物理和环境安全

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全技术测评-物理和环境安全 | 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 |

（2）网络和通信安全

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全技术测评-网络和通信安全 | 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 |

（3）设备和计算安全

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全技术测评-设备和计算安全 | 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 |

（4）应用和数据安全

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全技术测评-应用和数据安全 | 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 |

2、安全管理测评：包括安全管理（分为制度、人员、建设和应急四个子模块）的安全测评。

（1）管理制度

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全管理测评-管理制度 | 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 |

（2）人员管理

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全管理测评-人员管理度 | 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 |

（3）建设运行

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全管理测评-建设运行 | 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 |

（4）应急处置

|  |  |
| --- | --- |
| 测评类别 | 测评单元 |
| 安全管理测评-应急处置 | 应急策略 |
| 事件处置 |
| 向有关主管部门上报处置情况 |

## 服务要求

（1）服务提供方应详细描述本次项目的整体实施方案，包括项目概述、密评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

（2）服务提供方应详细描述实施人员的组成、资质及各自职责的划分。服务提供方应配置有经验的技术人员进行本次项目实施。

（3）本次项目实施过程中所使用到的各种工具软件由服务提供方推荐，经采购人确认后由服务提供方提供并在项目中使用。在响应文件中应详细描述所使用的安全技术工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

（4）本次项目实施过程中所使用到的测评工具，应包括自主密码专用检测工具、漏洞扫描工具等获得许可的检测工具，对系统数据进行分析，并以分析结果辅证评估报告。

（5）安全技术工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由服务提供方推荐，经采购人确认后由服务提供方提供并在项目中使用。

（6）项目实施需要的运行环境（如场地、网络环境等）由采购人提供，服务提供方应详细描述需要的运行环境的具体要求。

（7）本项目质量保证期为项目验收后3年，项目验收后，在3年运维期内，每年对项目开展密码测评，并出具测评报告。

# 测评文档要求

1、测评机构在开展安全测评前，应深刻理解本项目实施的背景，同时密切结合该项目的实际情况，提供针对性的项目实施方案，并提交完整的《密码应用测评工作计划》及《密码应用测评方案》。

2、初次现场测评完成后，应出具《测评问题汇总表》，视情出具《商用密码应用安全性评估差距分析报告》。

3、全部测评工作完成后，应出具整体项目《密码应用测评报告》。

4、在主体项目质量保证期内，应按规定期出具《商用密码应用安全性评估报告》。

# 验收要求

测评服务工作期限终止时，服务提供方应当以书面形式向采购方提交测评服务相关资料。采购方在收到服务提供方提交的相关资料后10个工作日内，对服务提供方的工作进行验收。如属于服务提供方原因致使安全服务未能通过验收的，服务提供方应当在15个工作日内进行整改，并自行承担相关密码应用测评相关费用，再次接受采购方的验收，直至符合约定要求。

# 服务组织和人员要求

选派在项目服务方面富有经验的团队人员负责项目的密码测评，项目团队应配置对应的人员，团队应至少配备项目负责人1人，项目经理1人，测评人员5人，保密和档案管理员1人，具体人员要求如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人数** | **人员要求** | **驻场**  **要求** |
| 项目负责人 | 项目计划的部署，组织会议制定整个项目计划。项目过程中的协调组织，项目过程中的风险控制。对测评过程中遇到的各类技术问题进行决策。 | 1人 | 通过国家密码管理局组织的商用密码应用测评人员测评能力考核和注册密码安全专业人员证书（NSATP-CSP），密码学或计算相关专业硕士以上学历，信息安全专业的高级职称，具备5年及以上密码应用测评工作经验。 | 不驻场 |
| 项目经理 | 负责项目实施过程中测评技术管理工作。参与项目计划的实施，测评过程中的协调组织，保障整个测评任务的完成。 | 1人 | 通过国家密码管理局组织的商用密码应用测评人员测评能力考核和密码技术应用员证书，具备4年及以上密码应用测评工作经验。 | 不驻场 |
| 测评人员 | 负责项目实施过程中技术应用的测评工作 | 5人 | 通过国家密码管理局组织的商用密码应用测评人员测评能力考核和密码技术应用员证书，具备4年及以上密码应用测评工作经验。 | 不驻场 |
| 保密和档案管理员 | 负责对各类档案的接收，分类，编目，编制等系统管理。做好文件，资料，档案的保密保管工作。 | 1人 | 通过国家密码管理局组织的商用密码应用测评人员测评能力考核，具备3年及以上密码应用测评工作经验。 | 不驻场 |

人员要求具体如下：

* 密码测评人员要求：需要3年及以上信息系统商用密码应用安全性评估工作经验；了解各类密码测评操作平台和软件工具，有独立判断网络和系统问题的能力。
* 有应急事项发生时，人员2小时内到达现场。

# 供应商综合能力要求

供应商具有中国合格评定国家认可委员会实验室CNAS检测机构认可证书(资质范围：信息系统商用密码应用安全性评估)、商用密码产品检测服务相关ISO9001质量管理体系认证证书、商用密码产品检测服务相关ISO 27001信息安全管理体系认证的优先考虑。

# 密码测评工具和模拟测评环境要求

## 测评工具要求

本次项目实施过程中所使用到的测评工具，应包括具有自主知识产权或计算机软件著作权的密码检测工具（详细描述所使用工具的型号、功能、使用的方式和对环境和平台的要求以及使用可能对系统造成的风险等），对系统数据进行分析，并以分析结果辅证评估报告。

检测工具包括但不限于以下几类：

1、密码算法验证工具，包括国密算法SM2、SM3、SM4，常见的国际通用算法AES、DES、RSA等的验证；

2、随机数随机性检测工具；

3、数字证书检测工具，包括数字证书的格式的合规性验证、数字证书的证书链的检验等；

4、网络协议分析工具；包括但不限于SSL协议、IPSec协议；包括主动协议分析工具和被动分析工具。

## 模拟测评环境要求

服务提供方具有密码测评模拟验证环境的能力及相关设备，包括但不限于以下的密码设备：

1、SSL VPN：支持国密算法；具有商用密码产品认证证书，用于搭建SSL VPN网络，模拟SSL VPN通信信道的测评。

2、IPSec VPN：支持国密算法；具有商用密码产品认证证书，用于搭建IPSec VPN网络，模拟IPSec VPN通信信道的测评。

3、服务器密码机：支持国密算法；具有商用密码产品认证证书，用于实现重要数据的加解密和完整性保护，模拟重要数据加解密和完整性保护的测评。

# 保密责任

项目过程中不出现任何泄密事件和安全事故，在合同期内或合同终止后，未征得有建设单位同意，不得泄露与本项目及本合同业务有关的保密资料。

（1）测评单位因为本项目提供测评服务而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、电子文件、访谈记录、现场实测数据、建设单位相关工作程序等）以及因为本项目提供测评服务而形成的数据、信息和任何形式的工作成果，属于建设单位所有，均是建设单位要求保密的信息。除法律法规另有规定外，未经建设单位书面同意，测评单位不得对外泄露建设单位要求保密的信息，不得用于其他用途，否则测评单位需承担由此引起的法律责任和经济损失，包括但不限于直接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

（2）测评单位应采取必要的有效措施保证其参与本项目的人员（包括测评单位聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及投供应商的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若测评单位参与本项目的人员或测评单位合作方违反本条规定，测评单位应承担连带责任。

（3）保密期限自测评单位知悉保密信息起始至保密信息被合法公开之日止。

（4）除法律法规另有规定外，测评单位（含测评单位参与本项目的人员）未经建设单位书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本合同有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

（5）在本项目合同无效、终止或解除之后，合同各方在本合同中的保密义务并不随之终止，各方仍需依据本合同的保密规定履行保密义务。