**2025年青浦区重要网络和信息系统密码应用安全性评估**

**项目采购要求**

**上海市青浦区政务服务中心**

**(上海市青浦区大数据中心)**

## （一）项目概况

1、项目背景

党的十八大以来，我国商用密码管理逐步向法治化、规范化、体系化方向迈进。2019年10月26日，第十三届全国人民代表大会常务委员会第十四次会议表决通过《中华人民共和国密码法》，自2020年1月1日起施行，这既是党中央作出的重要战略部署，也是顺应全球信息化发展趋势、 维护国家网络和信息安全的必然要求。

2023年6月，我市印发系列文件，明确提出要做好党政机关及事业单位、教育、卫生健康、国资、公安、电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、社会保障、国防科技工业等重要行业领域信息系统密码应用与安全性评估工作，应同步规划、同步建设、同步运行密码保障系统并定期进行密码测评；信息化项目在项目报批阶段，编制密码应用方案并开展密码应用方案评审，同时将方案和密码应用方案评审报告作为履行项目审批程序的必备材料；信息化项目在建设阶段，确保密码应用符合相关规定或者批复要求，建设完成后需组织对系统进行密码应用测评，将结论作为验收重要内容，验收不合格的不得通过项目验收；信息化项目在运行阶段，对于不符合密码应用要求的信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建信息系统；上海市密码管理局、大数据局等部门会同有关职能部门，对密码应用情况实施监督管理，视情予以通报批评、暂缓安排投资计划、暂停项目建设直至终止项目；各部门应当严格按要求采用密码技术，并定期开展密码应用安全性测评，确保重要信息系统运行安全和信息资源共享交换的数据安全。

开展密码应用安全性评估工作是完善信息系统密码应用安全防护能力的一个重要环节，也是信息系统密码应用安全建设和管理的重要组成部分。通过测评可以发现信息系统密码应用的安全现状与需要达到的安全等级或目标的差异， 进行全面有效的密码应用安全整改建设，使系统密码应用在技术和管理方面有针对性的加强和完善，以确保网络和信息系统的安全。

1. 项目服务期限：自合同签订之日起至4个月内完成所有测评项目工作。
2. 采购金额：本项目采购预算为316.14万元人民币，最高限价为252.9万元人民币,超过项目最高限价的投标不予接受。

4、供应商应须具备有效期内的国家密码管理部门颁发商用密码检测机构资质证书（业务范围：商用密码应用安全性评估）

项目服务要求，在商用密码应用测评项目实施过程中，需邀请上海市密码管理局认可的商用密码应用安全性评估机构进行测评，并出具符合规范的《商用密码应用安全性评估》，并协助被测评单位及相关技术支撑单位落实密码应用安全整改工作。

# 第二部分：采购项目要求

## （一） 项目概述

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》等相关法律法规，对青浦区不少于15个重要网络和信息系统密码应用的合规性，正确性，有效性进行安全性评估，通过评估可以发现信息系统密码应用的安全现状，进行全面有效的密码应用安全整改建设，使系统密码应用在技术和管理方面有针对性的加强和完善，以确保网络和信息系统的安全。

## （二） 项目系统范围

|  |  |  |
| --- | --- | --- |
| **序号** | **单位名字** | **系统名字** |
| 1 | 区农业农村委 | 青浦农业农村信息共享平台（二期） |
| 2 | 上海市青浦区环境监测站 | 青浦区环境自动监测信息化服务平台 |
| 3 | 区机管局 | 青浦区机关事务管理系统 |
| 4 | 上海市青浦区城市运行管理中心(上海市青浦区城市网格化综合管理中心） | 青浦区"一网统管”业务智能协同平台 |
| 5 | 青浦区城市运行管理平台 |
| 6 | 中共上海市青浦区委政法委员会 | 青浦区禁毒智能化管理平台 |
| 7 | 上海市公安局青浦分局 | 公安信息网 |
| 8 | 视频传输网 |
| 9 | 青浦三实大数据信息管理模块 |
| 10 | 大数据分析研判系统(DMC) |
| 11 | 上海市青浦区国有资产监督管理委员会(上海市青浦区集体资产监督管理委员会） | 青浦国资国企在线监管系统 |
| 12 | 上海市青浦区政务服务中心(上海市青浦区大数据中心) | 青浦区电子政务外网升级改造项目的密码应用安全性评估 |
| 13 | 青浦区政务云管理平台密码应用安全性评估 |
| 14 | 青浦区政府投资信息化项目监管系统(二期)升级建设项目密码应用安全性评估 |
| 15 | 青浦区级视频共享平台(二期)密码应用安全性评估 |

## 测评依据

1. 《中华人民共和国密码法》；
2. 《商用密码应用安全性评估管理办法》；
3. 《关于规范和加强我市重要网络和信息系统密码应用与安全性评估工作的通知》；
4. 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）；
5. 《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）；
6. 《信息系统密码应用测评过程指南》（GM/T 0116-2021）；
7. 《信息系统密码应用高风险判定指引》；
8. 《商用密码应用安全性评估量化评估规则》。

## （四）测评内容

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）标准，参照《商用密码应用安全性评估管理办法》、《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，逐一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，通过商用密码应用安全性评估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 |
| 电子门禁记录数据完整性 |
| 视频记录数据完整性 |

（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 |
| 重要数据存储机密性 |
| 重要数据传输机密性 |
| 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 |

## （五）测评工作原则

遵循以下若干原则，是评估结论真实、准确、可信的基础，也是评估组在独立实施评估时，在相似的情况下得出相似结论的前提。本次商用密码应用安全性测评实施方案设计与具体实施应满足以下原则：

（1）客观公正原则：评估实施过程中评估人员应保证在最小主观判断情形下，按照评估双方认可的评估方案，基于明确定义的评估方式和解释，实施评估活动。

（2）经济性和可重用性原则：评估工作可重用已有评估结果，包括商用密码应用安全性评估结果。所有重用结果都应以结果适用于待评估系统为前提，并能够客观反映目前系统的安全状态。

（3）可重复性和可再现性原则：依照同样的要求，使用同样的评估方法，不同的评估机构对每个评估实施过程的重复执行应得到同样的结果。可再现性和可重复性的区别在于，前者关注不同评估者评估结果的一致性，后者则与同一评估者评估结果的一致性有关。

（4）结果完善性原则：在正确理解《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》各个要求项内容的基础之上，检测所产生的结果应客观反映系统的运行状态。评估过程和结果应服从正确的评估方法，确保其满足要求。

## （六）测评服务总体要求

（1）供应商应详细描述本次项目的整体实施方案，包括项目概述、密码应用测评方案、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）供应商应详细描述实施人员的组成、资质及各自职责的划分。供应商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供应商推荐，经采购人确认后由供应商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供应商推荐，经采购人确认后由供应商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，供应商应详细描述需要的运行环境的具体要求。

（7）供应商应提供自报告交付后一年的售后服务，由项目售后服务专员支撑项目售后阶段存在的一系列咨询服务。

（8）供应商应提供至少两次培训服务。

## （七）测评服务过程及内容要求

测评服务过程包括四项基本测评活动：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。测评方与被测单位之间的沟通与洽谈应贯穿整个测评过程。

（1）测评准备活动

本活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制密码应用测评方案做好准备。

（2）方案编制活动

本活动是开展测评工作的关键活动，主要任务是确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容等，形成密码应用测评方案，为实施现场测评提供依据。

（3）现场测评活动

本活动是开展测评工作的核心活动，主要任务是根据密码应用测评技术方案分步实施所有测评项目，以了解被测信息系统真实的密码应用现状，获取足够的证据，发现其存在的密码应用安全性问题。

（4）分析与报告编制活动

本活动是给出测评工作结果的活动，主要任务是根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的有关要求，通过单元测评、整体测评、量化评估和风险分析等方法，找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统所面临的风险，从而给出各个测评对象的测评结果和被测信息系统的评估结论，形成商用密码应用安全性评估。

测评各阶段详细的服务内容如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **测评阶段** | **测评类** | **服务说明** |
| 1 | 评估准备 | 准备阶段 | 编制项目计划书、收集被测系统基本资料并完成调查表格，分析调查结果，准备工具和评估表单 |
| 2 | 方案编制 | 评估方案编制 | 识别并描述被测系统基本情况、确定测评对象、资产和威胁评估、系统定级结果和测评指标、确定检查点和检查方法、确定单元测评内容 |
| 3 | 总体测评 | 总体要求 | 通过访谈、配置检查和工具测试的方式评估信息系统的密码算法、密码技术、密码产品和密码服务的合规性 |
| 4 | 安全技术测评 | 物理和环境安全 | 通过访谈、配置检查和工具测试的方式测评信息系统机房环境的安全情况。主要涉及对象为机房环境的电子门禁系统。本次评测包括电子门禁的身份鉴别和电子门禁记录的完整性保护。 |
| 网络和通信安全 | 通过访谈、配置检查和工具测试的方式测评信息系统的网络和通信安全保障情况。本次重点测评包括通信对象的身份鉴别、访问控制信息完整性、通信数据完整性和通信数据机密性等 |
| 设备和计算安全 | 通过访谈、配置检查和工具测试的方式测评信息系统的主机安全保障情况，本次重点测评包括本地主机和数据库服务器身份鉴别、远程管理身份鉴别身份信息机密性、访问控制信息完整性、敏感标记完整性、日志记录完整性等 |
| 应用和数据安全 | 将通过访谈、配置检查的方式测评信息系统的数据安全保障情况，主要涉及对象为信息系统的管理数据及业务数据等,本次重点测评包括信息系统身份鉴别、访问控制信息完整性、数据传输机密性、数据存储机密性、数据传输完整性、数据存储完整性、日志记录完整性等 |
| 5 | 安全管理测评 | 安全管理 | 安全管理部分为全局性问题，涉及密码安全管理制度、密码安全管理人员、系统实施和系统应急管理等四个方面。 |
| 6 | 分析报告阶段 | 报告编制 | 根据测评编制《信息系统商用密码应用安全性评估报告》、（商用密码应用安全性评估），包括：概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评的结果记录及结果汇总、整体测评、测评结果汇总、风险分析、评估结论等内容。 |

测评服务流程如下图所示：



|  |  |  |  |
| --- | --- | --- | --- |
| 角色 | 主要职责 | 人数 | 人员要求 |
| 项目  经理 | 负责制定整个项目计划方案，管控项目实施进度、团队人员管理，协调处理项目过程中遇到的各类问题。 | 1 | 1.具备《商用密码应用测评人员测评能力考核》证书；  2.具有注册密码安全专业人员证书NSATP-CSP；  3、具有密码学或计算相关专业本科以上学历；  4、具有省市及以上人社部门或工信部门颁发的信息安全专业的高级职称证书。 |
| 测评  人员 | 负责项目实施过程中技术应用的测评工作 | 20 | 1.提供不少于20人商用密码应用安全性评估服务团队，需提供加盖供应商公章的人员名单表和投标人为其缴纳的社保证明；  2.具备《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； |
| 档案管理员 | 负责对项目档案的接收、分类、编目等资料档案管理工作。 | 1 | 具备《商用密码应用测评人员测评能力考核》证书 |

## （八）服务组织和人员要求

## （九）测评工具要求

## 9.1 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。

## 9.2 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。

## （十）保密责任

1、中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，中标人不得对外泄露采购人要求保密的信息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

2、中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及中标人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。若中标人人员或中标人合作方违反保密规定，中标人应承担连带责任。

3、中标人（含中标人参与本项目的人员以及其合作方）未经采购方书面许可，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、出售与本项目有关的技术成果、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。

4、以上内容的保密期限自中标人知悉保密信息起始至保密信息被合法公开之日止。

5、中标人对采购人提拱的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息安全的泄露。未经采购人的同意不得利用采购人的网络及平台进行短信、彩信、微信发送,造成的一切后果由中标人负责。

运维过程中标人如出现失、窃密事情，参照网络和数据安全事件处罚措施同等处置，具体处罚措施由中心保密管理部门确定。

## （十一）项目的变更、解除和终止

如果服务提供方丧失履约能力、发生资不抵债或进入破产程序，招标单位可在任何时候以书面形式通知服务提供方终止本项目的执行而不给予服务提供方补偿。该终止本项目将不损害或影响招标单位已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容需做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

## （十二）违约责任

1、因服务提供方违反保密义务或知识产权约定的，采购人有权要求服务提供方支付本项目费用总额不超过30%的违约金，违约金不足以弥补采购人损失的，采购人有权要求服务提供方赔偿超过部分。若服务提供方违反保密义务，采购人还有权立即单方解除维护服务合同而不承担任何违约责任。

2、服务提供方有下列情形之一，采购人有权解除维护服务合同：

（1）服务提供方在服务周期内出现重大网络与信息安全事故；

（2）因服务提供方服务质量问题导致采购人无法实现目的；

（3）擅自转让或者分包其应履行的义务的；

（4）违反或者未履行维护服务合同约定的其他相关义务，且在采购人要求的合理时间内未能纠正的。

## （十三）关于转让和分包的规定

本项目不得转让不得分包。

## （十四）项目成果

提供不少于15个系统商用密码安全应用性评估报告。

## （十五）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服务总结报告及其他测评服务相关资料。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，并自行承担相关商用密码应用安全性评估相关费用，再次接受采购方的验收，直至符合约定要求。

## 服务质量考核要求

服务质量的考核结果将作为确认采购方需支付的最终合同总价的依据之一。

《服务考核表》要求如下：

考核得分说明：95-100分（含95分），支付当期金额100%；95分以下，每低1分扣除当期费用的1%。

附件：考核表

|  |  |  |  |
| --- | --- | --- | --- |
| **大类** | **项目** | **考核内容** | **得分** |
| 前期准备  （10分） | 项目启动会  （5分） | 召开项目启动会，明确项目时间计划、测评范围、测评流程等。  未召开扣5分。 |  |
| 项目计划（5分） | 制定整个测评的项目计划，计划应满足招标文件时间节点要求，测评实施须严格按照此计划进行。  未制定项目计划扣5分，项目计划制定不合理酌情扣分。 |  |
| 测评过程  （40分） | 系统调研（10分） | 针对测评范围内的系统进行调研，收集系统信息，调研结果应全面完整。  出现1处调研不全面或错误扣2分。 |  |
| 技术支撑（10分） | 针对项目的密码应用建设与整改提供技术支撑，及时有效的反馈整改意见。  出现一次不及时，扣1分。 |  |
| 现场测评  （20分） | 针对测评范围内的系统进行现场测评，测评过程应符合规范，不影响分局正常业务。  出现1次不规范操作扣5分，出现1次影响分局正常业务情况扣10分。 |  |
| 报告输出  （20分） | 测评报告编制与分析（20分） | 整理并分析现场数据，进行最终的测评报告编制工作。报告应真实符合实际情况。  出现1处错误或不符合实际情况扣5分 |  |
| 项目管理  （30分） | 人员配置  （10分） | 项目成员严格按照用户要求进行配置，不得擅自进行人员调整。  未向用户申请擅自进行人员调整、变动，每人/次扣减1分。 |  |
| 保密管理（20分） | 签订保密协议，若涉及到敏感信息应严格遵循公安保密要求，杜绝信息泄露安全隐患。  出现1次信息泄露安全隐患扣5分。 |  |

## （十七）付款方式

合同签订且采购人在收到成交供应商出具相应的测评报告后15个工作日支付100%合同款项。