

北京市统计局智慧统计建设项目

软件测试、 网络安全等级保护测评、 密码应用安全性评估 合同

甲方：北京市统计局

乙方：北京软件产品质量检测检验中心

甲方：北京市统计局

地址：北京市通州区宋庄南三街 209 号院

邮政编码：101118

法人代表：李素芳

联系人：商冰冰 手机：18101086112

电话：(010) 55533876

传真：(010) /

乙方：北京软件产品质量检测检验中心

地址：北京市海淀区东北旺西路 8 号中关村软件园 3A 楼

邮政编码：100193

法人代表：王威

联系人：王洪南

电话：(010) 82825511-610, 手机：13601255380

传真：(010) 82826408

(填写说明：本合同正文中带“□”符号的各项条款，为选择项条款，被选中的条款请在“□”内打“√”。)

本合同甲方委托乙方就 北京市统计局智慧统计建设项目 提供 软件质量测试、网络安全等级保护测评、密码应用安全性评估 专项技术服务。双方经过平等协商，制订如下合同条款，供双方遵照执行。

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

- (1) 在合同实施过程中的修正、补充合同
- (2) 本合同条款
- (3) 中标通知书
- (4) 投标文件 (含澄清文件)
- (5) 招标文件 (含补充文件)
- (6) 有关技术文件，图纸

(7) 国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件

第1部分 服务内容

1.1 送检（抽检）产品信息、被测系统信息：

甲方委托乙方进行软件质量测试、网络安全等级保护测评和密码应用安全性评估，应由甲方向乙方提交软件测试样本、部署好的被测系统。甲方应保证该样本信息、被测系统与实际交与乙方的样本、系统相符。

1.2 技术测试服务的内容：

系统测试	☒ 功能测试； ☒ 性能测试； ☒ 网络安全等级保护测评； ☒ 密码应用安全性评估。
------	--

第2部分 甲方提供的工作条件和协作事项

2.1 提交技术资料

甲方需向乙方提交与测试样本相关的下述附属技术文档，甲方应保证该技术文档信息与实际交与乙方的样本相符：

用户文档	☒ 用户手册； ☐ 操作手册； ☒ 使用环境要求说明。
测试数据	☒ 基础数据库数据； ☐ 可执行程序（存储介质为光盘）； ☒ 与测试环境搭建等有关的必要的文件。
开发文档	☒ 需求说明书； ☐ 需求分析文档； ☐ 总体设计方案； ☐ 数据库设计文档； ☐ 概要设计文档； ☐ 详细设计文档； ☐ 工程实施方案； ☐ 验收标准或开发目标； ☐ 关键技术、产品特点说明。
系统情况	☒ 网络拓扑图； ☒ 参与人员名单； ☒ 信息系统基本情况表； ☒ 信息系统承载业务情况表； ☒ 信息系统网络结构情况表； ☒ 物理环境情况表； ☒ 网络设备情况表； ☒ 终端设备情况表； ☒ 安全设备情况表； ☒ 服务器设备情况表； ☒ 数据备份情况表； ☒ 系统软件情况表； ☒ 应用系统软件情况表； ☒ 业务数据情况表； ☒ 安全威胁情况表。
管理文档	☐ 定级报告； ☐ 测评报告； ☒ 系统运维手册； ☒ 管理制度。
其他文档	

2.2 提供工作条件

2.2.1 测试开工日前，甲方应在指定地点建成模拟测试环境以及被测系统，并负责协调开发方在测试环境中安装被测软件的测试版本。测试期间，甲方应保证测试样本版本的一致性。

2.2.2 甲方为需要使用系统生产环境的相关测试内容安排环境使用时间。

2.2.3 甲方为乙方在进行技术测试过程中提供必要的咨询和现场技术支持工作，并协助乙方做好测试人员的业务培训工作。

2.2.4 甲方对乙方提交的书面文档资料、缺陷列表在规定时间内完成审议并给予回复，必要时需签字确认。

2.3 甲方提供上述工作条件和协作事项的时间

前述第 1.1、2.1 款所述样本、样本信息及技术文档，甲方应在本合同签署后被测系统具备测试条件的 10 个工作日内向乙方提交完毕。乙方在接到上述资料后，应对该资料的完整性及与样本的相关性进行必要的形式上的检查。如果甲方所提交的资料与合同的约定不相符的，乙方应在 5 个工作日内通知甲方进行补充或变更，甲方应在接到通知后的 5 个工作日变更或补充完毕并重新提交给乙方。

第3部分 乙方应完成的技术服务工作

3.1 测试地点

北京市统计局

3.2 测试时间

经双方商定，自乙方接到本合同第 1.1、2.1 款所述的样本、信息及相关技术文档后，根据单系统测试任务在 30 个工作日内，非因不可抗力或本合同约定允许，乙方应当完成本合同约定的软件测试项目，完成相关的测试报告制作。因甲方整改及复测所需时间不计算在前述期限之内。

3.3 测试报告

3.3.1 测试完成后，如拟出具结论为不合格，则乙方应向甲方提供具体的不合格内容及具有可行性的改进措施，甲方整改完毕后，乙方在 30 个工作日内再次进行测试，复测完成达到合格要求后，乙方应当为甲方出具下述形式的测试报告：

软件测试报告（含软件缺陷报告）

网络安全等级保护测评报告

商用密码应用安全性评估报告

上述约定的测试报告乙方应当向甲方出具贰份。

- 3.3.2 乙方出具的前款约定的测试报告仅对于本合同约定的样本负责,并不表明乙方对于与样本相同的产品质量作出了与测试报告相同的结论。
- 3.3.3 测试报告应当经过编制人员、审核人员、批准人员的签字并加盖报告单位印章后具有法律效力。无上述任何一种人员的签字或报告单位印章的,均不发生法律效力。
- 3.3.4 任何经过涂改的报告均不发生法律效力,但经过乙方确认的涂改并在涂改处加盖报告单位印章的除外。
- 3.3.5 任何复印的测试报告均不具有法律效力,但经过乙方确认与测试报告正本一致并在复印件上加盖报告单位印章的除外。
- 3.3.6 乙方对于与测试报告结论相关的技术性问题可以向甲方进行咨询,甲方应当给予协助。
- 3.3.7 测试报告由甲方在乙方通知的时间内领取。经双方协商,也可以其它方式送达给甲方,如特快专递等。

3.4 测试终止条件

- 3.4.1 乙方按照软件用户手册说明进行操作却无法安装、运行,经甲方指派的技术人员协助仍无法安装、运行。
- 3.4.2 乙方测试过程中,软件运行出现严重错误(BUG),乙方通知甲方处理后,仍无法解决,导致测试无法继续进行。
- 3.4.3 甲方提供的用户手册与软件实际运行情况严重不符、技术资料与系统实际运行情况严重不符或未能提供必须的技术资料,乙方通知甲方处理后,仍无法解决。
- 3.4.4 甲方提供的测试产品或介质带有计算机病毒,乙方通知甲方重新提供,甲方未提供,或重新提供的产品或介质仍然带有计算机病毒。
- 3.4.5 系统维护人员(包括设备、系统及安全管理员等)未能提供必要的技术支持,如提供测试工具接入网口、协助运行测试脚本、提供制度文件及记录等,乙方通知甲方处理后,仍无法解决,导致测试无法进行。

第4部分 合同金额及付款方式

4.1 合同金额

本合同暂定金额：¥855,000 元（大写：捌拾伍万伍仟）元整。具体金额依据项目实际批复金额计取。以上金额是乙方履行本合同甲方应支付的所有费用（含税），除双方另有约定外，乙方不得要求甲方支付任何其他费用。

4.2 付款方式

4.3 支付方式：

自本合同生效之日起 十 日内，甲方须向乙方支付全部费用的 50%，即人民币大写：肆拾贰万柒仟伍佰（¥427,500.00）元整。

测试完成后乙方向甲方交付《测试报告》，甲方收到报告 十 日内向乙方支付剩余 50% 费用，即人民币大写：肆拾贰万柒仟伍佰（¥427,500.00）元整。

本项目为财政拨款，待财政资金到位后再行支付。如因财政原因延迟支付，不视为甲方违约，乙方不得因此延迟、暂停、终止、拒绝义务的履行。

4.3.1 甲方向乙方缴纳测试费用，乙方应向甲方开具有效的发票，发票类型为增值税普通发票，发票抬头“北京市统计局”。

4.3.2 发票由甲方在乙方通知的时间内领取。如甲方需要开具增值税发票，视发票类型填署如下内容：

发票类型：增值税普通发票

发票明细：信息技术服务*测试费

税率：6%

单位名称：北京市统计局

纳税人识别号： /

经双方协商，也可以通过快递方式寄送：

地址：北京市通州区宋庄南三街 209 号院北京市统计局/收件人：商冰冰/联系电话：18101086112 。

4.3.3 甲方支付的服务费用可以支票方式支付，如电汇请汇入乙方指定的下列银行账户：

开户名称：北京软件产品质量检测检验中心

开户行：北京银行上地支行

账号：01090946300120112000987

第5部分 违约责任

- 5.1 甲方逾期支付测试费用（包括因合同变更而增加的费用）的，每逾期一日，应向乙方支付万分之五的违约金。超过约定付款期限 三十 日的，乙方有权解除本合同。
- 5.2 由于乙方原因不能按时提交测试报告(除本协议 7.2.1 条约定的情形外)，每逾期一日，应向甲方支付测试费用总额千分之五的违约金。超过约定日期三十日的，甲方有权解除本合同，并可要求乙方返还全部已缴纳的测试费用及支付合同总额百分之二十的违约金。
- 5.3 甲乙双方违反保密约定的，按保密条款的约定承担违约责任。
- 5.4 甲乙双方违反其它的义务而给另一方造成损失的，按国家法律法规的相关规定承担对方的损失。

第6部分 知识产权

6.1 甲方所提供乙方的所有文件包括送测软件样本、技术文档和测试数据内容仅用于本次测试的专用目的，未经甲方书面允许，乙方不得用作他途。更不得以任何方式侵害上述送测软件样本、技术文档和测试数据的知识产权。

第7部分 合同的变更与解除

- 7.1 经过甲乙双方协商一致，可以变更或解除本合同。
- 7.2 变更
- 7.2.1 由于甲方的原因而变更《测试需求》和本合同的其它内容的，如果导致乙方需要对测试方案和本合同的相关内容变更并增加乙方的工作量和支出。
- 依本款进行合同变更而由甲方向乙方支付的费用，双方应进行书面确认，并商定给付的具体时间。
- 7.2.2 由于乙方的原因而需要变更本合同的内容的，并从而导致乙方迟延交付测试报告的，则按每延误一个工作日，乙方给付甲方即人民币 贰仟 元（¥2000 元）计算，但以甲方已经向乙方缴纳的费用数额为限。
- 依本款进行合同变更而由乙方向甲方支付的费用，应在甲方领取测试报告时由乙方退还或在甲方应缴纳的测试费用余额中扣除。
- 7.3 解除
- 7.3.1 在测试过程中，因甲方所提供的样品及所属技术文档原因，而导致本测试合同不能履行的，则合同终止。乙方应按实际完成的工作量收取费用。其

余部分不再收取，已经收取的，退还甲方；

7.3.2 甲方的样本软件必须进行改进而必须更改本合同的相关条款的，造成乙方的工作量和/或支出增加和/或影响测试报告提交时间的，按本条第 2 款处理，甲方如未能按本条第 2 款处理，乙方将按照实际工作量计算费用，扣除先期已付费用后，多余费用退还甲方。

7.4 对于本合同的变更和解除，均不影响双方的保密义务的承担以及本合同中对于争议的解决的条款的效力。

第8部分 争议的解决

8.1 因为本合同的签署、履行、解释而发生的任何争议，双方应先行协商解决。若自争议发生之日起三十日内双方仍未能达成一致意见，则任何一方均可向甲方所在地区的人民法院提起诉讼，通过诉讼方式解决争议。

第9部分 保密

9.1 乙方均须履行对甲方保密信息的保密义务。

9.2 对于甲方的保密信息，在乙方测试完成后，甲方选择下述处理方式：

甲乙双方通过签署《安全保密协议》，按该保密协议中的约定，乙方承担保密责任。

第10部分 其它条款

- 1、本合同未尽事宜，双方另行协商并达成书面协议，作为本合同的附件。
- 2、本合同附件与本合同具有同等法律效力。
- 3、本合同自双方签字盖章之日起生效。
- 4、本合同一式陆份，甲乙双方各执叁份。

附件一 采购标的

附件二 招标技术要求

附件三：《安全保密协议》

甲方：(盖章)

代表人：(签字)

签约日期：2024年8月24日



乙方：(盖章)

代表人：(签字)

签约日期：2024年8月24日



附件一 采购标的

包号	标的名称	采购包预算金额 (万元)	数量	简要技术需求或服务要求	是否允许 进口产品 参加投标
第 6 包	测评服务	86.3	1 项	为北京市统计局智慧统计 建设项目提供软件测试、 网络安全等级保护测评和 商用密码应用安全性评估 服务	否

附件二 招标技术要求

一、采购标的

1. 采购标的

包号	标的名称	采购包预算 金额（万元）	数量	简要技术需求或服务要求
第 6 包	测评服务	86.3	1 项	为北京市统计局智慧统计建设项目提供软件测试、网络安全等级保护测评和商用密码应用安全性评估服务

2. 项目背景/项目概述

为深入贯彻落实国家统计局《“十四五”时期统计信息化发展规划》和北京市智慧城市建设要求,加快推进统计现代化改革,全面提升履职能力和服务水平,市局研究制定了《北京市统计局智慧统计发展规划（2023 年—2025 年）》（以下简称《规划》）和《北京市统计局智慧统计顶层设计》（以下简称《顶层设计》），按照《规划》的实施计划，拟于今年启动智慧统计项目建设，依托全市“三京”和“七通一平”共性基础平台，充分运用新技术和服务手段，推动统计制度方法设计、数据采集生产、加工处理、融合共享、分析应用全过程数字化转型。

坚持首善标准，严格按照全市智慧城市总规、控规要求，立足统计部门发展需要，推进现代信息技术与统计业务工作深度融合，以智慧统计建设推进统计工作的标准化、规范化、便捷化、智能化，实现统计数据质量持续提高、统计制度方法科学健全、统计调查能力明显增强、统计分析服务优质高效、统计体制机制更加完善、统计法治监督纵深推进。为加快推进符合首都特点的统计现代化改革，有效发挥“两个中心”作用，更好服务首都高质量发展，提供有力的信息化支撑。

二、商务要求

1. 交付（实施）的时间（期限）和地点（范围）

本项目实施期限为：2025 年 12 月 31 日前完成全部测评工作。

实施地点：采购人指定地点。

2. 付款条件（进度和方式）

详见合同约定。

3. 售后服务（质保期）（如适用）

详见下文

三、技术要求

1. 基本要求

本测评包包括软件测试、网络安全等级保护测评和商用密码应用安全性评估相应工作。测评对象涉及 5 个系统、1 个应用支持平台、1 个数据资源中心及相应系统接口。

1.1 采购标的需实现的功能及测评对象

- 统计调查采集系统：包含第二、三产业数据采集系统、第一产业数据采集系统、智能语音调查系统、部门数据采集系统、企业电子统计台账系统、人口抽样调查系统、专项调查系统；
- 统计业务管理系统：包含调查对象管理系统、数据加工系统、统计数据管理系统、业务处理全流程监控系统、对外数据服务；
- 统计监督系统：包含统计基层基础建设、统计执法；
- 统计数据全景分析系统：建立统计数据分析指标体系，规划设计各项专题分析场景，多维度可视化方式展示各项统计分析成果，全面、立体、直观反映全市经济运行情况；
- 行政业务管理系统：建设外网门户及工作台、移动办公应用；
- 系统接口：为了充分利用北京市统计局已有的建设成果，通过合理的设计实现将往期建设的正在使用的相关系统与本项目建设的应用系统无缝对接和集成，实现统一身份认证、业务信息交换。
- 应用支撑平台：建设统计业务协同，科学管控统计业务全过程。建设包含业务组件、技术组件、数据组件内容的应用支撑平台，实现用户的统一登录、统一认证、统一权限管理，实现数据处理任务的统一调度，基于工作流定制统计业务计划、业务流程，以流程驱动业务方式，提升统计业务协同能力、统计业务管理能力、统计数据分析能力。
- 数据资源中心：构建全市统计数据资源中心，通过接口归集、库表归集、文件归集等方式，实现对历史数据（普查数据、统计调查数据、部门数据、互联网数据等）的全量归集。数据归集后，根据统计业务需要，利

用元数据匹配、数据采集处理规则对基层数据、综合数据进行整理，形成数据来源目录供数据进一步处理使用。数据加工处理从数据资源池中获取基层数据、综合数据、专题数据、结果数据，提供数据关联、数据替换、数据合并、数据汇总等加工处理，以数据资源目录方式，供后续的数据应用、数据共享使用。

1.2 采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

GB/T 25000.51-2016《系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第 51 部分：就绪可用软件产品(RUSP)的质量要求和测试细则》

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

GM/T 0115-2021《信息系统密码应用测评要求》

GM/T 0116-2021《信息系统密码应用测评过程指南》

《商用密码应用安全性评估量化规则》

以上政策及标准规范如有最新规定或最新版本，按最新规定或最新版本执行。

2. 服务内容及要求

(一) 软件测试

投标人按照采购人系统设计文档中提出的测试需求范围，依据 GB/T 25000.51-2016《系统与软件工程系统与软件质量要求和评价(SQuaRE) 第 51 部分：就绪可用软件产品(RUSP)的质量要求和测试细则》对被测系统进行软件测试，发现并反馈软件存在的缺陷。

工作包括但不限于：

制定测试计划，设计测试用例和测试场景，执行测试，报告缺陷，分析测试结果。

1) 功能性测试要求

根据系统设计文档及其他需求文档，分析各功能点测试的优先级别。对系统功能的完备性、正确性、适合性等进行全面的测试，利用专业的测试模型，设计

合理的测试用例，测试发现系统存在的功能问题，并提出合理的改进建议。

2) 性能测试要求

根据系统设计文档及其他需求文档，测试在大用户量、大数据量和长时间连续运行等条件下，系统的响应时间和稳定运行情况。包括用户类型和使用模式、用户规模、交易并发量、系统吞吐量、模拟系统真实环境，测试系统处理高峰数据量的性能指标。

3) 可靠性测试

对系统的成熟性、可用性、容错性、易恢复性等进行测试，对出现用户接口错误、程序自身逻辑错误、系统或网络资源可用性引发差错的情况下的软件继续运行能力进行测试检查，并对系统的数据保存和恢复能力进行测试。

4) 易用性测试

对系统的可辨识性、易学性、易操作性、用户差错防御性、用户界面舒适性、易访问性进行测试，对系统的易用性提出合理的改进建议。

5) 用户手册等文档检查：

对用户文档集的完备性、正确性、一致性、易理解性进行测试检查，提高用户文档集的质量。

6) 报告编制

根据软件测试结果，出具《软件测试报告》（含《软件缺陷报告》）。

（二）网络安全等级保护测评

根据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》、（GB/T 28449-2018）

《信息安全技术 网络安全等级保护测评过程指南》等标准第三级的要求，对智慧统计建设项目进行网络安全等级保护测评。经测评后，形成测评报告，对统计信息系统安全状况未达到安全保护等级要求的，提出切实可操作的改进措施，确保按照提出的改进措施整改加固后，信息系统满足等级保护相关要求并获通过，满足安全需求。通过网络安全等级保护工作的落实，使信息系统安全现状，符合我国法律、制度的规定，通过公安部门的认可的 2025 年度信息系统等级保护测评。

根据等级保护 2.0 标准的要求，测评内容包括安全通用要求、云计算安全扩展要求和移动互联安全扩展要求。本项目服务内容包括以下方面：

1) 通用要求技术测评

- a) 安全物理环境测评。对物理位置选择、物理访问控制、防盗和防破坏、防雷击、防火、电力供应等方面进行测评，并形成测评结果记录。
- b) 安全计算环境测评。对身份鉴别、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、数据保密性等方面进行测评，并形成测评结果记录。
- c) 安全区域边界测评。对边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面进行测评，并形成测评结果记录。
- d) 安全通信网络测评。对网络架构、通信传输、可信验证等方面进行测评，并形成测评结果记录。
- e) 安全管理中心测评。对系统管理、审计管理、安全管理、集中管控等方面进行测评，并形成测评结果记录。

2) 通用要求管理测评

- a) 安全管理制度测评。对安全策略、管理制度、制定与发布、评审与修订等方面。
- b) 安全管理机构测评。对岗位设置、人员配备、授权和审批等方面进行测评，并形成测评结果记录。
- c) 安全管理人员测评。对人员录用、人员离岗、安全意识教育和培训等方面进行测评，并形成测评结果记录。
- d) 安全建设管理测评。对定级和备案、安全方案设计、产品采购使用、自行软件开发、外包软件开发、测试验收、等级测评等方面进行测评，并形成测评结果记录。
- e) 安全运维管理测评。对环境管理、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、密码管理、备份与恢复管理、应急预案管理等方面进行测评，并形成测评结果记录。

3) 云计算安全扩展要求测评

对云计算安全扩展要求中的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面进行测评，并形成测评结果记录。

4) 移动互联安全扩展要求测评

对移动互联安全扩展要求中的安全物理环境、安全区域边界、安全计算环境、安全建设管理、安全运维管理等方面进行测评，并形成测评结果记录。

5) 等级保护差距分析

根据国家网络安全等级保护政策和标准，分析信息系统与相应安全保护等级要求之间的差距，并对差距分析过程中发现的问题和风险提出整改建议，形成相关文件。

6) 协助整改并复测

参照《网络安全等级保护基本要求》，指导系统整改与完善，协助采购人完成整改加固工作，并对物理机房、网络设备、安全设备、主机设备、应用系统和管理制度等发现的安全问题进行复测核验。

7) 报告编制

根据测评结果进行整体测评和风险分析，形成等级测评结论，按照国家监管部门统一报告模板，每个系统分别出具公安部门认可的《网络安全等级保护测评报告》。

8) 辅助定级及备案工作

根据系统实际建设情况，协助采购人组织开展系统的定级工作，并配合辅助采购人向网安部门进行各类备案。

(三) 商用密码应用安全性评估

依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、GM/T 0115-2021《信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》、《商用密码应用安全性评估量化规则》等国家相关标准要求和系统自身的安全需求，对系统中密码应用的合规性、正确性和有效性进行评估。服务内容包括但不限于以下方面：

1) 密码应用方案咨询

应按照国家密码管理局要求从技术角度结合密码应用安全需求，对密码应用方案涉及的总体方案设计、技术方案设计、管理体系设计、运维系统设计、安全与合规性方面进行分析，提供咨询建议，并协助采购人开展方案评审工作。包括从密码算法、密码技术、密码产品、密码服务、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、密钥管理和安全管理（制度、人员、实施、应急）等方面，对智慧统计建设项目开展密码应用安全性评估。

2) 密码技术应用测评

密码技术应用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、应用和数据安全四个方面的安全测评。

- a) 物理和环境安全测评。对身份鉴别、电子门禁记录数据完整性、视频监控记录数据完整性等物理和环境安全方面所采取的技术措施进行测评，并形成测评结果记录。
- b) 网络和通信安全测评。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网络方面所采取的技术措施进行测评，并形成测评结果记录。
- c) 设备和计算安全测评。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方面所采取的技术措施进行测评，并形成测评结果记录。
- d) 应用和数据安全测评。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方面所采取的技术措施进行测评，并形成测评结果记录。

3) 安全管理测评

安全管理测评包括管理制度、人员管理、建设运行、应急处置四个方面的安全测评。

- a) 管理制度测评。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管理制度方面所采取的管理措施进行测评，并形成测评结果记录。
- b) 人员管理测评。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管理方面所采取的管理措施进行测评，并形成测评结果记录。
- c) 建设运行测评。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运行方面所采取的管理措施进行测评，并形成测评结果记录。

- d) 应急处置测评。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处置方面所采取的管理措施进行测评，并形成测评结果记录。

4) 整体测评与风险评估

对系统结构进行整体安全测评，并采用风险分析的方法，分析密码应用存在的安全问题，以及可能对信息系统安全造成的影响，形成整体测评与风险评估结果。

5) 报告编制

根据整体测评与风险评估结果，出具《商用密码应用安全性评估报告》。

3. 验收标准

在完成测试后出具验收文件，为系统的验收使用提供质量保证。需提交的验收文件资料主要包括：

《软件测试报告》（含《软件缺陷报告》）；

《网络安全等级保护测评报告》；

《商用密码应用安全性评估报告》。

4. 其他要求

投标人应依据招标文件中各项需求提供及时、高效的服务，在项目实施过程中，应满足以下要求：

1) 投标人需拥有一支稳定的服务队伍，并具有较强的技术实力，遇到突发情况时能够及时解决问题。

2) 投标人应提供至少 1 人担任项目经理，要求具有

5 年及以上相关测评工作经验；

具有有效的信息系统项目管理师证书；

具有有效的软件评测师证书；

具有有效的网络安全等级测评师证书或信息安全等级测评师证书（中级及以上）；

信息安全工程师或注册信息安全专业人员（CISP）或信息安全保障人员认证证书（CISAW）证书；

通过商用密码应用安全性评估人员测评能力考核，并取得国家商用密码应用

安全性评估人员测评能力考核小组颁发的证书；

具备较强的沟通协调能力；具有预见和应对项目风险能力。

3) 提供项目实施的工作计划，工作内容以及服务进度安排，制订并遵循测评服务标准化规程。

4) 投标人拟派本项目的项目经理及项目组成员需具备丰富的信息系统测试服务的实施经验，应选派工作责任心强、技术水平高、业务熟练、具备相关测评实施经验的人员参加该项目。

5) 为确保项目顺利实施，项目实施队伍应保持适当的规模，项目组组织结构需分工合理、层次清晰，且分工要为适应项目实施需要，具有软件评测师证书、网络安全等级测评师证书或信息安全等级测评师证书（等保测评工程师资质）、通过商用密码应用安全性评估人员测评能力考核，并取得国家商用密码应用安全性评估人员测评能力考核小组颁发的资质证书。配备人员数量应满足项目需要，原则上实施人员（除项目经理外）不得少于6人，不允许职责交叉，不得因为人员离职影响项目的正常开展。

6) 项目经理、实施人员应满足项目需要，如果人员不能胜任，采购人有权要求投标人更换人员。

7) 投标人需拥有完善的技术保障服务体系，能够为本项目的所有用户提供统一快捷的技术保障服务。投标人必须向用户免费提供电话、E-Mail 技术支撑等方式。

8) 投标人应做到严格遵守合同规定，执行《中华人民共和国保守国家秘密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，服从采购人的管理，严格遵守采购人的保密规定和工作制度，并承担相应的保密责任，与采购人签订保密协议。

附件三 安全保密协议

安全保密协议

甲方：北京市统计局

乙方：北京软件产品质量检测检验中心

乙方住所：北京市海淀区东北旺西路 8 号中关村软件园 3A 楼

甲、乙双方于 北京市统计局智慧统计建设项目（第 6 包） 软件测试、网络安全等级保护测评、密码应用安全性评估 已经或将要知悉对方的相关保密信息。为了保护上述合作中涉及的保密信息，明确双方的权利义务，甲、乙双方在平等自愿、协商一致的基础上达成以下协议：

第一条 安全要求

一、乙方必须遵守甲方的各项规章制度，严格按照工作规范组织进行服务，制定切实可行的措施保障人身安全、设备安全、信息安全。

二、乙方必须制定合理的措施对本项目的服务人员进行管理和思想教育，加强保密意识，安全意识。

第二条 保密信息范围

本协议所称的“保密信息”是指乙方在合同履行过程中获得的下列信息，但不包括乙方通过公众渠道可以获得的信息或经甲方书面同意允许向第三方透露的信息：

一、工作秘密。一切与政府工作有关的信息资料或其他性质的资料，包括但不限于政府业务数据、人员机构信息、财务资料等；

二、技术秘密。指甲方的计算机信息系统网络和技术架构、信息安全体系结构、软件、数据库系统、系统数据、文档及技术指标、参数等；

三、其他保密信息。包括但不限于服务过程中获取的有关数据、流程、分析成果，甲方的内部管理资料，甲方其他项目的信息及有关政府行政机关规划、调整等尚未公开的资料。

上述保密信息的表现形式不限，无论是书面的、电子的、口头的或其它任何形式的信息。

第三条 安全保密期限

本协议约定的保密责任长期有效，不因项目合同的解除、终止等而失效。

第四条 保密义务人员

本协议的保密义务人员为乙方单位及乙方单位涉及保密信息的员工。

第五条 保密义务

乙方保证对所获悉的甲方保密信息按照下列规定进行保密，并在缺少相关保密条款约定时，应至少采取适用于对私密信息同样的保护措施和审慎程度进行保密：

1. 仅将本协议下保密信息使用于与服务工作有关的用途。
2. 除直接参与服务提供的人员之外，不得将保密信息透露给其他无关人员或任何第三方。
3. 不能将甲方保密信息的全部或部分进行发布、传播、复制或仿造。
4. 未经甲方书面许可并采取加密措施，不得擅自将载有保密信息的任何文档、图纸、资料、磁盘、胶片等介质，带离甲方工作场所。
5. 乙方单位应与本协议保密义务人员签订《保密承诺书》；应告知并以适当的方式要求其直接参与项目的人员，按照本协议规定保守保密信息。如工作人员违反本协议规定，泄露甲方保密信息的，乙方应承担违约责任。
6. 对于用户数据和服务结果数据的保管、访问，乙方无关人员不能访问；必需访问的人员，乙方要进行严格的访问控制；管理用户数据的人员应由乙方严格筛选。
7. 对于甲方提供给乙方使用的任何资源，如网络、注释说明等，乙方都只能将其用于甲方的工作项目，而不能用于其他目的，特别是从事侵害甲方利益的活动。

第六条 保密信息的交回

一、开发运维工作终止后，乙方应按照甲方的要求对相关保密信息做相应处理，如销毁或其他处理方式。乙方工作期间使用的软硬件设备，应允许甲方进行必要的检查和处理。

二、当甲方要求乙方交回保密信息时，乙方应立即交回所有的书面或其它有形的保密信息以及所有描述和概括保密信息的文件。

三、未经书面许可，乙方不得丢弃和自行处理保密信息。

第七条 违约责任

乙方未履行本协议下的任一款均视为违约。如果发生违约情况，乙方应按照甲方要求采取有效的补救措施，以防止泄密范围继续扩大，同时还应向甲方报告，甲方有权对由此引起的损失要求乙方予以赔偿。

第八条 其他

一、本协议未尽事宜，甲、乙双方另行签订补充协议，补充协议与本协议具有同等法律效力。

二、本协议一式陆份，甲、乙双方各执叁份。

三、本协议自甲、乙双方签章之日起生效，本协议签订之前乙方因已经开始履行合同等原因已知悉本协议项下的保密信息的，本协议的效力溯及至乙方知悉本协议项下的保密信息之时。

甲方：（盖章）

北京市统计局

法定代表人/



授权代表(签字):

郑江倩

2024年 8月29日

乙方：（盖章）

北京软件产品质量检测检验中心

法定代表人/



授权代表(签字):

王威

2024年 8月29日