海淀区信息系统等保和密码测评统一服务项目运维服务合同

项目名称：　海淀区信息系统等保和密码测评统一服务项目

甲　　方：　北京市海淀区大数据中心

乙　　方：　北京中科卓信软件测评技术中心

合同编号：

签订地点：　北京市海淀区

合同正文

甲方：北京市海淀区大数据中心

法定代表人：刘大鹏

地址：北京市海淀区中关村南大街 3 号海淀科技大厦

乙方：北京中科卓信软件测评技术中心

法定代表人：黄鹂

地址：北京市海淀区闵庄路 3 号 102 幢二层 207 室

根据《中华人民共和国政府采购法》《中华人民共和国民法典》等有关法律法规规定，海淀区信息系统等保和密码测评统一服务项目经甲方公开招标，确定乙方为中标供应商，甲乙双方本着平等、自愿和诚实信用原则，签订本合同。

第一条　定义

1. 下列名词和用语，除上下文另有规定外，应有如下含义：

（1）“项目”指甲方委托乙方的海淀区信息系统等保和密码测评统一服务项目。

（2）“甲方”是指承担直接投资责任和委托服务业务的一方。

（3）“乙方”是指在工商行政管理部门登记注册，取得企业法人营业执照，为甲方提供本合同约定运维服务的单位。

（4）“日”是指任何一天零时至第二天零时的时间段。

（5）“月”是指根据公历从一个月份中任何一天开始到下个月对应日期的前一天的时间段。

（6）“总投资”是甲方与乙方所签合同的总金额。

（7）“交付”指乙方按本合同约定向甲方提交运维服务过程中产生的技术资料、系统运行报告、故障处理记录、月度/季度服务总结等成果，并经甲方确认接收的过程。

（8）“培训”为确保甲方使用人员能够正常使用系统，乙方向甲方使用人员提供的必要技术培训和技术指导。

（9）“验收”指甲方按照本合同约定的验收要求，对乙方运维服务成果进行评审，验收通过以双方签署的《项目验收单》为标志。

（10）“运维服务”：指乙方根据本合同约定，为甲方指定的系统提供的运维相关持续性服务。

（11）“服务期限”：指本合同约定的乙方为甲方提供运维服务的起止时间。

（12）“保密信息”指乙方因履行本合同而取得的甲方未公开的信息，包括但不限于甲方的业务数据、技术文档、用户信息、系统架构、商业计划及本合同内容本身。

2. 本合同适用的法律包括中华人民共和国法律、行政法规、司法解释，以及与运维服务相关的部门规章、项目所在地的地方法规等。

3. 本合同文件（包括主合同、附件、补充协议、双方往来函件等）均使用汉语语言文字书写、解释和说明。若因特殊需要产生其他语言版本，仅作为参考，以汉语版本为准。

第二条　合同文件的组成

本合同由下列文件共同构成，彼此互为解释和补充。若文件内容存在冲突，按以下优先支配地位的次序适用（优先次序高的文件效力优先）

1. 本合同书正文

2. 本合同书的补充协议（含双方就服务变更、标准调整等签订的书面协议）

3. 本合同书、补充协议的附件（附件内容与主文或补充协议冲突的，以正文或补充协议为准）

4. 双方在合同履行过程中形成的书面确认文件

5. 中标通知书/中选通知书。

6. 乙方投标文件（包含澄清文件、承诺函等，若与甲方文件冲突，以本合同约定为准）

7. 甲方招标文件（含招标文件变更说明、补充通知等）

第三条　服务内容和要求

1.服务范围及目标

本项目服务目标以《北京市海淀区信息化运行维护项目预算申请报告》为基础设立，服务范围、核心目标应包含以下内容：

（1） 服务范围

2027 年度海淀区信息系统等保和密码测评统一服务项目测评范围包括为海淀区 97 个三级系统、11 个二级系统提供等级测评服务，为 78 个三级系统提供密码测评服务，具体系统名称和内容根据甲方要求指定。

（2） 总体要求

2027 年度海淀区信息系统等保和密码测评统一服务项目的服务内容包含对海淀区政务信息系统中 97 个三级系统（包括政务外网、视频专网、业务系统等）和 11 个二级系统开展 2027 年度的等级保护测评服务和对部署在政务云平台上的 78 个三级政务信息系统开展密码应用安全评估服务，促进密码应用安全建设。

具体服务要求如下：

（一）等级测评服务

为保障海淀区政务系统合法合规、安全稳定运行，本项目将依据等级保护基本要求为 97 个三级系统和 11 个二级系统提供完善的等级测评，等级测评主要内容包括信息系统资产梳理、定级备案变更服务、差距分析服务、脆弱性检测服务、渗透测试服务、安全加固咨询服务、安全管理制度更新服务、正式等级测评、网络安全事件应急处置协助以及网络安全等级保护培训等。

（二）密码测评服务

为加强密码应用安全建设，正确规范使用密码技术和服务保障政务信息系统数据安全，本项目需依据密码应用基本要求为 78 个部署在政务云平台上的三级信息系统提供全面的密码测评服务，主要内容包括密码应用调研、协助密码应用方案编制更新、密码应用差距分析、密码整改咨询、密码管理制度建设协助、正式密码应用安全性评估、密码应用安全培训等。

（3） 预期达到的效果：

通过统一组织对海淀区政务信息系统开展等级测评和密码测评工作，掌握信息系统的安全总体状况，发现存在的风险问题，完善信息系统安全防护体系，给出信息系统在安全管理、安全技术建设方面与等级保护要求及密码应用基本要求之间的差距，为政务系统进一步完善安全管理策略、落实安全管理和密码应用提供指导依据，全面提升海淀区政务系统的网络安全和密码防护水平，保障信息系

统的正常运行，满足国家信息安全对等级保护、密码应用相关政策、文件与标准的要求。

2.服务方案及要求

（一）等级测评服务

为保障海淀区政务系统合法合规、安全稳定运行，本项目将依据等级保护基本要求为97个三级系统和11个二级系统提供完善的等级测评，等级测评主要内容包括信息系统资产梳理、定级备案变更服务、差距分析服务、脆弱性检测服务、渗透测试服务、安全加固咨询服务、安全管理制度更新服务、正式等级测评、网络安全事件应急处置协助以及网络安全等级保护培训等。

1.信息系统资产梳理服务

对项目服务范围内三级系统的安全现状进行梳理，理清信息系统的资产构成和安全保护情况，明确被测系统的详细组成，包括网络拓扑、业务应用、业务流程、设备信息及其重要程度（服务器、数据库、网络安全服务等），以及管理人员、管理制度、安全应急事件等安全管理情况，输出完善的系统调查报告。

2.定级备案变更服务

对需进行备案变更或重新进行定级备案的系统（如整合后的信息系统）参照《定级指南》国家标准，对系统的安全保护等级进行确定；根据《信息安全等级保护管理办法》相关要求，协助系统建设和使用单位准备备案材料，完成备案或备案变更手续。

3.差距分析服务

根据《网络安全等级保护基本要求》等相关国家和行业标准，对服务范围内的各信息系统进行差距分析，分析其在技术和管理层面与《基本要求》之间存在的差距，出具问题清单和整改建议，形成全面、完整的差距分析报告。

4.脆弱性检测服务

针对系统的部署环境特点，针对性采取有效的漏洞扫描技术，对支撑业务系统运行的服务器、数据库和中间件等开展全面的漏洞检测，并与最新的漏洞库进行比对和验证，确认漏洞详情、数量、等级、修复意见等，输出系统漏洞扫描报告。

5.渗透测试服务

对海淀区重要的政务系统进行渗透测试，在取得授权的情况下，采取主动探

测和模拟攻击的方式对应用系统进行渗透，包括采取各种已知的脆弱性测试方法如 SQL 注入、XSS 跨站脚本、弱口令等，检测应用系统的高危漏洞和安全问题。根据渗透测试的结果，形成渗透测试报告，对在渗透测试中发现的高危漏洞进行通告并协助及时进行整改。

6. 安全加固咨询服务

依据差距分析报告、漏洞扫描报告、渗透测试报告等内容，为各系统建设单位提供整改建议，协助编制安全加固方案，提供全面的整改咨询服务，协助开发运维单位对服务器、数据库等进行全面的安全加固，修补漏洞，完善安全策略配置，在使系统满足等级测评要求的同时，保障系统安全运行。

7. 安全管理制度更新服务

依据差距分析情况，从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等方面出发，结合信息系统建设单位实际的安全管理制度及其执行情况，协助其根据需要修订和更新安全管理制度。

8. 正式等级测评服务

根据国家网络安全等级保护政策要求和国家标准，由服务单位开展正式的等级测评工作，对整改后的信息系统从物理安全环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个技术层面和安全管理制度等五个安全管理层面逐项进行单项测试、单元测试、整体测评、系统安全保障评估、安全问题风险分析等活动，确定最后的风险问题和系统等级保护测评结论，按照最新模板要求，出具规范完整的《网络安全等级测评报告》。

9. 网络安全事件应急处置协助

在项目服务期间，当服务范围内的信息系统遭受网络攻击时，根据信息系统受到的安全攻击情况，提供网络安全事件应急处置协助，配合运维单位进行风险应急处置，排查攻击源和问题发生原因，对攻击进行抑制，并协助运维单位根除风险和恢复系统运行。

10. 网络安全等级保护培训

统一组织网络安全培训，内容可覆盖安全意识培训、信息安全政策法规解读、等级保护安全建设范例解读、应急预案及模拟演练等，通过培训促进各单位安全相关人员理解最新政策法规要求、提升安全意识，促进各运维人员了解网络安全防护体系，提高网络安全技能，从提升安全人才的能力的角度提高信息系统安全

管理和安全运维水平。

（二）密码测评服务

为加强密码应用安全建设，正确规范使用密码技术和服务保障政务信息系统数据安全，本项目需依据密码应用基本要求为78个部署在政务云平台上的三级信息系统提供全面的密码测评服务，主要内容包括密码应用调研、协助密码应用方案编制更新、密码应用差距分析、密码整改咨询、密码管理制度建设协助、正式密码应用安全性评估、密码应用安全培训等。具体要求如下：

1.密码应用调研

组织专业的密评工作人员前往被测单位进行现场踏勘，了解被测单位系统建设情况、物理环境，为密评方案的编制收集信息，准备相应的材料和工具，完成商用密码应用调研表。

2.协助密码应用方案编制更新

结合海淀区政务云国产化和密码建设的最新情况，依据GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》等标准要求，与各系统开发单位、密码厂家协同，协助各单位编制或更新商用密码应用方案，并为密码应用方案的规范性、有效性把关。

3.密码应用差距分析

对各个系统的密码应用情况进行差距分析，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等技术方面，以及管理制度、人员管理、建设运行、应急处置、密钥管理等管理方面，查找与基本要求的差距，分析系统存在的风险问题，出具密码应用问题清单。

4.密码整改咨询

根据差距分析结果，依据GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》，提出各个问题的详细整改建议，并从正确使用密码技术保障真实性、机密性、完整性、不可否认性等方面协助指导各单位进行系统密码安全的建设整改。同时，协助各单位完善密码管理制度建设，提高密码管理工作的规范性。

5.密码应用安全性评估

对更新后的密码应用方案进行评估，包括分析安全控制措施描述及指标适用情况、安全控制措施评估结果等，确保密码应用方案符合相关标准要求，出具《密

码应用方案商用密码应用安全性评估报告》。在系统密码整改建设完成后，组织专业密评人员对信息系统开展正式密码应用安全性评估，并在测评工作结束后根据测评情况编制报告，出具最终《商用密码应用安全性评估报告》，指导被评估单位完成密码备案。

6. 密码应用培训

向被评估单位开展密评政策、标准解读和密码技术培训服务。向各单位提供关于安全管理、管理制度、人员制度、建设运行制度、应急制度以及相关国产密码技术知识的普及和咨询讲解等，促进各单位更加深入理解密码应用的政策及技术要求。

3.服务质量标准

本项目网络安全等保测评和密码测评应符合以下相应法律法规及国家标准要求，确保规范有效实施测评活动。

1.《中华人民共和国网络安全法》

2.《中华人民共和国密码法》

3.《关于信息安全等级保护工作的实施意见》

4.《信息安全等级保护管理办法》

5.《商用密码管理条例》

6.《商用密码应用安全性评估管理办法》

7. GB 17859-1999《计算机信息系统 安全保护等级划分准则》

8. GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

9. GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》

10. GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

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

12. GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》

13. GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》

14. GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

15. GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》

16. GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》

17.《商用密码应用安全性评估 FAQ》

18.《商用密码应用安全性评估量化评估规则》

4.服务期限

本合同自 2026 年 11 月 1 日起至 2027 年 10 月 31 日止。

在不改变合同其它条款的情况下，可视服务情况与乙方续签合同，续签次数不得超过两次，总服务期限不得超过三年。本合同为第【一】年服务期合同。

5.服务人员和要求

乙方不需提供驻场服务。

为保障项目实施质量和进度要求，乙方组成 29 人的服务团队（含等级测评师和密码测评人员），其中包括 1 名项目经理、1 名质量总监和 27 名项目组成员。

乙方更换驻场服务人员的，需提前 7 个工作日书面通知甲方并说明理由，经甲方书面同意后方可更换，新人员资质不得低于原人员。

若乙方擅自更换服务人员，未符合合同约定的人员要求，乙方应及时改正。甲方可按照乙方未符合约定人员要求的情况，扣减相应人员资质差额。

第四条 验收

1.验收流程

乙方完成服务期内所有服务内容，并在 3 个工作日内向甲方提交验收申请及验收材料，对验收材料不完整的，甲方应告知乙方需补充的内容，乙方需在 2 个工作日内补正。

甲方在 5 个工作日内组织验收工作，并出具项目验收单，即视为通过验收；验收不合格的，乙方应在 5 个工作日内完成整改，并重新申请验收。

2.验收材料

乙方应在项目期限内完成所有测评工作，并按项目要求为对应系统出具正式盖章的《网络安全等级测评报告》《商用密码应用安全性评估报告》。

若因乙方提供虚假材料，导致结算金额调整或甲方损失，甲方有权按照实际损失向乙方追偿。

第五条 价款及支付

1.本合同以人民币为货币单位，均为含税价格。

2.总价款

本合同总价款为：人民币 15,853,000.00 元（大写：人民币壹仟伍佰捌拾伍万叁仟元整）。

本价款为包含全部服务成本、税费、利润及合同约定的其他所有费用的最终固定价款，除本合同另有约定外，甲方无需向乙方支付其他任何费用。

3.付款方式

本合同分为两次付款。

首付款：合同生效之日起六个月内，甲方向乙方支付 50%服务费人民币 7,926,500.00 元（小写）（大写：人民币柒佰玖拾贰万陆仟伍佰元整）。

尾款：乙方完成本合同全部服务内容、经甲方验收合格后 60 日内，甲方在合同总价中扣除首付款和以下款项后，向乙方支付剩余金额。

（1）实际未测评的系统数量对应的测评费用；

（2）根据合同规定应扣减的款项；

（3）本合同约定的扣减款项（违约金、赔偿金及扣款），甲方均有权从任何一期应向乙方支付的款项中直接扣除。

尾款 = 合同总价款 – 首付款 – 上述扣减款项。

4.支付方式

甲方通过银行转账方式支付款项，乙方指定收款账户信息如下：

开户名：北京中科卓信软件测评技术中心

开户行：民生银行北京香山支行

账号：602089096

乙方账户信息变更的，应提前 5 个工作日书面通知甲方，否则因此产生的付款延误由乙方承担。

5.发票

甲方付款前，乙方应向甲方提供等额、合法、有效的增值税普通发票。因乙方发票问题导致甲方付款延迟的，责任由乙方承担，甲方不承担违约责任。

6.财政拨款延迟处理

乙方知晓甲方支付款项来源于财政拨款，若因财政拨款未及时到账导致甲方付款延迟的，付款时间自动顺延。顺延期间，甲方不承担违约责任，乙方不得因此暂停服务。

7.按照第四条验收的相关约定，如因乙方未能按时提供材料导致甲方未能按期付款，产生的付款延误后果由乙方承担。

第六条　合同变更和终止

1.合同变更的前提与变更形式

在本项目服务核心目标不变的前提下，因以下情形需变更合同内容的，双方应协商一致并签署书面补充协议：

（1）甲方因业务需求调整导致服务范围发生变化的；

（2）系统运行环境发生非预期变动，需调整运维方案的；

（3）双方约定的其他合理情形。

补充协议经甲乙双方法定代表人或授权人签章并加盖单位公章或合同专用章后生效，与本合同具有同等法律效力。

2.变更后的价款限制

除本合同另有约定或因不可抗力导致的必要变更外，合同变更后的总价款（含原合同价款及变更新增费用）不得超过本合同总价款。超出部分甲方不予支付，相关费用由乙方自行承担。

若变更导致服务内容减少的，总价款应按实际减少的服务量相应扣减。

3.发生下列情形，合同提前终止

（1）双方协商一致提前终止的。

（2）甲乙任何一方单方面提出终止合同，需提前【3】个月通知对方，双方协商解决。

（3）甲方违反本合同条款的，包括但不限于未按照合同约定履行付款义务或严重违反法律规定等。

（4）乙方违反本合同条款的，包括但不限于未按合同约定履行相关服务和承诺/保证或者严重违反法律规定等。

第七条　权利和义务

1.本合同服务期间产生的所有数据及成果（包括但不限于网络安全等级测评报告、商用密码应用安全性评估报告、服务总结报告等）的所有权及知识产权归

甲方所有。

乙方应在服务期满或合同终止后5个工作日内，将上述数据及成果按甲方要求的格式及方式，完整交付给甲方，不得留存副本（经甲方书面同意的除外）。

2.甲方应在本合同生效后5个工作日内，向乙方提供服务所需的基础信息、数据及相关资料，并确保所提供资料的真实性、完整性。因资料缺失或错误导致乙方服务延误的，责任由甲方承担，服务期限相应顺延。乙方仅可将甲方提供的基础信息、数据及相关资料，用于本合同约定的服务，不得用于其他用途，服务结束后应及时返还或销毁。

3.乙方履行合同需与第三方配合的，甲方应在收到乙方书面协调请求后5个工作日内牵头组织协调。若因甲方未及时协调或协调无果导致乙方服务无法正常进行的，乙方可书面申请本合同延长服务期限。

4.甲方应按本合同第五条价款及支付的约定，按时足额向乙方支付款项。

5.乙方应于每周一通过OA系统运维管理模块向甲方提交上周周报（电子版）。周报内容包括但不限于服务完成情况、故障处理明细、系统运行指标记录、存在问题及下周计划。

6.乙方应于每月5日前通过OA系统运维管理模块向甲方提交上月月报。月报内容包括但不限于月度服务总结、运维质量达标情况、备品备件实际发生费用明细及下月计划。

7.乙方应配合甲方对合同服务完成内容、进度、质量做验证。验证方式包含书面核查、现场核查、第三方验证。

8.乙方应在验收通过后5个工作日内，配合甲方梳理项目资料并按甲方要求归档（电子版存入指定服务器，纸质版装订成册）。

9.若乙方未履行资产管理义务，导致资产损失，甲方有权依据合同约定追究其违约责任，包括但不限于从应付款项中扣减款项、要求赔偿损失、解除合同等。

10.如果第三方机构或个人对甲方提出质疑或投诉，乙方应在知悉后24小时内书面通知甲方，双方应共同协商、友好解决。如经核实，该投诉确因乙方提供的服务所致，由乙方负责处理并承担全部责任及费用。未经甲方事先书面同意，乙方不得擅自采取中断、中止服务或删除甲方数据等措施。如司法机关或监管机构依法要求采取相关措施，乙方应在采取前立即通知甲方。

第八条　知识产权及保密义务

1.乙方保证依据本合同向甲方提供的服务（以下简称“知识产权标的”）均符合法律法规规定，不侵犯任何第三方的知识产权（包括但不限于专利权、商标权、著作权等）、所有权、担保物权等合法权益，也不违反社会公共利益。若第三方因甲方使用知识产权标的向甲方主张权利（包括但不限于提起诉讼、仲裁、索赔等），乙方应在收到甲方书面通知后 2 个工作日内主动出面处理，并承担由此导致甲方的全部损失（包括但不限于诉讼费、律师费、保全费、差旅费、公证费、赔偿金等）。

2.乙方应对保密信息严格保密，未经甲方书面事先同意，不得向任何第三方披露，也不得用于履行本合同以外的任何目的。乙方及其人员应遵守网络安全、数据安全和个人信息保护相关法律法规及甲方网络与数据安全管理制度。

3.乙方仅可为本合同目的，向其确有必要知悉保密信息的雇员披露，且应提前与该等雇员签订保密协议，明确其保密义务，并对雇员的违约行为承担连带责任。

4.下列情形不受保密义务限制：

（1）保密信息已通过合法渠道为公众所知悉；

（2）依据法律法规、司法机关或行政主管部门的强制性要求必须披露的；

（3）乙方在未违反保密义务的情况下，从第三方合法获得或独立开发的与保密信息相同或相似的信息。

5.本保密义务在本合同期满、解除或终止后持续有效。

6.乙方未遵守前述约定的，乙方负责处理相关问题并承担由此产生的全部费用，甲方因此受到损失的，乙方应赔偿甲方因此所受的全部损失，同时，甲方有权单方解除本合同。

第九条　违约责任

1. 甲乙双方如有一方违约，由违约方承担因此给对方造成的经济损失。

2. 乙方未按时提交周报、月报的，累计达到 5 次，构成“违约”。

3. 甲方验证乙方服务质量未达到服务质量标准的，累计达到 3 次，构成“违

约”。因服务质量不达标引发的后果应由乙方承担，甲方有权向乙方追偿损失。

4. 乙方对甲方造成严重损失的构成“违约”。

5. 其他构成“违约”的情形：

甲乙双方在完成双方签署的书面确认事项后，任何一方擅自提出变更要求，导致项目进度延迟的，视为对方违约。

6. 乙方构成“违约”的，应按照合同总金额 3‰的标准向甲方支付违约金。甲方优先从应付未付款项中扣减；应付未付款项不足的，乙方应在收到甲方书面通知后 5 个工作日内补足差额。逾期未补足的，甲方有权按日加收差额 1‰的滞纳金，且有权单方解除合同。

7. 因乙方未按约定开始服务的，每逾期一日，乙方应按相应阶段应付款项的 1‰支付违约金；逾期达到 5 个工作日的，甲方有权解除合同，乙方除退还甲方已支付但尚未产生的费用外，还应按照合同总金额 1%的标准向甲方支付违约金。违约金的支付并不能解除乙方继续履行合同的责任和义务。

8. 本合同约定的违约金不足以赔偿甲方实际全部损失（包括不限于律师费、诉讼费、保全费、检验费、公证费、差旅费等）的，乙方应当补足。甲方有权从后续应付的合同款中直接扣除上述违约金和赔偿款。

9. 乙方保证其具备在相关采购文件中已承诺的相关资质。若乙方不具备资质，甲方有权解除合同，乙方应返还全部款项。

10. 未经甲方书面同意，乙方不得将本合同项下的权利义务转让给第三方。若违反本项约定，甲方有权解除合同，乙方应返还全部款项，并向甲方支付违约金人民币 200,000.00 元（大写：贰拾万元整）。同时，乙方因此所得收益归甲方所有。

第十条　不可抗力

1. 本合同中不可抗力指不能预见、不能避免并不能克服且对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、瘟疫流行等以及社会事件如战争、动乱、火灾、爆炸及国家和地方政府等相关部门的政策。

2. 由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并在不可抗力发生之日起 30 日内提供相关政府

部门或公证机关出具的证明文件。

3. 由于不可抗力致使合同无法履行的，本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，甲乙双方无须承担违约责任。不可抗力事件消除后，甲乙双方应就合同的履行及后续问题进行协商，按照该事件对合同履行的影响程度，决定继续履行合同或终止合同。

第十一条　法律适用及争议解决

1. 本合同按中华人民共和国法律解释，受中华人民共和国法律管辖。

2. 因执行本合同所发生的或与本合同有关的一切争议，双方应首先通过友好协商解决。任一方不愿协商的，任一方均有权向北京市海淀区人民法院提起诉讼。除非生效裁判另有规定，各方为解决争议而实际支付的费用（包括但不限于诉讼费、保全费、评估费、拍卖费、执行费、合理的律师费等）由诉讼请求未被支持的一方承担。

第十二条　其他

1.本合同一式玖份，甲方执陆份，乙方执叁份，具有同等效力。

2.本合同自双方法定代表人或授权代表签字并加盖单位公章/合同专用章之日起生效，至双方权利义务履行完毕之日终止。

3.本合同附件应由双方签署，为本合同不可分割的组成部分，与本合同具有同等法律效力。

第十三条　附件

附件 1《报价明细表》

附件 2《项目人员表》

（以下无正文）

签署页（此页无正文）

甲方	单位名称	北京市海淀区大数据中心（盖章）
	法定代表人（或授权代表）	签字：
	项目负责人	张明伟
	电　　话	18813005419
	通讯地址	北京市海淀区中关村南大街 3 号海淀科技大厦
	签署日期	2026 年 10 月 30 日
乙方	单位名称	北京中科卓信软件测评技术中心（盖章）
	法定代表人（或授权代表）	签字：
	项目负责人	程超
	电　　话	15901412185
	通讯地址	北京市海淀区闵庄路 3 号 102 幢二层 207 室
	签署日期	2026 年 10 月 30 日

附件 1 《报价明细表》

序号	分项名称	单价（元）	数量	合价（元）	备注/说明
1	二级系统等保测评服务	62000.00	11	682000.00	无
2	三级系统等保测评服务	78000.00	97	7566000.00	无
3	三级系统密码测评服务	97500.00	78	7605000.00	无
一年总价（元）				15853000.00	无
三年总价（元）				47559000.00	无

附件 2 《项目人员表》

序号	在本项目中拟担任工作	姓名
1.	项目经理	程超
2.	质量总监	胡陈勇
3.	高级等保测评师	李远金
4.	高级等保测评师	付博雯
5.	高级等保测评师	黄楚皓
6.	中级等保测评师	李佳欣
7.	中级等保测评师	刘海明
8.	中级等保测评师	霍旺
9.	中级等保测评师	卢海龙
10.	中级等保测评师	黄炯辉
11.	中级等保测评师	高昭
12.	中级等保测评师	杨子昂
13.	中级等保测评师	邢颖颖
14.	中级等保测评师	张斓静
15.	密码测评工程师	孙士杰
16.	密码测评工程师	易琳
17.	密码测评工程师	朱宇璐
18.	密码测评工程师	刘畅
19.	密码测评工程师	李晶
20.	密码测评工程师	夏伟欣
21.	密码测评工程师	郭亚爽
22.	密码测评工程师	裴素瑶

23.	中级等保测评师	王郭毅
24.	初级等保测评师	金承硕
25.	初级等保测评师	蒋再春
26.	初级等保测评师	甘佩灵
27.	中级等保测评师	郑勇
28.	初级等保测评师	刘志恒
29.	初级等保测评师	杨莎