



开封市“一道墙”数字政府安全运维能力支撑服务项目 测试评估认证服务合同

(项目编号:汴财招标采购-2026-38-2)

甲方(采购人):开封市行政审批和政务信息管理局

住所地:开封市民之家6楼东头向北6015

联系人:刘荫

联系电话:0371-22911919

乙方(中标人):联通数字科技有限公司

住所地:北京市北京经济技术开发区科谷一街10号院8号楼12层1201
(北京自贸试验区高端产业片区亦庄组团)

联系人:姜南

联系电话:18601982318

根据《中华人民共和国民法典》《中华人民共和国政府采购法》《中华人民共和国网络安全法》《中华人民共和国密码法》《信息安全等级保护管理办法》《商用密码应用安全性评估管理办法》等法律法规,结合本项目招标文件、中标通知书及乙方投标文件,甲乙双方遵循平等、自愿、公平和诚实信用的原则,经协商一致,签订本合同。

第一章 服务内容与技术标准

第一条 服务内容

依据国家网络安全等级保护2.0标准及商用密码应用相关规范,乙方对开封市电子政务外网、政务云平台及承载的应用系统开展等级保护测评、密码安全能力提升、安全测试评估、墨攻安全运营等服务,保障系统安全可靠运行,满足合规要求。具体服务分项、技术指标及交付要求详见本合同附件





一《测试评估认证服务内容及技术要求》。

第二条 服务范围

覆盖全市市直不少于 50 套信息系统（含服务期内新增财政资金建设的政务应用系统），包含电子政务外网、政务云平台及云平台承载的各类政务应用。

第三条 技术标准

服务执行须符合《信息安全技术 网络安全等级保护测评要求》（GB/T 28448）、《信息安全技术 商用密码应用安全性评估通则》（GB/T 39786）、《信息安全技术 信息渗透测试指南》（GB/T 32920）等国家及行业现行有效标准；合同履行期间标准更新修订的，按最新版本执行。

第二章 服务期限与交付要求

第四条 服务期限

本合同服务期限为 3 年，自合同生效且乙方提交的项目总体实施方案经甲方书面确认之日起计算。合同生效后 5 个工作日内，乙方项目团队应完成进场对接并提交项目总体实施方案，经甲方书面确认后正式启动服务。

第五条 交付物清单

- （一）《信息系统等级保护测评报告》（每套系统对应 1 份）
- （二）《商用密码应用安全性评估报告》（每套系统对应 1 份）
- （三）《渗透测试报告》
- （四）《月度漏洞扫描报告》
- （五）《网站安全监测月报/年报》
- （六）《安全整改建议方案》
- （七）《年度安全工作总结报告》
- （八）项目实施过程文档：测评方案、原始记录、整改台账、复测意见、



培训课件等

(九) 其他甲方要求的专项支撑材料

第六条 交付标准

(一) 所有报告符合国家、行业主管部门规范要求,可直接用于公安部门、密码管理部门等监管单位的备案、检查与评审,具备相应法律效力。

(二) 测评工作客观公正,数据真实准确,不得弄虚作假、隐瞒问题或出具虚假报告。

(三) 交付文档格式规范、内容完整、结论清晰、建议可落地;同时提供纸质版(加盖乙方公章)与电子版(可编辑格式+PDF格式)。

(四) 所有交付成果须经乙方三级质量审核通过后方可提交甲方。

第三章 合同价款与支付

第七条 合同总价

本合同总价款为人民币(大写):伍佰玖拾柒万玖仟元整(¥5,979,000),为固定总价包干。每年服务费用:壹佰玖拾玖万叁仟元整(¥1,993,000)。该价款包含测评工具使用费、人员成本、报告编制费、驻场服务费、培训费、差旅交通费、耗材费、税金、保险费、复测费、整改指导费及合同履行期间所有不可预见费用。合同履行期间,无论市场价格波动、政策调整、系统数量增减(在约定总量内)或其他因素变化,合同总价均不作调整,甲方无需支付合同外任何费用。

第八条 付款方式

(一) 付款周期:本合同服务费每6个月支付一次,共支付6次。每次支付金额为合同总金额的1/6,即人民币玖拾玖万陆仟伍佰元整(¥996,500)。每期款项的支付须以该服务周期届满且甲方考核服务合格为前提;若当期考核不合格,甲方有权暂停支付直至乙方整改合格,或按本合同约定扣除相应



费用后支付剩余款项。

(二) 付款条件: 每 6 个月服务周期届满, 乙方提交当期交付成果清单、服务工作总结、服务台账、考核自评表及等额正规发票。甲方对服务质量考核合格后 15 个工作日内完成支付手续。由于乙方提供的正式发票不合格而引起的一切责任 (包括商业责任和法律责任) 和损失由乙方承担。

(三) 支付方式: 银行转账。

(四) 支付信息:

开户名称: 联通数字科技有限公司

银行账号: 0200013319200042469

开户银行: 中国工商银行股份有限公司北京灵境支行

(五) 支付变更: 乙方开户银行、账号等如有变更, 应在本合同规定的付款期限前 15 天, 以书面方式通知甲方。如未按时通知或通知有误而影响支付结算, 乙方应承担相应责任。

第四章 双方权利与义务

第九条 甲方权利与义务

(一) 有权对测评全过程、人员资质、工作质量进行全程监督, 对测评方法、抽样范围、工具使用提出质询, 对不符合要求的事项提出整改要求。

(二) 向乙方提供测评所需的系统资料、网络拓扑、账号权限、业务说明等必要基础信息, 协调各被测业务单位配合现场测评、访谈、整改等工作。

(三) 督促相关单位按整改方案落实安全整改, 配合乙方开展复测验证工作。

(四) 按合同约定及时支付合同款项。

(五) 不得要求乙方从事违反网络安全法律法规及保密规定的操作。

(六) 不得要求乙方出具虚假测评报告、隐瞒安全隐患或降低测评标准。

(七) 为乙方现场工作人员提供必要的工作条件、机房出入权限及安全



管理告知。

第十条 乙方权利与义务

(一) 乙方须具备国家网络安全等级测评与检测评估机构服务认证资质；具备商用密码应用安全性评估相应资质，测评人员持证上岗。

(二) 组建符合要求的项目团队，驻场人员遵守甲方各项管理制度与保密规定，服从甲方工作安排。实行 AB 角补位制度，未经甲方书面同意，乙方不得擅自更换核心人员；确需更换的，替换人员资质不得低于原人员标准。

(三) 严格按照国家规范、行业标准与合同约定开展测评工作，保证测评过程合规、方法科学、结果真实、结论公正。

(四) 对测评中发现的重大高危漏洞、严重安全隐患，须及时告知甲方，并协助制定临时应急处置措施，防范风险扩大。

(五) 对测评过程中接触的所有政务数据、系统信息、测评结果、漏洞细节严格保密，严禁向任何第三方泄露。

(六) 配合甲方完成上级主管部门的监督检查、备案评审等工作，负责解释测评相关技术问题，按要求补充相关支撑材料。

(七) 提供全程整改指导服务，协助被测单位制定整改方案，解答整改技术问题，整改完成后开展复测验证，直至符合合规要求。

(八) 有权要求甲方提供必要的工作条件与资料；有权拒绝违反法律法规、测评规范的不合理要求。

(九) 建立项目服务台账，如实记录每次测评、每次服务的工作内容、时间、人员、成果，按甲方要求定期报送。

第五章 项目团队管理

第十一条 人员配置要求

(一) 项目团队总人数不少于 6 人，岗位应包含项目经理 1 名、高级测评师 2 名、渗透测试工程师 1 名、密评工程师 1 名、驻场安全工程师 1



名,各岗位职责清晰、互为补位。项目团队提供 5×8 小时测评驻场服务及 7×24 小时技术支持。

(二) 项目负责人须具备项目管理经验,持有项目管理、安全运维相关认证。

(三) 所有现场测评人员须具备相应从业资质,持证上岗;测评师团队配置应当符合属地网络安全监管部门的相关规定。

第十二条 人员管理

(一) 乙方不得随意更换项目负责人及核心技术人员;确需更换的,须提前 15 个工作日书面通知甲方,替换人员资质不得低于原人员标准,经甲方同意后方可更换。

(二) 驻场人员考勤与甲方作息时间保持一致,请假须提前报备并安排顶岗人员。

(三) 甲方有权要求乙方更换不胜任工作、违反管理制度的人员,乙方须在 3 个工作日内完成更换。

(四) 乙方负责其工作人员的安全管理。乙方工作人员在履约过程中发生安全事故的,由乙方依法承担相应责任;因乙方或其工作人员过错造成甲方或第三人人身、财产损失的,由乙方承担赔偿责任。

第六章 服务质量与考核

第十三条 质量管理体系

(一) 测评工作须实行三级质量审核制度:项目组自查、质控审核、技术负责人终审,每级审核均须留存审核记录,确保测评结果准确无误。

(二) 甲方有权对测评过程进行旁站监督,对现场操作、工具使用、数据采集进行全程见证;乙方须予以配合并如实解答质询。

(三) 甲方或被测评单位对测评报告提出异议的,乙方须在 3 个工作日内予以书面答复;确有问题的须无偿重新测评或补充测评,直至符合要求。



第十四条 验收与考核

(一) 本项目实行半年度考核、年度验收制度。

➤ 半年度考核：每半年对乙方服务质量、响应时效、人员到岗、整改指导效果、报告交付时效进行综合考核。半年度考核不合格的，乙方须在 10 个工作日内完成整改；整改后仍不合格的，甲方有权扣除当期 20% 服务费用；连续两次考核不合格的，甲方有权解除合同。

➤ 年度验收：年度验收由甲方组织，结合全年考核结果、年度工作总结、服务目标达成情况开展年度验收，验收合格后方可进入下一服务年度。年度验收不合格的，乙方须在 15 个工作日内完成整改并申请复验，复验仍不合格的，甲方有权扣除当年度服务费用的 20% 并单方解除合同。

(二) 半年度考核内容：人员配置与到岗情况、报告质量与合规性、交付时效与履约率、整改指导与支撑效果、甲方满意度与配合度。

(三) 考核周期内出现报告失实、重大漏判误判、违规操作造成系统故障等情况的，当期考核直接判定为不合格，并按违约责任条款处理。

(四) 乙方须于每半年度结束后 5 个工作日内提交自评报告及相关证明材料，甲方在 10 个工作日内完成考核并出具书面考核意见。

第七章 保密与风险管控

第十五条 测评风险管控

(一) 乙方须制定专项测评风险管控方案，采取有效措施避免测评对业务系统正常运行造成影响；所有可能影响业务的测试操作，须提前 24 小时提交书面申请，明确测试内容、时间、影响范围及回滚方案，经甲方及被测单位批准后方可实施。

(二) 测评工作须避开业务高峰期，高危性测试操作须在业务低峰期（夜间或节假日）进行，并安排被测单位人员现场配合。

(三) 因乙方操作不当、未按审批流程实施造成系统中断、数据损坏、



业务停滞的,乙方承担全部赔偿责任,并在 4 小时内恢复业务正常运行。

(四) 渗透测试、漏洞扫描等攻击性测试,必须严格限定在授权范围内,严禁超范围测试、破坏性测试,严禁对非授权系统开展探测与攻击。

第十六条 保密义务

(一) 所有项目人员须签订保密协议,严禁泄露测评中获取的系统漏洞、账号密码、业务数据、网络架构、安全策略等敏感信息;保密义务永久有效,不因合同终止而失效。乙方及其工作人员严禁将上述信息用于本合同服务以外的任何目的(包括但不限于商业推广、数据分析、模型训练等),严禁向任何第三方泄露、出售或非法提供。

(二) 乙方须对测评工具、测试设备进行病毒查杀和安全检测,严禁携带恶意代码、未经授权的软件进入测评环境;现场测试设备须统一登记备案。

(三) 测评过程中产生的所有中间数据、临时文件、测试结果、原始记录,均属于甲方所有,服务结束后须全部移交甲方或在甲方监督下彻底销毁,不得私自留存、复制或带出工作场所。

(四) 乙方人员不得私自携带个人存储设备进入机房,不得擅自拷贝、传输政务数据;人员离岗时须彻底清除所有工作相关数据,交还所有工作资料与权限。

(五) 乙方须定期对项目人员开展保密教育与考核,确保所有人员知悉保密义务及违规责任。

第十七条 数据安全责任

(一) 乙方所有操作须符合《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等相关规定,严格保护政务数据与个人信息安全。乙方操作须符合政务信息系统安全管理规定,严格执行操作审批流程,严禁越权操作。

(二) 因乙方原因(包括操作失误、技术缺陷等)造成数据泄露、篡改、



丢失及系统中断等网络安全事件的,乙方须立即启动应急预案,承担全部应急处置费用,并按相关规定承担行政及法律责任。

(三)因乙方服务瑕疵(包括但不限于测评漏判误判、风险预警不及时、整改方案不可行或指导不力等)导致甲方系统被攻击、数据泄露、业务受损或遭受监管部门通报、处罚的,乙方应承担全部法律责任,并赔偿甲方因此遭受的全部损失(包括但不限于罚款、赔偿金、声誉损失修复费用等)。

第八章 知识产权

(一)乙方为本项目产出的所有测评报告、分析文档、整改方案、培训课件、专项支撑材料、定制开发的项目管理平台代码及文档等一切工作成果的知识产权(包括但不限于著作权、专利权、商业秘密等)均归甲方所有。乙方不得对上述成果主张任何权利,亦不得自行或许可第三方使用、复制、修改或进行商业化运作。乙方为履行本合同所使用的自有通用工具、模板、方法论及标准作业程序等背景知识产权仍归乙方所有,但乙方授予甲方永久的、免费的、不可撤销的使用权。

(二)乙方保证使用的测评工具、软件、技术方案具备合法授权,不侵犯任何第三方知识产权;如发生侵权纠纷,由乙方承担全部责任并赔偿甲方损失。

(三)乙方交付的所有文档、报告、方案等成果,甲方有权无偿使用、复制、修改及内部分发,用于本单位及相关单位安全管理、合规备案、监督检查等相关工作。

(四)乙方为履行本合同所使用的自有工具、软件,授予甲方永久的、非排他的、不可转让的免费使用权,使用范围包括本项目及后续管理工作。该授权不因本合同的终止、解除或期满而失效。

第九章 违约责任

第十八条 甲方违约责任



甲方逾期支付合同款项的,每逾期1日,按应付未付金额的0.05%向乙方支付违约金,累计违约金不超过应付未付金额的5%。

第十九条 乙方违约责任

(一)乙方出具的测评报告不符合规范、存在重大失实、重大漏判误判的,须无偿重新测评,并支付合同总金额10%的违约金;造成甲方合规风险、行政处罚或经济损失的,承担全部赔偿责任。

(二)乙方未按约定时限完成测评工作、交付成果的,每逾期1日支付合同总金额0.05%的违约金,累计违约金不超过合同总金额的5%;逾期超过20日的,甲方有权解除合同。

(三)乙方违规操作造成甲方系统故障、数据损坏、业务中断的,须在4小时内恢复业务,并赔偿甲方因此遭受的全部直接经济损失及合理的维权费用(包括律师费、鉴定费等)。若因乙方重大过失或故意行为导致重大网络安全事故,乙方除赔偿直接损失外,还应支付合同总金额20%的违约金。除故意或重大过失外,乙方承担的累计赔偿责任上限为合同总金额的100%。

(四)乙方连续两次或合同有效期内累计三次半年度考核不合格的,或因乙方服务质量问题导致甲方被上级主管部门通报批评或行政处罚的,甲方有权单方解除合同。合同解除后,乙方应退还甲方已支付但未实际发生服务期间的费用,并在10个工作日内配合甲方完成工作交接;乙方须支付合同总金额20%的违约金,并赔偿甲方因此产生的重新采购成本及过渡期聘请第三方服务的费用差额。

(五)乙方发生以下情形之一的,甲方有权立即解除合同。乙方应退还甲方已支付但未实际发生服务对应的款项,并向甲方支付合同总金额20%的违约金;若违约金不足以弥补甲方损失的,乙方应予补足:

(1)发生重大网络安全责任事故;

(2)驻场人员资质造假或未经甲方同意擅自更换核心人员超过2人次;



(3) 违反保密义务、数据安全规定的。

第十章 不可抗力

(一) 因地震、台风、水灾、战争、重大公共卫生事件等不能预见、不能避免且不能克服的不可抗力事件，导致一方不能履行合同的，受影响方应及时通知对方，并在 30 日内提供有效证明。

(二) 受不可抗力影响的一方须采取合理措施减少损失扩大，未及时采取措施导致损失扩大的，扩大部分责任自行承担。

(三) 根据不可抗力影响程度，双方协商决定部分免除、全部免除责任，或延期履行、解除合同。

(四) 不可抗力事件结束后 3 个工作日内，受影响方须向对方通报恢复履行计划，协商后续履约安排。

第十一章 合同的变更、解除与终止

(一) 本合同的变更、补充须经双方协商一致，签订书面补充协议，补充协议与本合同具有同等法律效力。乙方不得单方面无故终止本合同。若乙方无正当理由单方面终止合同，应向甲方支付合同总金额 20% 的违约金，并赔偿甲方因此遭受的全部损失（包括但不限于重新采购服务的差价、应急服务费用等）。

(二) 一方严重违约导致合同目的无法实现的，守约方有权书面通知解除合同。

(三) 本合同全部解除条款适用如下规则：解除合同的通知，自送达对方之日起生效。

(四) 合同期满，双方义务履行完毕，合同自动终止；如甲方有续约需求，可按政府采购规定办理后续手续。

(五) 合同解除或终止后，乙方须在 5 个工作日内提交完整的交接清单（含所有账号、密码、密钥、配置文档、未完成事项列表等），并在 15 个



工作日内配合甲方或新服务商完成全部权限移交、数据迁移及现场培训,经甲方书面确认交接完毕后,方视为交接完成。在交接完成前,乙方仍需履行安全保障义务。

(六) 合同终止后,乙方仍须对服务期内已知的安全隐患履行告知义务,并配合甲方做好收尾处置工作。

第十二章 争议解决

因本合同引起的或与本合同有关的任何争议,双方先友好协商解决;协商不成的,任何一方均有权向甲方所在地有管辖权的人民法院提起诉讼。

第十三章 其他约定

(一) 本合同附件为本合同不可分割的组成部分,与本合同正文具有同等法律效力。

(二) 本合同未尽事宜,参照招标文件、中标通知书及乙方投标文件执行。

(三) 本合同一式肆份,甲方执贰份,乙方执贰份,具有同等法律效力。

(四) 本合同自双方法定代表人(负责人)或授权代表签字并加盖公章之日起生效。

(五) 本合同载明的地址、联系人为双方法定送达地址与联系人。任何书面通知按该地址寄送或发送至指定邮箱,即视为有效送达。地址变更须提前3个工作日书面通知对方,否则承担送达不能的责任。

(以下无正文)

甲方(盖章): 开封市行政审批和政务信息管理局

法定代表人(负责人) / 授权代表(签字):

日期: 2026 年 8 月 28 日

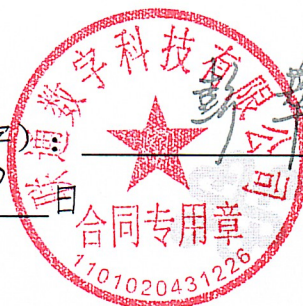




乙方（盖章）：联通数字科技有限公司

法定代表人（负责人） / 授权代表（签字）

日期：2026年8月28日





附件一

测试评估认证服务内容及技术要求

一、等级保护测评服务

1.依据相关法规标准,对全市市直 ≥ 50 套信息系统进行网络安全等级保护测评,衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求,出具等级保护测评报告。

2.配备具备自主知识产权的智能化测评工具,满足以下功能要求:

(1) 项目管理与协同:支持项目创建、测评分工、质量管理、项目状态可视化展示,且具备对应自主知识产权。

(2) 智能化辅助:支持测评结果记录生成、过程文档自动生成、整改对比、报告质量审核、差距分析自动生成,且具备对应自主知识产权。

(3) 基础测评功能:支持结果记录复制、批量替换、错误校验、一键风险分析、网络拓扑描述生成、管理制度自动检测等功能。

二、密码安全能力提升服务

1.依据密码相关法律法规,对开封市两大基础设施信息系统进行商用密码使用能力评估并提升改造,提供系统调研表、测评实施方案、密码应用方案及评估报告模板,保障系统商用密码应用合规、正确、有效。

2.使用三类不同的商用密码应用安全性评估工具开展测评:

(1) 密评基础测评工具:包含 IPSec/SSL 安全协议分析、数字证书格式验证、密码算法正确性验证、数据机密性验证、随机数统计检验工具。



(2) 密码应用安全性评估检测工具箱：具备评估指标管理、网络数据采集、多密码算法分析、密码模块漏洞库、电子签章检测、密评工作协同等能力。

(3) 商用密码应用安全性评估项目管理平台：支持密评全流程操作、多模板适配、在线质控、进度告警、报告附件管理、客户端离线测评功能。

三、网络安全相关咨询服务

- 1.协助完善单位信息安全管理体系统，服务频次不低于1次/年。
- 2.实时提供应用安全相关漏洞的安全通告以及解决方案。
- 3.开展信息安全意识培训，服务频次不低于2次/年。

四、渗透测试服务

模拟黑客攻击方法对政务云信息系统开展全方位渗透测试，涵盖弱口令、身份认证、SQL注入、跨站脚本、Web Services、SSL、文件操作等测试内容，编制渗透测试报告并制定加固方案。服务频次不低于4次/年。

五、安全加固指导服务

根据整体评估测试结果，针对发现的安全漏洞及风险提出可操作的整改建议，协助甲方完成安全整改，服务为即时响应。

六、应急响应及重大保障服务

- 1.参照国家信息安全事件响应标准，提供7×24小时紧急响应处理服务，按标准流程处置网络安全事件。
- 2.在重要会议、大型攻防演练期间提供专项安全保障，涵盖事前排查、事中监测、事后总结全流程。

七、漏洞扫描服务

对业务系统及数据库系统进行定期现场安全漏洞检测，掌握安全隐患并落实修补措施，提供报告。服务频次不低于1次/月。



八、网络安全监测服务

对甲方指定的 2 个网站进行 7×24 小时全方位安全监测,防范各类注入、攻击行为。定期出具网站监控报告。

九、安全驻场值守服务

根据甲方要求,在特定时间派遣 4 名符合资质的安全专家至现场提供 7×24 小时安全值守支持。

十、项目管理工具

提供等保测评项目管理工具一套,涵盖策划、立项、招采、验收、运维、等保测评全阶段流程管理。