

合同编号: DSJ - 2026 - 055

北京市大数据中心 服务采购合同



合同名称: 北京市政务云算扩容项目第三方测评服务

委托人(甲方): 北京市大数据中心

受托人(乙方): 国家工业信息安全发展研究中心

委托人（甲方）：北京市大数据中心

负责人：张琳

住所地：北京市通州区留庄路3号院2号楼

受托人（乙方）：国家工业信息安全发展研究中心

法定代表人：江明涛

住所地：北京市石景山区鲁谷路35号

甲、乙双方根据《中华人民共和国民法典》及相关法律法规的规定，经过友好协商，就乙方为甲方提供北京市政务云算扩容项目第三方测评服务事宜达成如下协议，以资共同遵守。

本合同 是 ☒ 否 中小企业预留合同。

第一条 服务事项及内容

本合同期限内，乙方应为甲方提供如下服务：

- 1、测试地点：数智北京创新中心；
- 2、测评对象：北京市政务云算扩容项目，包括北京市政务外网办公云、政务云综合监管平台；
- 3、软件测评服务内容：对政务云综合监管平台开展全面质量验收评测，包括软件功能测试、性能测试、兼容性测试、可靠性测试、易用性测试、维护性测试，验证其功能实现与性能指标是否达到建设目标要求；
- 4、等保测评服务内容：对北京市政务外网办公云和政务云综合监管平台的安全建设进行符合性测评，验证其是否符合等级保护要求，发现存在的安全隐患，提出安全防护相关合理化建议，出具网络安全等级保护测评报告，并协助进行整改，以达到国家网络安全等级保护相关要求。
- 5、密码测评服务内容：客观、全面、准确地评价北京市政务外网办公云和政务云综合监管平台密码应用的合规性、正确性和有效性，度量其与密码应用需求的符合性；找出其密码应用现状与相应等级密码保护要求之间的差距，并分析薄弱环节及面临的安全风险，为密码应用安全提供科

学评价，提出完善、可行的整改建议，出具密码应用安全评估报告。
详细服务内容及要求见附件 1《工作方案》。

第二条 服务质量要求及验收

1、乙方为甲方提供的服务质量应符合国家或相关行业的标准。

2、乙方提供的北京市政务云扩容项目测评结论真实、客观、准确；提交的项目成果文件完整、规范；应对北京市政务云扩容项目测评中发现的问题进行整改后的复核，直至等保测评报告和密码测评报告结论为“符合”或“基本符合”、软件测评报告结果全部为“通过”为止。

3、乙方完成合同全部工作后应及时通知甲方进行最终验收。甲方组织验收合格的，甲方在验收合格报告上签字；验收不合格的，乙方应当在10个工作日内进行返工或调整，并重新提交甲方验收。

4、合同最终验收合格后，乙方应向甲方提交如下合同成果：

(1) 软件测评服务：政务云综合监管平台《软件测评方案》、政务云综合监管平台《软件测评报告》；

(2) 等保测评服务：北京市政务外网办公云《网络安全等级保护测评方案》、北京市政务外网办公云《网络安全等级保护测评报告》、政务云综合监管平台《网络安全等级保护测评方案》、政务云综合监管平台《网络安全等级保护测评报告》；

(3) 密码测评服务：北京市政务外网办公云《商用密码应用安全性评估方案》、北京市政务外网办公云《商用密码应用安全性评估报告》、政务云综合监管平台《商用密码应用安全性评估方案》、政务云综合监管平台《商用密码应用安全性评估报告》。

第三条 项目小组及人员要求

1、双方各指派一名代表作为本项目负责人，项目负责人职责范围包括：人员协调，项目任务沟通和技术问题解决事项。

甲方项目负责人：刘鹏，联系方式：010-5529770。

乙方项目负责人：刘志尧，联系方式：18810464810。

2、项目主要人员要求

乙方须根据项目要求安排具备相应资质和经验的专业人员从事本项目的调研工作，并确保项目实施队伍的稳定（项目主要人员名单详见附件2）。项目实施过程中，乙方如因正当理由需要调整项目主要人员的，应当提前5个工作日通知甲方，获得甲方书面同意后方可更换。

第四条 服务期限

乙方为甲方提供上述服务的期限为：自合同签订之日起至乙方本合同项下全部义务履行完毕之日止。

第五条 服务费及支付方式

1、本合同项下服务费总额为人民币1,020,000元，大写：壹佰零贰万元。前述服务费已经包含乙方完成本合同项下服务的全部费用，除前述款项外，甲方无需向乙方另行支付其他任何费用。

2、甲方将按以下第（2）种方式向乙方支付服务费：

（1）一次性支付：甲方于本合同签署之日起 个工作日内，向乙方付清服务费。

（2）分期支付（三次）：

第1次付款：甲方在合同签订后，自收到乙方提供的符合要求的发票且财政资金到达甲方账户并可实际使用之日起10个工作日内，向乙方支付服务费的50%即（大写）伍拾壹万元（¥510,000元）；

第2次付款：乙方提供本合同项下的全部服务并向甲方正式提交全部成果物后，自收到乙方提供的符合要求的发票且财政资金到达甲方账户并可实际使用之日起10个工作日内，甲方向乙方支付服务费的40%即（大写）肆拾万捌仟元（¥408,000元）；

第3次付款：北京市政务云算扩容项目最终决算完成后，按照实际决算中确认的本项目金额进行最终结算。若甲方已付款少于结算金额的，甲方自收到乙方提供的符合要求的发票且财政资金到达甲方账户并可实际使用之日起10个工作日内，向乙方支付合同剩余款项；若甲方已付款超过结算金额的，则乙方自收到甲方结算金额通知之日起7个工作日内，将超付款项退回甲方；

乙方应在甲方付款前向甲方开具正规、合法发票，否则甲方有权暂不付款且不承担逾期付款的违约责任。因乙方原因（包括但不限于未开具发票、开具发票不符合甲方要求等）导致甲方因财政政策原因未能付款，相应责任由乙方承担。

第六条 甲方的权利义务

- 1、甲方有权要求乙方按照本合同约定提供各项服务。
- 2、甲方有权对乙方提供各项服务的情况进行监督和检查。
- 3、甲方应按照本合同约定向乙方支付服务费。

第七条 乙方的权利义务

1、乙方应按照本合同约定向甲方提供各项服务，确保服务质量符合法律法规、国家标准的规定及本合同约定或甲方要求；如因乙方提供服务不符合前述要求给甲方造成损失的（本协议中所指损失包括但不限于律师费、公证费、差旅费、向第三人支付的任何费用以及为减小损失、实现债权而支付的其他费用等，下文同义），乙方应予赔偿。

2、乙方有义务配合甲方或相关单位根据工作需要，对其提供服务情况及项目服务费支出、使用情况进行的监督和检查，出现问题的应及时整改。

3、乙方应保证为甲方提供服务的员工具备提供本合同项下服务所需的相应资质和许可，并保证乙方人员在为甲方提供服务的过程中，严格遵守甲方的各项规定、服从甲方安排。

4、如因乙方人员原因，给甲方或第三方造成人员人身伤害或财产损失的，乙方应承担赔偿责任。

5、未经甲方的书面许可，乙方不得以任何形式将其在本合同项下的权利义务转让给任何第三方。

6、除双方另有约定外，为本合同相关内容进行专家咨询（验收）、调查研究、分析论证、试验测定、专利申请以及乙方到外地进行调研、收集资料所发生的费用，均包含在本合同的项目费用中，甲方不再承担任何费用。

7、因乙方原因造成阶段性验收或最终验收超期，导致甲方无法按照合同约定正常付款或给甲方造成损失的，乙方应承担相应赔偿责任。

8、超出本合同约定内容或工作量5%以内的，乙方不再额外收取费用。

9、乙方应在实施阶段，接受甲方聘请第三方监理单位的管理。

10、乙方已全面知悉并保证严格遵守和履行我国网络安全法、数据安全法及个人信息保护法等法律、法规、规章及国家标准等规范性文件所规定的网络安全、数据安全及个人信息保护义务；在此前提下，乙方进一步保证不得擅自留存、使用、泄露或者向他人提供任何因履行本合同而获取的任何数据，且承诺仅为履行本合同之必要目的、范围、方式而处理数据；乙方违反本条约定，一经发现，甲方有权随时解除本协议并追究乙方由此给甲方或相关方带来的全部损失和责任；甲方因此承担责任的，有权就全部损失向乙方予以追偿。

11、乙方服务人员接受甲方意识形态安全的统一管理。乙方严格执行意识形态安全管理的各项法规和甲方意识形态安全管理的各项制度，认真履行意识形态安全管理的职责，具体落实甲方外包服务人员意识形态相关管理要求，并将《意识形态安全责任书》提交甲方备案。

第八条 保密义务

1、乙方因承接本合同约定项目所知悉的该项目信息或甲方信息，以及在项目实施过程中所产生的与该项目有关的全部信息均为甲方的保密信息，乙方应对上述保密信息承担保密义务。未经甲方书面同意，乙方不得将甲方保密信息透露给任何第三方。

2、乙方应对上述保密信息予以妥善保存，并保证仅将其用于与完成本合同项下约定项目实施有关的用途或目的。在缺少相关保密条款约定时，对上述保密信息，乙方应至少采取适用于对自己核心机密进行保护的同等保护措施和审慎程度进行保密。

3、乙方保证将保密信息的披露范围严格控制在直接从事该项目工作且因工作需要有必要知悉保密信息的工作人员范围内，对乙方非从事该项目的人员一律严格保密。

4、乙方应保证在向其工作人员披露甲方的保密信息前，认真做好员工的保密教育工作，明确告知其将知悉的为甲方的保密信息，并明确告知其需承担的保密义务及泄密所应承担的法律责任，并要求全体参与该项目的人员签署书面《保密协议》。

5、任何时间内，一经甲方提出要求，乙方应按照甲方指示在收到甲方书面通知后5个工作日内将含有保密信息的所有文件或其他资料归还甲方，且不得擅自复制留存。

6、非经甲方特别授权，甲方向乙方提供的任何保密信息并不包括授予乙方该保密信息包含的任何专利权、商标权、著作权、商业秘密或其它类型的知识产权。

7、乙方承担上述保密义务的期限为合同有效期间及合同终止后5年。

8、承担上述保密义务的责任主体为乙方（含乙方工作人员）。如乙方或乙方工作人员违反了上述保密义务，给甲方造成损失的，乙方均应向甲方承担全部责任，并赔偿因此给甲方造成的全部损失；如损失数额无法确定的，乙方同意按照人民币10万元赔偿甲方的损失。

第九条 知识产权归属

1、乙方为履行本合同或在本项目实施过程中形成的所有成果的所有知识产权（包括但不限于著作权、专利权、商标权、专有技术等权利）由甲方享有；本项目实施过程中形成的发明创造的专利申请权、非专利技术的使用权、转让权归甲方享有。

2、乙方保证向甲方提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权、商业秘密等合法权益。否则由此产生的任何纠纷，由乙方负责解决并承担全部责任和损失；甲方因此而承担任何责任的，有权随时解除合同并就全部损失向乙方全额追偿。

第十条 违约责任及合同的解除

1、甲乙双方均应全面履行本合同，任何一方不履行或不按约定履行均构成违约，违约方应赔偿因此给对方造成的全部损失。

2、乙方未按照本合同约定的期限，向甲方提供服务的，每延迟1日，应向甲方支付本合同项下服务费总额的0.1%违约金，累计延迟超过30日的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并向甲方支付服务费总额10%的违约金。出现延迟不足1日的，按1日计算。

3、乙方提供服务不符合本合同约定标准或甲方要求的，乙方应当在甲方规定的期限内进行返工、修改，并重新提交甲方验收；如乙方提供的服务经二次验收仍未通过甲方验收或乙方拒绝按照甲方要求进行返工、修改的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并向甲方支付服务费总额10%的违约金。因乙方返工等原因造成乙方提供服务迟延，应承担迟延履行违约责任。

4、乙方未按照本合同约定提供专业技术人员团队，或擅自更换人员的，经甲方通知后，应及时予以改正，经甲方通知后仍不改正的或上述情况累计发生3次以上的，甲方有权解除合同，如因此给甲方造成损失的，由乙方承担全部赔偿责任。

5、乙方不接受甲方和相关审计部门对本项目进行监督检查的，或经检查发现存在违法违规情况的，按照国家和北京市有关规定处理。

6、甲方未按本合同约定向乙方支付服务费的，每迟延一日，应向乙方支付拖欠款项0.1%的违约金（违约金总额不超过合同总价的5%）。

第十一条 争议的解决

因履行合同所发生的一切争议，双方应友好协商解决，协商不成的，按下列第2种方式解决：

- (1) 提交北京仲裁委员会仲裁，仲裁裁决为终局裁决；
- (2) 依法向甲方所在地人民法院起诉。

第十二条 廉政承诺

1、合同双方承诺共同加强廉洁自律、反对商业贿赂。

2、甲方及其工作人员不得索要礼金、有价证券和贵重物品；不得在乙方报销应由本单位或个人支付的费用；不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬；不得参加乙方安排的超标准宴请和娱乐活动。

3、乙方不得向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品；不得为其报销应由甲方单位或个人支付的费用；不得向甲方工作人员支付劳务报酬；不得安排甲方工作人员参加超标准宴请及娱乐活动。

第十三条 其他

- 1、 本合同自双方签字盖章之日起生效。
- 2、 未尽事宜，经双方协商一致，签订补充协议，补充协议与本合同不一致或相冲突的内容，以补充协议为准。
- 3、 本合同附件是本合同的重要组成部分，与本合同正文具有同等法律效力，双方均应遵照执行。如项目招标、投标文件与本合同内容存在矛盾的，按照有利于项目实施及保护甲方利益的方式理解和履行。

序号	附件名称
1	工作方案
2	项目主要人员名单

- 4、 本合同一式 陆 份，甲方执 叁 份，乙方执 叁 份，具有同等法律效力。

(以下无正文)

甲方（盖章）：

签署人：

签订日期：

张琳印

2026.9.3

乙方（盖章）：

签署人：

签订日期：

开户行：招商银行股份有限公司北京石景山万达支行

开户名称：国家工业信息安全发展研究中心

帐号：110954406910555

工作方案

一、工作内容

1. 针对政务云综合监管平台开展软件测评。软件测评旨在系统建设完成后，对其进行全面质量验收评测，验证是否满足需求，功能实现与性能指标是否达到建设目标要求。

2. 针对北京市政务外网办公云、政务云综合监管平台开展等保测评。等保测评即网络安全等级保护测评工作，旨在发现系统内、外部存在的安全风险和脆弱性，通过测评发现安全问题，整改之后，提高信息系统的信息安全防护能力，降低系统受到各种攻击的风险。

3. 针对北京市政务外网办公云、政务云综合监管平台开展密码测评。密码测评即商用密码应用安全性评估工作，旨在规范密码应用，同时对维护网络和信息系统密码安全、保障网络安全以及应对各类网络安全风险具有重要的意义。

二、工作要求

1. 软件测评

测试方案要求：

依据项目合同和项目进度安排确定测试内容和测试关键点，根据本测试项目技术标准要求和项目建设相关文件内容形成完整的、详细的测试方案（包括时间计划、实施地点、设计测试用例等），作为开展测试工作的依据。测试方案包括不局限于测试策略、测试计划、测试工具、测试用例以及测试辅助技术。

测试环境要求：

测试工作在测试环境及实际生产环境中进行。委托方提供应用系软件和安全测试环境；在生产环境测试时，供应商必须给出合理的使用计划，最大限度减少对正常生产的影响。

测试工具要求：

为保证测试的公正和准确，测试不准采用项目承建单位提供或拥有版权的测试工具，供应商必须在投标文件中详细说明用于本次测试的测试内容、测试方法

和测试工具及其使用计划，并对测试过程中使用的各种软件的版权负责。如果因此引起版权纠纷，由供应商承担相应责任。测试中使用的工具须确保版本统一，如工具版本有变更，所有测试工作须重新进行。

测试人员要求：

应根据项目实际需求安排适当的测试人员，项目经理应为网络信息安全正高级工程师，同时为软件测试高级工程师、具有注册信息安全专业人员（CISP）证书者佳。

平台质量测试要求：基于政务云综合监管平台开展软件功能测试、性能测试、兼容性测试、可靠性测试、易用性测试、维护性测试工作。

1) 功能测试

功能性测评主要是对政务云综合监管平台提供给用户的所有功能进行测试。功能测试主要验证以下功能模块是否按照要求正确实现：北京市政务云综合监管业务支撑模块、北京市政务云监管评估评价模块、监管业务汇聚数据挖掘分析模块、北京市政务云综合监管可视化展示模块、北京市政务云监管数据服务接口模块等，最终测试内容依据初步设计批复为准。

2) 性能测试

性能测试主要目的是评估测试系统在一定负载状态下系统能够处理的会话能力，以及是否出现错误。性能测试主要评估系统在以下几方面的表现：a. 支持的并发用户数：测试系统在事务响应时间可以接受的最低限度的情况下，能够承载的并发用户数；b. 响应时间：测试在特定应用的业务逻辑、用户界面、功能下事务操作的响应时间。

3) 兼容性测试

服务商应按照招标方要求，对政务云综合监管平台在国产终端上进行浏览器兼容性测试工作，确保在不同浏览器上用户体验和功能的一致性。

4) 可靠性测试

从系统连续使用情况下运行稳定性方面对软件的可靠性进行质量测试，评价软件的可靠性是否符合用户需求。在系统连续使用情况下进行稳定性测试，考察系统在一定负载下长时间运行时，系统的健康程度和稳定运行的可靠性。

5) 易用性测试

结合功能性测试，查看被测软件界面是否提供简洁、直观、友好的图形化的

管理界面，方便操作，界面风格和操作是否一致等。

6) 维护性测试

从模块化等方面对软件产品的维护性进行质量测试，主要对全市政务云监管数据接口进行测试，验证是否按照接口要求正确实现。

2. 等保测评

依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449—2018）《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627—2018）等相关标准要求，对北京市政务外网办公云、政务云综合监管平台的安全建设进行符合性测评，对其安全状态做出判断，验证其是否符合等级保护要求，发现存在的安全隐患，提出安全防护相关合理化建议，出具网络安全等级保护测评报告，并协助进行整改，全面达到国家网络安全等级保护相关要求。

测评现状调研：

收集整理系统配置、部署、业务运行模式、网络拓扑结构、技术架构、运行环境（周边控制、安全措施）以及信息安全策略等技术方案；开展调查和现场访谈，对系统信息（包括：主机、数据库、网络设备、系统软件、中间件、安全设备等）进行记录，将与信息系统有关的信息资产进行核查备案。

差距分析：

针对北京市政务外网办公云、政务云综合监管平台的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心 5 个技术层面；安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理 5 个管理层面，进行现场评估和差距分析，记录相关的评估结果，输出现场评估记录结果。

配合责任主体开展整改：

根据测评结果和风险分析结果，提供详细的整改加固指导服务，其整改工作内容包含技术和管理两大方面，帮助责任单位整改，直至通过回归测试，保证系统达到公安部等级保护三级的安全保护要求，出具《网络安全等级保护测评报告》。

测试人员要求：

应根据项目实际需求安排适当的测试人员，项目经理应为网络信息安全正高

级工程师，如同时为等级保护高级测评师、具有注册信息安全专业人员（CISP）证书者佳。

3. 密码测评

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）《信息系统密码应用基本要求》（GM/T 0054-2018）《信息系统密码应用测评要求》（GM/T 0115-2021）《信息系统密码应用测评过程指南》（GM/T 0116-2021）《商用密码应用安全性评估测评作业指导书》和系统自身的安全需求分析，发现各信息系统密码应用的薄弱环节和风险，为密码应用安全提供科学评价，提出完善、可行的整改建议。客观、全面、准确地评价各系统密码应用的合规性、正确性和有效性，度量其与密码应用需求的符合性；找出系统密码应用现状与相应等级密码保护要求之间的差距，并分析其密码应用的薄弱环节及面临的安全风险，提供科学的评估报告。

1. 实施步骤：

1) 确定测评对象：

按照等保三级系统密码应用相关要求，明确平台密评范围、密评内容、密评对象和密评指标。

2) 形成评估方案：

梳理平台密码应用相关现状，形成密码应用安全性评估方案。

3) 实施密评：

测评的内容包括但不限于以下内容：

（1）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等。

（2）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等

（3）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”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等。

（4）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等。

(5) 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等。

(6) 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等。

(7) 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等。

(8) 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等。

4) 复测及出具报告：

待甲方完成整改，完成整改后的复测工作，出具是否满足密码局要求的《商用密码应用安全性评估报告》，结合测评过程和问题整改，形成密评结论，提交密评报告。

2. 测试人员要求：

应根据项目实际需求安排适当的测试人员，项目经理应为网络信息安全正高级工程师，如具有密评资质或通过密评考试资格或具有注册信息安全专业人员（CISP）证书者佳。

三、工作组织

项目负责人

负责项目的技术指导、审核服务技术方案、服务工作规范以及服务方法，并

对服务过程中的技术难题提供指导、支持。

项目经理

项目经理的任务就是要对项目过程实行全面的管理，具体体现在对项目目标有一个全局的观点，并组织会议制定项目计划和报告项目进展，并对不确定的问题组织集体讨论决策，在必要的时候进行谈判及解决冲突。

项目经理对客户所应承担的责任，主要有：

保证项目的目标在实施中前后一致，实现客户的目标；

对各种项目资源进行适当的管理和充分有效的使用；

与客户进行及时有效的沟通，及时商讨项目进展状况，以及对可能发生问题的预测。

质量管理员

协助项目经理制定质量工作计划，并监督项目质量执行过程以确保项目按时保质完成；负责对项目实施全过程的质量活动进行跟踪、监督、检查和及时纠正。

技术测评组

技术测评组的任务是负责项目实施过程中主机系统、数据库、应用软件、物理机房、网络设备及安全设备的测评工作。

管理测评组

管理测评组的任务是负责项目实施过程中用户组织架构、管理体系及具体管理制度的安全符合性测评工作。

渗透测试组

负责项目具体的渗透测试和漏洞扫描。

软件测评组

负责政务云综合监管平台的软件测评工作。

四、计划安排

完成政务云综合监管平台的软件测评、北京市政务外网办公云和政务云综合监管平台的网络安全等级保护测评和商用密码应用安全性评估工作，贯彻和落实国家网络安全等级保护政策、标准及商用密码应用相关法规要求，按照国家等级保护相关文件的指导要求和网络安全等级保护工作的推进，对上述系统开展等级测评服务，形成符合公安部门要求的网络安全等级保护测评报告、商用密码应用

安全性评估报告及检测报告，输出整改建议，北京市大数据中心根据测评结果对系统进行安全加固工作，进而完善中心信息系统安全、稳定、规范、高效的信息系统安全保障体系，满足业务及安全需要，全面提升综合安全防护能力。

五、验收标准及要求

供应商应于合同签署后，根据合同具体内容完成规定服务工作，并提交满足要求的测试报告。其中：

软件测评：为政务云综合监管平台出具《检测报告》；

等保测评：为北京市政务外网办公云、政务云综合监管平台出具符合公安部门要求的《网络安全等级保护测评报告》；

密码测评：为北京市政务外网办公云、政务云综合监管平台出具《商用密码应用安全性评估报告》。

附件 2

项目主要人员名单和简历

姓名	性别	年龄	学历	职称	职务	项目角色	承担工作
刘志尧	男	32	硕士研究生	工程师	项目负责人	项目负责人 授权经办人	项目负责人 授权经办人
张哲宇	女	37	硕士研究生	高级工程师	项目经理	测评人员 (项目经理)	测评人员(项目 经理)
于盟	男	41	硕士研究生	正高级工程师	检查 评估所所长	测评人员 (实施负责人)	测评人员(实 施负责人)
李敏	女	36	硕士研究生	高级工程师	检查 评估所所长助理	高级软件测试 工程师	负责项目实 施, 根据项目 进展调整人 员力量。
张晓菲	男	35	硕士研究生	高级工程师	高级 工程师	测评人员 (等保测评 工程师)	
邱真真	女	40	硕士研究生	/	/	软件测试工 程师(高级)	
贾晨宇	女	33	本科	工程 师	/	软件测试工 程师(高级)	
郭笑敏	女	37	硕士研究生	高级 工程师	/	软件测试工 程师(高级)	
高晓然	男	30	硕士研究生	/	/	软件测试工 程师	
李喆	女	31	本科	/	/	软件测试工 程师(高级)	
杨凯峰	男	28	本科	/	等级 保护 测评 师	测评人员 (等保测评 工程师)	
付瑞峰	男	33	本科	/	等级 保护 测评	测评人员 (等保测评 工程师)	

					师		
宋鸿泽	男	26	本科	/	等级保护测评师	测评人员 (等保测评工程师)	
王广发	男	42	本科	/	测评人员 (商用密码测评人员)	测评人员 (商用密码测评人员)	
李喆	女	41	硕士研究生	/	测评人员 (商用密码测评人员)	测评人员 (商用密码测评人员)	
李力峰	男	33	本科	/	渗透测试人员	测评人员 (渗透测试工程师)	
李雪峰	男	43	本科	/	渗透测试人员	测评人员 (渗透测试工程师)	
唐毅	男	27	本科	/	渗透测试人员	测评人员 (等保测评工程师)	

