合同编号：

北京市大数据中心
服务采购合同

合同名称：2024 年大数据安全基础保障项目

委托人（甲方）：北京市大数据中心

受托人（乙方）：北京安信天行科技有限公司

受托人（丙方）：奇安信网神信息技术（北京）股份有限公司

受托人（丁方）：中国电子技术标准化研究院

委托人（甲方）：北京市大数据中心

负责人：张琳

住所地：北京市通州区潞城镇宏安街 9 号

受托人（乙方）：北京安信天行科技有限公司

法定代表人：翟建军

住所地：北京市海淀区北四环西路 68 号 10 层 1001 号

受托人（丙方）：奇安信网神信息技术（北京）股份有限公司

法定代表人：冯新戈

住所地：北京市西城区西直门外南路 26 号院 1 号楼 2 层

受托人（丁方）：中国电子技术标准化研究院

法定代表人：杨旭东

住所地：北京市东城区安定门东大街 1 号

甲乙丙丁四方根据《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，就乙丙丁三方为甲方提供 2024 年大数据安全基础保障项目服务事宜达成如下协议，以资共同遵守。

本合同为非中小企业预留合同。

第一条　服务事项及内容

本合同期限内，乙丙丁三方应为甲方提供如下服务：

一、乙方作为本项目的总负责单位，组织各参加方进行项目实施工作。

乙方为甲方提供服务完成附件 1《工作方案》中约定的如下工作内容：“1 漏洞专项治理、渗透测试、网络安全评估等”中的“1.1 安全漏洞专项治理”中的“1.1.2 安全技术检查”、“2 网络安全监测，保障中心软硬件版本更新”、“3 网络安全演习”中的“3.2　攻击面收缩服务”和“3.6 应急处置与重大活动保障”、“5 数据分类分级策略设计并实施分级”。

二、丙方为甲方提供服务完成附件 1《工作方案》中约定的如下工作内容："1 漏洞专项治理、渗透测试、网络安全评估等"中的"1.1 安全漏洞专项治理"中的"1.1.1 安全漏洞治理"和"1.1.3 应急演练"、"1.2 渗透测试"、"1.3 大数据中心网络安全评估"、"3 网络安全演习"中的"3.1 安全隐患排查与整改服务"、"3.3 内部红蓝对抗"、"3.4 安全预演习"以及"3.5 演习组织、监测与处置"约定的工作内容。

三、丁方为甲方提供服务完成附件 1《工作方案》中约定的如下工作内容："4、数据安全能力成熟度认证"。

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、乙丙丁三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、项目验收应满足以下要求：

（1）满足 2024 年大数据安全基础保障项目招标文件、乙丙丁三方投标文件的各项要求；

（2）满足附件 1 中的各项指标；

（3）项目各项工作应交付的报告、服务或成果符合项目预期；

（4）项目文档齐全，项目管理过程合规，项目人员管理到位；

（5）在规定时间前顺利通过专家验收评审。

3、乙丙丁三方应按附件 1《工作方案》中的具体要求按时完成对应工作，并及时通知甲方进行阶段性验收，甲方组织召开阶段性验收专家评审会；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，乙丙丁三方应当在 10 个工作日内进行返工或调整，并重新提交甲方验收。阶段性验收工作应在 2024 年 11 月 15 日前完成。

4、乙丙丁三方完成合同全部工作后应及时通知甲方进行终验验收。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，乙丙丁三方应当在 10 个工作日内进行返工或调整，并重新提交甲方验收。

5、验收流程

（1）甲方成立验收小组，根据合同条款认真核对项目服务内容和实施要求

等情况。

（2）甲方组织专家验收组进行验收。

（3）验收结果不符合合同约定的，甲方通知乙丙丁三方限期达到合同约定的要求。

6、本项目中，应提交的配套文档成果至少包括方案、报告等如下内容：

（1）乙方为甲方提供如下合同成果：

① 大数据安全技术检查报告（4 份）；

大数据安全技术检查年度报告（1 份）；

② 网络安全监测月度报告（12 份）（包含态势感知、网络流量监测、网络攻击诱捕、主机防护与微隔离、数据库审计、日志分析、监测溯源系统、统一认证授权系统等内容）；

网络安全监测年度总结报告（1 份）（包含态势感知、网络流量监测、网络攻击诱捕、主机防护与微隔离、数据库审计、日志分析、监测溯源系统、统一认证授权系统等内容）。

③ 攻击面收缩检测分析报告（4 份）；

④ 重大活动保障工作日报（重大活动保障期间每日 1 份）；

重大活动保障总结报告（1 份）。

⑤ 数据分类分级实施方案（1 份）；

数据安全培训实施报告（1 份）；

数据分类分级结果表（1 份）；

数据分类分级报告（1 份）。

⑥ 项目管理办法；

项目实施方案；

项目进度计划及每周进度报告；

项目质量管理相关文档；

项目其他过程文档：如项目周报、会议纪要、培训记录等。

（2）丙方为甲方提供如下合同成果：

① 漏洞治理年度报告（1 份）；

② 应急演练实施方案（4 份）；

应急演练总结报告（4 份）；

③ 渗透测试实施方案（4 份）；

渗透测试报告（4 份）；

④ 大数据中心网络和数据安全风险评估实施方案（1 份）；

网络安全风险评估报告（1 份）；

⑤ 安全隐患排查与整改报告（1 份）；

⑥ 红蓝对抗演练实施方案（1 份）；

红蓝对抗演练总结报告（1 份）；

⑦ 安全预演习实施方案（1 份）；

安全预演习总结报告（1 份）；

⑧ 网络安全演习防守工作日报（演习期间每日 1 份）；

网络安全演习总结报告（1 份）；

⑨ 大数据中心攻防能力成熟度评估实施方案（1 份）；

大数据中心攻防能力成熟度评估报告（1 份）。

（3）丁方为甲方提供如下合同成果：

数据安全风险调研报告（1 份）；

数据安全能力成熟度评估报告（1 份）。

第三条 项目小组及人员要求

1. 四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：负责项目承担部分的工作，组织协调推进项目实施 。

甲方项目负责人：张雯婷，联系方式： 13261289786 。

乙方项目负责人：李浩南，联系方式： 17812031601 。

丙方项目负责人：闫戎，联系方式： 13621007865。

丁方项目负责人：樊雅鑫，联系方式： 18500482790。

2. 项目主要人员要求

乙丙丁三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，乙丙丁三方如因正当理由需整项目主要人员的，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

乙丙丁三方为甲方提供上述服务的期限为：自合同签订之日起一年。

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¥3,390,000.00 元，大写：人民币叁佰叁拾玖万元。具体费用分配为：乙方服务费总额，人民币¥1,600,000.00 元，大写：人民币壹佰陆拾万元；丙方服务费总额，人民币¥1,590,000.00 元，大写：人民币壹佰伍拾玖万元；丁方服务费总额，人民币¥200,000.00 元，大写：人民币贰拾万元；前述服务费已经包含乙丙丁三方完成本合同项下服务的全部费用，除前述款项外，甲方无需向乙丙丁三方另行支付其他任何费用。

2. 甲方将按以下方式向乙丙丁三方支付服务费：

第 1 次付款：甲方在合同签订后，完成机构改革资金划转工作且财政预算到达甲方零余额账户并可实际使用后的 15 个工作日内，向乙丙丁三方支付服务费的 60 %即（大写）贰佰零叁万肆仟元（￥2,034,000.00 元）。其中：

甲方向乙方支付服务费，即（大写）玖拾陆万元（￥960,000.00 元）；

甲方向丙方支付服务费，即（大写）玖拾伍万肆仟元（￥954,000.00 元）；

甲方向丁方支付服务费，即（大写）壹拾贰万元（￥120,000.00 元）。

第 2 次付款：乙丙丁三方完成阶段性验收后 15 个工作日内，甲方向乙丙丁三方支付服务费的 20 %即（大写）陆拾柒万捌仟 元（￥678,000.00 元）。其中：

甲方向乙方支付服务费，即（大写）叁拾贰万元（￥320,000.00 元）；

甲方向丙方支付服务费，即（大写） 叁拾壹万捌仟元（￥318,000.00 元）；

甲方向丁方支付服务费，即（大写）肆万元（￥40,000.00 元）。

第 3 次付款：在项目终验完成且财政预算到达甲方零余额账户并可实际使用后 25 个工作日内，甲方向乙丙丁三方支付服务费的 20 %即（大写）陆拾柒万捌仟 元（￥678,000.00 元）。其中：

甲方向乙方支付服务费，即（大写）叁拾贰万元（￥320,000.00 元）；

甲方向丙方支付服务费，即（大写） 叁拾壹万捌仟元（￥318,000.00元）；

甲方向丁方支付服务费，即（大写）肆万元（￥40,000.00元）。

乙丙丁三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。因乙丙丁三方原因（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，相应责任由乙丙丁三方承担。

第六条　甲方的权利义务

1、甲方有权要求乙丙丁三方按照本合同约定提供各项服务。

2、甲方有权对乙丙丁三方提供各项服务的情况进行监督和检查。

3、甲方有权确定服务标准和要求，以及对乙丙丁三方服务人员管理工作提出要求。

4、甲方应按照本合同约定向乙丙丁三方支付服务费。

第七条　乙丙丁三方的权利义务

1、 乙丙丁三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；如因乙丙丁三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），乙丙丁三方应予赔偿。

2、 乙丙丁三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、 乙丙丁三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，并保证乙丙丁三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、 如因乙丙丁三方人员原因，给甲方或第三方造成人员人身伤害或财产损失的，乙丙丁三方应承担赔偿责任。

5、 未经甲方的书面许可，乙丙丁三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合同外主体。

6、 除四方另有约定外，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、专利申请以及乙丙丁三方到外地进行调研、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、 因乙丙丁三方原因造成阶段性验收或终验验收超期，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，乙丙丁三方应承担相应赔偿责任。

8、 超出本合同约定内容或工作量 10 %以内的，乙丙丁三方不再额外收取费用。

9、 自合同服务期满至下一年度服务商进入之前，乙丙丁三方应继续做好合同项下各项服务直至新服务商进驻，并做好与新服务商的交接，涉及知识产权的由乙丙丁三方自行协商解决。

10、乙丙丁三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，乙丙丁三方进一步保证不擅自留存、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；乙丙丁三方违反本条约定，一经发现，甲方有权随时解除本协议并追究乙丙丁三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丙丁三方予以追偿。

第八条　保密义务

1. 乙丙丁三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，乙丙丁三方应对上述保密信息承担保密义务。未经甲方书面同意，乙丙丁三方不得将甲方保密信息透露给任何合同外主体。

2. 乙丙丁三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，乙丙丁三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. 乙丙丁三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，对乙丙丁三方非从事该项目的人员一律严格保密。

4. 乙丙丁三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，乙丙丁三方应按照甲方指示在收到甲方书面通知后 5 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，甲方向乙丙丁三方提供的任何保密信息并不包括授予乙丙丁三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. 乙丙丁三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丙丁三方(含乙丙丁三方工作人员)。如乙丙丁三方或乙丙丁三方工作人员违反了上述保密义务，给甲方造成损失的，乙丙丁三方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，乙丙丁三方同意按照 合同金额 10% 赔偿甲方的损失。

第九条　知识产权归属

1、乙丙丁三方为履行本合同或在本项目实施过程中形成的文件、资料、观点及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、乙丙丁三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、著作权等合法权益。否则由此产生的任何纠纷，由乙丙丁三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丙丁三方全额追偿。

第十条　违约责任及合同的解除

1、甲乙丙丁四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。

乙丙丁三方未按照本合同约定的期限，向甲方提供服务的，乙丙丁三方其中一方未提供服务的，应由未提供服务的其中一方每迟延一日应向甲方支付本合同项下服务费总额 0.1 %的违约金，累计延迟超过 30 日的，甲方有权解除与其中一方合作，未履行合约一方不再履行合约自动解除该方部分约定部分，并向甲方支付服务费总额 10%的违约金，联合体其余两方对此承担连带赔偿责任。出现延迟不足 1 日的，按 1 日计算。

2、乙丙丁三方提供服务不符合本合同约定标准或甲方要求的，乙丙丁三方中提供服务不符合合同约定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；如乙丙丁三方中提供服务不符合合同约定方提供的服务经二次验收仍未通过甲方验收或乙丙丁三方中提供服务不符合合同约定方拒绝按照甲方要求进行返工、修改的，甲方有权解除违约方合同，乙丙丁三方中提供服务不符合合同约定方应返还甲方已经支付给责任方的全部款项，并向甲方支付对应责任方服务费总额 10%的违约金，联合体其余两方对此承担连带赔偿责任。因乙丙丁三方返工等原因造成乙丙丁三方提供服务迟延，应由乙丙丁三方承担迟延履行的违约责任。

3、乙丙丁三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，甲方有权解除违约方合同，如因此给甲方造成损失的，由乙丙丁三方承担全部赔偿责任。

4、乙丙丁三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。

5、甲方因为自身原因，未按本合同约定向乙丙丁三方支付服务费的，每迟延一日，应向乙丙丁三方中相应的服务方支付拖欠款项 0.1 %的违约金（违约金总额不超过合同总价的 5%），因财政资金未到位的情况除外（乙丙丁三方充分知悉并确认财政资金拨付到账是甲方履行本合同付款义务必要条件，在该条件未满足时，甲方在合理通知乙丙丁三方后有权暂不支付且不承担逾期付款责任）。

第十一条　争议的解决

因履行合同所发生的一切争议，四方应友好协商解决，协商不成的，按下列第 1 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_____人民法院起诉。

第十二条　廉政承诺

1. 合同四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；不得在乙丙丁三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，接受乙丙丁三方从该项目中支取的劳务报酬；不得参加乙丙丁三方安排的超标准宴请和娱乐活动。

3. 乙丙丁三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. 本合同自四方签字盖章之日起生效。

2. 未尽事宜，经四方协商一致，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，四方均应遵照执行。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
3	联合体协议（复印件）
4	中标通知书

4. 本合同正本一式 捌 份，甲方执 贰 份，乙丙丁三方各执 贰 份，具同等法律效力。

（以下无正文）

甲方（盖章）：北京市大数据中心

签署人：

签订日期：2024.6.28

乙方（盖章）：北京安信天行科技有限公司

签署人：

签订日期：2024.6.28

开户行：北京银行双清苑支行

开户名称：北京安信天行科技有限公司

账号：01090327800120102315974

丙方（盖章）：奇安信网神信息技术（北京）股份有限公司

签署人：

签订日期：2024.6.28

开户行：招商银行北京建国路支行

开户名称：奇安信网神信息技术（北京）股份有限公司

账号：110902261210404

丁方（盖章）：中国电子技术标准化研究院

签署人：

签订日期：2024.6.28

开户行：工行北京北新桥支行

开户名称：中国电子技术标准化研究院

账号：0200004309088116710

附件 1 工作方案

一、工作内容

大数据安全基础保障项目目标为保障北京市大数据中心系统安全稳定运行、数据安全使用，服务期内不发生重大网络安全事件。具体分为以下五个方面：

- 开展漏洞专项治理、安全技术检查、应急演练、渗透测试、安全评估等工作，系统性排查中心各系统安全隐患，掌握中心各系统的真实安全状况，辅助各应用系统发现安全隐患并推进整改加固，加强中心各系统安全防御纵深，提高攻击发现能力，缩短攻击发现时间。
- 开展网络安全监测，对中心的软件、硬件进行监测分析，并对网络安全事件和状态进行监测研判，掌握业务流量访问关系、主机软件版本、业务流量、漏洞和弱密码、安全基线、网络攻击等安全台账，发现安全隐患，推进整改加固。
- 开展网络安全演习，在实战中有效提升中心网络安全实战保障能力。
- 开展数据安全能力成熟度认证，系统性提升中心数据安全保护水平。
- 开展数据分类分级，制定数据分类分级策略并实施，满足国家相关法律法规的要求，作为数据安全保护的基础性工作，指导数据的加密、脱敏等处理过程。

1 漏洞专项治理、渗透测试、网络安全评估等

1.1 安全漏洞专项治理

1.1.1 安全漏洞治理（**丙方**）

通过主动排查隐患、动态跟踪漏洞态势等手段，及时发现安全隐患，并提出整改意见和建议，督促整改。

1.1.1.1 工作内容

（1）通过自动化漏洞扫描工具，结合中心工作安排，定期对中心各系统安全漏洞进行发现、评估工作，评估各系统漏洞治理绩效。协助开展网络安全漏洞治理体系流程建设，形成有效的工作机制，确保各类安全漏洞能够有效的形成漏洞闭环。

（2）通过工具或人工方式对各系统安全基线进行定期检查，排查安全隐患并督促整改。检查内容包括但不限于系统边界防护情况、账户权限情况、系统配

置情况、补丁更新情况、敏感数据和重要数据保护情况等。

（3）跟踪业内最新发布的漏洞态势，及时进行预警、排查和督促整改。

（4）建立漏洞台账，对漏洞进行评估分析，进行漏洞修复的优先级排序，指导中心各系统开展漏洞修复，并跟踪修复结果和效果。漏洞来源包括但不限于：上级单位下发的漏洞报告、漏洞扫描报告、渗透测试报告、主机安全软件漏洞报告等。

（5）服务期内开展漏洞扫描不少于 4 次、安全基线检查不少于 4 次，每次不少于 8 个系统，服务期内覆盖中心所有系统。

1.1.1.2 工作成果

《漏洞治理年度报告》1 份。

1.1.2 安全技术检查（**乙方**）

1.1.2.1 工作内容

（1）按照上级检查要求，开展中心范围内的系统和数据的安全技术自查。

（2）配合上级主管部门开展安全检查，做好技术支撑。

（3）重大活动和节假日等重点时期前，开展安全隐患排查。

（4）对自查和检查中发现的问题，给出整改建议，配合完成整改。

（5）对服务期内检查工作进行分析，并提出工作建议。

（6）支撑中心安全自查及配合迎检工作，确保中心业务系统满足上级监管单位要求的同时满足中心网络安全工作考核要求。

1.1.2.2 工作成果

《大数据安全技术检查报告》4 份。

《大数据安全技术检查年度报告》1 份。

1.1.3 应急演练（**丙方**）

1.1.3.1 工作内容

（1）根据基础检查结果，结合中心系统或平台的安全防护状况以及节假日及重大活动的安全保障要求，开展网络安全应急演练，演练方式包括实战演练、模拟演练和桌面推演，每次演练均应编制演练计划方案和脚本，并形成攻防应急演练总结报告。开展应急演练培训，根据演练结果，配合制修订中心相关的应急预案，维护应急预案库。

（2）服务期内开展应急演练不少于 4 次，每次不少于 8 个系统，服务期内覆盖中心所有系统。

1.1.3.2 工作成果

《安全应急演练方案》4 份。

《安全应急演练总结报告》4 份。

1.2 渗透测试**（丙方）**

1.2.1 工作内容

（1）测试范围

统筹考虑我市重大活动安全保障要求和中心工作安排，服务期内开展至少 4 次中心范围内的系统渗透测试，每次不少于 8 个系统，服务期内覆盖中心所有系统。

（2）测试内容及方法

在互联网和政务外网侧，综合利用渗透测试工具和人工分析等手段，在安全可控情况下，模拟黑客攻击系统，进行信息收集、分析和权限提升等一系列操作，及时发现系统存在的安全风险。

开展 API 接口安全测试，根据中心工作安排，根据接口数量及重要程度，对重要系统的重要接口测试，检查对外 API 接口存在数据泄漏的安全风险情况，包括但不限于：敏感信息泄漏错误配置、注入漏洞、弱身份鉴别、弱会话控制、越权、接口滥用等情况。

（3）测试实施要求

开展渗透测试可能会对系统造成一定的影响，因此测试实施应满足以下要求：与系统负责部门和相关责任人充分沟通确认，明确渗透测试的实施人员、时间、测试内容和配合事项等。测试过程中如发现安全隐患，不应尝试任何破坏行为（如修改密码、上传木马等）。未经允许，禁止截图留存或违规下载系统数据，禁止将测试数据提供给任何第三方。配合系统责任部门根据渗透测试结果开展必要的应急攻防演练和应急预案修订工作。

1.2.2 工作成果

《渗透测试实施方案》4 份。

《渗透测试报告》4 份。

1.3 大数据中心网络安全评估（丙方）

1.3.1 工作内容

（1）开展网络安全风险评估，对中心所有平台和系统及其相关数据、人员、制度等，开展资产识别、威胁识别、安全措施识别、脆弱性识别，进行风险分析和评价，给出风险整改建议。并从攻防对抗角度，开展中心攻防能力评估，给出整改建议。

（2）评估依据：《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）、《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 个人信息安全规范》（GB/T 35273-2020）、《信息安全技术 大数据服务安全能力要求》（GB/T 35274-2023）

（3）评估内容

1）本项目的安全风险评估内容包括但不限于中心管理制度落实情况、网络安全状况、数据安全防护情况、敏感资产保护情况、个人信息保护情况、人员安全管理情况、服务外包安全情况、应急保障情况等，并梳理和维护中心系统和数据资产清单、制度清单、风险清单和改进措施清单等，并形成评估报告。

2)本项目的安全攻防能力评估内容包括但不限于设计攻防能力成熟度模型、对攻击预防能力、防御加固能力、事件检测能力、事件响应能力、关联分析能力、反制能力、安全运营能力等进行评估，形成相应的评估报告。

（4）评估方法

应遵循定性与定量相结合的原则，采取访谈和检查、工具扫描、渗透测试等常规方法以及攻防演练等相结合的评估方法，风险值的计算应采用相对成熟的计算公式。

1.3.2 工作成果

《网络安全风险评估实施方案》1 份。

《网络安全风险评估报告》1 份。

《攻防能力成熟度评估实施方案》1 份。

《攻防能力成熟度评估报告》1 份。

2 网络安全监测，保障中心软硬件版本更新（乙方）

2.1 工作内容

（1）网络监测工具服务。针对已经部署的网络流量监测、网络攻击诱捕、态势感知等工具，提供6个月的服务授权。

（2）通过安全态势、网络流量监测、蜜罐、主机防护与微隔离、数据库审计、日志分析、监测溯源系统、统一认证授权系统等工具与系统，7*24小时监测发现中心系统状态、安全漏洞、安全攻击等，及时上报，并协调进行处置，跟踪处置进度并定期报告进展。

2.2 工作成果

网络流量监测、网络攻击诱捕、态势感知等工具6个月服务期授权。

网络安全监测月度报告12份（包含态势感知、网络流量监测、网络攻击诱捕、主机防护与微隔离、数据库审计、日志分析、监测溯源系统、统一认证授权系统等分报告）

网络安全监测年度总结报告1份（包含态势感知、网络流量监测、网络攻击诱捕、主机防护与微隔离、数据库审计、日志分析、监测溯源系统、统一认证授权系统等分报告）

3 网络安全演习

3.1 安全隐患排查与整改服务**（丙方）**

3.1.1 工作内容

（1）安全隐患自查。协助组织各系统开展资产梳理自查工作，梳理主机开放的服务、互联网入口、终端、网络设备等资产信息，发现和清理老旧资产，过期资产、无用账号、无用的服务等，明确各自防守边界。

（2）隐患统一排查。通过渗透测试、漏洞扫描与基线配置检查监测漏洞、安全配置、控制权限等内容，发现应用和主机的配置风险及基线规则问题，下发整改通知，协助完成整改。

（3）隐患专项排查。开展弱口令、靶标系统、VPN、跳板机等集中管控系统、安全设备、社工隐患等专项隐患排查

（4）开展大数据中心各系统的数据安全基线与合规性评估，重点发现各系统的数据安全隐患与数据安全规范性差距，发现问题并针对性提出数据安全隐患治理策略等建议。

（5）结合隐患排查开展整改加固，降低被外部攻击利用的脆弱性和风险，

包括但不限于跟踪整改已知漏洞、优化策略配置、补充网络安全防护能力等。

（6）攻击路径分析。以实战攻防的视角，全面梳理互联网和政务外网通往中心重要系统和业务的访问路径，全面掌握可能存在的攻击路径，绘制攻击路径分析图以便优化排兵布阵方式，制定精准的布防优化方案。

（7）高危攻击路径布防优化。优化并验证高危攻击路径布防能力，模拟实战场景，构造攻击者的行为和技术，验证中心在主要攻击场景下的防护有效性。

（8）主要攻击场景布防优化，优化主要攻击场景布防方案，按照完整攻击流程，验证中心防护体系能否有效的检测或防护相应攻击。构造的攻击手段包括但不限于域渗透、C2 连接、webshell 攻击、漏洞利用、异常行为等。构造的攻击环节包括但不限于信息收集、边界突破、权限维持、横向移动等。形成应对攻击场景的防护有效性验证评估和优化报告。

（9）安全产品策略有效性验证及优化。验证中心各系统使用的安全防护产品的策略有效性。验证结果包括但不限于如下指标：检测率、阻断率、绕过率等。形成安全防护产品有效性评估验证评估报告下发改进。

3.1.2 工作成果

《安全隐患排查与整改报告》1 份

3.2 攻击面收缩服务**（乙方）**

3.2.1 工作内容

（1）检测和识别中心暴露在互联网上的资产数据，检测的全网数据内容包括但不限于：资产测绘、WHOIS 数据、域名数据、ICP 备案数据、DNS 服务器、APP 移动应用、公众号/小程序、公共代码仓库 GIT/SVN/GITLAB、脉脉等招聘平台信息、微博/QQ/微信等社交媒体公开信息、开发者社区信息、电子邮件地址等。分类形成中心攻击暴露面数据报告。

（2）分析中心暴露在互联网信息的安全风险。评估中心各系统互联网攻击面。分析评估内容包括但不限于高危漏洞风险、应用程序安全风险、数据泄露风险、商誉风险、钓鱼风险、供应链风险、影子资产风险。

（3）结合中心工作安排，开展 4 次攻击面收缩，形成相应的报告。

3.1.2 工作成果

《攻击面收缩检测分析报告》4 份。

3.3 内部红蓝对抗（**丙方**）

3.3.1 工作内容

（1）组织不少于 8 人的红蓝对抗团队，包含红队、蓝队、紫队角色，编制场景化的红蓝对抗方案，开展不少于 1 次红蓝对抗演练。

（2）红队服务。组织安全人员以拿到预定目标主机权限或数据库权限为目标，实施可控的真实网络攻击。红队攻击内容应包括但不限于 Web 渗透、旁路渗透、VPN 渗透、集权平台渗透、社工钓鱼、近源攻击、漏洞挖掘、移动安全、内网安全、二进制安全等。并记录攻击过程和成果证据。

（3）蓝队服务。组织安全人员与中心的安全团队共同参与防守，按照监测分析、事件研判、应急处置、联络协调进行分工分组。各小组对攻击事件实时监测、分析、处置、并按照攻防演练流程进行事件的应急处置及上报。带动现有安全团队提升面对真实攻击时的事件响应和处理能力、发现入侵痕迹的能力、安全设备响应和报警的能力。

3.3.2 工作成果

《红蓝对抗演练实施方案》1 份

《红蓝对抗演练总结报告》1 份

3.4 安全预演习（**丙方**）

3.4.1 工作内容

（1）从实战角度出发，用沙盘推演的方式组织安全预演习，检验中心参演团队准备情况，磨合中心参演团队应对演习的工作流程，培训中心参演团队的演习工作经验。

（2）制定预演习实施方案，应包含预演习目标，计划，组织，角色，内容，流程，评价准则，预期成果等内容。开展培训宣贯，培训内容包括但不限于网络安全演习背景，攻击队采用的常见攻击手法、攻击路径、攻击目标，业务系统的防守及应急处置优秀案例。

（3）场景设计。设计不少于 5 个攻击场景方案，方案应包含攻击目标安全隐患、攻击所造成的影响、攻击的步骤及路径、每一步采用的技战法、攻击的策略优势。针对攻击设计一一对应的防守方案，方案应包括防守体系及恢复体系的整体介绍，针对攻击的防守动作，防御恢复体系的优势。

（4）预演习和总结。组织开展预演习，汇总分析所有攻击思路与方案，进行充分、全面的复盘分析，总结经验教训，形成改进建议下发整改。

3.4.2 工作成果

《安全预演习实施方案》1 份

《安全预演习总结报告》1 份

3.5 演习组织、监测与处置**（丙方）**

3.5.1 工作内容

（1）现场值守。演习期间应提供不少于 6 人的安全专家 7*24 小时现场值守。并作为主防守方组织完成现场管理及协调防守工作。工作内容包括但不限于：实时分析日志、流量，判断攻击方动向、预警攻击事件，输出防御报告、协助指挥者决策、调整防御策略；报告记录安全事件处置过程与具体应对操作，包括问题表现、深层原因、处置流程与手段、处置结果等。

（2）监测分析。及时梳理和分析安全设备告警日志，包括但不限于 WAF、网络流量安全分析、蜜罐、主机安全、态势感知、数据库防火墙、数据库审计等，研判告警有效性，并对攻击方法、攻击方式、攻击路径和工具等进行分析研判，找到攻击者的源 IP 地址、攻击服务器 IP 地址、邮件地址等信息，及时上报事件和处置意见。

（3）应急处置。根据相关告警处置建议对受影响主机进行快速处理和响应，按照应急预案完成处置流程，根据攻击影响可采取封禁攻击地址、系统下线等方式进行处置，并全面排查清理系统内攻击者创建的系统账号、后门程序等，确保攻击不扩散。

（4）防守反制。对已发现攻击开展攻击溯源和攻击反制，按要求形成防守成果。

（5）威胁情报。要求及时提供 0day 漏洞等精准威胁情报。及时提供攻击事件、攻击队 IP、攻击特点等威胁情报供现场值守人员学习参考。

（6）复盘总结。要求完成每日防守工作复盘总结，提炼技战法，包括发现的安全问题，处理的方案，下发的策略，总结优点和不足，提出改进建议。完成上级管理部门要求的防守数据汇总统计、数据分析判断、每日汇总汇报工作。

（7）演习后总结整改。演习完成后开展全面复盘总结，针对暴露出的漏洞、

脆弱性等问题开展监督整改，开展技战法研究，继承和发展演习期间的有效安全监测机制，及时调整中心各系统常态化的安全监测和事件处置机制，补齐演习中发现的安全短板，优化完善中心安全防护体系。

3.5.2 工作成果

《网络安全演习总结报告》1 份。

3.6 应急处置与重大活动保障（**乙方**）

3.6.1 工作内容

（1）应急处置。根据相关告警处置建议对受影响主机进行快速处理和响应，按照应急预案完成处置流程，根据攻击影响可采取封禁攻击地址、系统下线等方式进行处置，并全面排查清理系统内攻击者创建的系统账号、后门程序等，确保攻击不扩散。支撑应急排查溯源工作，协调专业应急人员进行排查溯源，溯源分析攻击路径及排查攻击影响范围等，为重大网络安全事件应急处置储备人员及技术支撑。

（2）重大活动保障。确保在如元旦春节、端午与五一、中秋与国庆等重要节假日以及重大活动期间开展网络安全值守、监测和应急，提升中心业务系统综合安全保障水平。重大活动保障期间应提供不少于 4 人的安全专家 7*24 小时开展值守、监测和应急。

3.6.2 工作成果

《年度应急处置报告》1 份。

《年度重大活动保障报告》1 份。

4 数据安全能力成熟度认证（丁方）

4.1 工作内容

（1）调研评估。调研评估中心主要业务系统的数据使用情况，基于业务场景，开展数据安全现状和风险调研。完成数据安全现状调研报告。提供咨询服务，以应对新业务、新场景、新的网络安全形势，对中心网络环境进行全面的审视与防护水平的能力提升。

（2）通过调研，在全面了解大数据中心的数据安全管理运行现状的基础上，参照 GB/T 37988-2019 《信息安全技术 数据安全能力成熟度模型》，以数据的全生命周期为各个安全过程域，从组织建设、制度流程、技术工具和人员能力四

个维度对大数据中心数据安全防护能力进行评估并协助完成整改。完成数据安全能力成熟度评估报告。

（3）开展数据安全能力成熟度三级认证。开展不少于 2 人的 CISP-DSG 认证培训，确保在通过数据安全能力成熟度认证过程中人员能够满足认证要求。

4.2.工作成果

《数据安全风险调研报告》1 份。

《数据安全能力成熟度评估报告》1 份。

5 数据分类分级策略设计并实施分级（乙方）

5.1 工作内容

制定数据分类分级实施方案。开展数据分类分级培训。梳理中心数据库和数据，形成中心数据库资产表和数据资产表。针对各业务系统数据现状，对系统承载的数据依据相关法律法规和国家标准开展分类分级。

5.2 工作成果

《数据分类分级实施方案》 1 份

《数据安全培训实施报告》 1 份

《数据分类分级结果表》 1 份

《数据分类分级报告》 1 份

二、工作要求

本项目服务期：合同签订之日起一年。

相关实施要求如下：

1、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：

（1）《中华人民共和国民法典》

（2）《中华人民共和国网络安全法》

（3）《中华人民共和国个人信息保护法》

（4）《中华人民共和国数据安全法》

（5）《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）

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

（7）《信息安全技术 个人信息安全规范》（GB/T 35273-2020）

（8）《信息安全技术 大数据服务安全能力要求》（GB/T 35274-2017）

（9）《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）

（10）北京市大数据中心各类安全管理制度等

以上规范如有更新，以国家、地方、行业最新标准为准。在实施本项目期间除应遵循上述规范外，还应遵循未列出的其它法律、法规及相关国家、地方、行业标准规范。

2、项目实施要求

2.1 项目进度要求

乙丙丁三方应提供项目实施进度控制方案，具有详细进度计划和里程碑节点，保障项目按照进度计划顺利完成验收。

2.2 项目组织管理要求

在项目实施全过程中，在组织管理中做好以下几点：

(1) 项目实施过程中，严格按照投标文件中承诺提供的项目人员，不得随意更换。

(2) 在采购人的未验收项目中涉及的人员不纳入本项目人员名单。

(3) 明确项目的组织机构和参与人员，确保其经验丰富、人员稳定充足。

(4) 制定完整、详细的研究工作方案，至少包含项目启动、项目验收等关键环节，研究过程要形成相关纪要和文档。

(5) 全程进行项目跟踪和管控，建设完善的项目管理体系，建设长效沟通机制，每周提交项目进度报告。

(6) 及时提供工作进展、阶段成果，配合做好有关成果工作汇报；定期召开项目会议，沟通汇报各项工作的落实情况，解决遇到的实际问题。

(7) 项目实施过程中可能产生需求变更，如果需求变更在现有基础上的 15%之内，须承诺视同包含在项目需求之中，不做合同和工期调整。

3、项目团队人员

3.1 项目团队构成

遵守市政务服务和数据管理局项目管理的有关规定，根据采购人的要求组建项目工作组，指派项目负责人，在合同执行期间，项目人员原则上不变更，如需变更需经甲方同意。配备以下人员：

（1）项目负责人

具有良好的专业素质，具有丰富的项目全局把控和资源管理经验，负责总体设计、组织管理和协调，并作为本项目的实际主持者担负实质性工作；具有与本项目相关专业的高级职称，对政务部门信息化建设有充分了解，具有与本项目类似网络安全保障项目经验。

（2）驻场人员

除项目负责人外，具有不少于 2 人的全职支撑工作的驻场人员，能够服从采购人的工作安排，具备较强的专业素质，有优秀的书面表达能力、组织能力和沟通能力，具有与本项目类似网络安全保障项目经验。

（3）核心团队人员

除项目负责人和驻场人员以外，具有不少于 15 人的核心工作团队，要求人员具有信息安全保障人员认证（CISAW）或注册信息安全专业人员（CISP）证书，专业结构及分组合理，覆盖项目所涵盖的业务领域，具备较强的调查研究能力和组织实施能力，具有网络安全项目经验。

网络安全演习期间，网络安全演习队伍应驻场服务，驻场安全专家不得少于 6 人。参与网络安全演习及重大活动保障的专家队伍应具有参加 3 次及以上网络安全攻防经验。其负责人应作为主要成员在国家行业主管部门组织的网络安全大赛中获奖，同时应具备 0day 漏洞研究和挖掘能力、网络安全攻防能力、丰富的国家级网络安全演习经验。其他队员应具有国内外网络安全大赛参赛经验。

（4）支撑团队人员

为项目的实施提供强大的后台支撑团队，并根据项目进展动态调整人员力量，以应对突发任务或关键节点的繁杂工作。除项目负责人、驻场人员和核心团队人员以外，具有不少于 10 名支撑团队人员，支撑团队构成应覆盖所有工作内容，并按照项目的主要组成分组，分组方案合理，各组负责人不允许兼任，负责人及人员专业与工作内容相符。

（详细服务人员清单见附件 2）

3.2 服务商资质

具有质量管理体系认证证书、信息安全管理体系认证证书。

4、保密管理

制定安全保密工作方案，详细介绍相关保密措施，针对本项目涉及的所有系

统数据（纸质文档、电子文档、光盘等）进行严格保密，并与每个项目人员签署安全保密协议。

5、培训要求

本项目中开展应急演练、渗透测试、风险评估、数据分类分级等工作，对相关人员开展必要的安全培训，相关要求如下：

5.1 培训范围：所有参与人员和配合人员。

5.2 培训目的：使受训人员能够了解和熟悉应急演练流程、渗透测试、风险评估和分类分级的注意事项和配合事项，有效支撑相关安全工作的开展。

5.3 培训内容：

说明培训内容。培训的内容包括但不限于：

1)应急演练实施方案和处置流程。

2)渗透测试、风险评估配合事项和注意事项。

3)数据分类分级流程及要求。

4)常见安全问题应对措施。

5.4 培训资料及语言

1)培训资料：培训的全部内容都应提供详细的技术资料。

2)培训语言：培训资料使用的文字为中文。

5.5 培训开展的方法

根据采购人的上述要求及服务方认为应予补充的内容制订一个详细的培训计划，并于培训开始前交给采购人，征求意见，以确保培训工作的顺利进行，达到预期的目的。

6、成果归属

本项目实施完成新产生的所有技术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）的所有权、使用权、转让权以及收益等一切权利由甲方享有，本项目实施完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。

7、保密要求

乙方应制定安全保密工作方案，详细介绍相关保密措施，针对本项目涉及的所有系统数据（纸质文档、电子文档、光盘等）进行严格保密，并与每个参与项

目人员签署安全保密协议。

8、咨询与技术支持要求：

（1）提供本项目服务期内的响应服务，提供 7×24 小时电话支持和远程支持响应服务。

（2）对特殊演示或推广情况要制定技术服务预案和应急预案，配合完成应急演练，并承诺提供 7×24 小时的不间断服务支持。

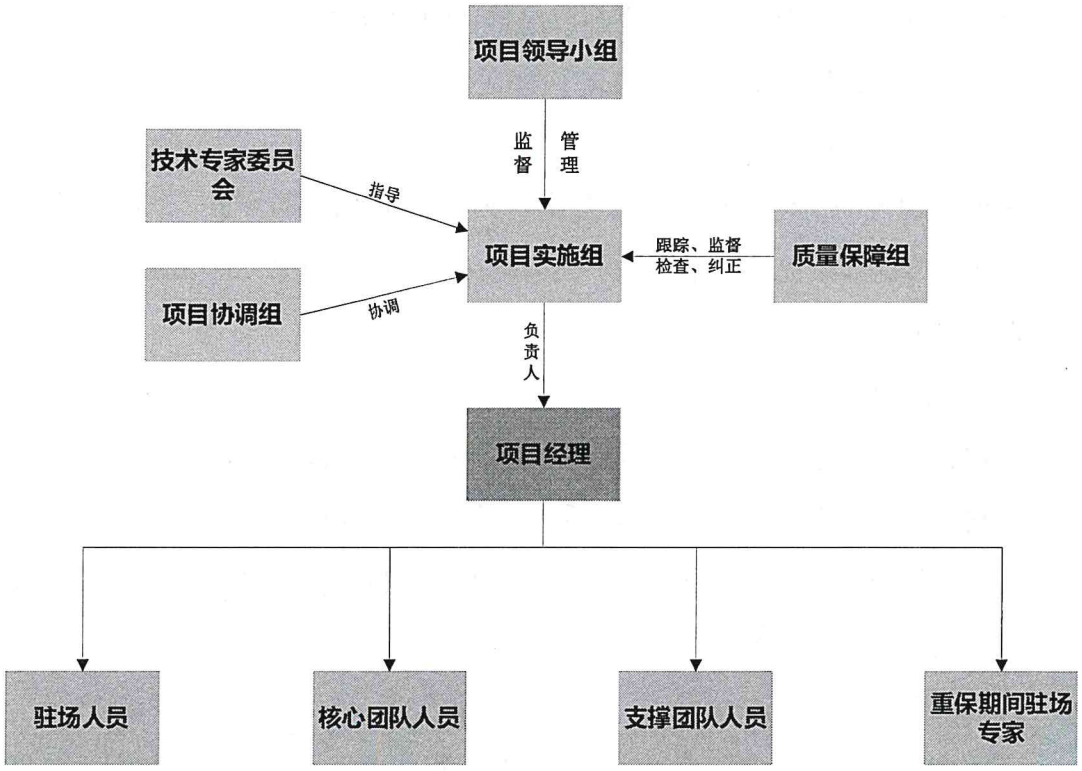
9、售后服务要求：

（1）自合同服务期满至下一年度服务商进入之前，乙丙丁三方继续按原合同提供合同内各项服务直至新服务商进驻，并与新服务商做好工作交接。交接内容包括但不限于系统配置信息、工作日志、项目技术资料、常见问题处理方法、项目遗留问题等。

（2）服务期满后不得擅自留存、使用、泄露或者向他人提供因履行本合同而获取的任何数据。

三、工作组织

乙丙丁三方为本项目成立了专门的项目组织，项目组织框架图如下：



项目组织框架图

项目各小组职责分工如下：

1、项目领导小组

乙丙丁三方与用户各指定负责人作为项目主管，并加入乙丙丁三方销售代表，共同组成项目领导小组。用户负责对乙丙丁三方的项目建设工作进行总体监督、对技术人员进行工作安排、考核，对乙丙丁三方的工作进行评价和反馈；乙丙丁三方项目经理负责对项目建设和系统运行维护支持工作的总体管理，包括本项目工作制度的建立、执行、人员的工作调派、考核、售后服务工作的总结等，是乙丙丁三方的第一责任人和接口人；乙丙丁三方销售代表负责商务总协调。

2、技术专家委员会

由乙丙丁三方相关技术高层管理人员、资深技术专家和外协单位信息安全技术专家组成。主要负责指导、审核技术方案、工作规范以及方法，并对项目过程中的技术难题提供指导和支持。

3、项目协调组

负责对本项目的整体协调进度控制，并在工作中的重大问题组织各方面力量进行支持、处理。人员由乙丙丁三方的部门经理组织相关人员构成。

4、质量保障组

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。

5、项目实施组

由项目经理和项目实施团队共同组成，项目经理作为项目实施组的负责人，多角度保障项目顺利完成实施。

6、项目经理

由乙丙丁三方委派熟悉用户业务、项目综合能力强、并具备丰富信息安全服务经验的管理人员担任，主要负责项目工作的具体制定、开展，率领各项目小组规范执行各项工作。总体负责整个项目的开展和完成，按照合同规定的工作内容、进度安排、乙丙丁三方的质量保证体系、安全生产管理制度以及保密制度的要求，负责项目的组织服务任务实施、项目质量管理、项目进度控制、项目风险控制、项目绩效考核、用户响应以及沟通等事宜，具体职责如下：

- 主持项目现场调研工作；
- 主持项目管理体系编制工作；

- 主持方案的编制工作；
- 主持项目进度计划和实施方案的编制工作；
- 负责项目的协调与调度、管理工作；
- 负责项目质量的控制和保证；
- 负责协调、组织产品维护、维修、测试以及其他任务的组织执行；
- 负责项目文档计划、管理和审核；
- 组织项目成果的检查、交付与确认。

7、项目实施团队

项目实施团队在项目经理带领下，负责项目的具体实施工作。

在科学的项目管理组织领导下，乙丙丁三方将调配对用户系统熟悉、有丰富实施服务经验的资深专业安全技术人员，确保本项目的顺利实施。

四、计划安排

为保证本项目的顺利实施，根据用户的实际情况，编制项目实施进度计划。将此次项目任务加以分解，并确定每一阶段任务的详细计划进度，以指导和保证项目组按照项目进度要求完成项目所包括的服务任务。

实施进度计划通过科学应用启动、实施、收尾、验收、售后技术支持和服务等项目管理过程，规范地完成项目的需求分析及实施进度计划的确定。

时间进度初步计划如下表所示：

本项目的主要时间安排如下：

（一）2024 年 11 月 15 日前完成阶段性验收。

阶段性验收需至少完成如下工作：

（1）渗透测试工作完成不少于 2 次；

（2）安全漏洞专项治理完成不少于 2 次；

（3）完成阶段验收前各项网络安全监测服务内容；

（4）攻击面收缩服务完成不少于 2 次；

（5）完成内部红蓝对抗；

（6）至少完成数据安全能力成熟度调研工作；

（7）至少完成数据分类分级实施方案和调研工作。

（二）2025 年 7 月底前完成项目终验验收

按照项目合同约定完成各项工作，以及项目终验验收。

五、服务质量要求及验收

详见合同正文第二条。

附件 2 项目主要人员名单

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
陈青民	男	41	硕士	高级	高级项目经理	项目经理	项目总体协调和管理
李浩南	男	25	大专	无	安全工程师	核心团队成员	提供安全服务
刘元焜	男	22	本科	无	安全工程师	核心团队成员	提供安全服务
丁立凡	男	31	本科	无	安全工程师	驻场人员	提供驻场安全服务
张辰雨	男	36	本科	无	安全工程师	驻场人员	提供驻场安全服务
梁晨	男	42	本科	无	安全工程师	核心团队成员	漏洞专项治理、渗透测试、网络安全评估
陈士如	男	46	本科	无	安全工程师	核心团队成员	漏洞专项治理、渗透测试、网络安全评估
相照文	男	37	本科	无	安全工程	核心团队成员	漏洞专项治理、渗透测

					师		试、网络安全评估
陈亮亮	男	36	本科	无	安全工程师	核心团队成员	网络安全监测，保障中心软硬件版本更新
薛克伟	男	37	本科	无	安全工程师	核心团队成员	网络安全监测，保障中心软硬件版本更新
林素霞	女	31	本科	无	安全工程师	核心团队成员	网络安全监测，保障中心软硬件版本更新
张铁铮	男	52	本科	无	安全工程师	核心团队成员	网络安全演习
闫邵鹏	男	33	本科	无	安全工程师	核心团队成员	网络安全演习
张春	男	27	本科	无	安全工程师	核心团队成员	网络安全演习
赵东	男	37	本科	无	安全工程师	核心团队成员	网络安全演习
徐春雨	男	35	本科	无	安全工程师	核心团队成员	网络安全演习

翟佳辉	男	29	本科	无	安全工程师	核心团队成员	网络安全演习
郭晟君	男	34	本科	无	安全工程师	核心团队成员	网络安全演习
胡松	男	47	本科	无	安全工程师	核心团队成员	网络安全演习
徐羽佳	女	32	本科	无	安全工程师	核心团队成员	数据安全能力成熟度认证
高晨涛	男	24	本科	无	安全工程师	核心团队成员	数据安全能力成熟度认证
任英杰	男	30	本科	无	安全工程师	核心团队成员	数据安全能力成熟度认证
高超	男	高超	本科	无	安全工程师	核心团队成员	数据安全能力成熟度认证
刘行	男	35	本科	无	安全工程师	核心团队成员	数据安全能力成熟度认证
李海东	男	32	本科	无	安全工程师	核心团队成员	数据安全能力成熟度认证

刘璐	男	40	本科	无	安全工程师	核心团队成员	数据分类分级策略设计实施
刘彬	女	44	本科	中级	安全工程师	核心团队成员	数据分类分级策略设计实施
刘涛	男	38	本科	无	安全工程师	支撑团队人员	漏洞专项治理、渗透测试、网络安全评估
王成	男	40	本科	无	安全工程师	支撑团队人员	漏洞专项治理、渗透测试、网络安全评估
彭钊	男	36	本科	中级	安全工程师	支撑团队人员	漏洞专项治理、渗透测试、网络安全评估
王建宇	男	32	本科	无	安全工程师	支撑团队人员	网络安全监测，保障中心软硬件版本更新
邢永乐	男	35	本科	无	安全工程师	支撑团队人员	网络安全监测，保障中心软硬件版本更新
郭嘉	男	30	本科	无	安全工程师	支撑团队人员	网络安全监测，保障中

							心软硬件版本更新
张远	男	43	本科	无	安全工程师	支撑团队人员	网络安全演习
车文君	男	40	本科	无	安全工程师	支撑团队人员	网络安全演习
赵博	男	45	本科	无	安全工程师	支撑团队人员	网络安全演习
曹畅	男	26	本科	无	安全工程师	支撑团队人员	网络安全演习
李赛	男	39	本科	无	安全工程师	支撑团队人员	网络安全演习
单学武	男	39	本科	中级	安全工程师	支撑团队人员	数据安全能力成熟度认证
房家乐	男	28	本科	无	安全工程师	支撑团队人员	数据安全能力成熟度认证
时越	男	27	本科	无	安全工程师	支撑团队人员	数据安全能力成熟度认证
马天宁	男	33	本科	中级	安全工程师	支撑团队人员	数据分类分级策略设计实施

张园园	女	31	本科	无	安全工程师	支撑团队人员	数据分类分级策略设计实施
王翌崑	男	31	本科	无	安全工程师	支撑团队人员	数据分类分级策略设计实施
白旭东	男	44	本科	中级	安全专家	网络安全演习及重大活动保障期间驻场安全专家	网络安全演习及重大活动保障期间驻场
安亚鹏	男	42	本科	中级	安全专家	网络安全演习及重大活动保障期间驻场安全专家	网络安全演习及重大活动保障期间驻场
王洪星	男	43	本科	中级	安全专家	网络安全演习及重大活动保障期间驻场安全专家	网络安全演习及重大活动保障期间驻场
张鑫	男	40	本科	中级	安全专家	网络安全演习及重大活动保障期间驻场安全专家	网络安全演习及重大活动保障期间驻场
赵冠雄	男	38	本科	中级	安全专家	网络安全演习及重大活动保障期间	网络安全演习及重大活

						驻场安全专家	动保障期间驻场
赵少川	男	42	本科	高级	安全专家	网络安全演习及重大活动保障期间驻场安全专家	网络安全演习及重大活动保障期间驻场
李兵兵	男	41	本科	中级	安全专家	网络安全演习及重大活动保障期间驻场安全专家	网络安全演习及重大活动保障期间驻场
黄晖	男	41	本科	中级	安全专家	网络安全演习及重大活动保障期间驻场安全专家	网络安全演习及重大活动保障期间驻场

附件 3 联合体协议书

3 本项目的特定资格要求（如有）

3-1 联合协议（如有）（实质性格式）

联合协议

北京安信天行科技有限公司 、 奇安信网神信息技术（北京）股份有限公司及中国电子技术标准化研究院就"2024 年大数据安全基础保障项目（项目名称）" / 包招标项目的投标事宜，经各方充分协商一致，达成如下协议：

一、 由北京安信天行科技有限公司牵头，奇安信网神信息技术（北京）股份有限公司、中国电子技术标准化研究院参加，组成联合体共同进行招标项目的投标工作。

二、 北京安信天行科技有限公司为本次投标的牵头人，联合体以牵头人的名义参加投标，联合体中标后，联合体各方共同与招标人签订合同，就采购合同约定的事项对招标人承担连带责任。

三、 联合体各方均同意由牵头人代表其他联合体成员单位按招标文件要求出具《授权委托书》。

四、 牵头人为项目的总负责单位：组织各参加方进行项目实施工作。

五、 北京安信天行科技有限公司负责 1 漏洞专项治理、渗透测试、网络安全评估等中的（1.1 安全漏洞专项治理(1.1.2 安全技术检查)）；2 网络安全监测，保障中心软硬件版本更新；3 网络安全演习(3.2 攻击面收缩服务、3.6 应急处置与重大活动保障)；5 数据分类分级策略设计并实施分级，具体工作范围、内容以投标文件及合同为准。

六、 奇安信网神信息技术（北京）股份有限公司负责 1 漏洞专项治理、渗透测试、网络安全评估等中的(1.1 安全漏洞专项治理(1.1.1 安全漏洞治理、1.1.3 应急演练)、1.2 渗透测试、1.3 大数据中心网络安全评估)；3 网络安全演习(3.1 安全隐患排查与整改服务、3.3 内部红蓝对抗、3.4 安全预演习、3.5 演习组织、监测与处置)，具体工作范围、内容以投标文件及合同为准。

七、 中国电子技术标准化研究院负责:4 数据安全能力成熟度认证，具体工作范围、内容以投标文件及合同为准。

八、 本项目联合协议合同总额为¥3,390,000 元，联合体各成员按照如下比例分摊（按联合体成员分别列明）：

（1）北京安信天行科技有限公司为☑大型企业□中型企业、□小微企业（包含监

狱企业、残疾人福利性单位）、□其他，合同金额为¥1,600,000元；

（2）奇安信网神信息技术（北京）股份有限公司为☑大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为¥1,590,000元；

（3）中国电子技术标准化研究院为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、☑其他，合同金额为¥200,000元。

九、 以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他投标人另外组成联合体参加同一合同项下的政府采购活动。

十、 其他约定（如有）：无。

本协议自各方盖章后生效，采购合同履行完毕后自动失效。如未中标，本协议自动终止。

联合体牵头人名称：北京安信天行科技有限公司　　盖章：

联合体成员名称：奇安信网神信息技术（北京）股份有限公司　盖章：

联合体成员名称：中国电子技术标准化研究院　盖章：

日期：2024年05月26日

注：

1. 如本项目（包）接受投标人以联合体形式参加采购活动，且投标人以联合体形式参与时，须提供《联合协议》，否则**投标无效**。
2. 联合体各方成员应在本协议上共同盖章，不得分别签署协议书。

附件 4 中标通知书

北京国际贸易有限公司

BEIJING WORLD TRADE CORPORATION

中国北京建国门外大街甲 3 号　邮编：100020

A-3　JIANGUOMEN　WAI　STREET,BEIJING　100020　CHINA

TEL:86-10-85343309

中标通知书

北京安信天行科技有限公司、奇安信网神信息技术（北京）股份有限公司、中国电子技术标准化研究院（联合体）：

在我公司组织的 2024 年大数据安全基础保障项目项目(招标编号：0686-2411BE060719Z)中，经评标委员会评审后，确定贵公司为本项目的中标单位，中标金额为：￥3,390,000.00（人民币叁佰叁拾玖万元整）。

请贵公司在中标通知书发出之日起 30 日内，按照招标文件确定的事项与采购人签订政府采购合同，并在合同签订之日起 2 个工作日内将合同原件扫描件发至招标文件中指定邮箱。

特此通知。

北京国际贸易有限公司

2024 年 5 月 30 日