合同编号：DSJ－2025-031

北京市大数据中心

服务采购合同

合同名称：2025 年大数据安全基础保障

委托人（甲方）：北京市大数据中心

受托人（乙方）：杭州安恒信息技术股份有限公司

受托人（丙方）：国家工业信息安全发展研究中心

受托人（丁方）：中国工业互联网研究院

委托人（甲方）：北京市大数据中心

负责人：张琳

办公地址：北京市通州区留庄路 3 号院 2 号楼

受托人（乙方）：杭州安恒信息技术股份有限公司

法定代表人：张小孟

住所地：浙江省杭州市滨江区西兴街道联慧街 188 号

受托人（丙方）：国家工业信息安全发展研究中心

法定代表人：蒋艳

住所地：北京市石景山区鲁谷路 35 号

受托人（丁方）：中国工业互联网研究院

法定代表人：鲁春丛

住所地：北京市朝阳区酒仙桥北路甲 10 号院 403 号楼

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 2025 年大数据安全基础保障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、丙、丁三方应为甲方提供如下服务：

1、乙方提供驻场服务、网络安全演习保障、漏洞专项治理、渗透测试、网络安全评估等服务。

2、丙方提供等级测评服务。

3、丁方提供密码测评服务。

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、乙、丙、丁三方分别交付本项目服务范围内的相关成果报告。

3、乙、丙、丁三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、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。

4、验收涉及软件测试、安全测试的，应出具具有相应资质的独立第三方提供的软件测试报告、安全测试报告，测试费用由 乙、丙、丁三方各自 承担。

5、合同最终验收合格后，乙、丙、丁三方应向甲方提交如下合同成果：

（1） 乙方服务事项：

1.驻场服务相关文档如下：

《安全监测周报》；

《安全事件应急处置报告》；

2.网络安全演习保障相关文档如下：

《资产风险分析报告》4 份；

《红蓝对抗演练实施方案》1 份；

《红蓝对抗演练总结报告》1 份；

《安全应急演练方案》4 份；

《安全应急演练总结报告》4 份；

《演习期间网络安全监测报告》；

《安全事件应急处置报告》；

《网络安全演习总结报告》4 份；

3.漏洞专项治理、渗透测试、网络安全评估等相关文档如下：

《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；

《漏洞扫描报告》4 份；

《漏洞治理年度报告》1 份；

《渗透测试实施方案》4 份；

《渗透测试报告》4 份；

《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。

（2） 丙方服务事项：《网络安全等级保护测评报告》19 份；

（3） 丁方服务事项：《商用密码应用安全性评估报告》11 份。

第三条 项目小组及人员要求

1、 四方各指派代表作为本项目负责人，项目负责人职责范围包括：负责项目实施对接，统筹项目进度管理，技术决策及节点跟踪，保障项目交付质量 。

甲方项目负责人：

1，于佳（职责：整体进度管理、技术决策），联系方式：010-55529779 。

2，刘仁（职责：乙方服务事项节点跟踪）联系方式：010-55529455 。

3，杨杰（职责：丙、丁方服务事项节点跟踪）联系方式：010-55529776 。

乙方项目负责人：许世明，联系方式：18001128898。

丙方项目负责人：刘志尧，联系方式：18810464810。

丁方项目负责人：闫飞，联系方式：15201300319。

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、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 6335000 元，大写：陆佰叁拾叁万伍仟元整。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。乙、丙、丁三方服务费如下：

乙方服务费金额（大写）叁佰叁拾捌万元整（￥3380000 元）；

丙方服务费金额（大写）壹佰玖拾柒万伍仟元整（￥1975000 元）；

丁方服务费金额（大写）玖拾捌万元整（￥980000 元）。

2、甲方将按以下方式向乙、丙、丁三方支付服务费：分期支付（两次）：

第 1 次付款：本合同签署后，甲方自收到乙、丙、丁三方提供的符合甲方要求的发票之日起 10 个工作日内，向乙、丙、丁三方共支付服务费（大写）叁佰陆拾壹万伍仟玖佰元整（￥3615900 元），其中：

向乙方支付服务费金额（大写）壹佰玖拾伍万贰仟柒佰元整（￥1952700 元）；

向丙方支付服务费金额（大写）壹佰壹拾万捌仟捌佰元整（￥1108800 元）；

向丁方支付服务费金额（大写）伍拾伍万肆仟肆佰元整（￥554400 元）。

第 2 次付款：乙、丙、丁三方提供本合同项下的全部服务并经甲方最终验收合格后，甲方自收到乙、丙、丁三方提供的符合甲方要求的发票且财政资金到达甲方零余额账户并可实际使用之日起 10 个工作日内，甲方向乙、丙、丁三方共支付服务费（大写）贰佰柒拾壹万玖仟壹佰元整（￥2719100 元），其中：

向乙方支付服务费金额（大写）壹佰肆拾贰万柒仟叁佰元整（￥1427300 元）；

向丙方支付服务费金额（大写）捌拾陆万陆仟贰佰元整（￥866200 元）；

向丁方支付服务费金额（大写）肆拾贰万伍仟陆佰元整（￥425600 元）。

3、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、丙、丁三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、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第三方。

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、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 5 %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。

10、乙、丙、丁三方应在实施阶段，接受甲方聘请第三方监理单位的管理。

11、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。

12、乙、丙、丁三方应当依照《北京市数字经济促进条例》第四十三条规定，依法依约移交软件源代码、数据和相关控制措施，保证项目质量并履行不少于两年保修期义务，不得擅自留存、使用、泄露或者向他人提供公共数据。

13、乙、丙、丁三方服务人员接受甲方意识形态安全的统一管理。乙、丙、丁三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、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第三方。

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 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、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、丙、丁三方同意按照人民币 15 万元赔偿甲方的损失。

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、商业秘密等合法权益。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。

2、 乙、丙、丁三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、丙、丁三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、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、丁三方提供的服务经二次验收仍未通过甲方验收或乙、丙、丁三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、丙、丁三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、丙、丁三方返工等原因造成乙、丙、丁三方提供服务迟延，应承担迟延履行的违约责任。

4、 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。

5、 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。

6、 甲方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，四方应友好协商解决，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、 本项目的招标文件、答疑文件、投标文件及相关承诺、协议、本合同附件等均为本合同不可分割之一部分，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	联合协议

4、 本合同一式 玖 份，甲方执 叁 份，乙、丙、丁三方执 贰 份，具有同等法律效力。

（以下无正文）

甲方（盖章）：北京市大数据中心

签署人：

签订日期：2025.7.16

乙方（盖章）：杭州安恒信息技术股份有限公司

签署人：

签订日期：2025.7.16

开户行：杭州银行股份有限公司科技支行

开户名称：杭州安恒信息技术股份有限公司

账号：77818100000385

丙方（盖章）：国家工业信息安全发展研究中心

签署人：

签订日期：2025.7.16

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

账号：110954406910555

丁方（盖章）：中国工业互联网研究院

签署人：

签订日期：2025.7.16

开户行：中国建设银行北京望京支行

开户名称：中国工业互联网研究院

账号：11050160360000001026

附件 1

工作方案

一，项目目标

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：

（1）驻场服务。对中心系统进行实时安全监测、安全事件应急响应，通过7*24 的服务模式，确保中心能够及时发现网络安全异常行为和安全事件。

（2）网络安全演习保障。包括攻击面收缩服务、内部红蓝对抗、安全应急演练、演习期间分析研判、演习期间应急处置、演习总结与整改。

（3）漏洞专项治理、渗透测试、网络安全评估等。包括安全漏洞专项治理（安全技术检查、安全漏洞治理）、渗透测试（制定渗透测试方案、渗透测试实施、渗透测试整改结果检查）、大数据中心网络安全评估（制定安全评估方案、现场安全评估实施、安全评估总结和整改）。

（4）等级测评。根据等保 2.0 相关要求，完成北京市大数据中心的 19 个三级系统等级测评工作。测评将从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理、其他安全要求指标等方面开展测评，在相应的安全加固基础上确保安全等级测评通过，确保系统安全运行。

（5）密码测评。根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等相关标准及规定要求，完成北京市大数据中心的 11 个三级系统商用密码应用安全性评估工作。密码应用安全性评估将从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置等方面开展测评，在相应的安全加固基础上确保安全测评通过，确保系统安全运行。

二，服务内容

（一）驻场服务（中心系统安全监测、安全应急响应 7*24 驻场服务）

由乙方杭州安恒信息技术股份有限公司负责。

（1）驻场人员需对中心信息系统进行 7*24 小时实时监测和应急，保障业务系统的连续性。对监测过程中发现的安全事件及时上报并进行深层技术分析，评估事件影响范围，制定应急策略，对安全事件进行应急处置，协助中心对安全事件进行溯源，提出解决方案，给出修复意见，总结经验改进。

（2）服务商需提供不少于 4 名的驻场人员，包括 1 名组长、3 名组员，4 人倒班。

工作成果：每周提交《安全监测周报》，提供《安全事件应急处置报告》。

（二）网络安全演习保障

由乙方杭州安恒信息技术股份有限公司负责。

1、攻击面收缩服务

（1）服务商需对中心互联网资产进行全面清查，与各系统业务方充分沟通，梳理所有可能的攻击面，明确潜在风险区域。资产暴露面数据内容包括但不限于：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/ GITLAB、微博/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。

（2）服务商需对中心政务外网资产进行全面清查，梳理所有可能的攻击面，明确潜在风险区域。资产暴露面数据内容包括但不限于：资产开放的端口信息、协议信息、敏感数据、资产漏洞等。

（3）暴露面工作梳理完成后，对采集的数据进行风险分析，深入研讨资产暴露在互联网中的风险，结合业务需求与各系统业务方共同制定应对策略。

（4）服务商需提供资产暴露面检测工具，工具的部署不能对现有网络系统造成影响。

（5）结合中心工作安排，每年开展 4 次攻击面收缩服务，形成相应的报告。

工作成果：提供《资产风险分析报告》4 份。

2、内部红蓝对抗

（1）服务商需组织开展内部红蓝对抗演习工作，分析并梳理中心业务系统安全现状，如漏洞情况、防护措施等，编制红蓝对抗计划与方案。提供 1 支攻击队，攻击队人员不少于 3 人，且所提供的攻击队人员需具备攻防演练项目经验。防守队由中心技术人员组成，进行攻击防守。同时服务商需提供 1 名安全技术专家，对演练整体风险进行管控，对演练过程中可能产生的问题进行分析，并对攻防成果进行研判。整体演练模拟真实攻击方式，对中心目标系统开展为期 5 天的攻击演练，检验中心网络安全防护有效性以及监测处置能力。服务期间开展不少于 1 次红蓝对抗演练。

（2）演练过程中服务商需提供攻防演练平台协助开展演练工作，进行演练的统一管理及展示。平台需能够支持 SAAS 化和本地化部署，能够展示攻击方团队和防守团队双方数据；可查看系统受攻击次数和应急响应次数，并能查看防御详情，同时平台能够导出攻击方团队和防守团队的成果报告统计数据，便于总结分析。大屏展示支持 2D、3D 切换，展示攻防对抗统计数据、实时流量监测数据、演练倒计时、参演人数、隐患类型占比、团队排名、攻击流量线、攻击成功数等信息。

工作成果：提供《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、安全应急演练

（1）服务商需与各系统业务方进行沟通，充分了解业务需求和安全关注点，制定针对性的演练方案，编制应急演练计划与流程，同时组建现场技术支持队伍，为演练提供技术层面的支持与协助。

（2） 服务商需在服务期内每年开展网络安全应急演练，网络安全事件场景包括但不限于网页被篡改、系统中病毒、数据库误操作、数据泄漏等。通过开展应急演练，检验评估中心当前网络安全事件应急预案流程、机制的可操作性、实用性。网络安全应急演练开展内容包括演练前期准备、实施、总结各阶段相关工作。

应急演练前期准备：结合中心需求，梳理常见网络安全突发事件场景并设计编制相应场景的演练方案、脚本，明确演练目标、范围、计划以及人员安排。组织中心相关部门人员进行演练前的动员及培训，确保参演人员掌握演练规则、应急流程以及应急知识。同时，服务商准备好演练所需硬件设备、软件工具、模拟数据等资源，搭建演练环境，每次演练支撑人员不少于 3 人，保障演练的顺利开展。

应急演练实施：基于预设的网络安全事件场景演练方案和脚本，服务商在安全可控的条件下模拟事件发生、进行演练解说。中心相关部门人员按照应急流程进行快速响应处置。

应急演练总结：演练结束后服务商根据演练实施情况编制演练总结报告，评估本次演练组织实施的效果情况，包括响应速度、处置能力、问题及不足之处等。针对相关问题，提出合理、有效的改进提升建议，协助中心完善优化现有应急预案。

（3）服务期内开展应急演练不少于 4 次，服务期内覆盖中心所有系统。

工作成果：提供《安全应急演练方案》4 份、《安全应急演练总结报告》4 份。

4、演习期间分析研判

（1）服务商在演习期间应派遣至少 3 名服务人员进行每日值守保证，对中心业务系统安全告警信息进行分析和挖掘，对各类告警数据进行深层次分析，挖掘隐患、判断隐患威胁的严重程度，并对分析结果归类整理。具体的值守时间参考国家攻防演练时间要求。

（2）服务商需在演练前对中心现有安全防护措施进行调研，针对中心不足的防护措施在演习期间提供对应的设备或平台，补齐中心防护的不足。演习期间至少提供 1 套安全态势感知系统、1 套攻击预警平台，对中心流量数据和日志数据进行采集分析，通过态势感知系统和攻击预警平台协助中心对演练期间的攻击行为进行监测和分析。平台或系统能够支撑云环境部署，实现对云环境流量的采集。

（3）安全态势感知系统能够对多维度的信息和多源数据进行整合、关联、

智能分析和预测，基于攻击意图、攻击策略、攻击方法、攻击次数、攻击时间、处置状态等影响因子构建资产评级模型，在大量资产中识别失陷资产；通过对网络数据包、文件元数据、终端日志、威胁情报、漏洞知识库等进行智能分析，洞悉攻击的人员、目标、时间、地点和手段，发现高级潜伏威胁；可以实现 AI 智能研判安全威胁并自动给出研判结果，并进行攻击报文辅助解读；可与防火墙、EDR 等防护系统进行联动，实现快速自动阻断。

（4）攻击预警平台能够有效发现暴力破解攻击、拒绝服务攻击、扫描行为攻击等异常流量的检测；能够对 web 攻击、文件攻击、邮件威胁等进行实时的攻击预警；可与防火墙、EDR、WAF 等防护产品进行联动，实现各种控制行为的阻断防护。

工作成果：提供《演习期间网络安全监测报告》。

5、演习期间应急处置

服务商需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。

工作成果：提供《安全事件应急处置报告》。

6、演习总结与整改

（1）演习期间服务商需完成每日防守工作总结，分析发现的安全问题、处置方案、下发的策略，提出改进建议，每日汇报工作。

（2）演习完成后服务商应对整体的演习保障工作进行总结复盘，分析演习保障中存在的问题、不足，提供安全防护增强建议。

工作成果：提供《网络安全演习总结报告》4 份。

（三）漏洞专项治理、渗透测试、网络安全评估等

由乙方杭州安恒信息技术股份有限公司负责。

1、安全漏洞专项治理

1.1、安全技术检查

按照网络安全、数据安全检查要求，开展中心业务系统的安全技术自查，做好技术支持，将检查中出现的问题进行整改，提供工作建议。

（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

（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。

工作成果：提供《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。

1.2、安全漏洞治理

通过主动漏洞扫描服务，及时发现安全隐患，并提出整改意见和建议，督促整改。

（1）服务商需派遣服务人员使用专业检测工具对中心指定的信息系统进行全面扫描与分析，检测工具的检测规则库及知识库应涵盖 CVE、CNCVE、CNVD、CNNVD 等标准。通过工具扫描发现信息系统安全隐患、数据库、中间件等存在的漏洞，分析漏洞和配置缺失等。

工具自动化扫描完成后，人工验证所发现的系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题，并评估漏洞风险程度。此外，针对漏洞扫描中出现的问题，提供针对性的安全修复建议，协助进行解决，并进行修复后再次复测工作。

（2）服务商需提供漏洞扫描工具，工具具备 VPN 代理扫描，可在工具界面添加代理网络配置，实现公有云、隔离网络等特殊网络环境下的漏洞扫描；同时根据系统给出的漏洞参数、HTTP 请求/响应数据，快速验证，一键验证漏洞。

（3）服务商需提供资产管理系统，系统能够对接第三方漏洞扫描设备的扫描结果，通过将扫描结果进行导入系统，实现对资产的漏洞管理，通过系统的工

单管理功能，对资产漏洞修复流程进行监测，实现漏洞的闭环管理。

（4）服务期内开展漏洞扫描不少于4次，每次覆盖所有指定系统。

工作成果：提供《漏洞扫描报告》4份、《漏洞治理年度报告》1份。

2、渗透测试

（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，服务期内覆盖中心所有系统。

（2）制定渗透测试方案：服务商需与各业务系统责任部门进行沟通收集系统软件架构、开发语言、可用性要求、相关服务器、网络拓扑、设备部署情况等基本资料，确定测试目标与范围。制定渗透策略，考虑多种渗透路径与场景，对方案进行审核与完善，确保方案具有可行性与有效性，为后续渗透测试提供准确指导。

（3）渗透测试实施：服务商测试人员需根据测试目标与系统业务方充分沟通确认，明确渗透测试的实施时间、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。

（4）通过中心授权后，服务商渗透测试工程师以模拟黑客攻击的方法对目标授权系统进行非破坏性攻击测试。测试内容包括但不限于：信息收集类、配置管理类（HTTP方法测试、信息泄露等）、认证类（用户枚举、密码猜解、密码重置测试等）、会话类（cookie测试、会话固定测试等）、授权类（URL越权、路径遍历、业务逻辑、文件下载测试等）、数据验证类（SQL注入、跨站脚本、代码注入、URL跳转、文件上传测试、参数被篡改等）、API接口类（未验证身份、参数未加密或可篡改等）、系统应用漏洞以及服务商认为需要的其他测试内容。

（5）测试整改结果检查：测试完成后，服务商渗透测试工程师需整理测试过程及测试结果，编制对应系统的渗透测试报告，针对所发现的问题提出相应的安全改进建议，以指导、监督应用系统开发商、运维服务商进行整改并及时复测。

工作成果：提供《渗透测试实施方案》4份、《渗透测试报告》4份，包含每个系统的测试内容。

3、大数据中心网络安全评估

（1）制定安全评估方案：服务商需对中心所有平台和系统及其相关数据、人员、制度等进行调研，收集并整理相关文档，为评估提供基础资料。选择适合的评估方法，制定评估方案。

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。

（2）安全评估实施：服务商需依据《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）等标准开展安全评估工作，在现场安全评估实施中，深入分析收集的资料确定评估重点，实地查看物理安全措施、网络架构等，严格审查安全策略文件及执行情况，结合多方面结果评估风险。评估内容包括但不限于中心安全管理制度落实情况、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。

（3）安全评估总结和整改：服务商完成安全评估工作后，全面总结与整改。对评估过程及结果进行深入整合，明确安全隐患与风险点，分析潜在影响并分类梳理。结合现场勘查、技术检测和安全策略审查等多方面信息，为整改提供准确依据。在整改阶段，制定详细整改建议，指导整改过程，确保各项措施有效落实。

（4）服务商需提供数据安全风险评估工具，通过工具和人工的方式，对指定核心信息系统进行数据安全风险评估，识别和评估中心在数据处理和存储中所面临的潜在风险，确定安全时间的可能性和损失，完成对数据资产的综合风险评估，提出合理化风险处置建议。评估工具需具备数据质量评估能力，具备对结构化数据类型任务进行相关配置，包括：数据源、抽样策略、执行逻辑、打标方式。同时具备数据库风险检测能力，至少包括数据库漏洞检查、配置项检查、弱口令检查等手段实现安全评估。

工作成果：提供《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

（四）等级测评

由丙方国家工业信息安全发展研究中心负责。

根据等级保护 2.0 标准的要求，测评内容包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理、云计算安全扩展要求等。完成北京市大数据中心的 19 个三级系统等级测评工作。测评完成后，提供整改建议书，配合进行整改实施。

测评方需从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等 10 个安全层面开展测评工作；

(1)安全物理环境测评需通过访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况；

(2)安全通信网络测评需通过核查和验证测试的方式验证通信网络安全性，主要验证对象为广域网、城域网和局域网等；涉及的安全控制点包括网络架构、通信传输和可信验证；

(3)安全区域边界测评需通过核查和验证测试的方式验证网络区域边界的安全性，主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证等；

(4)安全计算环境测评需通过核查和验证测试的方式验证计算环境安全性，主要对象为边界内部的所有对象。包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的控制点包括身份鉴别、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、数据备份恢复、剩余信息保护、个人信息保护等；

(5)安全管理中心测评需通过核查和验证测试的方式验证安全管理中心的安全性，主要对象为集中管控平台、集中运维平台、日志审计系统等。涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控等；

(6)安全管理制度测评需通过访谈和检查的方式测评信息系统的安全管理制

度建立情况。主要涉及对象为：信息安全管理体系、日常安全管理制度、重要操作规程及相关执行记录等；

(7)安全管理机构测评需通过访谈和检查的方式测评信息系统的安全管理机构建立情况。主要涉及对象为：安全管理机构设立文档、信息安全小组名单、岗位说明书等文档及执行记录；

(8)安全管理人员测评需通过访谈和检查的方式测评信息系统的人员安全管理方面情况。主要涉及对象为：人事管理制度、外部人员访问要求等安全管理制度及执行记录；

(9)系统建设管理测评需通过访谈和检查的方式测评信息系统的系统建设管理方面情况。主要涉及对象为：系统建设过程中涉及的相关文档，如：系统定级报告、安全设计方案、测试验收报告等文档及软件开发、工程实施等方面的安全管理制度及执行记录；

(10)系统运维管理测评需通过访谈和检查的方式测评信息系统的系统运维管理方面情况。主要涉及对象为：系统运维过程中涉及的安全管理制度及执行记录；

工作成果：提供符合公安及相关主管部门要求的19个被测系统的《网络安全等级保护测评报告》。

（五）密码测评

由丁方中国工业互联网研究院负责。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等相关标准及规定要求，完成北京市大数据中心的11个三级系统商用密码应用安全性评估工作。密码应用安全性评估将从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置等方面开展测评，在相应的安全加固基础上确保安全测评通过，确保系统安全运行。

(1)物理和环境安全测评。主要包括身份鉴别、电子门禁记录数据存储完整性、视频监控记录数据存储完整性等方面。

(2)设备和计算安全测评。主要包括身份鉴别、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方面

(3)网络和通信安全测评。主要包括身份鉴别、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、安全接入认证等方面。

(4)应用和数据安全测评。主要包括身份鉴别、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、不可否认性等方面。

(5)管理制度测评。主要包括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方面。

(6)人员管理测评。主要包括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方面。

(7)建设运行测评。主要包括制定密码应用方案、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方面。

(8)应急处置测评。主要包括应急策略、事件处置、向有关主管部门上报处置情况等方面。

工作成果：提供符合相关主管部门要求的 11 个被测系统的《商用密码应用安全性评估报告》。

三，培训要求

本项目中开展安全培训工作，应对相关人员开展必要的安全培训，相关要求如下：

1.培训范围：中心指定人员。

2.培训目的：提升中心相关技术人员网络安全技术能力。

3.培训内容：

(1)提供 2 个 CISP 的培训认证。

(2)不少于 1 次的安全技术培训，如安全测试、攻防技术等内容，具体内容

根据中心需求制定。

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.培训开展的方法

乙方应根据甲方的上述要求及投标人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甲方，征求意见，以确保培训工作的顺利进行，达到预期的目的。

附件 2

项目主要人员名单

姓名	性别	年龄	学历	职称	职务	项目角色	承担工作
许世明	男	36	本科	/	项目负责人	项目负责人授权经办人（乙方）	负责项目进度，商务流程。
刘志尧	男	32	硕士	工程师	项目负责人	项目负责人授权经办人（丙方）	
闫飞	男	29	本科	工程师	项目负责人	项目负责人授权经办人（丁方）	
苏启波	男	44	本科	高级	项目经理	项目经理（乙方）	负责项目总体设计、组织管理和协调，把控项目全局，具备相关证书和项目经验。
甘雁南	男	35	本科	高级	高级安全工程师	安全服务实施负责人（乙方）	负责安全服务项目管理，具备丰富经验和相关证书。
于盟	男	41	硕士研究生	正高级工程师	检查评估所副所长	测评人员（等保测评实施负责人）（丙方）	负责网络安全等级保护测评，具备相应高级证书和职称。
张晓菲	男	35	硕士研究生	高级工程师	中级工程师	测评人员（等保测评工程师）（丙方）	
查奇文	男	39	博士研究生	高级工程师	副所长	测评人员（密评测评实施负责人）（丁方）	负责网络安全商用密码应用安全性评估，具备

唐明环	女	37	硕士研究生	高级工程师	工程师	测评人员（密评测评工程师）（丁方）	相应高级证书和职称。
梅志钦	男	22	本科	/	安全工程师	驻场组长（乙方）	负责中心系统实时监测和应急响应，服从采购人安排。
王帅	男	26	本科	/	安全工程师	驻场人员（乙方）	
林任伟	男	26	本科	/	安全工程师	驻场人员（乙方）	
成茜	女	26	本科	/	安全工程师	驻场人员（乙方）	
李新	女	28	本科	/	数据安全专家	核心团队人员（乙方）	负责项目实施，根据项目进展调整人员力量。
石岩	男	30	本科	/	高级安全工程师	核心团队人员（乙方）	
郭婷婷	女	30	本科	高级	高级安全工程师	核心团队人员（乙方）	
高凡	男	36	本科	高级	安全运营专家	核心团队人员（乙方）	
郑宇	男	27	本科	中级	安全攻防专家	核心团队人员（乙方）	
杨建设	男	27	本科	中级	高级安全服务工程师	实施支撑人员（乙方）	
黄澄	女	31	本科	中级	高级安全服务工程师	实施支撑人员（乙方）	
王志红	女	28	本科	/	安全服务	实施支撑人员（乙方）	

					工程师		
张海成	男	28	本科	高级	项目经理	实施支撑人员（乙方）	
张余师	男	31	本科	/	高级攻防研究员	实施支撑人员（乙方）	
邵宛岩	男	34	本科	/	高级攻防研究员	实施支撑人员（乙方）	
吴晨	男	32	本科	高级	高级安全工程师	实施支撑人员（乙方）	
李雅苹	女	32	本科	高级	高级安全工程师	实施支撑人员（乙方）	
张旗	男	29	本科	中级	安全服务工程师	实施支撑人员（乙方）	
李肇	男	26	本科	中级	安全服务工程师	实施支撑人员（乙方）	
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）（丙方）	
周嵩琛	男	27	本科	/	等级保护测评师	测评人员(等保测评工程师）（丙方）	
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）（丙方）	
李力峰	男	33	本科	/	渗透测试人员	测评人员(渗透测试工程师）（丙方）	
闵浩亮	男	29	本科	/	渗透	测评人员(渗	

					测试人员	透测试工程师）（丙方）	
唐毅	男	27	本科	/	渗透测试人员	测评人员（等保测评工程师）（丙方）	
王伟忠	男	40	博士	高级工程师	密评测评工程师	测评人员（密评测评实施人员）（丁方）	
彭浩楠	男	31	博士	高级工程师	密评测评工程师	测评人员（密评测评实施人员）（丁方）	
封琳业	男	29	学士	/	密评测评工程师	测评人员（密评测评实施人员）（丁方）	
孟成瑞	男	30	硕士	工程师	密评测评工程师	测评人员（密评测评实施人员）（丁方）	
陈建	男	27	学士	/	密评测评工程师	测评人员（密评测评实施人员）（丁方）	
张永镇	男	25	本科	/	密评测评工程师	测评人员（密评测评实施人员）（丁方）	
闫瑞泽	男	29	硕士	工程师	/	密评管理人员（丁方）	
纪婷钰	女	34	硕士	工程师	/	密评管理人员（丁方）	

附件 3

联合协议

杭州安恒信息技术股份有限公司 、国家工业信息安全发展研究中心 及中国工业互联网研究院就"（2025 年大数据安全基础保障）" / 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、 由杭州安恒信息技术股份有限公司牵头，国家工业信息安全发展研究中心、中国工业互联网研究院参加，组成联合体共同进行招标项目的投标工作。

二、 联合体中标后，联合体各方共同与采购人签订合同，就采购合同约定的事项对采购人承担连带责任。

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、 杭州安恒信息技术股份有限公司负责大数据安全基础保障，包括驻场服务、网络安全演习保障、漏洞专项治理、渗透测试、网络安全评估等，具体工作范围、内容以投标文件及合同为准。

六、 国家工业信息安全发展研究中心负责等级测评，具体工作范围、内容以投标文件及合同为准。

七、 中国工业互联网研究院负责 密码测评 ，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 6335000 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）杭州安恒信息技术股份有限公司为☑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 3380000 元；

（2）国家工业信息安全发展研究中心为☐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 1975000

元；

（3）中国工业互联网研究院为□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980000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供应商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：杭州安恒信息技术股份有限公司

盖 章：

联合体成员名称：国家工业信息安全发展研究中心

盖 章：

联合体成员名称：中国工业互联网研究院

盖 章：

日期：2025年6月24日