TAIJI 太极

创新融合 让我们的世界更智慧

北京市市级政务云服务协议

项目名称：政务云租用

甲　　方：北京市规划和自然资源委员会

乙　　方：太极计算机股份有限公司

合同签订时间：2025年12月26日

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，在《北京市市级政务云管理办法》的基础上，经过友好协商，就乙方为甲方提供北京市政务云服务（下称“服务”）事宜订立以下协议，以资共同遵守。

第一条 项目角色定义

1、云服务商：协议乙方，太极计算机股份有限公司。

2、使用单位：协议甲方，北京市规划和自然资源委员会。

3、政务云管理单位：北京市政务服务和数据管理局。

4、云综合监管服务商：经政务云管理单位授权，开展政务云安全、技术监督管理和服务评价的单位。

5、信息系统服务商：为甲方提供信息系统等建设或维护服务的服务商。

第二条 服务内容

1、 甲方应按照《北京市市级政务云管理办法》的有关规定，将如下信息系统部署或迁移至乙方云平台，同时对信息系统开展运维工作。

1	北京市规划和自然资源委员会规划编制与实施监督平台
2	北京市规划和自然资源委员会批后监管与全过程监督平台
3	北京市规划和自然资源委员会自然资源监测管理平台
4	北京市不动产登记信息管理基础平台
5	北京市规划和自然资源委员会综合执法与专项治理平台
6	北京市规划和自然资源委员会多规合一协同信息平台
7	北京市规划和自然资源委员会国土空间基础信息平台
8	北京市规划和自然资源委员会项目审批办事服务平台
9	北京市规划和自然资源委员会领导决策指挥平台
10	北京市规划和自然资源委员会行政办公平台
11	北京市规划和自然资源委员会门户

2、本协议期限内，乙方向甲方上面11个平台系统，提供如下扩展云服务或云资源租用服务。甲方根据业务需要，与乙方协商选择云服务项目，如下：

（1）政务云租用服务（详见附件1 分项明细及报价表）

（2）基础安全保障服务

基础安全保障服务是云服务商应具备的云平台层安全保障能力，使用单位无需购买即可

享受服务，具体服务内容如下表：

服务类别	服务目录	项目
安全管理服务	运维人员管理	7x24 小时运维人员管理、安全登记
	机房运维管理	机房设备管理、安全控制
	应急演练	协助云使用单位进行安全应急演练
安全技术服务	物理访问控制	机房进出控制、监控等
	机房三防服务	机房防火、防盗、防雷电
	设备访问审计	设备访问记录、日志统计、安全事件
	出口流量监测	出口流量控制、检测，并且可观测数据，互联网网络行为审计
	本地抗 DDoS 防护	云平台整体提供总带宽为 10Gb 的抗 DDoS 防护
	防火墙安全防护	出口安全
	防入侵监测 IPS	防入侵监测
	远程接入服务	提供 1 个远程登录堡垒机的运维账号
	租户隔离	租户虚拟化层隔离
	租户内部访问控制	租户内部访问权限控制，用户可以自由分配
	云主机监控	提供云上资源的基本监控，CPU、内存使用率等
	角色权限管理	提供通过代入角色实现获取操作权限

第三条 服务水平

1、乙方应为甲方提供本协议约定的全部服务，协助甲方开展信息系统部署迁移工作，做好云主机等云资源或云服务的运维工作。

2、乙方应配合甲方搭建信息系统上云的测试环境，测试期由甲乙双方协商确定。

3、乙方为甲方提供的服务质量应符合国家有关质量法规、质量标准的规定及相关行业的标准。

4、乙方提供的云平台整体可用性应不低于 99.99%，数据可靠性应不低于 99.9999%，云平台应按照等保三级标准建设并通过测评，云平台可按需 7 个自然日快速扩容。

5、乙方提供的云平台应具备资源动态调整机制，根据甲方信息系统运行情况进行资源的动态调整，如遇信息系统使用高峰期，经双方协商可短期内提供的云资源扩容服务，如需要长期使用扩容服务，以北京市级政务云基础服务目录价格为准双方协商费用，并签订补充协议。

6、乙方应提供技术服务热线(7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法，方式应包括邮件、电话、即时通讯工具等。邮件：zhengwuyun@mail.taiji.com.cn，电话：010-57702888/江河 13683636708。

7、在服务期内，提供 7*24 小时的现场和技术支持服务，对故障 10 分钟内响应。

8、乙方须具备故障快速定位和恢复能力，故障定位排除时限不超过 60 分钟。

第四条 项目小组及人员要求

甲乙双方应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：

1、制定项目计划：牵头制定项目计划。

2、跟踪项目执行：迁移方案设计，云服务使用培训，云服务各阶段验收，服务成果确认等管理工作。

3、项目检查和控制：检查云服务使用过程中各阶段工作质量和进度。协调各种资源，确保项目按计划进度实施。

4、项目沟通协调：负责协调解决组织接口及技术接口问题，沟通项目售前、售后情况，解决云服务使用过程中出现的相关问题。

5、甲方项目负责人及联系方式：贺宁 13691219980。

6、乙方项目负责人及联系方式：于洋 15101029530。

第五条 服务期限

1、乙方应自协议签署之日起，在甲方提交《北京市市级政务云服务统一工单》后 10 个工作日内，完成云资源分配、新用户创建，并交付使用。

2、乙方为甲方提供为期12个月的政务云资源租用服务，自2026年1月1日起，至2026年12月31日止。

3、合同履行期限：2026年1月1日起至2027年3月31日止。

4、本协议期满，乙方应协助甲方完成系统及数据的迁移，以免丢失重要信息。

第六条 服务验收

1、项目验收分为项目中期检查和项目终验：

（1）项目中期检查验收：乙方应于2026年 7 月 15 日前，向甲方提交运维工作中期总结报告和相关材料，得到甲方认可后，由甲方组织开展项目中期检查。检查标准以本合同附件以及相关说明文档为标准，具体时间和地点由甲乙双方商议安排，检查结果出具书面意见。

（2）项目终验：乙方应于2027年1月 15 日前向甲方提交运维工作全年总结报告和相关材料，得到甲方认可后，由甲乙双方组织对项目进行验收，验收标准以本合同附件以及相关说明文档为标准，具体时间和地点由甲乙双方商议安排，验收结果出具书面意见。

（3）验收结果分为通过与不通过。对于未通过的情况，由乙方按照甲方的意见采取补救措施后再次进行项目验收。如两次验收不通过，甲方有权单方解除本合同，并有权要求乙方退还甲方已支付的全部费用，赔偿给甲方造成的全部损失。

2、验收材料清单如下：

阶段	**输出成果**	**成果形式**
云服务商选择阶段	《服务协议》	纸质/电子
系统入云阶段	政务云服务需求调研表，附：系统现状拓扑图、信息系统资产清单	纸质/电子
系统运行阶段	政务云运维服务方案	纸质/电子
	日常运维、巡检工作记录、事件处理报告	纸质/电子
	服务维护操作流程、工作手册	纸质/电子
	服务周报、月报（含云资源清单、云效率、云主机备份、数据库运行、数据备份、安全设备监控分析及安全防护情况，重要核心系统运行情况等）	纸质/电子
	漏洞扫描报告/月	纸质/电子
	应急预案，应急演练方案、报告	纸质/电子
	政务云服务总结报告（年报）	纸质/电子

	其他（云平台重大事件通知、重保期间值守记录、服务满意度调查表等）	纸质/电子

第七条 服务费用及支付方式

本协议总金额共计人民币小写：¥19,998,420.00元，大写：人民币壹仟玖佰玖拾玖万捌仟肆佰贰拾元整。上述合同价款已包含乙方为完成合同约定全部工作和义务所需的一切费用，包括增值税在内的全部税金；除此之外，甲方无需再向乙方支付任何费用。支付方式以电汇或银行转账方式支付。

1、合同生效后【15】个工作日内，乙方向甲方提供合同价款的10%作为履约保函，即人民币小写：¥1,999,842.00元，大写：壹佰玖拾玖万玖仟捌佰肆拾贰元整，用以保证乙方全面地履行本合同项下的各种义务。

2、第一笔款：在甲方收到乙方提供的履约保函后15个工作日内，甲方向乙方支付合同款的55%，即人民币小写：¥11,000,000.00元，大写：壹仟壹佰万元整；

3、第二笔款：乙方完成6个月的租期服务工作，提交中期运维服务报告及相关材料，并通过中期验收后15个工作日内，甲方向乙方支付合同款的35%，即人民币小写：¥7,000,000.00元，大写：柒佰万元整；

4、第三笔款：乙方按照合同要求完成12个月租期服务工作，提交政务云服务工作全年总结报告及相关材料，并通过终期验收后15个工作日内，甲方向乙方支付合同款的10%，即人民币小写：¥1,998,420.00元，大写：壹佰玖拾玖万捌仟肆佰贰拾元整。

5、乙方收取相应款项前，应向甲方提供正式等额发票，因乙方未提供发票造成付款延迟，甲方不承担违约责任。

6、以上具体支付进度和比例以财政拨款到位情况为准。乙方不得因此向甲方提出索赔或主张权利。

第八条 甲方权利义务

1、甲方有权对乙方提供的各项服务进行监督、检查和评价。

2、甲方应提出有关管理、技术需求和要求，协调乙方与信息系统服务商的关系，协调信息系统服务商配合调研、迁移、运维、安全和应急演练等过程的工作。

3、甲方需按照《北京市市级政务云管理办法》的要求申请、变更、退出云服务；在系统入云、上线、服务变更、退出等关键节点，甲方应提前提交《北京市市级政务云服务统一工单》相应部分内容至政务云管理单位进行备案作为工作依据。甲方应按本协议约定使用乙

方提供的云资源，做到资源专用，协议未约定或未提交《北京市市级政务云服务统一工单》至政务云管理单位备案的信息系统不得部署入云。

4、甲方的信息系统在迁移、部署到乙方云平台之前，应开展必要的系统入云安全测试。

5、甲方负责本单位信息系统和相关基础软件的日常维护、管理、安全和应急保障。

6、甲方应确保部署在政务云平台的软件具有合法授权，不得擅自安装、使用非法软件。

7、甲方如需对已上线信息系统进行维护升级、渗透测试、安全加固等操作， 应提前告知乙方。

8、甲方有权要求乙方现场技术指导、处理故障及其他服务。

9 、甲方其他的权利义务：无。

第九条 乙方权利义务

1、乙方须按照协议所约定的服务内容标准向甲方提供相关资源和服务。

2、乙方应针对甲方建立健全信息系统管理配套制度，包括：运维制度、应急预案、安全保障制度、运行监管办法等。

3、乙方负责云平台基础安全保障和运维工作。

4、乙方应负责本单位人员的安全培训、技术培训，确保工作人员符合岗位要求。

5、乙方需按照有关规定进行操作，确保各系统不被人为损坏。

6、乙方负责提供资源调度管理和维护，提供云主机状态监控，对甲方所购买使用的资源提供运维服务，未经授权不得擅自修改信息系统数据或发布信息等。

7、乙方负责管理甲方申请的 IP 地址，为甲方提供 IP 地址分配和管理服务 。

8、信息系统正式上线后，乙方需定期向甲方提供政务云服务报告，以便甲方及时获取政务云资源或服务的使用情况。

9、甲方如需乙方提供重启服务器操作时，乙方有权要求甲方提供书面申请。除本款约定外，乙方原则上不接受甲方提出的其他可能对甲方服务器造成损坏的任何操作要求。

10、乙方应提供技术支持服务，以维护甲方系统的正常运行。

11、重大活动期间，乙方应配合甲方制定重保方案并提供云平台的现场值守等服务。

12、乙方应配合甲方制定信息系统应急预案，并配合开展信息系统应急演练工作，做好日常应急响应工作。

13、乙方接到甲方故障报告后，应及时做好相关信息的登记工作，并进行故障排查。乙方应定时向甲方反馈检查进度及结果，故障排除后，乙方应将结果及时反馈甲方并做好书面报告和故障记录。

14、由于甲方指定的其他技术服务提供商提供的软件或产品的缺陷，造成的信息系统运行故障、安全漏洞、信息泄露等事故，乙方不承担相应责任，但需要配合甲方进行整改。

15、当甲方入云信息系统出现严重影响政务云平台安全稳定运行的事件时， 乙方有权暂时中断甲方的云服务并通知甲方，事件处理完毕后恢复服务。

16 、乙方其他的权利义务：服务期间乙方应就作业安全制定完整可行的方案，作业人员应严格遵守各项规章制度，乙方工作人员在履行本合同期间自身遭受人身损害、财产损失，或致甲方人身损害、财产损失，其后果均由乙方承担。

第十条 安全责任边界

1、甲方安全责任

（1）甲方承担本单位入云信息系统的基础软件、信息系统、数据等方面的安全责任。

（2）甲方负责组织信息系统的应急演练，如有需要，甲方有权要求乙方配合应急演练。

2、乙方安全责任

（1）乙方承担云平台层面（主要包括物理资源、计算资源、存储资源、网络资源）的安全责任。

（2）乙方在取得甲方许可后，开展云平台应急演练；乙方有义务配合甲方完成信息系统的应急演练。

（3）乙方须按照《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14 号）的要求和有关网络安全标准，落实并通过所建设的云平台的第三方网络安全审查。

第十一条 知识产权归属

1、乙方保证向甲方提供的服务成果是其独立实施完成或取得相应授权，不存在任何侵犯第三方专利权、商标权、著作权等合法权益的情形。如因乙方提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究甲方责任的，乙方应负责解决并赔偿因此给甲方造成的全部损失。

2、双方在对外宣传（如在各自官网、市场营销活动）时，如有涉及对方的内容，应提前通知对方，在取得对方同意后方可发布信息 。

3、在本协议签订前已经存在的或履行过程中产生的其他与本协议无关的成果，包括但不限于设计方案、各种说明书、测试数据资料、计算机软件以及其他技术文档，知识产权归属原权利人所有。

4、本协议执行期间产生的相关电子文档（技术文档等）的知识产权归甲方所有，未经

甲方书面许可，乙方不得对本次项目所形成的资料及文件擅自复制，或向第三方透露、转让、扩散，或用于本合同外的项目。否则，乙方应承担由此引起的法律后果及赔偿甲方的所有损失。

第十二条 违约责任及协议解除

1.乙方违反本合同任意一条均视为违约，乙方须向甲方支付违约金为合同总价款的3‰，计人民币伍万玖仟玖佰玖拾伍元贰角陆分（¥59,995.26元）。

2、在运营期间，如发生附件2 中所列 A 级事件 1 次，甲方有权解除本协议，乙方除应向甲方返还已付款项，还应支付合同金额20%的违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

3、在运营期间，如发生附件2 所列 B 级事件 3 次，甲方有权解除本协议，乙方除应向甲方返还已付款项，还应支付合同金额20%的违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

4、乙方提供服务过程中可能发生的违约行为及相应应承担的违约金详见附件 3、4 规定，违约金优先从尾款中抵扣，超过尾款部分由乙方支付。系同一事件或原因导致的事故，甲方不可就同一事件重复要求乙方承担违约责任，经甲乙双方协商，择其重者确定乙方支付违约金的办法。

5、在运营期间出现下列情况，甲方向乙方提出整改要求和期限，且乙方在规定期限内未能履行甲方正当要求的，甲方有权与乙方解除本合同，已完成成果归甲方所有，乙方除应返还甲方已付款项外，还应支付合同金额的20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任：

（1）多次在云综合监管服务商已发出整改通知后未正确处置，出现问题并造成 B 级及以上事故；

（2）重大活动期间所承诺的骨干人员和管理人员未到场；

（3）连续 2 个月所承诺的运维服务人员人数未达到协议要求。

6、乙方擅自将工程转包、分包给第三方实施的，甲方有权解除合同，已经完成的项目成果归甲方所有，乙方除应向甲方返还已收取的合同款项外，还应向甲方支付本合同金额的20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

7、乙方违反保密义务的，应当赔偿甲方因此遭受的全部损失，并按合同金额的20%向甲方支付违约金。情节严重的，应依法追究相关责任人的法律责任。

8、合同生效后，甲方应按照合同约定支付费用，因甲方原因未能按时支付，甲方需以

欠付金额为基数，按照银行同期贷款市场报价利率标准支付相应违约金。任何一方的违约行为给他方造成其他损失的，均应承担相应的赔偿责任，具体事宜以双方友好协商为准。

第十三条 退出

1、服务期内，如乙方提出退出要求，需在服务期截止前至少 6 个月向甲方提出退出申请，并获得甲方的书面许可后方可退出，对于由此给甲方带来的经济损失，由甲乙双方协商解决。

2、服务期内，如出现政务云管理单位责令乙方退出，相关补偿费用甲乙双方另行协商；在信息系统迁移和交接工作中，乙方应在甲方提出系统迁出需求后 15 天内配合甲方完成信息系统迁移的相关工作，包含梳理迁出系统的云资源、安全策略配置等。确保系统在新环境运行稳定后，关停原服务，并对原有系统数据进行安全擦除。否则乙方除应返还甲方已支付未履行的付款项外，还应支付合同金额的 20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

第十四条 免责条款

1、本协议中不可抗力指地震、台风、火灾、水灾、战争、罢工以及其他双方共同认同的不能预见、不能避免并不能克服的客观情况。

2、由于网络运营商的核心设备故障造成的网络中断、阻塞，从而影响到系统的正常访问或响应速率降低，属于不可控事件和不可抗力，甲方应对此表示认同。

3、由于不可抗力致使协议无法履行的，受不可抗力影响一方应立即将不能履行本协议的事实书面通知对方，并在不可抗力发生之日起 15 天内提供相关政府部门或公证机关出具的证明文件。

4、由于不可抗力致使协议无法履行的，本协议在不可抗力影响范围及其持续期间内将中止履行，本协议执行时间可根据中止的时间相应顺延，双方无须承担违约责任。不可抗力事件消除后，双方应就协议的履行及后续问题进行协商，按照该事件对协议履行的影响程度，决定继续履行协议或终止协议。

第十五条 保密条款

1、乙方因承接本协议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，乙方应按照甲方关于保密工作的相关要求，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协议项下约定项

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 日内将含有保密信息的所有文件或其他资料归还甲方，且不得保留任何复印件及数据备份。

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、乙方需要定期向政务云管理单位和云综合监管服务商提交云平台及入云系统相关信息，内容包括但不限于：云资源租用情况、系统迁移进展、已租用资源的使用绩效情况、安全监控分析、IP 管理、重大活动值守、工作建议等，此时如涉及甲方信息，不属于保密违约。

8、乙方承担上述保密义务的期限为协议有效期间及协议终止后 1 年。

9、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，乙方均应向甲方承担全部责任，乙方应支付合同金额的 20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。情节严重的，甲方将追求乙方的相关工作人员的法律责任。

10、乙方发现涉密的信息及载体可能被泄露或已经被泄露时，应及时穷尽手段采取有效措施防止知悉范围及损失的进一步扩大，并及时向甲方通报相关情况。

第十六条 争议的解决

1、本协议按中华人民共和国相关法律、法规进行解释。

2、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）依法向甲方住所地有管辖权的人民法院起诉。

第十七条 协议内容变更

在本协议履行过程中，甲方提出服务需求变更，应与乙方协商一致并签署补充协议；在

变更达成一致前，双方应继续履行其原约定义务。

第十八条 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。

第十九条 其他

1、本协议自双方法定代表人或其委托代理人签名并加盖本单位合同专用章或单位公章后生效，至双方履行完毕本协议约定的全部义务时终止。

2、未尽事宜，经双方协商一致，签订书面补充协议，补充协议与本协议不一致的，以补充协议为准。

3、本协议一式 陆 份，甲、乙双方各执 叁 份，每份具有同等法律效力。

附件：

（一）本合同的组成文件如下：

1. 在合同实施过程中双方共同签署的补充与修正文件；

2. 本合同正文；

3. 本合同附件：

（1）《分项明细及报价表》

（2）《重大违约行为表》

（3）《严重违约行为表》

（4）《一般违约行为表》

4. 项目实施方案。

（二）上述文件均为本合同的组成部分，并互为补充和解释，与主合同具有同等法律效力。甲、乙双方同意在出现合同理解上的不明确或不一致时，以所列顺序在前的为准执行，如果同一顺序的文件中的约定之间产生歧义或不一致，则以签署时间在后的为准。

（以下无正文）

委托人（甲方）	名称（或姓名）	**北京市规划和自然资源委员会**			合同专用章或单位公章
	联系人（承办人）	贺[illegible]		（签章）	
	住所（通讯地址）	北京市通州区承安路1号	邮政编码	101160	
	电话	010-55594486	传真	55594074	
	开户银行	北京银行燕京支行			
	账号	20000036505700020494413			2025年12月26日
受托人（乙方）	名称（或姓名）	**太极计算机股份有限公司**			合同专用章或单位公章
	联系人（经办人）	[illegible]		（签章）	
	住所（通讯地址）	北京北京市朝阳区来广营镇容达路7号	邮政编码	100012	
	电话	010-57702896	传真	010-57702889	
	开户银行	工行北太平庄支行			
	账号	0200010009200088408			2025年12月26日

附件 1：《分项明细及报价表》

序号	分项名称			单价（元）	数量	合价（元）	备注/说明
	租用服务类别	服务项	计价单位				服务期限（月）
1	定制化物理服务器	配置 1：2 路 10 核 2.0GHz，192G 内存，2 块 600G SAS 硬盘，2 个 HBA 卡，4 个万兆端口	台	498	64	382464	12
2		配置 2：4 路 10 核 2.0GHz，288G 内存，2 块 600G SAS 硬盘，2 个 HBA 卡，4 个万兆端口	台	680	23	187680	12
3		刀片服务器：4 颗 CPU，8*16GB DDR4，2*600GB 12G SSD 2.5 寸硬盘，2*10GE 接口卡，2*10Gb FCoE 接口卡，1* RAID 卡，刀片服务器	台	2100	32	806400	12
4		（刀片服务器机框）：10*FAN，6*POWER，2*OA 管理模块，单相电源输入，统一基础架构系统，含网卡：4 个 10GB 光模块、4 个 8GB FC 模块、4 个 GE 电口模块。	台	2800	4	134400	12
5	小型机物理服务器	配置核心数*处理器主频≥40GHz，256GB 内存，2 块 600G 以上 SSD 硬盘（含操作系统）	台	14000	8	1344000	12
6	集中式存储 1	SAN 架构存储系统，标配双控制器;配置 48Gb 缓存；配置虚拟资源调配软件、数据迁移软件、数据镜像功能、支持存储虚拟化及存储网关复制功能、块级压缩软件；12 个 16Gb FC 端口，控制器数量*2；企业级 SSD；支持 FC 、ISCSI 、NFS、CIFS、FCOE；支持 FCoE 主机接口；管理方式 GUI/CLI；10000 转速 SAS 盘，做完 raid 1+0 后容量为 50TB；10000 转速 SAS 盘做完 raid5 后容量为 50TB，支持存储扩容。多路径负载均衡软件。	台	24000	3	864000	12
		SAN 架构存储硬盘框(2U,交流\240V 高压直流,2.5″,级联模块,25 盘位，1.8TB 10K RPM SAS 硬盘单元(2.5″)25 个。	台	5000	2	120000	12

7	集中式存储 2	SAN 架构存储系统，标配双控制器;配置 48Gb 缓存；配置虚拟资源调配软件、数据迁移软件、数据镜像功能、支持存储虚拟化及存储网关复制功能、块级压缩软件；12 个 16Gb FC 端口，控制器数量*2；企业级 SSD;支持 FC 、ISCSI 、NFS、CIFS、FCOE；支持 FCoE 主机接口；管理方式 GUI/CLI；10000 转速 SAS 盘，做完 raid 1+0 后容量为 30TB；10000 转速 SAS 盘做完 raid5 后容量为 70TB，支持存储扩容。多路径负载均衡软件。	台	23500	3	846000	12
8	集中式存储 3	SAN 架构存储系统，标配双控制器;配置 48Gb 缓存；配置虚拟资源调配软件、数据迁移软件、数据镜像功能、支持存储虚拟化及存储网关复制功能、块级压缩软件；12 个 16Gb FC 端口，控制器数量*2；企业级 SSD;支持 FC 、ISCSI 、NFS、CIFS、FCOE；支持 FCoE 主机接口；管理方式 GUI/CLI；10000 转速 SAS 盘，做完 raid 1+0 后容量为 50TB；10000 转速 SAS 盘做完 raid5 后容量为 50TB，支持存储扩容。多路径负载均衡软件。	台	23000	1	276000	12
		2 套 SAN 架构存储盘柜：硬盘框(2U,交流\240V 高压直流,2.5″,级联模块,25 盘位，1.8TB 10K RPM SAS 硬盘单元(2.5″)25 个。	台	5000	2	120000	12
9	对象存储	2 颗 12 核 2.4GHz 处理器，256GB 内存，2 块 480GB RI SSD，空余硬盘插槽 14 个，2 块 2 端口万兆光接口网卡（包含多模光模块），空余 PCIE 插槽 1 个，4 端口千兆电接口 MLOM 网卡，三副本，实际可用 200TB	台	7500	1	90000	12
10	光纤交换机 1	万兆 48 个 10000BASE-T 电口以太网交换机，(全部端口激活，含 48*10Gb 多模 SFP)-单电源(交流)	台	1900	2	45600	12
11	光纤交换机 2	光纤交换机-48 端口(全部端口激活,含 48*16Gb 多模 SFP)-单电源(交流)	台	5200	14	873600	12
12	路由器	主机*1，双主控，双电源，满配交换网板，万兆光≥2；千兆电≥8；千兆光≥8；千兆 WAN≥2，2 个万兆多模光模块；2 个千兆多模光模块	台	3500	2	84000	12
13	核心交换机	以太网交换机主机，支持 48 个 100/1000/10000BASE-T 电口，支持 4 个 10G BASE-X SFP+端口，支持 2 个插槽，无电源需风扇	台	4900	6	352800	12

14	接入交换机	以太网交换机主机，支持 48 个 100/1000/100000BASE-T 电口，支持 4 个 10G BASE-X SFP+端口，支持 2 个插槽，无电源需风扇	台	600	14	100800	12
15	抗拒绝服务系统	2U，交流冗余电源，2*USB 接口，1*RJ45 串口，2*GE 管理口，2 个万兆 SFPP 插槽（不含光纤接口模块），支持万兆多模光纤接口模块、万兆单模光纤接口模块，3 个链路扩展卡插槽。含 64 字节 2G 容量许可。最大 4G 清洗容量。	台	3700	2	88800	12
16	VPN 防火墙	标准 2U 机架式设备，冗余电源，吞吐量 18G，并发连接数 450 万。6 个千兆电口，4 个千兆光口，4 个万兆光口(含光模块),国密算法	台	3800	6	273600	12
17	防病毒网关	标准 2U 机架式设备，冗余电源，吞吐量 12G，防毒墙吞吐量 2.5G，并发连接数 220 万。6 个千兆电口，4 个千兆光口，1 个 RJ45 串口，2 个 USB 接口。	台	2500	4	120000	12
18	流量控制	2U 设备，单电源，千兆电口 6 个，千兆光口 2 个，万兆光口 2 个（支持接口扩展），吞吐量 2.5Gbps，并发会话数 150 万，可实现用户的上网行为管理，流量控制，身份认证，应用识别，规则库可升级	台	4000	4	192000	12
19	业务域防火墙	标准 2U 机架式设备，冗余电源，吞吐量 16G，并发连接数 300 万。6 个千兆电口，4 个千兆光口，2 个万兆光口。	台	3500	4	168000	12
20	数据库域防火墙	标准 2U 机架式设备，冗余电源，吞吐量 16G，并发连接数 300 万。6 个千兆电口，4 个千兆光口，2 个万兆光口。	台	3500	4	168000	12
21	管理域防火墙	标准 2U 机架式设备，冗余电源，吞吐量 16G，并发连接数 300 万。6 个千兆电口，4 个千兆光口，2 个万兆光口。	台	3500	2	84000	12
22	应用负载均衡	2U 设备，6 千兆电口，8 个千兆光口，L4 层吞吐量 11Gbps、L4 并发连接数 940 万、L4 新建连接数 30 万，L7 新建连接数 15 万，冗余电源。设备支持串接、旁路部署、支持三角传输，设备支持虚拟化负载功能	台	3200	4	153600	12
23	数据库审计	2U，含交流冗余电源模块，2*USB 接口，1*RJ45 串口，千兆电口≥4 个，千兆光口≥4 个，万兆光口≥2 个，4T SATA 硬盘。含数据库入侵检测模块，包含 SQL 注入、提权、缓冲区溢出检测等功能。 SQL 处理性能 40000	台	3500	4	168000	12

		条/秒，存储天数≥180 天，日志检索≥60000 条/秒					
24	堡垒机	标准 2U 机架式设备，硬盘≥2TB，企业级，千兆电口≥6 个，提供≥600 个资源授权，提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护三级建设要求	台	3000	3	108000	12
25	NTP 时间服务器	授时精度 1-10ms；	台	400	1	4800	12
26	应用流量分析	双电源，磁盘存储空间 16TB， 4 个千兆电口/光口数据口或者 1 个万兆光口，2 个千兆管理口，处理能力≤2Gbps 或 每秒 10K 以内 TCP 会话。	台	6500	1	78000	12
27	网络审计系统	标准机架式设备，硬盘≥1TB，冗余电源，千兆电口≥4 个，千兆光口≥4 个，具备 RJ45 串口和 USB 接口。默认接口均可作为监听口。	台	4000	2	96000	12
28	TAP 分路器	流量复制/汇聚一体化	台	800	1	9600	12
29	安全态势感知系统	标准机架式设备，CPU≥4 核，物理内存≥32G，SSD ≥128G，SATA ≥4T*4，支持 RAID50，单电源，≥6 个千兆电口，1 个 DB9 串口，6 个 USB 接口。	台	5000	1	60000	12
30	安全态势感知系统探针	标准机架式设备，千兆电口≥4 个，千兆光口≥4 个，1 个 RJ45 串口，2 个 USB 接口。支持流量性能≥1.5Gbps，包转发率≥2.232Mbps，每秒新建连接数≥10 万，最大并发连接数≥200 万，CPU≥2 核，物理内存≥4G，硬盘≥SATA 1T。功能：1、IDS 漏洞利用检测；2、异常会话检测；3、Web 攻击检测；4、僵尸网络检测；5、违规访问检测，包含升级服务	台	2500	2	60000	12
31	日志审计系统	标准机架式设备，支持≥400 个主机审计许可，系统盘≥64G，硬盘≥8TB，千兆电口≥6 个；支持获取各种主流网络及数据库访问行为，支持 Syslog、WMI、OPSEC Lea、SNMP trap 专用协议等协议事件日志，支持通过 Http、Https、FTP、SFTP、SMB 等协议获取各类文件型日志，支持基于 SQL/XML 标准内容获取； 2 套审计节点许可-100 ：每许可证包含 100 个节点审计许可。	台	2900	2	69600	12

32	网络流量回溯分析	网络接口，2 个千兆采电口采集口，2 个千兆采光口采集口，2 个电口管理口；流量处理能力：800Mbps，数据包处理能力：200，000pps，TCP/UDP 会话处理能力： 每秒 50，000，存储空间 8TB	台	4000	1	48000	12
33	容灾备份一体机	机架式，800W（1+1）冗余电源，2 颗 64 位八核处理器，128GB 高速缓存；16 个热插拔位，配备 480TB 以上硬盘,2 个千兆以太网接口，2 个万兆口。	台	23500	3	846000	12
总价						9423744	-

序号	分项名称		单位	单价（元）	数量	合价（元）	备注/说明 服务期限（月）
	服务子类	服务项					
1	平台云主机服务（包含 X86、ARM、C86）	vCPU（vCPU ARM 架构主频不低于 2.4GHz，C86 和 x86 主频不低于 2.2GHz，平均虚拟化率，即物理 CPU/虚拟 CPU≥1/4，虚拟 CPU 利用率不低于物理 CPU 的 25% ）	1CPU	14	2367	397656	12
2		内存	1GB	40	6040	2899200	12
3	GPU 卡算力服务（适配 X86、ARM、C86）	GPU 显存（需同时租用算力资源、云主机或物理服务器资源，联合使用）	1 GB	45	368	198720	12
4		半精度浮点运算能力（需同时租用 GPU 显存、云主机或物理服务器资源，联合使用）	1 TFLOPS	8	1160	111360	12
5	普通性能存储	普通存储（单盘技术指标:单盘 IOPS2000-5000）	100GB	25	1411	423300	12
6	高性能存储	高性能存储（单盘技术指标：单盘 IOPS10000-25000）	100GB	60	2820	2030400	12
7	静态存储	提供大容量、高可靠的数据存储服务，具备 PB 级线性扩展能力	1TB	70	246	206640	12
8	本地备份服务	本地备份服务	100GB	50	1411	846600	12
9	异地备份服务	异地备份服务	100GB	50	120	72000	12
10	互联网链路服务	互联网链路带宽	1Mb	49	455	267540	12
11		互联网 IP 地址租用服务、并提供备案服务	1IP	20	44	10560	12

12	主机负载均衡服务	主机负载均衡服务	1IP（内网）	10	24	2880	12
13	远程接入服务	远程接入服务	1 账号	350	96	403200	12
14	SSL 证书服务	提供 SSL 证书服务	1 域名	10	1	120	12
15	Web 应用防火墙（WAF）	针对网站及 Web 应用系统提供应用层安全防护，支持各类 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护（200Mbps）	1 套	10	17	2040	12
16	商用操作系统套餐	Windows Server 套餐：Windows Server 租用、安装及维护。	1 套	90	350	378000	12
17		国产 Linux 套餐：国产 Linux 操作系统服务租用、安装及维护。	1 套	150	48	86400	12
18	开源操作系统套餐	提供开源操作系统安装和维护服务。	1 套	1	245	2940	12
19	商用数据库套餐	国产商用数据库租用、安装及维护（至少支持 3 种国产数据库）	1 套	5000	2	120000	12
20	主机杀毒服务	主机杀毒服务	台	100	734	880800	12
21	主机漏洞扫描加固	主机漏洞扫描加固	台	125	734	1101000	12
22	网页防篡改服务	网页防篡改服务	1 站点	100	10	12000	12
23	VPN 专线接入服务	提供 VPN 接入政务云环境服务	1 套	4000	1	48000	12
24	数据库审计服务	数据库审计服务	1 套	470	13	73320	12
总价（元）						10574676	-
总价合计（元）						19998420	-

附件 2：《重大违约行为表》

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（云服务商主责）	服务中断	云平台整体	因非不可抗力造成超过 30%以上信息系统中断、影响人数 50 万以上、导致 500 万元以上经济损失。	2小时以上	A级	1次
	重大篡改事件	信息系统	在重大或特别重大保障期间，因云服务商的安全隐患原因造成的系统被恶意篡改事件。事件发生后云服务商未按照应急预案进行处置，造成信息安全事件处置延误。且该事件被国家级机构或媒体通报、市级领导批示或关注的。	30分钟以上		
	数据丢失	等保三级或重要信息系统的核心业务数据	因非不可抗力造成的云平台超过 3个信息系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	等保三级或重要信息系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在 24 小时内做有效处置或应急防护措施，造成信息系统在重大或特别重大保障期间被恶意篡改或敏感信息泄露事件。	——		
	服务中断	云平台整体	因非不可抗力造成超过 10%至 30%信息系统中断、影响人数 10 万以上、导致 100 万元以上经济损失。	2小时以上	B级	一年内3次以上
	重大篡改事件	信息系统	因云服务商的安全隐患原因造成的系统被恶意篡改事件，事件发生后云服务商未按照应急预案进行处 置，造成信息安全事件处置延误， 且该事件被市级机构或媒体通报、市级领导批示或关注的。	30 分钟以上		
	数据丢失	信息系统核心业务数据	因非不可抗力造成 1 个信息系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	信息系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在 24 小时内做有效处置或应急防护措施，造成信息系统被恶意篡改或敏感信息泄露事件。	——		

附件 3：《严重违约行为表》

罚款金额=信息系统云服务费/服务月数*惩罚系数（惩罚系数参见《严重违约行为表》）

序号	问题描述	惩罚系数
1	所提供的云服务可用性低于 99.99%，或数据可用性低于 99.9999%，出现问题并造成重大损失的	200%
2	因未做好系统和数据互备，由于另一家云服务商服务中断，而导致系统和数据无法正常应用的，但影响未达到 B 级及以上事故影响的	200%
3	因所提供的安全服务出现故障，导致某系统网页被篡改，造成重大影响	600%
4	因所提供的安全服务出现故障，导致某系统数据丢失，造成重大影响	600%
5	因所提供的安全服务出现故障，导致某系统被入侵，造成重大影响	600%
6	在云安全监管服务商已发出整改通知后未正确处置，出现问题并造成重大事故	200%
7	平均响应时间大于 10 分钟且小于 30 分钟，造成重大事故	200%
8	运维需求平均响应时间大于 30 分钟且小于 60 分钟，造成重大事故	200%
9	运维需求平均故障恢复时间大于60 分钟且小于 90 分钟，造成重大影响	100%
10	运维需求平均故障恢复时间大于90 分钟且小于 120 分钟，造成重大影响	200%
11	现场无人值守超过大于 1 小时且小于 2 小时，造成重大事故	100%
12	现场无人值守超过大于 2 小时且小于 4 小时，造成重大事故	200%

附件 4:《一般违约行为表》

罚款金额=信息系统云服务费/服务月数*惩罚系数（惩罚系数参见《一般违约行为表》）

序号	问题描述	惩罚系数
1	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，出现问题但未造成重大损失的	50%
2	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，且在服务期内接到用户投诉此类情况 3 次以上的	20%
3	在运营期间，甲方对乙方实施月度考核，如乙方连续 3 次未能通过考核，经限期整改后仍不能达到甲方要求的	20%
4	在运营期内，如乙方未能按照用户方的扩容需求，在 7 个自然日内完成云平台的资源扩容，且经管理单位书面通知仍未能限期满足用户需求的	20%
5	因所提供的云服务或安全服务出现故障，造成某系统宕机 2 小时以上	30%
6	因所提供的云服务或安全服务出现故障，造成某系统连续宕机 3 次以上或累计8小时以上	60%
7	在云安全监管服务商已发出整改通知后未正确处置，出现问题的，未造成重大影响	50%
8	运维需求平均响应时间大于 10 分钟且小于 30 分钟，出现问题但未造成重大影响	30%
9	运维需求平均响应时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	50%
10	运维需求平均故障恢复时间大于 60 分钟且小于 90 分钟，出现问题但未造成重大影响	30%
11	运维需求平均故障恢复时间大于90 分钟且小于 120 分钟，出现问题但未造成重大影响	50%
12	现场无人值守超过大于 1 小时且小于 2 小时，出现问题但未造成重大影响	30%
13	现场无人值守超过大于 2 小时且小于 4 小时，出现问题但未造成重大影响	50%