合同编号：JSZKS2500508CGN00

江苏省交通运输厅
2025年度网络安全防护服务项目合同

项目名称：江苏省交通运输厅2025年度网络安全防护服务项目

项目编号：JSZC-320000-SCZX-C2025-0552

甲方（采购方）：江苏省交通通信信息中心
统一社会信用代码：12320000466003334A
法定代表人：赵渝

乙方（供应商）：中国电信股份有限公司江苏分公司
统一社会信用代码：91320000743917098X
法定代表人：彭鹏

甲、乙双方根据江苏省政府采购中心就江苏省交通运输厅2025年度网络安全防护服务项目项目（项目编号：JSZC-320000-SCZX-C2025-0552）开展的竞争性磋商采购程序采购结果，签署本合同。

一、合同内容

1. 产品/服务内容：江苏省交通运输厅2025年度网络安全防护服务项目

2. 交付物：主要服务内容包括厅本级基础安全防护软件续保及威胁预警推送运维服务、网络安全监测防护系统续保及运维服务、网络安全设备续保及运维服务、外网异常流量清洗与抗DDOS攻击系统续保运维及应急演练等有关服务、第三方网络安全人员驻场服务等。

3. 服务期限：本次合同签订之日起一年。

4. 运维要求：详见附件

5. 其他要求（如有）：无

二、合同金额

2.1 本合同金额为：2097700元（大写：贰佰零玖万柒仟柒佰圆）人民币。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供服务（包含与服务相关的产品）的有关技术资料。招标文件没有规定的，应于提供服务同时提供技术资料；分批次交付的应随每批次同时提供。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品、软件代码、源码、数据映像、密钥或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，乙方也应注意保密并限于履行合同的必需范围，并与有关人员签订不低于本合同约定的保密责任。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同服务（包含与服务相关的产品）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉、仲裁、行政举报/投诉、申请宣告无效、申请撤销登记等。一旦出现侵权，由乙方负全部责任并承

担由此给甲方造成的一切损失（包括但不限于诉讼费、仲裁费、差旅食宿费、误工费、律师费、保全费、取证支出、专家费等）。

4.2 如乙方怠于维权，为维护甲方权益需要，乙方同意将知识产权相应权能授权或转移给甲方，并就甲方维权提供充足配合（包括但不限于配合提供所需材料等）。甲方维权实现的，有权保留自身部分权益，并有权扣除代为维权所支出的一切费用（包括但不限于诉讼费、仲裁费、差旅食宿费、误工费、律师费、保全费、取证支出、专家费等）。

五、产权担保

5.1 乙方保证所交付的服务（包含与服务相关的产品）的所有权完全属于乙方，且乙方对服务（包含与服务相关的产品）具有完整的可独立处分的权利，且无任何抵押、查封等权利瑕疵。

六、合同转包或分包

6.1 乙方不得将合同标的转包给他人履行。

6.2 采购公告许可或甲方书面许可的，乙方可以在许可范围内分包中标项目非主体部分的工作。

6.3 乙方如有转包或未经甲方同意的分包行为，甲方有权解除合同。

七、服务期限及双方权利义务

服务期限：壹 年

7.1 乙方应按采购文件规定和响应文件承诺的性能、技术要求、质量标准向甲方提供服务。

7.2 乙方提供的服务在服务期限内因其本身出现质量问题，根据实际情况，经双方协商，可按以下办法处理：

（1）重做（重新提供特定服务）：由乙方承担所发生的全部费用。

（2）合同终止、解除处理：合同终止、解除，并退还甲方支付的合同款，同时应承担由此产生的所有费用，甲方不承担发生任何费用。

7.3 如在使用过程中发生质量问题，乙方在接到甲方通知后在 1 小时内到达甲方现场。

7.4 在服务期内，乙方应对服务（包含与服务相关的产品）出现的质量及安全问题负责处理解决并承担一切费用。如甲方人为故意损坏或造成故障等，乙方无需因此额外承担赔偿责任，仅在维护义务范围内继续开展工作。

7.5 服务期限内，发生质量及安全问题，按约定应由乙方承担的费用，乙方拒不承担或甲方先行垫付的，甲方有权从待付合同款中直接抵扣。

7.6 服务期限内，甲方有权定期、不定期开展服务质量检查，乙方应配合甲方检查。

八、合同款项支付

8.1 双方议定按照以下第【 A 】种方式支付

A. 项目费用分两个阶段支付（委托服务类）：

项目费用分两个阶段支付：

第一阶段：合同签订后，在甲方收到乙方符合甲方财务要求的发票 20 日内，甲方支付第一笔款项，占合同总额的 50%，共计人民币 1048850 元（大写：壹佰零肆万捌千捌佰伍拾 圆）；

第二阶段：服务期满后，经甲方确认服务良好，乙方提供运维服务总结报告或相关服务报告，并经验收通过后，甲方自验收通过之日起，于收到乙方符合甲方财务要求的发票 20 日内支付第二笔款项，占合同总额的 50%，共计人民币 1048850 元（大写：壹佰零肆万捌千捌佰伍拾 圆）。但根据合同约定，甲方提前已经抵扣的，支付时应扣除已抵扣款款项。

B. 根据运营商出账周期及约定的支付方式，按周期支付当期账单金额。

8.2 甲方付款前，乙方应当按甲方要求依法开具全额票据。乙方未按约定提供发票前，甲方有权暂缓支付并不能因此被认定为违约。甲方选择在开票前支付的，不免除乙方未开票的违约责任。

8.3 双方约定考核方案，甲方根据考核方案扣减服务费用的，按考核方案执行。甲方可以选择在前述每期费用支付前直接扣减相应费用，也可以选择要求乙方另行退还扣减费用。

C. 项目费用分三个阶段支付（货物采购类）：

第一阶段：合同签订后，在甲方收到乙方符合甲方财务要求的发票 20 日内，甲方支付第一笔款项，占合同总额的 50%，共计人民币 / 元（大写：/ 圆；

第二阶段：设备到货安装调试完成，甲方于收到乙方符合甲方财务要求的发票 20 日内支付第二笔款项，占合同总额的 40%，共计人民币 / 元（大写：/ 圆；

第三阶段：设备试运行正常三个月后，甲方于收到乙方符合甲方财务要求的发票 20 日内支付第三笔款项，占合同总额的 10%，共计人民币 / 元（大写：/ 圆。乙方未按约定及时支付质保金的，甲方也有权选择直接在第三笔款项范围内扣留质保金，并支付剩余合同款。

8.2 甲方付款前，乙方应当按甲方要求依法开具全额票据。乙方未按约定提供发票前，甲方有权暂缓支付并不能因此被认定为违约。甲方选择在开票前支付的，不免除乙方未开票的违约责任。

8.3 双方约定考核方案，甲方根据考核方案扣减服务费用的，按考核方案执行。甲方可以选择在前述每期费用支付前直接扣减相应费用，也可以选择要求乙方另行退还扣减费用。

九、税费

9.1 本合同执行中相关的一切税费均由乙方负担。

十、项目验收

10.1 甲方对乙方提供的服务（包含与服务相关的产品）依据采购文件上的项目需求要求、乙方响应文件及国家有关质量标准组织验收。

10.2.乙方交货前应对产品或服务作出全面检查和对验收文件进行整理，并列出清单，作为甲方验收和使用的技术条件依据。

10.3 对于实际使用人和甲方分离的项目，甲方可邀请实际使用人参与验收。

10.4 服务期满后，甲方按照采购合同的约定对乙方的履约情况进行验收。验收时,乙方须出具运维总结报告等相关材料。

10.5 验收合格的项目,甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的,甲方将及时报告本级财政部门。

10.6 使用财政性资金采购政府集中采购目录以内或者限额标准以上的货物、工程和服务的政府采购项目，在政府采购合同约定的履约验收条件达到时，采购人应在 5 个工作日内启动履约验收工作，并向供应商发出《政府采购履约验收通知单》。

10.7 使用财政性资金采购政府集中采购目录以内或者限额标准以上的货物、工程和服务的政府采购项目，采购人应当成立验收小组采购人应当成立验收小组，负责采购项目履约验收具体工作。组成验收小组应符合以下要求：

（一）验收小组一般由采购人指定的本单位 3 名（含）以上单数工作人员组成，并确定一名负责人。参与本项目评审的采购人代表不能作为负责人，分期（分段）验收的负责人原则上应当保持一致，负责人不得无故更换。

（二）根据采购项目特点和实际需要，可以邀请相关领域专业技术人员等作为验收小组成员参与验收。前期参与本采购项目相关采购活动的采购代理机构工作人员、评审专家以及与供应商有利害关系的人员，不得作为验收小组成员参与履约验收。

（三）财政部门政府采购监管人员不得作为验收小组成员参与履约验收。

10.8 使用财政性资金采购政府集中采购目录以内或者限额标准以上的货物、工程和服务的政府采购项目，验收小组应当制定验收工作实施方案，按照方案开展验收，出具验收意见。验收意见应当客观真实地反映政府采购合同履行情况。

验收工作实施方案应当至少符合以下要求：

（一）明确验收工作的起止时间，涉及分期（分段）验收的，应当明确每一期（段）的起止时间。

（二）履约验收范围应当完整，与政府采购合同一致，不得省略、遗漏和缺失，也不得擅自扩大范围。

（三）履约验收内容应当具体，形成详细的验收过程性资料，客观反映货物供给、工程和服务承接完结情况。

（四）履约验收方式应当符合项目特点，科学确定验收周期，指派具体验收人员分别实施验收。不能明确客观标准、涉及主观判断的，可以通过在使用人中开展问卷调查等方式予以客观、量化。

（五）履约验收标准应当符合政府采购合同约定、法律法规以及国家强制性标准等，对服务类采购项目，可以参照行业标准、专业标准等。

10.9 使用财政性资金采购政府集中采购目录以内或者限额标准以上的货物、工程和服务的政府采购项目，采购人、供应商应当对验收小组出具的验收意见进行确认，并形成政府采购履约验收书。对验收意见存在异议的，采购人与供应商双方可以协商解决，或通过法律途径解决。

10.10 使用财政性资金采购政府集中采购目录以内或者限额标准以上的货物、工程和服务的政府采购项目，对为社会公众提供的公共服务项目，采购人应委托代理机构于验收结束之日起 2 个工作日内按有关政府采购信息公开要求在网上公开验收结果。

10.11 履约验收中产生的专家评审费、检测（检验）费等费用支出，由乙方承担。

十一、保密义务

11.1 双方同意，就双方在履行本合同过程中所知悉或获取的对方的保密信息，双方应严格遵守保密义务，具体内容详见附件安全保密协议。

十二、违约责任

12.1 乙方逾期提供服务的，乙方应按逾期提供服务合同总额每日千分之六向甲方支付违约金，由甲方从待付合同款项中扣除。逾期超过约定日期 10 个工作日不能提供服务的，甲方可单方解除本合同。乙方因逾期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同价款总额 5 % 的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

12.2 乙方所提供服务（包含与服务相关的产品）的标准不符合合同规定及招标文件规定标准的，甲方有权拒绝接受服务，并可单方面解除合同。

12.3 因乙方运维不当，发生以下情形之一的：被部省有关部门通报或考核扣分，给甲方造成较大不良影响的；发生较严重网络安全事件并产生舆情的。甲方有权追究乙方责任，包括但不限于由此产生的律师费、诉讼费、保全费等，并扣除乙方有关违约金，每发生一次，乙方应向甲方支付违约金5000元，如果造成甲方经济损失超过5000元的，违约金按照实际损失扣除，甲方有权选择从待付合同款抵扣。

12.4 乙方怠于主张债权，导致合同僵局或甲方无限期累计逾期费用、违约金，或侵害国家、集体利益等结果的，甲方可以选择解除合同并按约定支付违约金，以终止逾期费用、违约金计算，防止合同履行陷入僵局。甲方上述解除权应自甲方最后一期义务届满时起五年内行使。

十三、其他条款

13.1 乙方管理技术团队要相对独立、稳定，团队人员为正式员工，有专门网络安全负责人。乙方如发生业务转型、合并重组、投资并购等重大事项，或者管理技术团队人员发生重大变化，应提前向甲方书面报告。合同履行中，乙方业务转型、合并重组、投资并购等过程应当保持项目参与人员素质不低于采购文件、响应文件，否则视为重大违约，甲方有权因此单方解除、终止合同履行。

13.2 乙方在合同执行期间产生的政务数据、系统运行数据及收集的个人信息等数据资产归甲方所有。乙方并应保证甲方完整、准确、及时访问、利用、支配相关数据的权利。乙方应采取有效技术措施加强对合同执行期间收集个人信息的保护。乙方必须将政务数据与其他数据分开存储、处理。未经甲方书面同意，乙方不得变更数据用途、用法，不得访问、修改、公开、披露、利用、转让、销毁、私自留存或向第三方提供。合同终止时，乙方应按规定及时处理相关数据。

13.3 乙方应建立健全网络和数据安全保护机制，严格遵守不断完善的法律、法规、规章、规范性文件、政策关于信息处理、储存、共享等的规定，发现重大安全漏洞和风险隐患应按规定及时向甲方和相关部门报告。乙方应积极配合相关部门开展网络安全检查、测评、审计等监督管理工作。乙方按规定每年向甲方提交网络安全报告。

13.4 根据《中华人民共和国政府采购法》第五十条第二款或其他法律、法规、规章规定，继续履行将损害国家利益和社会公共利益的，双方当事人应当变更、中止或者终止合同。有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。甲方履行本条义务要求变更、中止、终止合同的，乙方无权拒绝。

十四、不可抗力事件处理

14.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，经双方协商一致，则合同履行期可延长，其延长期与不可抗力影响期相同。延长期限，不得超过关权威机构出具的证明所载明的起止时间。因一方违约导致该方遭受不可抗力的，不得援引不可抗力主张延期履行。如一方不同意延长合同履行期限，双方协商一致，可解除合同。

14.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

14.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

14.4 不可抗力导致延期，致使部分合同权利义务已不可能履行，或履行无价值，义务方不履行延期后义务的，不认为是违约。但因一方拒绝协商、配合，导致权利义务不可能履行或履行无价值的，拒绝协商、配合乙方应承担因此导致的对方损失。

十五、诉讼

15.1 双方在执行本合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲

方实际所在地法院起诉。

十六、合同生效及其它

16.1 合同经双方加盖单位公章后生效。

16.2 双方确认以下信息为本合同履行的默认账户、地址、联系方式，并认可作为诉讼、仲裁等法律程序的文书送达地址和联系人。如相关信息变化的，自书面信息变更送达次日起生效。

甲方	联系人	-	联系电话	-
	联系地址	江苏省南京市秦淮区升州路 16 号		
	账户名	江苏省交通通信信息中心		
	开户行	招行城南支行		
	银行账户	252080719910001		
	税号	12320000466003334A		
乙方	联系人	郑翔	联系电话	15301586723
	联系地址	江苏省南京市玄武区中央路 260 号		
	账户名	中国电信股份有限公司江苏分公司		
	开户行	工商银行南京察哈尔路支行		
	银行账户	4301011219001023493		
	税号	91320000743917098X		

16.3 本合同未尽事宜，遵照《民法典》有关条文执行。

16.4 本项目采购文件、成交供应商的响应文件及采购过程中有关澄清、承诺文件均为本合同有效附件，是本合同不可分割的组成部分，与本合同具有同等法律效力。

16.5 本合同附件：

（1）《安全保密协议》；

（2）外包网络安全协议要点

（3）签约授权委托材料；

（4）运维要求。

16.6 本合同正本一式陆份，具有同等法律效力，甲方、乙方各执叁份。

（正文到此结束，以下签署区）

甲方：	江苏省交通通信信息中心		乙方：	中国电信股份有限公司江苏分公司
地址：	江苏省南京市秦淮区升州路 16 号		地址：	江苏省南京市玄武区中央路 260 号
法定代表人或授权代表：	赵渝		法定代表人或授权代表：	

签订日期：2025 年 11 月 20 日

附件 1：

安全保密协议

甲方（采购方）：江苏省交通通信信息中心

统一社会信用代码：12320000466003334A

法定代表人：赵渝

乙方（供应商）：中国电信股份有限公司江苏分公司

统一社会信用代码：91320000743917098X

法定代表人：彭鹏

根据我国有关网络安全及信息保密相关法律法规，本着平等、自愿、公平、诚信的原则，双方就江苏省交通运输厅 2025 年度网络安全防护服务项目 项目（项目编号：JSZC-320000-SCZX-C2025-0552 ）合作过程中有关网络安全保密事项达成以下协议，并由双方共同遵守。采购网络产品和服务的一方应为“甲方”，提供网络产品和服务的一方应为“乙方”。

1 安全、保密内容和范围

甲乙双方确认，乙方承担保密义务的甲方信息包括但不限于以下内容：

1.1 技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；

1.2 业务信息：同甲方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息；

1.3 安全信息：包括账号、口令、密钥、授权等用于对网络、应用系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息。

2 安全、保密义务

2.1 乙方明确所接收的保密信息及其载体均为甲方所有。乙方承认甲方在本协议规定的保密信息上的利益和/或一切有关的权利，乙方应当考虑甲方的利益并对该信息予以妥善保管。乙方应按照最新的法律、法规、规章、规范性文件、政策要求及行业技术标准要求对储存、处理、共享数据采取必要安全措施，以避免数据被未经授权的删除、篡改、查看、复制，确保数据和数据储存、处理、共享环境免于病毒、黑客、不良软件的入侵或攻击。

2.2 乙方遵守相关法律、法规、政策、规章 、制度和协议，基于授权的基础上，合理使用甲方信息，不得以任何其他手段获取、授权或协议规定以外的甲方信息。

2.3 乙方未经授权，不应在工作职责授权范围以外使用、分享甲方信息。未经授权，不得泄露、披露、转让以下信息：

2.3.1 技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；

2.3.2 业务信息：同甲方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息；

JSZKS2500508CGN00

2.3.3 安全信息：包括账号、口令、密钥、授权等用于对网络、应用系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息。

2.4 若第三方要求披露甲方敏感信息时，乙方不应擅自响应，并应立刻将情况通告甲方。

2.5 乙方对违反协议或可能导致违反协议、规定、规程、法律的活动、策略或实践，一经发现，应立即通告甲方。

2.6 乙方应协助甲方或经甲方同意采取必要的方式（备份、冗余存储等技术、物理手段），避免合同履行过程中数据遭受丢失、污染、被篡改、人为删除等风险。

2.7 合同结束后，乙方应返还甲方本协议中规定的信息和甲方数据。所有由甲方提供给乙方的材料，包括但不限于文件、设计和清单应仍为甲方的财产，且甲方要求时应立即归还原件和所有据此制作的副本。

3 违约责任

乙方承认并明确同意：其对本协议的任何违约仅有法律的救济尚且不足，并且因其违约行为而造成的甲方损失是难以用金钱来衡量的。因此，当乙方出现任何违约情形时，甲方有权要求乙方立即返还相关保密信息，且乙方有义务立即采取合理补救措施。同时，乙方还应赔偿：

3.1 因乙方违约行为，而使甲方遭受的全部经济损失(包括直接损失和间接损失)，若损失难以估算，则乙方应将因本次政府采购活动所获得的所有收益，返还给甲方，并按照收益金额的 20%，向甲方支付违约金；

3.2 甲方因调查乙方的违约行为、采取补救措施而支出的所有合理费用(包括但不限于甲方向乙方及第三方追索、取证、调研而发生的仲裁费、诉讼费用、律师费、交通费、劳务费、专家费、鉴定费等)。

4 协议有效期

本协议自生效之日起永久持续保有完全的效力。本协议有效期内任何时间双方可通过合意终止协议。终止仅豁免乙方对终止后被提供、产生的保密信息所负有的保密责任，不应豁免乙方在本协议下就终止生效日前已经提供给乙方的保密信息所应履行的全部保密义务。

5 如果所涉及的保密信息依照国家主管机关或相关法律、法规另有规定的，适用其相关规定。

6 适用法律及争议解决

本协议的法律适用及争议解决，依主合同之约定。如无主合同的，适用中华人民共和国法律，并受甲方所在地人民法院管辖。

7 本协议于签订之日起生效。本协议签订晚于项目主合同签订时间或项目实际启动（相关人员获得保密信息等）时间的，以时间在前的为准。

8 本协议一式陆份，甲乙双方各执叁份，具有相同法律效力。

（正文到此结束，以下签署区）

甲方：	江苏省交通通信信息中心	乙方：	中国电信股份有限公司江苏分公司
地址：	江苏省南京市秦淮区龙州路16号	地址：	江苏省南京市玄武区龙蟠大路266号
法定代表人或授权代表：	赵渝	法定代表人或授权代表：	

JSZKS2500508CGN00

附件 2：

外包网络安全协议要点

一、协议依据及类型要点

根据《中华人民共和国民法典》及《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等有关法律法规及规范性文件的规定，甲（委托单位）、乙（承包单位）双方经协商一致，就江苏省交通运输厅 2025 年度网络安全防护服务项目 项目（项目编号： JSZC-320000-SCZX-C2025-0552 ）（以下简称“本服务项目”），签订本网络安全协议。

二、甲方的权利和义务要点

1. 本服务项目中产生的政务数据、系统运行数据及收集的个人信息等数据资产（以下简称“外包数据资产”）归甲方所有，甲方可以随时访问、利用、支配该数据资产，并督促乙方应采取必要技术措施防范该数据资产的泄露、流失和违规操作。

2. 甲方建立对本服务项目的常态化网络安全监督管理，可采取随机抽查、派驻人员或委托第三方机构等方式，对本服务项目网络安全管理情况开展常态化检查评估，通报问题隐患，责令限期整改；乙方应配合检查并及时整改。

3. 甲方应提供乙方必要的工作条件，并按照最小必要原则授予乙方提供服务所需的相应权限，授权期满后及时收回相关权限，乙方应予以协助配合，不得设置后门程序或者恶意程序。

4. 本服务项目终止时，甲方应要求乙方销毁或转移相关数据，乙方应予以配合实施，并向甲提供《网络安全承诺书》，承诺采取必要措施保证相关数据不可恢复，不私自留存、非法买卖或提供给第三方，不公开、披露、利用服务中知悉各类信息，否则乙方应承担一切法律责任。

5. 在接受服务过程中，甲方发现乙方存在如下情形之一，导致合同继续履行将损害国家利益和社会公共利益的，甲方有权单方终止合同，且仅支付乙方相应服务期限内合理费用的 80%；乙方应及时返还多收取的价款：

（1）乙方规模能力、经营范围、资本构成、高管背景、技术水平、安全团队以及企业信用等方面发生重大变化，可能造成本服务项目存在重大网络和数据安全风险的；

（2）乙方（含相关工作人员及委托服务的第三方）因涉嫌违反网络安全、数据安全和个人信息保护相关法律法规，正接受有关主管部门立案调查（乙方应主动告知甲方该情况），甲方经评估后认为，乙方继续本服务项目可能存在重大网络和数据安全风险的；

（3）因乙方对服务合同中约定的网络和数据安全保护措施建设、使用不到位等，导致

发生网络和数据安全事件，或者产生网络和数据安全风险隐患被省级以上有关主管部门通报的；

（4）乙方违反本协议的约定、承诺或保证，尚未造成严重后果，甲方责令限期整改，乙方拒不整改或者整改不到位的；

（5）因乙方原因造成重大网络舆情的。

6. 在接受服务过程中，甲方发现乙方存在如下情形之一，导致合同履行将损害国家利益和社会公共利益的，甲方有权单方终止合同，并要求乙方返还全部合同价款，同时追究乙方的法律责任；乙方应及时返还已收取的合同价款：

（1）在服务合同签订前的三年内，乙方因违反网络安全、数据安全和个人信息保护相关法律法规，受到过行政处罚、刑事处罚，或者仍在接受有关主管部门立案调查，但未主动告知甲方该信息的；

（2）乙方在本服务项目中的相关管理人员、操作运维人员经公安或国安部门背景审查存在问题，甲方要求乙方更换相关人员，乙方拒不更换的；

（3）违反网络安全、数据安全和个人信息保护等相关法律法规，拒不按照甲方要求改正、补救的。

（4）违反网络安全、数据安全和个人信息保护相关法律法规的规定，或者违反本协议的约定、承诺或保证，导致本服务项目发生重大网络和数据安全事件，或造成其他严重后果的。

三、乙方的权利和义务要点

1. 在签订服务合同前，乙方应向甲方如实、完整提供其规模能力、经营范围、资本构成、高管背景、技术水平、安全团队、信用等级等经营管理信息，以及近三年因违反网络安全、数据安全和个人信息保护有关法律法规规章而受到约谈、行政处罚或刑事处罚等信息；未经乙方同意，甲方不得公开或向第三方提供相关信息。

2. 乙方应当严格按照网络安全、数据安全和个人信息保护相关法律法规、国家标准及政策文件的规定提供安全可靠的产品、平台或服务，确保网络系统运行安全及相关数据资产的保密性、完整性、可用性；对在服务过程中接触到的甲方工作信息及相关文件，应予以严格保护，不得对外提供、公开、泄露或利用。

3. 乙方应建立相对独立的管理技术团队，具体提供服务的相关人员应为乙方正式员工，并指定网络安全负责人。

4. 乙方不得转包、分包合同任务；确需分包的，应报经甲方同意，并在分包合同中明确相应的网络安全义务和责任，但不得对合同任务主体和关键部分进行分包。

5. 乙方应严格按照法律法规规定及服务合同约定，收集、使用、存储、处理数据和个人信息。

6. 乙方应将政务数据与其他数据分开存储、处理，未经甲方书面同意，不得变更用途、用法，不得访问、修改、公开、披露、利用、转让、销毁、私自留存或向第三方提供；合同终止时，应当按照甲方的要求及时处理。

7. 乙方在本服务项目中涉及采购相关产品和服务的，应当严格遵守如下规定要求：

（1）建设政务信息平台的，应当优先采用安全可信的软硬件产品；确无相关安全可信产品的，应当研究制定针对性措施防范安全风险；

（2）建设云平台的，应当选择供应链来源可靠的云平台管理软件、业务系统以及服务器 CPU、操作系统、数据库等；

（3）使用云计算服务（含 PaaS、IaaS、SaaS 等）的，应当按要求采用安全可信的云计算服务，并明确云服务商的网络和数据安全责任；

（4）使用商用密码的，应当符合国家密码管理规定。

8. 乙方发现本服务项目中存在网络安全漏洞、缺陷或其他严重网络安全风险，应及时向甲方报告，或者直接向同级网信、公安部门报告；未经网信或公安部门同意，不得公开或向第三方提供。

9. 乙方应严格落实相关开放性、兼容性标准和规范要求，优先采用通用系统解决方案，避免因采用特定的技术架构、应用接口、数据格式等，导致后续扩建、运营、维护等被绑定，形成技术壁垒或者市场垄断而引发重大技术风险。

10. 乙方发生业务转型、合并重组、投资并购等重大事项，或者管理技术团队人员发生重大变更，可能影响服务项目的网络和数据安全的，应提前向甲方报告。

11. 乙方建设、运维的政务信息平台注册用户超过 100 万人或者涉及人民群众出行、教育、求职、医疗、缴费等重要业务，乙方应每年向甲方提交网络安全报告，报告至少包括网络安全管理、数据安全管理、平台关键软件和核心硬件供应链安全、管理技术团队变化等情况。

12. 乙方应建立外包服务项目安全管理工作规范，明确本单位及相关工作人员的网络安全责任，不断提升网络安全防护能力水平；定期组织本服务项目相关人员开展网络安全培训，规范安全操作规程，增强安全风险意识。

13. 乙方应积极配合网信、公安、审计、保密、密码管理等部门开展网络安全检查、测评、审计等监督管理工作，如实、完整提供相关网络安全管理情况，不得拒绝、隐匿、瞒报。

14. 乙方应当严格遵守并履行《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等有关法律法规中的相关规定和法定义务。

四、违约责任要点

1. 乙方违反网络安全、数据安全和个人信息保护相关法律法规，或者违反本协议的约定、承诺或保证的，甲方有权追究乙方责任，乙方应按服务合同总价款的 20%或按照人民币 10 万元的金额（以两者中较高的金额为准）向甲方支付违约金；如造成甲方损失的，乙方应当全额赔偿。

2. 因甲、乙双方共同责任造成甲方损失的，乙方须按比例承担相应的法律责任。

五、协议期限要点

与服务合同起止期限相同，但相关法律法规规定的网络和数据安全责任义务不受该期限的限制。

（正文到此结束，以下签署区）

甲方：	江苏省交通通信信息中心	乙方：	中国电信股份有限公司江苏分公司
地址：	江苏省南京市秦淮区升州路16号	地址：	江苏省南京市玄武区中央路260号
法定代表人或授权代表：	赵渝	法定代表人或授权代表：	

JSZKS2500508CGN00

附件 3：签约授权委托材料

中国电信股份有限公司

授 权 书

股委 [2025]10-1 号

为确保中国电信股份有限公司江苏分公司（简称“江苏分公司”）各项工作正常开展，根据中国电信股份有限公司（简称“股份公司”）章程的规定，兹向江苏分公司出具如下授权书：

一、被授权单位

中国电信股份有限公司江苏分公司

负责人：彭鹏

二、授权事项

（一）代表股份公司决定被授权单位所在江苏省行政区划内的股份公司市、县（市、区）分公司、营业厅等各类分支机构（简称“所属分支机构”）的设立、变更、注销。

（二）以被授权单位名义办理被授权单位和所属分支机构的公司登记、信息公示等事项，负责营业执照、贷款卡（编码）、房屋所有权证、国有土地使用证、机动车行驶证办理及银行账户开立、变更、注销等事项，负责办理相关资源、资质申请等事项。

（三）作为投后管理单位，代表股份公司根据法律法规及其公司章程的规定行使股东权利，委派董事、监事，决定推荐经营负责人等高级管理人员。

（四）任免和管理所属分支机构的领导成员，以被授权单位名义按照国家有关规定与被授权单位及所属分支机构的员工签订、变更、解除和终止劳动合同。

（五）以被授权单位名义对外签订单笔标的金额在人民币 5

亿元以下的借款类合同(包括但不限于银行借款合同、银行承兑汇票合同、商业承兑汇票的开立及贴现、非融资性保函合同等)和单笔标的金额在人民币 10 亿元以下的其他各类合同（除担保合同外）。

（六）以被授权单位名义或者代表股份公司对外参加招投标活动，签署相关合同。

（七）代表股份公司处理与被授权单位及所属分支机构有关的诉讼、仲裁等纠纷案件。

三、转授权事项

被授权单位可根据需要在本授权范围内将授权事项转授给所属分支机构。

四、其他相关事项

（一）上述授权事项和授权范围中需使用股份公司公章的，授权被授权单位使用被授权单位的公章。

（二）上述授权事项和授权范围中需对外签署相关文件的，由被授权单位负责人或该负责人授权的人士签署。

五、有效期限

本授权书的有效期限自 2025 年 3 月 25 日起至 2026 年 12 月 31 日止。

本授权书一式两份。

法定代表人：

2025 年 3 月 25 日

JSZKS2500508CGN00

附件 4：运维要求

一、网络安全防护服务整体要求

为保证本项目服务质量，供应商应具备相关资质，能够满足项目整体网络安全防护要求，具备完善的服务保障体系、合理的故障响应时间，根据用户需求，提供高质量、高标准、高效率的技术服务。

1、服务保障体系要求

供应商应具备本地化的技术支持与售后服务机构，具备优秀的技术人员和雄厚的技术力量，提供专业的项目经理来负责本项目的技术支持与售后服务的统一协调工作，能够提供远程技术支持和现场技术支持等多种服务方式。

建立完善的运维机制、故障响应机制，第一时间响应和解决运维需求。

故障响应时间要求

提供 7*24 小时的故障响应服务，如出现技术故障，按如下要求进行响应：

序号	响应级别	问题描述	响应时间
1	紧急	核心业务功能及组件不可用或全部瘫痪的严重故障类问题	15 分钟内进行响应
2	高	部分业务功能或组件受到影响，或业务软件时断时续等故障类问题	30 分钟内进行响应
3	中	单一业务简单故障方面问题	2 小时内进行响应
4	低	针对于业务使用方法、产品需求等一般技术咨询类问题	4 小时内进行响应

2、服务质量要求

（1）供应商应提供高质量的技术服务，所提供的技术服务应具备合理的质量管理及考核体系。

（2）供应商应设立服务质量监督员并定期向采购人汇报合同要求范围内的技术服务（包含网络巡检、安全运维、故障处理等）执行情况及质量状况，针对采购人提出的意见及建议进行服务质量整改措施并跟踪落实。

（3）如因供应商技术能力导致设备故障引起采购人应用服务中断，采购人将视故障的影响程度，对供应商进行服务考核和处理，若导致重大故障或数据丢失，采购人有权利要求供应商赔偿因此造成的相关损失。

3、服务流程要求

3.1 主动式服务

3.1.1 定期预防性维护服务

维护团队根据系统维护服务计划或用户要求为用户提供定期预防性维护服务。此类服务是有计划有步骤进行的，目的是为了提高系统的可使用率和高可靠性，把系统故障的可能性降低到最低。在硬件维护方面，要求维护团队工程师每两周进行一次现场例行检查。

3.1.2 系统运行健康检查

维护团队应提供一月一次的系统运行健康检查，按计划由专家定期对主机系统性能进行诊断，根据结果出具性能诊断报告，并征得用户同意后调整系统参数，使系统始终在最佳状态下运行。对可能出现的问题提供科学预测，并采取必要的预防和补救措施，防患于未然。

3.1.3 信息系统安全性测试

每月按甲方要求，针对重要信息系统开展渗透测试。利用专业工具和技术人员研判，扫描排查重要信息系统存在的各类风险隐患，并协助整改，整改后进行安全复测，形成闭环管理。

3.2 纠错性维护/维修服务

维护团队应提供电话技术支持服务或到场维修服务。在硬件服务方面，维护团队应及时确认故障原因，并更换故障硬件，恢复系统正常运行。解决安全系统、软件问题，恢复系统软件正常运行，并做系统备份，递交系统检查报告等。

4、 服务报告要求

维护团队定期提供服务报告，服务期结束前应提供年度总结报告，并对每一次重大故障和问题的原因、解决方法、完成情况等形成专项报告，并及时报送用户。在运维服务过程中将产生不限于以下的记录和报告：

- 日常维护报告
- 系统巡检日志
- 系统维护记录
- 系统优化记录
- 各类优化的管理制度
- 故障分析处理记录
- 故障整改方案和建议
- 重大故障记录报告

5、 质量管理要求

维护团队应根据本项目要求提出服务质量管理具体措施，并对所提供的服务质量和标准做出明确可量化的承诺。

6、其他要求

该项目在实施过程中，由采购人单位组织运维考核工作，对运维服务单位进行打分考核，以实现高标准运维。考核结果的评分、结论将作为合同付款、下年度运维预算及后续省厅其他系统招标的重要参考依据。如因运维服务单位原因出现重大安全事故或安全通报，造成的损失及相关责任由运维服务单位承担。同时有权立即终止运维服务单位对相关系统的维护服务，并扣除剩余的服务费用。具体要求参照江苏省交通运输厅软硬件系统运维服务管理办法。具体考核指标：

1、保障各类网络安全硬件设备运行正常，及时处理故障更换设备，能实现厅本级网络防护各项需求。

2、保障各类网络安全软件运行平稳，及时更新版本定期巡检，建立起网络安全监管体系。

3、提交年度运维报告。

4、发表省级以上期刊论文两篇（网络安全类）。

5、完成其他约定的交付内容。

JSJS-250050SCG00

二、服务内容要求

（一）基础安全防护软件续保及运维服务

为保证厅数据中心虚拟化环境的安全稳定性，对部署在专网、外网过保的虚拟化安全防护软件进行续保，以及提供相关安全运维服务。

维保内容：

产品名称	配置描述	数量
控制台	无限控制台	2 个控制台
外网终端	虚拟服务器个数版，基于虚拟安全，需在虚拟机中安装客户端才能使用该功能	180 个终端
专网终端	虚拟服务器个数版，基于虚拟安全，需在虚拟机中安装客户端便能使用该功能	310 个终端
全安全功能模块开启（防病毒、弱口令、入侵威胁监测、安全监控、合规基线扫描、威胁预警等）		

服务要求：

1）每月至少一次系统巡检，对系统升级维护，根据实际情况进行相关策略优化，并出具巡检报告；

2）根据甲方需求配合提供现有态势感知系统等威胁预警筛选、分析和推送服务；

3）提供 7*24 小时应急响应服务，在各国家重大活动或重要网络安保时期提供驻场保障服务；

4）服务期为合同签订之日起一年，包括软件及病毒库、各安全模块等升级。

（二）网络安全监测防护系统续保及运维服务

1．主机安全防护与攻击阻断综合安全防护系统续保及运维服务

针对厅本级部署的应用主机综合防护服务和网络攻击阻断系统服务进行重点防护，为应对日益严峻的网络安全形势，有效防范外部渗透和恶意扫描威胁，实现重要互联网业务主机防护和网络攻击行为联防处置。同时，配套相关专业安全服务，包括国家重大活动或重要网络安保时期现场保障、安全运维巡检、日常监测防护、应急等服务内容。

a.维保内容：

1	应用主机综合安全防护软件	70 节点	1 年防护功能授权
2	网络攻击阻断系统 （对网络攻击行为进行联防处置）	1 套	含 1 年威胁预警数据服务
3	配套专业安全服务	1 套	包括特殊时期保障、安全运维巡

JSZKS2500508CN00

			检、安全监测、应急响应等

b. 服务要求：

1）应用主机综合安全防护软件

软件授权	提供自合同签订后一年期防护功能授权

2） 网络攻击阻断系统服务

预警数据服务要求	提供自合同签订后一年期威胁预警数据服务授权

3） 配套安全服务

本项目中标方须提供一年的配套安全服务，包括安全评估服务、安全运维巡检服务、安全监测服务、应急响应服务，具体服务内容及要求如下：

序号	服务项目	服务内容	服务频次
1	安全评估服务	结合主机应用综合防护系统和网络攻击阻断系统的安全防护数据开展一次安全评估工作，对被保护对象的整体安全状态进行评估。	2 次/年
2	安全运维巡检服务	针对主机应用综合防护系统和网络攻击阻断系统的运行状态及安全防护策略有效性每月开展一次安全运维巡检服务。	1 次/月
3	安全监测服务	**国家重大活动或重要网络安保时期，安排技术人员提供现场驻点保障**，并提供 7X24 小时远程安全监测服务。	按需
4	应急响应服务	国家重大活动或重要网络安保时期，提供 7X24 小时安全应急响应服务，以及在重要网站应用或服务器遭到攻击后，技术人员能够第一时间配合处置。	按需

4）服务期为合同签订之日起一年；

2. 高级持续型攻击及新型网络攻击行为分析防御系统续保及运维服务

高级持续型攻击及新型网络攻击行为分析系统续保，并提供专业服务团队的 APT 及其它未知攻击事件监测及处置服务。

a.维保内容：

项目	要求	频次
软硬件维保	硬件设备和软件版本的升级和维护	1 次/月
高级威胁狩猎与溯源	对内建的应用服务（wiki、zabbix、tomcat、oa、crm	1 次/月

ISZK2500060CGN00

系统（蜜罐系统）	等 12 种）支持系统服务（ssh、ftp、samba、mailbox 等 11 种）支持 Windows（Win7、WindXP、WinServer 2008）对应真实版本升级	
智能资产风险监控系统（巡哨系统）	最新的应用及服务漏洞验证脚本扩展，对资产进行管理以及扫描	1 次/月
主机安全防护检测系统（剑幕）	提供 110 个终端授权，对主机进行数据采集并有效发现阻断异常入侵行为，包含资产梳理、风险发现、入侵检测、响应防护等核心模块	1 次/月

b. 服务要求：

1）针对江苏省交通运输厅本级现有的高级持续型攻击及新型未知攻击行为防御系统提供定期巡检服务，包括系统运行状况、安全态势、黑客画像等，并提交巡检报告。

2）定期对核心应用的高级威胁事件进行现场分析及处置，并积累形成知识库。

3）国家重大活动或重要网络安保时期的现场支撑服务，结合产品对核心应用服务器的安全状态分析处置。

4）定期对感知节点的部署形式（端口、服务、位置等）调整，增强对 APT 及其它未知威胁的感知能力和感知范围。

5）提供产品一年质保和软件升级服务，包括系统资源池更新，其他系统新功能迭代的升级，提供 7*24 小时售后服务响应。

6）资产暴露面梳理服务：从攻击者视角，协助江苏省交通运输厅及下属单位梳理发现互联网暴露的资产以及第三方泄露的敏感信息，全面展现当前互联网资产暴露的风险点。收敛风险，提供解决建议。

7）定期梳理专网及互联网资产、应用并形成台账，动态更新。提供针对资产的风险态势监控，并给出专业修复意见，形成漏洞响应知识库。

8）为防患专网与外网交叉攻击，提供服务器主机底层防护。涵盖事前风险检查及加固，事中攻击发现及处置，事后取证与溯源等相关服务。

9）提供重大安全事件追踪溯源服务。从多维度（流量、日志、主动防御、自动化响应）、高精度、多协同出发，整合现有安全体系，在发生安全事件时，还原出恶意行为的大体原貌并提供技术支撑；

10）服务期为合同签订之日起一年。

3. 威胁预警系统续保及运维服务

维保服务内容及要求： 通过现有 IPS 系统及相关安全服务实时分析江苏省交通运输厅本级信

息系统和网络全流量，结合威胁数据及网络行为分析技术，深度检测所有可疑活动，并每月、每季度进行数据统计生成月度、季度报告以利报交通运输部和行业季度简报编制；服务期内每季度进行一次全面巡检并提交巡检季度报告；在**国家重大活动或重要网络安保时期**提供技术力量保障；提供相关设备一年质保。服务期为合同签订之日起一年。

4．云监测防护平台续保及运维服务

维保服务内容及要求：通过现有云监测防护平台系统，实时对厅本级部署于互联网有关系统进行 7*24 小时监测和防护，重点监测针对站点网站篡改、黑客入侵、信息泄露、0day 攻击、挂马等安全问题，在发生网络安全事件的第一时间通过技术人员及时提供攻击威胁处理和应急响应服务，恢复网站页面，保障网站的可用性和安全性；在重大活动期间提供技术力量保障；上述服务期限为合同签订之日起一年。

（三）网络安全设备续保及运维服务

全省各设区市及厅属单位边界等网络安全加固设备续保及运维服务

a．维保内容：

序号	设备型号	部署节点	用途	数量
1	启明星辰天清汉马 USG-12600GP	厅本级机房	省厅交通专网边界防护加固	2 台
2	启明星辰天清汉马 USG-3620EP	交通大厦、港航中心、苏北航务处、各设区市交通运输局边界	各接入单位交通专网边界防护加固	16 台
3	绿盟 ADSNX3-4000F-2010	厅本级机房	省厅交通专网防异常流量攻击	2 台
4	绿盟 RSASNX3-E	厅本级机房	交通专网整体安全扫描及基线配置核查系统	1 台
5	山石 WAF SG-6000-W3300	厅本级机房	应用防火墙	1 台
6	密钥管理系统 SYT1306	厅本级机房	密钥管理系统	1 台
7	SSL VPN 安全网管	厅本级机房	传输加密	2 台
8	签名验签服务器	厅本级机房	签名验签	2 台

9	深信服防毒墙 AF-2000-B2150	厅本级机房	各网络边界安全防护和防病毒	3 台
10	安恒日志审计 DAS-LOG-2800	厅本级机房	日志采集分析审计	1 台
11	深信服负载均衡 AD-1000-G642	厅本级机房	业务应用负载	4 台
12	山石防火墙 Z2300	厅本级机房	交通部网络链路防护	1 台
13	山石下一代防火墙 SG-6000-E2860	厅本级机房	公文交换防护设备	1 台
14	深信服数据库审计 DAS-1000-A640	厅本级机房	专网数据库审计	1 台
15	山石数据库审计 DBA2115	厅本级机房	互联网数据库审计	1 台
16	启明网闸 GAP-6000-6600BD	厅本级机房	网络隔离防护	1 台
17	深信服 VPN-1000	厅本级机房	VPN	1 台

b. 服务要求：

部署于厅本级以及与交通大厦、各设区市交通运输局网络边界等各类网络安全设备，提供一年续保（包括产品保修、系统升级、软件更新等）服务，同时提供巡检、日常联调、故障排修、应急处置等服务，服务期为合同签订之日起一年。

巡检要求：每季度对设备的工作情况进行梳理排查，对日志中的不合规信息进行分析筛选，定制不同的防护策略。

日常联调要求：根据交通专网业务发展情况，配合各交通专网部署节点单位对安全规则进行变更与适配，达到符合业务需求的安全标准。

故障排修与应急处置要求：当设备疑似故障时，供应商需在当天到达设备部署节点现场进行分析排查，确认为设备故障时，供应商需在 24 小时内提供不低于故障设备性能的备机并恢复业务。当发生如病毒、木马爆发等需到场处理的特殊安全情况下，供应商需在收到应急处置单后 2 小时内到达设备部署节点进行处理。

（四）外网异常流量清洗与抗 DDOS 攻击系统续保运维及应急演练等有关服务

a. 维保内容

序号	项　目	单位
1	2G 抗 DDOS 设备	1 台
2	4G 抗 DDOS 设备	1 台
3	相关安全服务	1 年

b. 服务要求：

针对厅本级互联网网络出口、备用网络及电子政务外网边界等 DDOS 攻击及异常流量威胁，为有效应对行业内频发的各类 DDOS 攻击威胁，对异常流量检测及处理，阻止黑客造成目标主机的 TCP/IP 协议层拥塞、或者导致应用层异常终止而形成拒绝服务的现象出现。面向厅本级外网网络、电子政务外网边界等需分别对网络层、传输层、应用层进行 DDoS 防护，网络层 DDoS 防护 包含:Land 防护、Smurf 防护、Winnuke 防护、分片攻击防护;传输层 DDoS 防护包含:端口扫描防护、SYN Flood 攻击防护、Conn Flood 攻击防护、ACK Flood 攻击防护、序号攻击防护、慢速攻击防护；应用层 DDoS 防护包含 :DNS Flood 攻击防护、HT TP Flood 攻击防护、CC 攻击防护。**国家重大活动或重要网络安保时期，安排技术人员提供现场驻点保障。**

同时随着 Web2.0 的到来，外网业务遭受攻击面变得越来越大，一旦网络受到 DDoS 攻击，将严重影响单位形象，甚至造成重大的政治经济损失和恶劣的社会影响。服务重点应对以下几类攻击进行防护：

a)利用 TCP/IP 协议的漏洞，消耗目标主机的系统资源，使业务过度负载。规避攻击者发起的几十兆甚至上百兆的攻击流量，避免造成业务彻底瘫痪。如 SYN Flood，UDP Flood，ICMP Flood 等等；

b)利用某些基于 TCP/IP 协议的软件漏洞，造成应用异常。规避针对某个软件特定版本的攻击；

c)规避不断尝试，频繁连接的野蛮型攻击。如 WEB Stress，CC Proxy Flood 等。

安全服务具体包含以下几个方面：

安全巡检服务

检查相关安全设备的各项运行指标和运行状态是否正常；查看各类安全设备的软件版本是否更新，并在得到管理人员同意的情况下协助对各项内容进行升级。

漏洞扫描

提供定期开展漏洞扫描服务，通过漏洞扫描验证安全设施效果的有效性，及时查出网络体系中存在的安全问题，避免发生严重的安全事件。提供的服务包括针对服务器、网络设备的漏洞扫描，

通过扫描去发现系统补丁、账号口令、共享目录、应用服务等多方面的安全情况，以及发现黑客可利用哪些应用层面的漏洞破坏应用系统。每月提供一次相关服务。

应急响应与应急演练

1）对抗 DDOS 设备提供 7×24 小时现场故障排除及安全维护工作；

2）应急安全事件的处理；

3）DDOS 调查及分析，协助检查和追踪攻击来源

4）对系统的安全进行重新评估；

5）消除未来的攻击隐患，提出安全整改建议，提供解决和防范报告并与技术人员共同实施；

6）应急事件应重点包括：DDOS 攻击、病毒、非法入侵、网页篡改等，在事故发生后应提交相应的调查报告：包括事故原因、过程描述、入侵来源、证据报告、解决方案、安全建议、处理结果等。同时提供相应的网络安全技术支持和咨询。每次事故处理后均作详细记录，记录中应详细描述处理流程；

7）演练服务：搭建模拟环境，提供年度网络安全事件实战应急演练服务，包括场景设定、方案设计、演练实施、总结等，进一步提升单位应急处置能力，提高突发事件发生时应急响应效率。

（五）第三方网络安全人员驻场服务

维保内容及服务要求：

要求提供一名网络安全专业技术人员驻场，对厅本级网络安全日常防护与保障技术支撑、应急处置、巡检加固等服务，对厅本级网络系统及应用系统进行日常监测预警和有效防护，对各类网络安全软硬件运维提供技术保障等。工作时间为 5*8（需提供加盖投标人公章的承诺函）。

投标人须在投标文件中提供驻场人员服务方案，做出详细描述，至少包括：网络安全日常监测、安全运维保障、安全测试、巡检加固、应急处置、隐患排查与处置、安全规划建设等内容。

网络安全专业技术驻场人员所具备能力包括：

1、熟悉各类 IT 系统环境下的安全规划、设计及实现，熟悉主流操作系统、数据库和应用程序的安全评估及加固，精通渗透测试流程，熟练运用 Kali、MSF、Burp Suite、AWVS、Nesssus 等主流安全工具；

2、熟悉常见安全系统的原理及使用，如：FW、IPS/IDS、WAF、防病毒、堡垒机、日志审计等，为我厅网络安全运维与监测提供有力保障；

3、驻场人员主要做好厅网络安全日常监测、安全运维保障、安全测试、日志分析、防护策略更新加固、应急处置、安全规划建设等工作，并在国家重大活动期间为厅本级网络安保提供专业技术支撑。

4、具备扎实的实战攻防能力与漏洞研究素养。在国家级、省级网络安全竞赛（如 CTF、攻防演练等）中取得优异成绩，或曾在主流 SRC（安全应急响应中心）平台上提交过高质量漏洞并获得证书。

驻场人员需设置 AB 角，作息时间参照江苏省交通通信信息中心具体要求执行（原则上为 5*8），同时特殊时期需参加信息中心值班备勤工作；驻场人员必须服从采购人的管理，包括工作时间、工作安排，严格执行请销假制度，在服务期内不得兼任采购人规定以外的工作；供应商应承诺保持所提供驻场人员的连续性和稳定性，如有特殊情况需要更换，供应商需提前两个月书面通知采购人，并经过采购人同意后方能更换；服务期满，向厅信息中心提交运维报告和工作总结。

JSZKS25005080GN00