江苏省政府采购合同（服务）

项目名称：江苏省交通运输厅 2025 年度应用系统类运维服务项目

项目编号：JSZC-320000-SCZX-G2025-0565

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）：联通（江苏）产业互联网有限公司
统一社会信用代码：91320106MA1WH7D7XE
法定代表人：曲扬

甲、乙双方根据江苏省政府采购中心江苏省交通运输厅 2025 年度应用系统类运维服务项目（项目编号：JSZC-320000-SCZX-G2025-0565）公开招标的结果，签署本合同。

一、合同内容

1.1 产品/服务内容：

序号	服务名称	分项单位	数量	服务期限
1	江苏省交通运输厅 2025 年度应用系统类运维服务（具体维护内容和要求详见附件）	套	1	合同签订后 5 个工作日内，按本项目要求提供相应服务，服务期限为一年

1.2 交付物：江苏省交通运输厅 2025 年度应用系统类运维服务
1.3 服务期限：合同签订后 5 个工作日内，按本项目要求提供相应服务
1.4 运维要求：按本项目要求提供相应服务
1.5 其他要求（如有）：附件 3

二、合同金额

2.1 本合同金额为（大写）：陆佰陆拾玖万玖仟圆（6699000.00 元）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（包含与服务相关的货物）的有关技术资料。

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，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同服务（包含与服务相关的货物）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。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的服务（包含与服务相关的货物）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

不涉及

七、合同转包或分包

7.1 乙方不得未经甲方同意将合同标的转包给他人履行。

7.2 乙方不得未经甲方同意将合同标的分包给他人履行。

7.3 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。

八、合同款项支付

8.1 合同款项的支付方式及进度安排

8.1.1 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%；

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%。

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 甲方依法组织履约验收工作。

10.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

10.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

10.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

10.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时，甲方按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付条

件挂钩。履约验收的各项资料存档备查。

10.6 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。

十一、违约责任

11.1 甲方无正当理由拒绝接受乙方提供服务的，甲方向乙方偿付拒绝接受服务合同价款总值5%的违约金。

11.2 甲方无故逾期验收和办理合同款项支付手续的，甲方应按逾期付款总额每日千分之六向乙方支付违约金。

11.3 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。

11.4 乙方所提供服务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。

十二、不可抗力事件处理

12.1 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，则合同履行期可延长，其延长期与不可抗力影响 期相同。

12.2 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。

12.3 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。

十三、解决争议的方法

13.1 双方在签订、履行合同中所发生的一切争议，应通过友好协商解决。如协商不成，由甲方住所地人民法院管辖。

十四、合同生效及其它

14.1 合同经双方法定代表人或授权委托代表人签字并加盖单位公章后生效。

14.2 本合同未尽事宜，遵照中华人民共和国现行法律法规有关条文执行。

14.3 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。

甲方：	江苏省交通通信信息中心	乙方：	联通（江苏）产业互联网有限公司
地址：	江苏省南京市秦淮区升州路16号	地址：	南京市建邺区庐山路230号
法定代表人或授权代表：	赵渝	法定代表人或授权代表：	
	2025年12月1日		2025年12月1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）：联通（江苏）产业互联网有限公司
统一社会信用代码：91320106MA1WH7D7XE
法定代表人：曲扬

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 厅协同办公平台 2024 年功能提升 项目（项目编号： YC2024-JC37307）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；

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：	联通（江苏）产业互联网有限公司
地址：	江苏省南京市秦淮区升州路16号	地址：	南京市建邺区庐山路 230 号
法定代表人或授权代表：	赵渝	法定代表人或授权代表：	
	2025年12月1日		2025年12月1日

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《中国人民共和国网络安全法》《中国人民共和国数据安全法》《中国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⑨其他信息技术的服务项目（可选填：①建设信息系统或云平台<以下统称“信息平台”>；②运维信息平台；③检查、监测、测评信息平台；④采购使用云计算服务；⑤采用社会网络平台提供对公服务；⑥采用社会网络平台发布政务信息；⑦采用社会网络平台实施社会管理；⑧采用社会网络平台处理党政事务；⑨其他信息技术）（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《中国人民共和国网络安全法》、《中国人民共和国数据安全法》、《中国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。

甲方：	江苏省交通通信信息中心	乙方：	联通（江苏）产业互联网有限公司
地址：	江苏省南京市秦淮区升州路 16 号	地址：	南京市建邺区庐山路 230 号
法定代表人或授权代表：	赵渝	法定代表人或授权代表：	
	2025年12月1日		2025年12月1日

附件 3：

具体维护内容及要求

一、维保需求

本次厅本级应用系统类运维服务包括江苏省一体化在线交通运输政务服务平台、厅网站维护、交通云运维、江苏省公路水路安全畅通和应急处置系统（含物联网卡通信服务费）、江苏省交通运输信用信息共享应用服务平台、江苏省交通运输科技管理系统-标准管理模块、江苏省交通运输管理系统-运输管理模块、江苏省交通运输管理系统-多式联运模块、江苏省交通运输管理系统-网络货运运行监测模块、交通服务热线、交通统计分析和投资计划管理信息系统、江苏交通建设管理信息系统-建设管理模块、江苏省交通运输建设管理系统-公路水路建设市场信用信息服务模块、江苏省交通办公管理系统-协同办公模块、江苏省交通办公管理系统-档案管理模块、江苏省交通办公管理系统-财务综合管理模块、江苏省交通运输厅短信平台、江苏省交通运输数字底座系统-视频联网监控平台、江苏省交通运输数字底座系统-地理信息服务平台模块、江苏省交通运输管理系统-危货监管模块、江苏交通运输电子证照系统等 21 项应用系统运维，厅网站内容监测、电子印章等 2 项通用平台运维以及全省航班动态等数据接口和服务费、百度路况、数据库日常运行维护、数据服务费、服务热线大数据分析、公安数据交换、数据质量治理服务、交通应急通信保障、运维，信息化系统提升项目管理、DSG 数据同步服务费、高德地图、信用信息共享应用服务平台目录修订和数据资源完善费用（单项目）、地理信息数据更新、部支撑跨省通办、部热线相关数据监测服务费、部电子证照系统对接服务费、数字交通统一平台页面优化等 15 项数据和服务工作，具体运维需求清单如下表所示：

序号	运维系统、数据、服务名称	维护内容及要求	维护方式及范围
一	应用系统类		
1	江苏省一体化在线交通运输政务服务平台	系统软件更新、补丁安装、数据管理运维、安全防护运维、应急处置	现场维护、远程维护；省、市、县
2	厅网站维护	厅网站日常维护、栏目调整、专题制作等。	远程维护；省级

3	交通云运维	系统日常巡检工作，包括人工巡检和自动巡检，进行平台功能检查及第三方应用健康检查；系统日常维护工作，包括平台缺陷修复、软件优化升级、安全加固，第三方应用对接等；移动端版本运维工作，包括新版本测试及正式版本发布，各大安卓应用市场及苹果应用商店上架更新；系统定期数据备份与恢复性测试，持续性用户培训，日常使用指导，故障响应	现场维护、远程维护；省级
4	江苏省公路水路安全畅通和应急处置系统（含物联网卡通信服务费）	平台日常维护、升级，定时数据测试，长期性用户体验改进，日常功能运维，异常迅速解决。	现场维护、远程维护；省级、市级、县级
5	江苏省交通运输信用信息共享应用服务平台	系统运行稳定性保障、用户支持和培训、应急响应和处置	现场维护、远程维护；省、市、县
6	江苏省交通运输科技管理系统-标准管理模块	交通运输标准文本资源采集、加工处理、资源入库；完善江苏省交通运输标准化信息管理系统标准体系标签设置及查询等功能。	现场维护、远程维护；省级
7	江苏省交通运输管理系统-运输管理模块	为省本级和各设区市的运政在线系统、企业服务平台和相关的数据库提供日常维护和巡检，定期进行数据备份与恢复性测试；并安排 10 人以上的技术团队持续为全省运输管理业务领域的管理人员、经营业户和从业人员提供系统使用与业务办理方面的指导、答疑和问题处理。	现场维护、远程维护；省、市、县
8	江苏省交通运输管理系统-多式联运模块	建立监控运维机制、数据安全防护和备份、制定完善的应急预案	现场维护、远程维护；省、市、县
9	江苏省交通运输管理系统-网络货运运行监测模块	系统日常维护、巡检、故障处理，定期数据备份与恢复性测试；与新的网络货运平台进行数据对接，并汇总数据按交通部要求上报。	远程维护、电话支持。省级
10	交通服务热线	系统日常维护、巡检，定期数据备份与恢复性测试，持续性用户培训，日常使用指导，故障响应。	远程维护、现场维护；省、市
11	交通统计分析和投资计划管理信息系统	对系统进行定期的功能测试、建立快速响应机制，及时处理用户遇到的问题和故障、定时开展数据验证和清理工作、故障应急响应	现场维护、远程维护；省级
12	江苏交通建设管理信息系统-建设管理模块	对系统进行软件优化、定期进行安全漏洞扫描、定期开展数据备份	现场维护、远程维护；省级
13	江苏省交通运输建设管理系	对系统进行性能监测和评估，定期数据备份与恢复性测试，制定完善的数据恢复策略，及时对系	现场维护、远程维护；省级

	统-公路水路建设市场信用信息服务模块	统功能进行优化和升级。	
14	江苏省交通办公管理系统-协同办公模块	系统日常维护、巡检，定期数据备份与恢复性测试，持续性用户培训，日常使用指导，故障响应。	现场维护、远程维护；省级
15	江苏省交通办公管理系统-档案管理模块	系统定期更新、检测，周期性数据备份，实时操作协助，问题应急处理。	现场维护、远程维护；省级
16	江苏省交通办公管理系统-财务综合管理模块	系统日常维护、巡检，定期数据备份与恢复性测试，持续性用户培训，日常使用指导，故障响应。	现场维护、远程维护；省级
17	江苏省交通运输厅短信平台	开展软件平台维护、数据备份与恢复、网络安全管理、系统性能监控等方面	现场维护、远程维护；省级
18	江苏省交通运输数字底座系统-视频联网监控平台	开展对监控平台的设备管理、系统维护、性能监控等	现场维护、远程维护；省级
19	江苏省交通运输数字底座系统-地理信息服务平台模块	最新的基础测绘成果数据、交通专题地理信息数据服务发布，平台日常维护、巡检，定期数据备份与恢复性测试，持续性用户培训，日常使用指导，故障响应。	现场维护、远程维护；省、市、县
20	江苏省交通运输管理系统-危货监管模块	系统日常维护、巡检，定期数据备份与恢复性测试，持续性用户培训，日常使用指导，问题应急处理	远程维护、现场维护；省、市
21	江苏交通运输电子证照系统	对系统进行日常维护、巡检；定期数据备份；建立快速响应机制，及时处理用户遇到的问题和故障；对报送省证照库的问题配合排查处理	远程维护、现场维护；省、市
二	**通用平台**		
22	厅网站内容监测	厅网站运行内容月度监测和季度普查。	远程维护；省级
23	电子印章	电子印章接口服务	提供 7*24 小时不间断的服务接口，提供接口对接、调试技术支持。省级
三	**数据服务**		
24	全省航班动态等数据接口和服务费	全省航班动态等数据服务购买。包含数据接口对接、接口调试、运维保障及故障处理，确保数据服务的稳定性和时效性。	提供 7*24 小时不间断的服务接口，提供接口对接、调试技术支持。省级

25	百度路况	百度路况数据服务购买。包含数据接口对接、接口调试、运维保障及故障处理，确保数据服务的稳定性和时效性。	提供 7*24 小时不间断的服务接口，提供接口对接、调试技术支持。省级
26	数据库日常运行维护、数据服务费	数据库日常运行维护、数据服务购买，保障系统运行稳定和数据安全。	现场维护、远程维护；省级
27	服务热线大数据分析	全方位深入挖掘分析交通服务热线 12328 数据，编制江苏交通服务热线 12328（月度、季度、半年度、年度）统计分析报告，以及重大节假日专题分析报告和重大节日交通出行信息预测报告、月度舆情分析报告等，为交通运输管理部门提供决策支撑。	现场维护、远程维护；省级
28	公安数据交换	实时向公安推送 15 张表，同时将公安提供的 5 个查询接口地址转换到省厅，维护中心提供省厅到联网中心到公安的链路保障和数据转换服务。	现场维护、远程维护；省级
29	数据质量治理服务	提供数据中心日常运营服务，主要包括全厅新建信息化系统数据资源的对接、归集、更新编目，新数据申请的对接、审核与共享接口开发，以及根据省大数据管理中心的新要求进行相关数据服务开发与挂接等工作。	现场维护、远程维护；省、市、县
30	交通应急通信保障、运维，信息化系统提升项目管理	提供交通应急通信保障及运维服务，做好信息化系统提升项目管理，提高项目管理质量和效率。	现场维护、远程维护；省级
31	DSG 数据同步服务费	DSG 数据同步服务费。	现场维护、远程维护；省级
32	高德地图	采购高德地图的 API 服务接口，为"江苏交通云"移动应用平台及其集成的各类第三方应用提供专业级的地理信息服务。包括高精度的矢量地图数据支持、实时定位功能以及相关地理编码服务，应用于平台的路线规划、实时导航、位置标注等核心功能模块。	现场维护、远程维护；省级
33	信用信息共享应用服务平台目录修订和数据资源完善费用（单项目）	对平台数据库涉及的建设市场和运输市场企业和人员基本信息、评价信息、资质信息、奖惩信息和双公示信息等共 152 个目录数据进行完善，支撑信用服务平台	现场维护、远程维护；省级
34	地理信息数据更新	提供全省交通时空信息要素运维服务，对门户子系统、数据管理子系统、地理信息服务子系统、运维管理子系统、综合地图子系统在内的 5 大子系统进行运维，支撑全省交通运输管理的地理信息服务	现场维护、远程维护；省级

35	部支撑跨省通办	提升互联网道路运输便民政务服务质量功能，提供道路运输数据质量提升支撑服务。做好与部级道路运政系统基础数据核对清理过程中的技术支持与咨询服务工作，加强部省业务系统数据协同，提高运政系统中数据准确率。	现场维护、远程维护；省级
36	部热线相关数据监测服务费	对 12328 业务受理类、办理类、回访及整改类、货车司机专属服务和业务数据报送管理类指标进行监控服务，提供日统计分析，问题指标查询	现场维护、远程维护；省级
37	部电子证照系统对接服务费	提供道路运输经营许可证、道路运输证等 9 类道路运输证照与部电子证照接口保障服务服务，对系统性能监控及优化，支撑开展统计分析服务	现场维护、远程维护；省级
38	数字交通统一平台页面优化	配合数字交通统一平台的发布上线，进行页面优化，配合做好相关宣传工作	现场；省级

二、维保服务要求：

按照《省交通通信信息中心关于进一步做好系统开发与运维有关工作的通知》（交通信〔2024〕30 号）有关要求，本项目对省交通运输厅 38 个业务系统和数据服务系统进行全面的运维服务。运维单位需接受信息中心领导，与用户单位、信息中心等相关方保持沟通与协作，应建立规范化的运维服务保障体系，制定运维相关管理制度，配备合格的运维团队，制定运维方案和运维计划，规范运维流程，并不断优化改进运维工作，协助信息中心建立有效的沟通和反馈机制，及时处理各方的需求和问题；同时针对用户单位反馈的问题，组织提出相应的改进方案和优化措施；及时引入新的技术和管理方法提升软件系统运维的质量，为软件运维工作提供有力的支持和保障。

对于正式运行或开展试点应用的系统，如果要进行功能调整、账号权限变更、数据修正、BUG 修复等运维操作，应当落实专人加强全流程闭环管理。

对于涉及重要数据报送和重大功能调整的运维升级，运维单位应当在测试环境充分验证,通过内部测试和用户测试，并按需组织第三方进行功能、性能测试。

在运维实施工作完成或系统更新发布前，对于可能影响系统功能的运维,运维单位应当提交测试验证报告给责任科室审核，内容包括:修改内容、影响性分析、验证截图等，审核通过后由信息中心相关科室签字确认，方可更新上线或发布。

运维操作完成后，信息中心将会同需求部门核实是否已满足运维需求，并在运维工单

上签字确认，形成闭环。

做好数据库建设和运维是保障系统运行稳定和数据安全的关键。运维单位要严格执行中心数据库建设管理有关要求，原则上应当使用中心统一提供的数据库,不得自建数据库。所有数据库的访问控制、硬件运行环境、剩余存储空间巡检等必须纳入中心数据库运维统一管理。

具体要求如下：

1、服务保障体系要求

供应商应具备完善的服务保障体系、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。提供高质量、高标准、高效率的技术服务。

具体包括：

（1）软件系统运行维护对象包括:平台支撑类、应用系统类和数据服务类进行全面的运维服务，建立相应的运维信息表，并且及时更新。平台支撑类：主要维护数据库管理系统和其他工具集，保证平台支撑类的稳定性、安全性、完整性和高性能；应用系统类：主要包括运输管理系统维护、厅门户网站维护、协同办公系统维护等系统；数据服务类：持续接入数据，保证数据质量可靠，开展数据资源动态运行监测和数据资源管理；以数据资源共享服务为基础，支持数据资源共享。

（2）为系统运维提供驻场、现场或远程运维服务、建议和技术指导服务；

（3）建立运维管理体系，包括人员管理、机构管理、运维管理、建设管理与制度管理等多个方面；

（4）建立运维技术体系，覆盖存储、虚拟化、操作系统、数据库等层面；

（5）针对不断发展的技术和运维手段，以及服务采购方提出的要求，提供相应的技术咨询服务，并提出相应的建议。

2、维保驻场服务要求如下：

根据实际需要提供驻场工程师进行厅大院（地址：南京市升州路16号）对重点系统的现场保障，负责系统的日常操作管理和技术维护保障，具体要求为：维保单位至少派驻3名技术熟练的工程师长期驻场交通运输厅维保单位工程师按照交通运输厅或各地市的作息时间按时上下班（原则上为5*8h），同时按要求参加节假日等值班备勤。维保单位工程师必须遵守交通运输厅工作制度和会议室操作管理制度；严格遵守相关保密制度。

A.驻场工程师应具有系统维护工作三年及以上的工作经验；

B.应熟悉交通运输厅的协同办公系统等重点系统，系统故障时需现场维修解决故障；

C.人员考核由采购方负责，驻场人员必须服从采购方的管理，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方以外项目的工作；

D.具有良好的沟通能力；

E.具有良好的团队合作精神；

F.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方，并经过采购方同意后方能更换。

3、服务响应时间要求

（1）提供7*24小时的技术支持和服务。10分钟内对甲方所提出的需求做出响应，一级故障要求半小时内到达现场（包含省厅和各设区市局等）。

（2）保证24小时（在不影响业务系统正常运转情况下最迟72小时）内解决故障问题，甲方特别要求除外。

4、日常巡检

日常运维包括技术运维和业务运维。技术运维是指维护系统软件的稳定性、安全性和性能优化，确保软件系统的技术环境可靠运行。技术运维由信息中心和运维服务单位联合开展。业务运维是指维护业务系统功能、业务流程及用户体验的顺畅性，确保技术与业务目标

对齐。业务运维由软件系统业务主管单位或部门、信息中心和运维服务单位联合开展。运维服务单位可采用人工巡检和自动巡检结合的方式，监控和分析软件系统运行状态和资源使用情况，及时消除问题隐患。巡检完毕应填写技术巡检报告，巡检发现问题应及时向信息中心主管部门报告。

依据不同类型的运维内容，及时记录并填写软件系统运行情况巡检记录单，建立运维台账。包括：平台服务类、应用系统类、数据服务类。在春运、全国两会、国庆等国家各重大活动期间，应增加系统巡检的力度，对系统进行全面检查，重点针对“两高一弱”问题清零安全漏洞。

服务期内定期对系统进行预防性巡检维护，包括检查系统状态、系统备份，以及与甲方工程师的技术交流。运维服务单位根据软件系统的分类分级情况制定技术运维方案报信息中心审定。技术运维方案应包括巡检计划、巡检内容、巡检频率等内容。其中，重要系统巡检频率不应低于 2 次/天，一般系统不应低于 1 次/天，巡检时间应在工作开始前半小时完成。运维服务单位按月将技术巡检报告和业务运维台帐汇总并形成月度分析报告。

定期数据备份与恢复性测试，数据更新和交换，定期数据备份与恢复性测试。

通过例行巡检能够及时发现并排除故障隐患，有效保证客户系统的正常运行。

数据服务采购方的实际业务需求、软硬件资源等情况，制定、审核备份和恢复策略。定期的系统和数据备份可以快速恢复业务应用，一旦系统故障可以把损失的风险降到最小。

经常化制度化的巡检可以保持双方技术人员的活跃接触，有更多的机会交流在系统使用及系统维护方面的经验，有利于提高系统维护的效率。

系统的安装、升级、补丁服务：系统（包含数据库系统、相关操作系统、安装包等）软件的安装等服务和软件的升级、补丁服务。

通用平台类日常巡检内容包括：平台所在的服务器运行状态、平台系统运行状态、数据库运行状态等。数据库维护内容包括：数据库补丁更新、性能监控和优化、故障处理、数据库健康状态检查、数据库存储管理、数据库碎片整理、配合应用开发人员处理相关数据库问题等。

应用系统类日常巡检内容包括：软件系统的一、二级功能、主要性能状态、安全性等。

数据服务类日常巡检内容包括：服务系统的数据报送、运行监测、数据交换、统计分析、数据资源加工与共享等。

运维服务单位采用多种线上或线下多种服务方式，为各级管理用户提供账号权限配置、业务流程配置等内部运维服务，为社会公众和从业人员提供政策咨询、业务指导、信息查询等外部咨询服务，并按日形成业务运维台帐

5、应用维护

维护包括系统修复和系统优化。系统修复是指对软件系统中存在的问题和故障定位、分析和修复；系统优化是指使系统功能、性能、安全性、用户体验等方面得到改进或提升。系统维护统一实行工单制。系统修复和系统优化上线前，运维服务单位应在测试环境充分测试和验证，经信息中心软件系统运维负责部门认定后正式上线。重要系统优化如影响面较大，信息中心软件系统运维负责部门应提请信息中心软件系统运维服务牵头管理部门和安全管理部门共同商定，并提供系统上线后的总结性报告

包括系统 bug 修复、需求修改、 账号权限配置等维护，记录并提交工单。

Bug 修复：对软件系统中发现的 bug 进行定位、分析和修复。包括：程序错误、逻辑错误、性能问题等；验证修复后的软件是否解决了 bug，并确保没有引入新的问题；bug 修复上线前，需进行必要的测试和验证。

用户需求修改：对于用户单位提出的较小规模需求，进行评估、分析和设计；实现用户需求的功能，并进行系统测试和性能测试。验证其是否符合用户期望。

账号权限配置：负责系统中账号的新增、删除、变更和赋权等维护工作；根据用户单位需求，创建新的账号并分配相应的权限；对不再需要的账号进行删除或禁用，确保系统安全；根据业务需求或用户变更，调整账号的权限设置。

6、系统安全

根据国家信息安全等级保护的规定和技术要求，按照服务采购方要求加强对软件升级

开发过程中的安全管理，制定系统安全设计方案，数据加密预备方案等，提供相关安全服务。在日常运维和重大活动的过程中，供应商需安排专业技术人员，对系统进行全面检查，补充完善系统漏洞，清零安全漏洞，即时排除相关隐患，确保系统安全。

运维服务单位的权限由管理员根据日常运维工作需要统一配置，并严格执行"专人专用、用后即销"的账号管理制度。各系统应明确一名运维联系人，并保障手机 24 小时畅通，做好系统应急保障。运维服务单位应妥善保管数据库账号和口令，不得以明文形式出现或移交他人使用。禁止未授权的数据库远程访问，对于已经批准的远程访问，应采用相关安全措施进行保障。

运维服务单位应对系统安装、设置更改、账号变更、表空间变更、数据对象变更、数据库备份等维护工作进行记录，以备查阅，执行关键操作时须有在场进行监督和确认。

运维服务单位应实时监控数据库的运行状态，识别存在的问题并及时处理解决，主动预防可能发生的问题，确保数据库系统安全运行，并保证数据的一致性和完整性。

运维服务单位应加强对系统维护过程中的安全管理。不得自行搭建测试环境，不得使用代码托管平台，严禁将代码上传到境外服务器存储。系统优化功能访问地址需对外开放的，应开展等保测评或渗透测试并完成整改，同时填报《防火墙对外映射资源申请表》后，方可上线运行。

要优化策略及软件版本，系统运行期间要避免因策略配置不当、应用软件质量问题等导致的系统安全事件。要做好日志留存要求，关联系统的数据库、中间件等的日志应保留不少于六个月。应履行数据安全和个人信息保护义务，规范数据获取和使用行为，不得将数据用于授权以外的场合。

运维服务单位应做好日常安全运维工作。严防“两高一弱”漏洞，加强日常安全巡检，定期组织病毒查杀、补丁更新、漏洞修复和版本升级等工作。日常运维工作应使用堡垒机授权账号进行登录，不得使用其他方式绕过江苏省交通运输厅安全管控访问业务系统，不得私自更改业务及运维服务端口，不得明文存储系统各类账号及口令信息。

运维服务单位应做好重要时期系统安全运行保障，在国家各重大活动期间，应增加系统巡检的力度，对系统进行全面检查，重点针对“两高一弱”问题清零安全漏洞，并配合信

息中心落实软件系统“白名单”制度，签订《软件系统安全隐患清零承诺书》。

7、故障处置

运维服务单位应根据软件系统分类分级情况制定相应的应急预案，并定期开展演练，避免或减少故障引起的严重后果。软件系统发生故障时，运维服务单位应第一时间通知信息中心并启动应急预案。对于系统瘫痪、宕机、数据丢失、中高风险安全漏洞等重大故障，原则上 1 小时内解决；发生其他影响系统正常运行或用户使用的一般故障，原则上 8 小时之内解决。对于严重影响业务的软件系统故障，信息中心应及时通知软件系统业务主管单位或部门，共同做好应急响应工作。故障恢复后的 24 小时内运维服务单位应提交软件系统故障分析报告，详尽描述故障原因及处理情况，并从源头杜绝下次类似事件发生。

8、提供持续性用户培训和相关技术支持

持续性用户培训和甲方技术人员培训，系统操作指导，帮助解答省厅及其他市、县级用户等用户提出的与系统使用操作相关的各种咨询问题，并能为相关业务系统的第三方对接开发单位提供相关技术支持。

三、档案管理要求

1、建立系统维护档案

对厅信息中心的所有服务范围内的维护系统，承保单位须建立相应的系统维护档案，并根据每次故障维修报告建立技术档案，记录每次故障相应服务、处理过程、处理结果和用户意见。

2、巡检维护报告

乙方根据各系统具体要求，按月（季度）委派经验丰富的系统工程师到厅信息中心，对其服务范围内的系统进行预防性巡检维护，并在两周内提供预防性巡检维护报告。

3、重大活动维护报告

针对重大活动期间，乙方应根据活动要求和系统情况，安排经验丰富的系统工程师到厅信息中心进行专人值班，及时处理突发情况，加强巡检力度，并在活动结束两周内提供重

大活动维护报告。

4、年度总结

中标人在每年维护完成后提供年度维护报告，在报告中需要提供本年度的主要故障次数统计、系统性能评估报告、系统维护建议及日常故障处理的报告单。年度报告作为年度付款重要依据。

四、质量考核要求

运维服务考核主要包括服务保障情况、系统安全、响应反馈、满意度 4 个方面，按百分制设置考核打分指标（附件 8）。考核得分 90 分以上，评价为“优”；考核得分 60~85 分，评价为“合格”；低于 60 分评价为“不合格”。

因运维服务单位原因出现重大责任或安全事故，造成严重损失或不良影响的，当年度考核为“不合格”。因运维服务工作出色被行业主管部门或被服务对象表扬或感谢的，酌情给予考核加分。

对于考核评价为“优”的运维服务单位，信息中心给予表彰，并在下一年度的运维服务招标中予以信用加分；对于考核评价为“不合格”的运维服务单位，信息中心责令整改，整改到位后才拨付全部运维服务经费，并在下一年度运维服务招标中予以信用扣分。