常州市公安局 2026-2029 年度数字集群通信系统维保服务采购项目

甲方： 常州市公安局　　**签订地点：常州市**

乙方： 中国联合网络通信有限公司 常州市分公司

签订时间： 2026年9月4日

根据常州市政府采购中心 2026 年 8 月 25 日进行的 JSZC-320400-JZCG-G2026-0251 号文招标，甲、乙双方就乙方中标的常州市公安局 2026-2029 年度数字集群通信系统维保服务采购项目，本着平等互利的原则，通过共同协商，根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及有关法律法规，就相关事宜达成如下合同。

一、服务清单

常州市公安局 2026-2029 年度数字集群通信系统维保服务采购项目 (JSZC-320400-JZCG-G2026-0251)涉及的维保服务及价格具体如下：

序号	服务名称	服务内容	单位	数量	单价	总价
1	硬件维保服务	硬件维保服务内容包括系统故障处理、系统日常巡检、设备维护保养、各类任务通信保障、技术支持服务、设备维修、终端设备管理等。设备维护保养、技术支持服务、设备维修服务和日常工作耗材（设备线缆、接头等）等均由供应商负责，并保证设备安全稳定工作。工作结束后，详细记录各类工作台账。	年	3	437000	1311000
2	驻场服	维保期内提供 2 名驻场技术人员常驻	年	3	310000	930000

	务	常州市公安局提供 6*8 小时现场技术服务，为了保障维保质量，驻场人员应每人配备 1 台远程图像传输终端用于实时记录外场工作，配套 1 辆驻场维护车辆用于外场工作。				
3	机房铁塔租赁	提供 21 座铁塔机房基础设施租赁，铁塔和机房位置由甲方根据数字集群通信覆盖情况合理布局，配套提供环境监控、设备用电及 UPS 保障、机房环境维护、安全管理、上塔维护等服务。若自有基站需要调整，供应商应免费提供相关服务。	年	3	480900	1442700
4	专用网络租赁	提供 1 套专用基础通信网络（拓扑结构图如下），该网络与其他有线网络物理隔离，实现市局数字集群通信系统交换中心与市区（天宁、钟楼、新北）所有 PDT 系统站点和市区外（武进、金坛、溧阳、经开区）汇聚中心的联网通信，包括网络链路 76 条、交换机 28 台、网络监控平台 1 套等。	年	3	161424	484272
总价（人民币：元）						4167972

具体服务要求见采购代理机构的招标文件。

二、合同金额及服务期限

合同金额：本次项目合同金额为人民币 4167972 元，大写：肆佰壹拾陆万柒仟玖佰柒拾贰元整，其中 3766536 元适用税率 6%，401436 元适用税率 9%。

服务期限：网络割接专项验收合格之日起三年。

三、合同文件组成

下列文件是构成合同不可分割的部分，并与本合同具有同等法律效力，这些文件包括但不限于：

1、JSZC-320400-JZCG-G2026-0251 号招标文件。

2、乙方提交的投标文件。

3、乙方投标的其他资料及承诺。

4、评标记录。

四、服务内容

乙方所提供的相关服务必须符合国家有关标准和JSZC-320400-JZCG-G2026-0251号采购招标文件和投标文件的要求。维保服务期间，乙方须提供完整的售后服务方案，包括服务内容、响应时间、服务流程、人员力量、支撑手段等内容。

1、硬件维保服务。硬件维保服务内容包括系统故障处理、系统日常巡检、设备维护保养、各类任务通信保障、技术支持服务、设备维修、终端设备管理等。设备维护保养、技术支持服务、设备维修服务和日常工作耗材（设备线缆、接头等）等均由供应商负责，并保证设备安全稳定工作。工作结束后，详细记录各类工作台账。乙方针对合同内万格设备提供原厂维保。

2、驻场服务。维保期内提供3名驻场技术人员常驻常州市公安局提供6*8小时现场技术服务，为了保障维保质量，驻场人员应每人配备1台远程图像传输终端用于实时记录外场工作，配套1辆驻场维护车辆用于外场工作。

3、机房铁塔租赁。提供21座铁塔机房基础设施租赁，铁塔和机房位置由甲方根据数字集群通信覆盖情况合理布局，配套提供环境监控、设备用电及UPS保障、机房环境维护、安全管理、上塔维护等服务。若自有基站需要调整，供应商应免费提供相关服务。

4、专用网络租赁。提供1套专用基础通信网络，该网络与其他有线网络物理隔离，实现市局数字集群通信系统交换中心与市区（天宁、钟楼、新北）所有PDT系统站点和市区外（武进、金坛、溧阳、

经开区）汇聚中心的联网通信，包括网络链路 76 条、交换机 28 台、网络监控平台 1 套等。

五、服务要求

1、日常巡检和中心值班要求

1.1 日巡检。每日早中晚三次对市公安局数字集群交换中心及各基站进行远程巡检，对基础通信网络进行远程巡检。

1.2 中心值班。每日在市公安局数字集群交换中心参与值守，值守时间 8:00-18:00，每日做好市局常用通信组号的值守监听，及时处置监听中发现的故障，配合甲方进行电台使用测试，对出现的故障及时报甲方并采取故障处理应急措施，降低故障影响。值班员应做好每日工作记录。

1.3 现场服务。对常州市公安局各单位反映的系统、电台使用问题及时受理，并进行现场服务，1 个工作日内作出实质响应，完成后 1 个工作日内提供现场服务情况记录。

2、设备管理要求

2.1 乙方为甲方建立规范化的基础信息管理维护体系，对设备档案信息、配置信息进行日常维护，保证系统基础运维资料的准确。

2.2 乙方需在签订合同后一个月内对所维保的设备进行全面排查并对设备布置和接线进行优化整理，建立和完善信息台帐：包括设备的资产、位置、状态等全生命周期信息和设备拓扑结构图等，并进行统一登记，建立完整的设备档案。对各类重要设备系统配置文件等进行备份，并以电子资料的形式提交。

2.3 维保期内，发生设备信息变化（如返修、调整优化等）的将在一个工作日内变更设备档案。

3、设备维护保养要求

3.1 系统维护。每三个月对维保设备、基站及所在机房环境进行现场巡检。三个月期满 5 个工作日内出具详细检查记录。

3.2 清洁保养。每三个月进行一次设备清洁保养及中心机房的清洁工作。三个月期满 5 个工作日内出具保养记录。

3.3 天馈系统检测。在维保期内，每座基站每年至少开展 1 次对天线及馈线的全面检测和上塔维护，并及时处理发现的问题，对天馈系统老化，驻波比超过 1.5 的天馈系统和功放设备及时更换，对天线固定器件松动脱落的应及时予以紧固。

3.4 信道设备维护。在维保期内，乙方应积极采取措施，在不影响用户使用的情况下，优化信道设备运行维护，确保信道设备保持良好运行。

3.5 优化维护措施响应。乙方应积极响应甲方的最新维护要求，不断优化维护措施，提升维保工作质态，5 个工作日内作出实质响应。

3.6 维护质量保障。乙方应确保维护保障质量，为驻场团队提供必要的工具装备、专业培训，签订合同后 10 个工作日内制定科学的工作规程，并取得甲方认可，后期根据系统运维情况协商优化。

3.7 终端管理。配合甲方对终端进行管理、优化升级和调整配置等，按照甲方制定的进度计划完成工作。

4、重大任务通信保障要求

4.1 重大任务保障前巡检。至少提前一天进行相关设备巡检、维护、测试，必要时进行任务现场信号测试等，及时形成任务前测试文档提交甲方。

4.2 重大任务保障要求。根据任务需要安排后台值守力量，按照

任务要求时间到岗，检查数字集群系统运行情况，任务中做好值守，任务中系统如有异常及时处置降低影响。特别重大任务，乙方需根据甲方要求增派工程师加强值守，结束后 2 个工作日形成任务保障记录提交甲方。

4.3 遇有甲方提出在重大保障任务区域进行数字集群通信信号临时增强需求的，任务开始前乙方须临时架设数字集群基站并通过独用有线网络通道接入常州市公安局数字集群交换中心，为该区域警力提供数字集群通信服务，并做好任务期间通信保障服务，网络通道由甲方提供。相关基站设备（基站控制器、信道机、合路器、分路器）由甲方提供的，天馈线、天线塔、机房及供电由乙方保障，服务次数根据常州市公安局通信保障任务需要。如基站设备需乙方提供的，甲方应提前 15 日通知乙方，服务次数不超过 3 次。

5、技术支持服务要求

5.1 根据常州市公安局各单位需求，对各单位开展电台使用现场培训，形成培训记录。

5.2 维保期内免费提供相关升级服务，对维保范围内集群通信设备提供原厂升级服务；维保期内确保防火墙 IPS 与防病毒功能启用，并保持威胁情报/特征库最新。

5.3 现场办公。每月安排项目组成员在常州市公安局现场办公，会商系统阶段性运行情况，对系统维护提出专业建议，形成会议纪要。

5.4 响应甲方提出的技术咨询，以及技术升级改造方案的建议。

5.5 本项目的维护保修服务通过对数字集群通信系统交换中心、基站、直放站等进行驻场技术人员定期主动式预防性维护，以提高数字集群通信的可靠性、稳定性；对存在问题及突发故障提供及时有效

的技术支持；不断完善解决方案和事前防范机制，使数字集群通信系统保持或迅速恢复其良好的工作状态；消除产生故障的薄弱环节，使数字集群通信系统更趋于稳定、安全。

5.6 新规范响应。如遇公安部及江苏省公安厅新出台或修订标准和规范的，乙方应按上级公安部门要求按期免费对数字集群通信系统进行完善，直至符合新的要求，相关调整不应影响警务通信的正常开展。

6、故障处理要求

乙方应在常州建设完备的备品备件库，提供 7*24 小时响应服务，制定完备可行的全天候保障方案。为做好故障排查工作，乙方应对系统进行必要的改进，完善系统运行日志、操作日志、通话录音等功能，确保通话问题及故障可追溯。

设备发生故障后，需 10 分钟内做出实质性响应，30 分钟内到达现场，一般故障（单基站通话容量降低少于 30%）24 小时内排除，较大故障（1 个基站不能正常通信）4 小时内排除，重大故障（2 个及以上基站不能正常通信）2 小时内排除。

发现故障设备短时间内不能修复的，乙方应按照先恢复、后维修的原则迅速处理。由乙方负责调取备品先行替换使用，保证甲方系统运行正常。乙方承担设备维护、维修、更换过程中所涉及的全部费用（含硬件、软件、系统调整以及设备间连接线缆接头的更换等）。

对于多次出现的影响电台使用的短时性问题，乙方应采取临时措施降低对应用的影响，并在 2 个工作日内制定排查解决方案，并得到甲方确认后，按方案约定进行处理。

所有故障在处理结束后 2 个工作日内应向甲方提供书面故障处

理报告。

7、基站优化配置和实施

在服务期内常州市公安局需要对基站频率、配置参数进行调整的，或涉及分合路器及信道机等设备改造的，乙方须根据甲方需求1个月内调整及改造完毕，并承担调整、改造所产生的全部费用。调整及改造期间，不得影响警务工作正常开展。

8、现场频率测试服务

在服务期内市区范围内发现频率干扰等情况的，乙方须免费提供现场频率测试服务，10个工作日内对受扰区域进行全面排查，找到干扰源头，消除频率干扰，保证常州市区350兆PDT数字集群通信系统通信畅通。

9、备品备件库

9.1 备品备件库建设。乙方应在合同签订后30个日历日内在常州建设完备的备品备件库，备件配置不低于维保设备清单内对应设备，在系统出现故障时能实现系统的应急抢修、恢复，备品备件库至少包含交换中心服务器1套、数字集群基站控制器2套，信道机6台，信道控制器6套，移动基站小型化射频共用系统1套，一近一远光纤直放站1套，高增益全向天线5对，交换中心交换机1台，汇聚交换机1台，基站交换机2台、防火墙2台。

9.2 除上述备件外，为提升基站运行稳定性，降低主要设备故障率，需在3年维保期间另外提供全新设备20套（每套含数字集群基站控制器1台、主控信道机1台、主控信道控制器1台）对现有20座基站（具体由甲方指定）的相应设备进行更换，所用新设备性能参数应不低于被更换设备（更换进度不低于：第一年7座基站、第二年

7 座基站、第三年 6 座基站）。

9.3 备品备件库管理。使用库内设备后，应在 10 个日历日内完成补充。

10、专用基础通信网络要求

乙方应对现有数字集群通信系统及专网进行充分的调研，降低专网割接对数字集群通信系统的停服风险，根据项目实际情况妥善专网服务方案，明确要割接新建和保留沿用的现有专用基础通信网络设备、链路等，保留沿用的须提供与原服务提供商达成一致的合同或协议，割接新建的按照“交付要求”完成交付。网络割接前，乙方应安排熟悉数字集群通信系统设备、具备丰富建设运维经验的原厂工程师和原专网服务提供单位，提前到达现场开展相关工作，共同完善割接方案。网络割接过程中，乙方须确保资料完整，系统平滑过渡，不得中断业务，原专网服务提供单位和原厂工程师须全程指导参与。相关联系协调工作以及由此所产生的费用（包括且不限于资料对接、网络费用等）均由乙方承担。

现有基础通信网络结构如下：

乙方应提供有线通信链路租赁 76 条，含市局主交换中心、备份交换中心间光纤链路 2 条，辖市（分）局汇聚中心、市区基站至主备中心光纤链路 51 条，信源站至直放站光纤链路 22 条，移动基站用 VPN 链路 1 条，4G 流量卡（50GB/月）2 张。所提供光纤链路需满足数字集群通信专网的衰减要求，确保主备交换中心与各汇聚中心、基站通信稳定高效，确保信源站至直放站通信正常；移动基站 VPN 配置合理，并配套通信流量卡 2 张，确保移动基站稳定接入运行。

为提高设备的可管理性、快速排查故障点，乙方配套提供一套网

络设备管理平台，用于监控专用基础通信网络内传输链路、交换设备的运行状况，实时管理、监控每一个通信端口。监控平台支持监控100台以上网络交换设备,并可根据需要扩展监控网络交换设备数量。

乙方应提供网络交换设备租赁28台，含交换中心核心交换机2台，辖市（分）局汇聚交换机4台，市区基站交换机22台。所提供相关网络交换设备均需符合或超过有关国际工业标准和国家标准。市局主换中心、备份交换中心间的通信链路带宽要求在1G及以上；辖市（分）局至市局主换中心、备份交换中间的通信链路带宽要求在100M以上；数字集群基站与市局主换中心、备份交换中间的通信链路带宽要求在100M以上。

- 各网络设备具体参数如下：

序号	设备名称	具体参数	数量
1	交换中心交换机租赁	10/100/1000M的电口≥48，可选4个1G或2个10G上联扩展插槽 交换带宽≥160Gbps 转发速率≥100mpps VLAN ID≥4K 支持多种路由协议，如：静态、RIP、OSPF、EIGRP、IS-IS、BGP、WCCP和FBR等 支持组播路由pim-dm、pim-sm，支持igmpv2、v3协议。	2
2	金坛、溧阳、武进、经开汇聚交换机租赁	10/100/1000M的电口≥24，可选4个1G或2个10G上联扩展插槽 交换带宽≥160Gbps 转发速率≥100mpps VLAN ID≥4K 支持多种路由协议，如：静态、RIP、OSPF、EIGRP、IS-IS、BGP、WCCP和FBR等 支持组播路由pim-dm、pim-sm，支持igmpv2、v3协议。	4
3	基站交换机租赁	接口数量为24个10/100/1000M，千兆光接口≥4 交换带宽≥216 Gbps 转发速率≥70 mpps Mac地址表　≥16K 路由协议：支持静态路由，静态路由数量不小于16条 支持组播协议：igmpv2、v3协议。	21

11、铁塔机房基础设施要求

为保持数字集群通信系统运行稳定和市区覆盖22座基站机房租赁原则上为现有机房，如需另选机房的，须取得甲方同意，并提供服务不受影响的搬迁方案，于合同签订后15个工作日内搬迁完毕。

所安装的基站设备用电由机房出租方提供,用电负荷应满足PDT基站使用需求。租赁期间内甲方需调整基站位置的，乙方需免费按甲方要求1个月内完成站址迁移及设备调整、安装调试工作，新选择的基站机房和铁塔需满足机房环境及配套基础设施要求。

12、驻场人员要求

12.1 维保期内提供3名驻场技术人员，为了保障维保质量，乙方可与万格厂家合作，提供万格厂家驻场技术人员，提供6*8小时现场技术服务。

12.2 驻场维护人员外场工作时必须佩戴远程图像传输终端，主要工作过程需录像保存备查。

12.3 乙方须承诺保持驻场工程师的连续性和稳定性。人员调整更换必须经甲方同意，中途更换人员需提前一个月告知甲方，待甲方批准后才可更换，以正式函件送达甲方并由甲方签字确认为准，更换的人员必须能胜任岗位工作需求并得到甲方同意,更换驻场工程师需根据岗位情况至少保证两周的工作交接期，保证甲方系统维护稳定性。

12.4 驻场工程师食宿自理，自行准备维护终端（维护期满后，硬盘不返还），驻场人员的工作的时间由甲方负责安排，包括正常工作时间、周末、节假日或夜间加班值班；驻场人员工作的所有费用（包括工资、因甲方工作安排产生的差旅费、加班费等）由乙方承担。

12.5 乙方必须符合甲方相关工作规范要求，驻场人员应按照甲

方管理要求进行日常工作。驻场人员考核由甲方负责，服从甲方的管理，包括工作时间、工作安排，严格执行请销假制度和甲方的管理规定，在服务期内不得兼任其他项目的维护工作。乙方应加强驻场人员管理，提升工作绩效。

12.6 维保期内提供 1 辆驻场维护车辆，车辆使用产生的全部费用（包括但不限于保险费、保养费、维修费、审验费、油费、违章罚款等）由乙方负责，用于本项目维修维护工作，车辆出厂时间不早于 2021 年，行使总里程不高于 10 万公里，车况良好，配备定位设备，可以实时查看当前位置和历史轨迹。该车辆日常由乙方驻场人员使用，驻场人员须具有车辆驾驶证，可熟练驾驶驻场维护车辆。

13、其他要求

13.1 乙方对派驻人员和临时施工人员做好日常施工管理，施工中注意生产安全，发生人身伤害等安全事故的，乙方负全部责任，甲方不承担相关责任。

13.2 乙方应保证高空设备设施固定牢固，维保期内发生高空设备设施掉落，造成人员伤亡、财产损失等情况的，由乙方承担全部责任，影响到甲方业务正常运行的，甲方保留进一步追偿损失的权利。

13.3 乙方执行过程中按照《常州市公安局科技信息化运行维护类项目管理办法（试行）》按时提供运维台账、巡检日志、阶段性维护报告等运维过程资料，交付物清单见附件 2。

六、验收标准和方法

1、交付要求：乙方须在项目中标（成交）后 10 日内，在投标响应文件的基础上提供符合“提供数字集群通信专网”、“专用基础通信网络要求”的专用基础通信网络、完整的专用网络测试方案以及切实

可行的网络割接方案，并通过甲方组织的第一次专项验收；验收通过后，乙方应在 5 日内完成基础通信网络割接，在割接过程中须保证数字集群通信系统正常运行，不得造成中断影响业务，割接完成后 5 日内通过甲方组织的第二次专项验收。验收合格后开始计算三年服务期，验收不通过甲方有权终止合同，并追究乙方法律责任。

2、第一次专项验收验收标准：

2.1 网络割接方案，割接工作实施时长不超过 5 日，割接过程中仍能为网内所有通信设备提供满足《江苏省公安系统警用数字集群（PDT）通信系统建设暂行规范》的基础通信网络，能满足业务不中断的要求，并有可靠的应急处理措施保证，相关工作措施、方法符合网络割接质量的通用技术要求。

2.2 网络测试方案，应符合《江苏省公安系统警用数字集群（PDT）通信系统建设暂行规范》中对基础网络的要求，割接后对所有在用线路进行端到端逐条逐项测试，每条线路测试时间不低于 2 小时，总测试长不高于 4 小时，应详细列出测试项目、测试指标要求、测试步骤等，相关测试方法符合网络测试的通用技术要求。

3、第二次专项验收验收标准：

3.1 检查所有割接工作已按照网络割接方案按时实施完成。

3.2 按照网络测试方案列出的项目进行逐项测试，须全部合格。

七、费用支付方式

预付款支付时间：合同签订后 15 日内，预付款支付比例：合同金额的 10%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

第二笔款支付时间：服务满半年后，款项支付比例：合同金额的

15%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

第三笔款支付时间:服务满一年并经服务考核后,款项支付比例:合同金额的 15%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

第四笔款支付时间：服务满一年半后，款项支付比例：合同金额的 15%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

第五笔款支付时间:服务满两年并经服务考核后,款项支付比例:合同金额的 15%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

第六笔款支付时间：服务满两年半后，款项支付比例：合同金额的 15%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

尾款支付时间：服务满三年并经服务考核后，尾款支付比例：合同金额的 15%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

八、违约责任

1、甲方无正当理由拒绝接受乙方提供的合同标的的，甲方向乙方偿付拒绝接受合同价款总值 10%的违约金。

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 5‰每日向乙方支付违约金，但最多不超过合同总价款的 10%。

3、乙方逾期交付合同标的的，乙方应按逾期交付合同总额每日 5‰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 个工作日不能交付合同标的的，甲方可单方面解除合同，按合同终止的约定处理。

4、乙方交付合同标的的标准不符合合同规定及磋商文件规定标准的，甲方有权拒绝接受合同标的，并可单方面解除合同，按合同终止的约定处理。

5、乙方在基础网络割接或运维过程中，不得造成甲方数字集群通信系统业务中断，一旦出现属于严重事故，甲方有权终止合同，由此引起的一切损失由乙方承担。

6.合同中止指因政策变动、需求调整、乙方整改不力、不可抗力或双方协商一致等特定原因导致项目暂时无法实施，待因素消除后恢复的情形。中止期间合同关系存续，工期相应顺延。提出方需制定包含原因、责任认定及资产清单的处置方案，经甲方审批后发出《中止通知书》。乙方收到通知后应暂停新增投入，保留必要应急值守，并做好资产盘点与保护。费用承担遵循过错原则：非过错方原因由双方协商，乙方过错则由乙方承担。中止因素消除后，甲方发出《复工通知书》，双方确认顺延工期及费用，并在复工前完成关键系统健康检查。

7.合同终止指因政策导致实施必要性消失、外部环境变化致使目标无法实现、不可抗力、乙方经整改仍不合格或严重违约等情形，导致项目无法继续或目标落空，双方解除合同关系。提出方需制定处置方案，经甲方审批后签订《项目终止协议》；若协商不成，甲方可依法启动行政处理、诉讼或仲裁程序并保全证据。终止后需进行清算与交接：乙方须移交所有运维文档、账号及配置脚本，并配合完成 15-30 天的重叠期交接以确保服务平稳过渡。若因乙方违约终止，甲方有权

扣留履约保证金及未付款项作为赔偿，并委托第三方承接后续服务，超额费用由乙方承担，如因乙方原因致使合同终止且乙方未支付履约保证金的，乙方应向甲方偿付合同总价款10%的违约金。双方需将全过程资料建档备查。

九、网络安全和保密要求

1、网络安全责任

1.1 基本安全要求

1.1.1 乙方应针对本项目设置安全负责人岗位，全面负责和管理本项目的网络安全相关工作。

1.1.2 乙方须承诺在本服务中所使用的服务工具满足以下供应链安全管理要求：

a）服务工具具备一定的安全性，有资质证明或者甲方认可，不存在已知安全问题；

b）服务工具应在《网络关键设备和网络安全专用产品目录》中并通过认证；

c）服务工具的版权合法且授权在有效期内，运行状态良好；

d）服务工具均有对应的详细使用方法，并已对工具使用人员进行技术培训；

e）定期检验服务工具的安全性，包括对工具进行杀毒、对工具产生的网络流量进行分析等，避免工具存在有害功能，以及隐蔽的链接、协议或者端口；

f）密切关注服务工具及其组件的安全漏洞公告和相关信息，在发现漏洞被披露时，第一时间评估漏洞的影响，采取更新补丁、下线工具等措施，以确保此类安全漏洞不影响服务涉及的系统或者平台。

1.1.3 乙方须承诺参与本服务中的相关人员满足以下供应链安全管理要求：

a）服务项目负责人须具备 2 年以上相关经验；

b）服务人员能够理解和应用相关的法律法规、政策和标准；

c）服务人员满足《信息安全技术 网络安全从业人员能力基本要求》（GB/T 42446）中关于网络安全运营类人员的要求；

d）服务人员已接受岗前培训并经考核评定合格后上岗；

e）已与服务人员签订保密协议，约定服务项目实施中的通用保密要求，并会定期进行安全保密教育。

1.1.4 在本服务中，乙方应持续关注安全领域的技术动态和威胁情报，保持服务技术的先进性。

1.1.5 在本服务中，甲方应定期对服务技术进行评估和升级，不断更新和优化服务工具和服务方案，以确保服务的安全性和有效性。

1.1.6 在本服务中，乙方应深入调研甲方现状和需求，提出可行性高的服务建议并提供定制化的安全服务方案。

1.1.7 乙方应配合甲方对其开展的远程检测和现场检查。

1.2 信息防泄露

1.2.1 “信息防泄露”是指在本服务中防止与甲方相关的敏感信息、保密信息或者未公开的信息在未经授权的情况下被透露、传播或者获取，包括但不限于个人身份信息、网络拓扑、系统/软件信息、知识产权、技术方案等电子及纸质材料。

1.2.2 乙方须将涉及服务内容的 U 盘等存储设备进行加密处理。

1.2.3 禁止乙方在本服务中将涉及服务内容的纸质材料带出甲方指定服务场地，如需带出，须向甲方申请（材料类型、使用时间、使

用目的、归还时间、责任人），批准后方可带出场地。

1.2.4 乙方应当采取技术措施和其他必要措施，确保其网络和数据安全，防止出现信息泄露、毁损、丢失等风险。在发生或者可能发生信息泄露、毁损、丢失等情况时，应当立即采取补救措施，并将相关情况及时告知甲方。

1.2.5 甲方有权利对乙方服务人员的身份背景进行安全审查，包括但不限于主合同要求具备的学历、学位、专业资质证书和过往工作经验要求以及安全保密协议签字等方面内容，乙方须配合提供与本服务相关的证明审查材料，存在泄密风险的乙方服务人员不得参与本服务。

1.2.6 本服务所涉及的乙方服务人员均须与甲方签订保密协议，乙方应做好人员安全保密教育工作，因服务人员违规恶意泄露敏感信息，所产生的相关法律责任由乙方承担。

1.2.7 乙方在本服务中处理或者存储甲方数据时，应采用国产加密算法对数据进行加密处理，并确保数据传输过程的安全性。

1.3 人员操作

1.3.1 “人员操作”是指乙方服务人员在本服务中的现场及远程技术行为，包括但不限于上机操作、运行自动化脚本、应用安全测试、漏洞扫描测试、渗透测试以及接入测试设备等。

1.3.2 在本服务中，甲方应对服务人员实施最小权限原则，确保乙方服务人员仅拥有完成任务所需的访问权限。

1.3.3 本服务中所包含的运营、运维的信息系统、应用、数据库等，乙方开通相关账号、权限等必须经过甲方审批允许，不得私开账号、擅自更改权限等。

1.3.4 乙方应合理使用操作账号，本服务中严禁存在多名人员（2人及以上）共用一个操作账号的情形，同时操作账号应采用高强度的口令，乙方应妥善保管口令并定期（每月至少一次）更新账号口令，不得在电脑终端桌面存放账号口令信息。

注：高强度口令应满足以下基本条件：

a）口令长度至少为 8 位；

b）包含大小写字母、数字和特殊符号的组合，例如@#$%^&*()_+;

c）避免使用连续的某个字符（如 AAAAAAAA）或者重复某些字符的组合（如 abcdabcd）;

d）避免使用姓名、手机号、生日等个人信息作为口令，包括父母、子女和配偶的姓名和出生日期、纪念日期等。

1.3.5 未经甲方允许，乙方不得对服务资源私开端口，不得利用服务资源进行与本服务无关的工作，不得将公安网络和互联网私自打通。

1.3.6 乙方派驻的服务人员应按照甲方要求办理入场、离场等手续，并且遵守甲方劳动、工作纪律、安全管理制度和保密制度，并按照甲方要求的工作时间进行出勤。

1.3.7 在乙方服务人员进行上机操作时，须由甲方调取数据，服务人员读数据，操作结束后双方复核签字确认。

1.3.8 在本服务中需要在甲方真实网络及业务环境中运行自动化脚本前，须经甲方审核脚本对系统的影响，待审核通过后，乙方方可实施，且在操作结束后双方复核签字确认。

1.3.9 乙方在本服务中进行应用安全测试时如需分配高权限账

户，甲方必须在场监督，操作结束后双方复核签字确认。

1.3.10 乙方在本服务中进行漏洞扫描测试时，须填写《漏洞扫描申请单》，不得进行拒绝服务和溢出等对系统影响的测试，并对应用状态进行监控，操作结束后复核签字确认。

1.3.11 乙方在本服务中进行渗透测试时，不得进行对系统正常运行有影响的测试，不得留后门和木马，并提前通知甲方进行相关数据备份和系统状态监控，操作结束后复核签字确认。

1.3.12 乙方在本服务中需接入测试工具时，须制定详细接入方案，由甲方审核，接入时由甲方指定人员监督，操作结束后复核签字确认。

1.4 第三方安全

1.4.1 “第三方安全”是指独立于甲乙双方的公司或者组织提供的服务、产品或者评估的安全性。

1.4.2 当发现所使用的第三方服务或者软件存在安全漏洞时，乙方须立即评估漏洞影响，采取更新补丁、下线工具等措施，以确保此类安全漏洞不影响本服务涉及的系统或者平台。

1.4.3 乙方应与可靠的第三方供应商合作，并签订明确的安全责任协议，在服务过程中明确因第三方的问题导致发生信息泄露等安全事件，甲方有权对乙方进行追责。

1.4.4 乙方须对所使用的第三方服务或者软件进行安全审查和定期的安全评估，建立及时更新和补丁管理流程，保证所有组件保持最新状态，确保所使用的第三方服务和组件符合甲方的安全标准。

1.5 服务方案变更

1.5.1 “服务方案变更”是指在主合同中甲乙双方约定的服务期

限、服务内容和实施计划因外界因素发生变化和调整。

1.5.2 在本服务中，若甲方需要变更服务方案、服务范围或者增加服务内容，造成工作量增多，应提前与乙方充分协商、考虑进度因素，适当延迟工期或者增加人力，保证服务进度。

1.5.3 在本服务中，乙方应提供充足的人力资源、人员备份，以应对人员工作调动等因素造成减员的影响，保证服务进度。

1.5.4 乙方应建立健全本服务标准化交付的流程和模板，并在服务过程中严格按照标准流程实行，减少因方案变更、范围变更、人员变动、外部因素等导致的服务进度波动。

1.6 服务商变更

1.6.1 “服务商变更”是指甲方因成本、服务质量、技术能力等原因决定更换服务提供商。

1.6.2 产生服务商变更时，原服务商与新服务商需进行工作内容的交接，具体交接内容包括但不限于以下内容：

a）服务终止时，原服务商需与甲方签订数据删除协议，确保所有遗留数据被安全删除；销毁存储介质时，乙方应当邀请甲方派员到现场全程监督，并制作销毁记录，由双方签字确认。

b）服务终止时，甲方应立即变更服务账号密码，同时撤销原服务商的所有访问权限；

c）服务终止时，原服务商应立即转交涉及甲方业务和敏感数据的所有材料，包括但不限于网络拓扑、系统软件信息、实施方案、应急处置方案、服务日志、巡检报告等，并禁止备份留存和外发；

d）服务终止时，原服务商须基于甲方现状，出具运维运营与安全服务报告，详细梳理服务现状以及现存的遗留性问题及风险，并与

甲方、新服务商三方开会同步，达成一致后方可退出。

1.7 业务连续性

1.7.1 “业务连续性”是指甲方在面对突发事件、灾难或者其他中断情况下，能够持续提供关键业务和服务的能力。

1.7.2 在本服务中，乙方须提前制定和实施业务连续性计划和灾难恢复计划，包括数据备份和系统冗余，并测试恢复流程，确保在突发事件发生后能快速恢复业务连续性。

1.7.3 乙方须在甲方参与下制定应急预案，并定期组织演练测试，确保在突发事件发生时能够迅速启动应急预案，减小影响面。

1.8 应急响应

1.8.1 “应急响应”是指甲方在面对安全事件或者危机情况时，乙方采取的一系列计划、策略和行动，以快速、有效地识别、评估、控制和解决安全事件，从而减轻事件对甲方的影响。

1.8.2 乙方应建立快速应急响应机制，并根据突发事件风险等级（一级至四级）设置不同层级的应急处置预案，确保在发生安全事件时能够及时监测发现、应急处置并向甲方报告。

1.8.3 乙方在服务过程中涉及甲方业务系统时，应提前与甲方协调，制定详细的维护计划和变更管理流程，最小化对甲方业务的影响。

1.8.4 乙方在本服务中，应实施性能监控和优化措施，确保甲方的服务水平协议得到满足。

1.9 其他

1.9.1 乙方应按照《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》《中华人民共和国密码法》《网络数据安全管理条例》《关键信息基础设施安全保护条例》

《商用密码管理条例》等法律法规及规章制度的要求，履行网络和数据安全保护义务。

1.9.2 合同有效期内，由乙方服务不到位造成的安全事件由乙方承担安全责任。

2、保密要求

2.1 乙方须与甲方签订安全保密协议，落实公安网络安全及信息保密的各项规定。

（1）乙方应做好文档资料（含电子文档资料）的管理工作，不得向第三方透露涉及本项目线路、机房、点位、业务等内容。

（2）未经甲方允许，乙方向第三方提供（直接、间接、口头或书面等形式）涉及保密内容的行为均属泄密，将追究乙方责任。

（3）乙方不得有其他任何危害公安信息安全的行为。

2.2 公安业务系统数据属于公安秘密，乙方应当严格遵守相关规定，严禁泄漏公安秘密，未经甲方确认，乙方公司人员不得对甲方业务系统作任何操作，参与本项目人员必须做到以下几点：

（1）只在规定的区域实行规定的工作，不得进入与之无关的工作区域；

（2）不得在机房设备上建立与工作无关的网站、网页和服务；不得在设备中传输、粘贴有害信息或与工作无关的信息；

（3）不得擅自对设备进行扫描、探测和入侵信息系统；

（4）不得对工作信息和资源越权访问、违规使用；

（5）不得私自允许他人接触和使用机房设备；

（6）严禁将工作用设备和文件带离机房；

（7）未经机房管理部门同意，严禁以任何方式和介质拷贝服务

器上的任何信息及项目中涉及的信息；

（8）对工作中接触到的信息做到保密。

十、考核要求

服务考核分为日常考核和专项考核两项,考核分为三个年度，即服务每满一年考核一次，每年度考核要求如下。

1、日常考核

维保服务质量实行按三个月为一个周期的定量考核制度，考核打分办法如下：

（1）日巡检值守服务（10 分）

完全按照甲方规定的流程进行日巡检的不扣分，发生一次未遵循规定流程巡检或者不巡检的，扣 0.5 分，发生 2 次的扣 2 分，发生 3 次的扣 5 分，超过 3 次的，本项分值扣为 0 分。

（2）季度巡检维护保养服务（10 分）

完全按照甲方规定的流程进行季度巡检的不扣分，发生一次未遵循规定流程巡检或未完成巡检的，超期一天扣 1 分，直至本项分值扣为 0 分。

（3）重大任务通信保障服务（15 分）

完全按照甲方规定的流程进行重大任务保障工作的不扣分，发生一次未遵循通信保障要求的，每次扣 5 分，直至本项分值扣为 0 分。

（4）故障响应处理（30 分）

发生重大及严重故障在时，非值班期间到达现场时间不超过 30

分钟。（每迟 10 分钟扣 1 分，直到本考核期得 0 分）

对甲方根据合同提出的人员、设备需求，乙方未及时有效响应的，每次扣 5 分，直到本考核期得 0 分。

重大故障，业务恢复时间不超过 2 小时，每超过 30 分钟扣 5 分，直至本考核期得分为 0 分。

较大故障，业务恢复时间不超过 4 小时，每超过 1 小时扣 2 分，直至本考核期得分为 0 分。

一般故障，业务恢复时间不超过 24 小时，每超过 1 小时扣 1 分，直至本考核期得分为 0 分。

短时性问题，2 日内未提出双方认可的排查方案或未按排查方案严格执行的，排查期后该问题没出现 1 次 1 分，直至本考核期得分为 0 分。

因乙方操作失误导致所维保设备或其他相关设备出现故障，正常运行的业务受影响或者不可用，按照影响情况扣 1-10 分/次，直至本考核期得分为 0 分。

（5）文档提交及时性(15 分)

每日巡检记录（发生 1 次未按要求记录的扣 1 分，直到本考核期得 0 分）。

外场服务情况记录（每迟 1 天扣 1 分，直到本考核期得 0 分）。

故障报告（每迟 1 天扣 1 分，直到本考核期得 0 分）。

季度服务报告（含详细检查记录、保养记录）（每迟 1 天扣 1 分，直到本考核期得 0 分）。

任务保障记录（每迟 1 天扣 1 分，直到本考核期得 0 分）。

（6）驻场人员管理（20 分）

驻场人员须按照甲方要求正常上下班；

每出现 1 人/次迟到、早退扣 1 分；

每出现 1 人/半天旷工扣 5 分；

办公区域不整洁、着装不规范等，发现 1 人/次扣 1 分；

未按时完成交办任务的，每 1 人/次扣 1 分；

交办任务不执行或不完全执行的，每 1 人/次扣 1 分；

未按要求佩戴远程图像传输终端并录像的，每 1 人/次扣 1 分；

被所在部门或上级部门检查发现或通报批评的，每 1 人/次扣 10 分；

以上扣分至本项分值扣为 0 分。

（7）加分奖励（15 分）

针对系统维护提出优化建议，得到甲方认可的，并协助甲方落实的，加 5 分。

本考核期内没有出现任何故障，加 5 分。

开展技术培训，加 3 分。

获得甲方书面表扬的，加 5 分。

本项加分上限为 15 分。

（8）一票否决项（扣 100 分）

乙方触犯以下任意一条，甲方都可以执行一票否决。

乙方发生违反公安相关管理规定的；

乙方发生违反保密协议规定的；

巡检及故障处理中违规操作，造成甲方设备损坏、数据丢失等严重后果的；

遇到设备故障，故意拖延处理，导致严重后果的；

在巡检报告、故障处理报告等文件中弄虚作假，情节严重的；

乙方在合同执行中有触犯法律法规的其他情形。

每考核期得分=100-（日巡检值守服务+季度巡检维护保养服务+重大任务通信保障服务+故障响应处理+文档提交及时性+驻场人员管理+一票否决项）+加分奖励。每考核期得分最高 100 分，最低 0 分。

结果应用：连续两个考核期得分低于 80 分的，甲方有权终止维保服务合同。日常考核年度得分（每考核期得分之和/4），低于 95 分的，扣除该年度合同应付款的 5%。

2、专项考核

（1）甲方在合同服务期限内随机抽查考核。按附件 2《科技信息化运行维护类项目交付物清单》的内容进行抽查考核，如发生一次乙方未能按磋商采购文件提供相应服务并整理形成规范记录的，则每次按照 1000 元扣款，每累计三次未按要求提供服务的可追加扣款 2000 元。

（2）因甲方未按要求提供服务，造成甲方损失或产生严重影响的，则每次酌情扣款 4000-20000 元，并赔偿甲方损失，同时甲方有权依照法律程序解除合同，并追究乙方的违约责任。

（3）在上级公安机关对常州市公安机关数字集群电台通信时，因乙方工作失误发生绩效扣分或被上级公安机关通报的情况，每次酌情扣款 4000-20000 元。

（4）乙方未按 “设备管理”、“信道设备维护”、“优化维护措施响应”、“维护质量保障”、“网络监控平台要求”、“铁塔机房基础设施要求”、“基站优化配置和实施”、“现场频率测试服务”、“备品备件库建设”要求按时保质完成的，每晚一天扣 1000 元。

5）乙方未按“现场办公”要求和投标承诺响应的，每人每天扣 1000 元，响应质量较差的扣 1000 元。

6）乙方未按“新规范响应”完成工作的，每晚一天扣 5000 元。

7）乙方未按“保持驻场工程师的连续性和稳定性”的要求按期履行相关义务的，按每人/天 500 元扣款。

8）乙方未按“天馈系统检测” 完成工作的，每少一站扣 1000 元。

9）除上述情况外，发生其他乙方未按采购文件要求履行义务情形的，每次按照 1000 元扣款。

10）下一年度维保开始前，如果维保设备、服务范围发生较大变化的，双方根据具体变化情况协商核定。

十一、不可抗力

1、 “不可抗力”指在本协议签署后发生的、本协议签署时不能预见的、其发生与后果是无法避免或者克服的、妨碍任何一方全部或者部分履约的所有事件。上述事件包括地震、台风、水灾、火灾、战

争、流行病、罢工，以及根据法律认作不可抗力的其他事件。

2、 如果发生不可抗力事件，影响一方履行其在本协议和项目合同项下的义务，则在不可抗力造成的延误期内中止履行，该遭受不可抗力的一方不承担违约责任或赔偿对方因之而产生的经济损失。

3、 宣称发生不可抗力的一方应迅速书面通知另一方，并在其后的十五天内提供证明不可抗力发生及其持续时间的足够证据。

4、 如果发生不可抗力事件，各方应立即互相协商，以找到公平的解决办法，并且应尽一切合理努力将不可抗力的影响减少到最低限度。

十二、合同纠纷处理

1、凡涉及本合同或因执行本合同而发生的一切争执，应通过协商解决。

2、如果协商不能解决，则提交常州仲裁委员会进行仲裁。该仲裁是终局的，对双方均有约束力。

3、争议在处理过程中，除正在进行仲裁的部分外，合同的其他部分将继续执行。

十三、合同生效

本合同经甲、乙双方盖章签字后生效，如有变动，必须经双方协商一致后，方可更改。本合同一式肆份，甲方贰份，乙方贰份。

其他未尽事宜，参照相关法律，甲乙双方协商解决。

(此页无正文)

甲方：常州市公安局（盖章）

代表：

地址：常州市龙锦路 1588 号

日期：　　年　　月　　日

乙方：中国联合网络通信有限公司常州市分公司（盖章）

代表：

地址：常州市通江南路 168 号

开户银行：

账户号：

日期：　　年　　月　　日

附件 1：维保设备清单

序号	设备名称	品牌	规格型号	数量	单位
1	核心网交换中心	万格	VT-3100	1	套
2	网管中心	万格	VT-3400	1	套
3	路由器	华三	RT-MSR3620	1	套
4	以太网交换机	华三	LS-3600V2	1	台
5	录音服务器	万格	VT-3630	1	套
6	调度服务器	万格	VT-3610	1	套
7	位置定位服务器	万格	V-3620T	1	套
8	UPS	Reros	KCRT-10K	2	套
9	E1 光端机	恒信和安	DDT-D-T/R16E1S	2	对
10	E1 光端机	恒信和安	DDT-D-T/R4E1M	6	对
11	E1 光端机	恒信和安	DDT-D-T/R4E1S	2	对
12	基站控制器	万格	VT-3300	43	套
13	信道控制器	万格	VT-3810-C	117	套
14	信道机	万格	VT-3810	109	套
15	网络交换机	华为	S2700	6	台
16	合路器	万格	VT-3220	112	路
17	分路器	万格	VT-3210	120	路
18	高增益全向天线	西南通讯	TQJ-350H	40	根
19	UPS	Reros	KCRT-6K	11	套
20	基站链路控制器	万格	VT3260	6	套
21	链路自动切换设备	银讯	ZMUX-124S-2E1	2	套
22	集群同播中心控制器	万格	VT3261	2	套
23	路由器	H3C	RT-MSR2600-10	3	台
24	路由器扩展板卡	华三	RT-HMIM-8E1T1-F	1	张
25	网络交换机	华三	SMB-S2626	3	台
26	馈线	珠海汉胜	7/8”普通馈线	3000	米
27	信道电源	万格	VT-3810-PW	1	台
28	基站控制器热备热切软件	万格	hotBackUp.jar	36	套
29	数字常规信道单元	万格	VR9000	2	套
30	近端机	万格	VIG-F0800J4	3	台
31	远端机	万格	VIG-F0800Y	12	台
32	近端机	万格	VIG-F0800J1	1	台
33	远端机	万格	VIG-F0800Y	1	台
34	小型化射频共用系统	万格	VT-3271	3	套
35	4G 路由器	万格	VT-3280	2	套
36	中心服务器	H3C	H3C R4900 G2	2	套

37	备份交换中心软件	万格	VT-3100S	1	套
38	与省厅互联网关	万格	VT-3930	1	台
39	防火墙	天融信	tg-41410	2	套
40	移动基站接入网关	H3C	RT-MSR-2600-10	1	台
41	媒体网关	万格	VT-3910	1	台
42	手台远程控制系统	万格	定制开发	1	套
43	信道单元数字化定制升级	万格	VT3800	8	台
44	光纤直放站（1 近 1 远）	泉州立泰	LT-RP350MHz	1	套
45	350MHz 微型直放站	海能达	DS-9300	18	台
46	馈线	国产		18	根
47	定向壁挂天线	国产		18	个
48	手持式常规中转台	海能达	PD980/SW00074	5	台
49	光纤直放站近端机	四川云策	RL500N	3	台
50	光纤直放站远端机	四川云策	RL500F	11	台
51	智能 PDU	大唐保镖	HP9001	9	台
52	自动调谐合路器	IR	IR-HLQ	4	台

附件 2：科技信息化运行维护类项目交付物清单

序号	服务目录	触发条件	交付物	备注	交付时效
巡检类					
1	日常巡检	每天	每日巡检记录	数字集群通信系统相关设备功能测试记录 需包括设备安全用电情况、设备功能是否正常。	工作日当天
2	季度巡检	每季度	季度巡检报告	数字集群通信系统相关系统测试记录 需包括数字集群通信系统各基站、直放站相关系统功能是否正常。	巡检期满 5 个工作日内
3	年度巡检	每半年	半年度运维报告	需包括故障分析、应对建议，年度运维情况总结等。	完成运维工作六个月、十二个月后 5 个工作日内
清洁保养类					
1	设备清洁保养	每季度	设备清洁保养记录	数字集群通信系统相关设备清洁保养记录，中心机房清洁保养记录	保养期满 5 个工作日内
故障处理类					
1	设备故障响应	设备产生故障	故障报验单、故障处理报告	故障报验单需包括故障发生情况、发生时间、故障处理人、预计故障处理时间。 故障处理报告需包括故障发生情况、发生时间、影响程度、故障处理人、故障解决情况说明等。输出纸质报告。	故障处理完成后两个工作日内
2	系统故障响应	系统产生故障			故障处理完成后两个工作日内
3	调试检测	设备需更换时	调试检测报告	调试检测报告需包括更换设备型号、更换设备安装位置、更换人员、调试检测情况说明等。	完成设备更换后两个工作日内
专项工作类					
1	信息台帐	第一个月	信息台账电子资料	信息台帐：包括设备的资产、位置、状态等全生命周期信息和设备拓扑结构图等，并进行统一登记，建立完整的设	签订合同后一个月内

				备档案	
2	工作规程	签订合同后 10 个工作日	工作规程	针对维护工作开展制定具体的工作规程	签订合同后 10 个工作日内
专业培训类					
1	专业培训	共完成两次	培训记录表	公司组织对驻场人员专业培训一次、对甲方相关人员培训一次。	培训完成后两个工作日内
技术咨询类					
1	技术咨询	用户有需求时	技术方案、建议	响应用户提出的技术咨询，对技术升级改造方案提出建议。	根据需求具体情况确定
注：所有纸质输出物须甲、乙、用户方（如有）多方签字。					