政府采购项目

公开招标

西安市机关事务服务中心市级机关公务用车管理维保服务项目

合 同 书

（编号：XCZX2025-0056）

甲　方：西安市机关事务服务中心

乙　方：易迅通科技有限公司

2025 年 6 月

中国　西安

服 务 合 同

甲方：西安市机关事务服务中心
统一社会信用代码：12610100MB24277619
住所：西安市凤城八路109号五号楼227房
法定代表人：王晓东

乙方：易迅通科技有限公司
统一社会信用代码：91610132693807 48XR
住所：西安市经济技术开发区文景路以西乙方中港国际第2幢1单元16层11606号房
法定代表人：刘永华

经2025年3月28日中心第8次党组会会议研究决定，委托西安市市级单位政府采购中心采取公开招标的方式，确定易迅通科技有限公司为西安市机关事务服务中心市级机关公务用车管理维保服务项目（项目编号：XCZX2025-0056）中标供应商。依据《中华人民共和国政府采购法》、《中华人民共和国民法典》以及西安市市级单位政府采购中心招标文件、中标通知书，经甲、乙双方协商一致，达成如下合同条款：

一、合同标的物内容及数量（以投标文件正本和澄清表〈函〉为准）

第一年度服务费报价明细表

单位：元

序号	维保服务项目	数量	单位	单价	合计
1	系统模块及数据模块日常运维	1	项	362000.00	362000.00
2	系统安全管理	1	项	164500.00	164500.00
3	系统功能需求变更	1	项	364000.00	364000.00
4	服务台远程运维服务	1	项	198300.00	198300.00
5	项目运维管理服务	1	项	123000.00	123000.00
6	硬件设备维护	3120	台/年	223.00	695760.00
7	平台短信服务	3120	台/年	113.00	352560.00

8	物联网 SIM 卡流量	3120	张/年	240.00	748800.00
总价：大写：叁佰万捌仟玖佰贰拾元整					小写：3008920.00

第二年度服务费报价明细表

单位：元

序号	维保服务项目	数量	单位	单价	合计
1	系统模块及数据模块日常运维	1	项	362000.00	362000.00
2	系统安全管理	1	项	164500.00	164500.00
3	系统功能需求变更	1	项	303821.60	303821.60
4	服务台远程运维服务	1	项	198300.00	198300.00
5	项目运维管理服务	1	项	123000.00	123000.00
6	硬件设备维护	3120	台/年	223.00	695760.00
7	平台短信服务	3120	台/年	113.00	352560.00
8	物联网 SIM 卡流量	3120	张/年	240.00	748800.00
总价：大写：贰佰玖拾肆万捌仟柒佰肆拾壹元陆角整				小写：2948741.60 元	

第三年度服务费报价明细表

单位：元

序号	维保服务项目	数量	单位	单价	合计
1	系统模块及数据模块日常运维	1	项	362000.00	362000.00
2	系统安全管理	1	项	164500.00	164500.00
3	系统功能需求变更	1	项	244846.77	244846.77
4	服务台远程运维服务	1	项	198300.00	198300.00
5	项目运维管理服务	1	项	123000.00	123000.00
6	硬件设备维护	3120	台/年	223.00	695760.00

7	平台短信服务	3120	台/年	113.00	352560.00
8	物联网 SIM 卡流量	3120	张/年	240.00	748800.00
总价：大写：贰佰捌拾捌万玖仟柒佰陆拾陆元柒角柒分					小写：2889766.77

二、服务条件：

（一）维保服务地点：甲方指定地点。

（二）服务期：合同自签订之日起成立，为期三年。合同一年一签，本年度为第一年，自签字盖章之日起生效。

（三）维保期：本年度自 2025 年 6 月 28 日起至 2026 年 6 月 27 日止。

三、合同价款

【第一年度】人民币 3008920.00 元（小写，精确到小数点后两位），即叁佰万捌仟玖佰贰拾元整（大写）。

【第二年度】人民币 2948741.60 元（小写，精确到小数点后两位），即贰佰玖拾肆万捌仟柒佰肆拾壹元陆角整（大写）。

【第三年度】人民币 2889766.77 元（小写，精确到小数点后两位），即贰佰捌拾捌万玖仟柒佰陆拾陆元柒角柒分（大写）。

合同履行期间，合同总价固定不变，不受市场价格变化因素的影响。

（二）合同总价包括平台维护费、硬件维护费和其他费用。

四、款项结算

（一）合同签订后，一个月内支付年度合同总价款的 50%，即大写：壹佰伍拾万肆仟肆佰陆拾元整，小写：¥1504460.00 元整，服务期满并经专家组验收合格后，一个月内支付年度合同总价款的 50%，即大写：壹佰伍拾万肆仟肆佰陆拾元整，小写：¥1504460.00 元整。

（二）支付方式：银行转账。

（三）结算方式：验收合格后填写政府采购项目验收单（一式伍份），乙方开具发票（按本合同总价直开甲方），持成交通知书、服务合同、发票，政府采购项目验收单，与甲方结算。

五、双方的权利和义务

（一）甲方的权利和义务

1、在乙方进行现场维护时，甲方应在维护地点附近为乙方人员提供贮物空间，为乙方维保工作提供便利。

2、在甲方安全规定允许的前提下，为乙方的人员进入维护现场提供方便。

3、在条件允许的情况下，甲方可按照乙方的指导进行非现场维护操作。

4、甲方及时将本合同下维保范围内出现的故障情况通知乙方，乙方负责做好故障有关资料的记录工作。

5、甲方对乙方工作人员在甲方现场的人身及财产的安全不负责任，除非损害是甲方故意造成的。

6、甲方有权对乙方工程师的工作态度、技术水平进行监督和评判并提出相应的要求，乙方也会由独立的服务质量监督人员对甲方予以不定期的回访。

7、未经甲方书面同意，乙方不得将本合同部分或全部技术服务工作转让给第三人承担，但不包括转让给维护产品的原厂商进行服务。甲方不对乙方将本合同部分或者全部服务工作转让给第三人所产生的费用负责。

8、甲方负责提供故障发生前后相关的系统或设备资料、数据和原始记录。

（二）乙方的权利和义务

1、乙方确保提供维保服务的设备、系统能够稳定安全的运行。保证备件和备机的技术指标先进、质量性能可靠、进货渠道正常，配置合理，全面满足招标文件要求。

2、乙方为甲方提供定期巡检，做好预防性维护。

3、乙方保证在甲方现场的工作人员严格按照甲方现场管理要求和工作纪律行事。

4、因乙方技术问题或维护问题造成甲方的硬件受到损坏，乙方应负责赔偿甲方因此所遭受的全部损失。

5、乙方应按甲方要求如期向甲方交付相关文档，如定期的巡检报告服务季度报告、现场服务单等。

6、乙方在服务过程中发现非本合同服务范围内的软硬件问题导致系统故障，应及时向甲方汇报，在获得甲方的许可和费用确认后，应向甲方提供不低于本合同约定服务范围内软硬件的维保

服务。

7、乙方应当保证，依本合同为甲方提供的技术服务过程或其为甲方提供的服务成果不侵犯任何第三人的合法权益。如果有人提出法律诉讼或启动行政程序（合称“侵权指控”），声称甲方使用的技术服务成果侵犯了其知识产权，乙方同意赔偿甲方就此所承担的所有费用和给甲方造成的损失，包括但不限于上述侵权指控中所产生的一切诉讼费用、合理的律师费用、和解金额或终审判决中规定的赔偿金额等。

如果在侵权指控的审理过程中有关法院或行政机关禁止甲方继续使用技术服务成果的部分或全部，乙方应当采取以下措施之一避免甲方损失的扩大，同时应对甲方造成的损失给予全额赔偿：

（1）使甲方重新获得使用上述技术服务成果的权利；

（2）更换或改造上述技术服务成果，使甲方不受上述禁令限制继续使用技术服务成果。

8、乙方为履行本合同约定义务，所需更换的备件的运输及运输费用由乙方负责，运杂费已包含在技术服务费总价内，运杂费包括但不限于从货物供应地点所含的运输费、装卸费、仓储费、保险费等。

六、质量保证

乙方所供服务必须履行下列条款：

（一）乙方服务方案和方式科学、可行，人员配置合理，全面满足要求。

（二）符合国家有关服务规范要求，确保各项服务达到最佳运行效果。

（三）乙方提供的服务，若发生侵权而产生的一切后果，由乙方负责。甲方保留索赔权力。

（四）乙方提供维保技术服务期间，应当保证甲方设备、应用系统及数据的安全，并对甲方的所有相关数据进行保密，不得外泄。

（五）对于甲方系统出现的任何故障，乙方接到甲方通过书面通知、电话、信函、传真、电子邮件等任何一种方式提出的故障通知后，应在 10 分钟内响应， 2 小时内派专业技术人员到达甲方指定的用户现场，采取有效措施，排除故障，使系统恢复至正常使用状态。

（六）乙方应具备备件维修和提供备机的服务能力，提供服务期间，因甲方设备部件损坏需要配件的，更换周期不得超过 5 个工作日，并对备件、配件提供自更换之日起至少 1 年的质保期，且乙方对所有服务设备的全部故障件的维修、配件的运输等均是免费的。所有备件均为与原设备或模块的型号相同，或各项性能规格不低于原有设备或模块的备件。所有因乙方备件问题引发的故障或造成的损失均由乙方承担全部责任。乙方在为故障设备提供备件、配件期间，应自行向甲方提供备机，保证甲方系统及硬件设备的正常运行，不因备件、配件的更换影响甲方系统及设备的运行。

（七）乙方应在接到甲方故障通知后 2 小时内，完成故障修复工作，并经甲方验收确认。甲方工作人员在验收单上签署的验收合格时间为乙方实际完成维保技术服务的时间。

（八）乙方应建立完善的服务受理记录，并可由甲方随时进行纸质或电子化查阅，乙方的服务受理记录与甲方工作人员签署的技术服务验收合格的验收单不符的，以验收单为准。

（九）乙方对于系统故障处理应有详细的报告记录，包含故障原因、响应时间、解决方案以及合理建议等。

七、验收

（一）服务内容完成后先由乙方进行自检（见附件 3），自检合格后邀请甲方进行验收。甲方确认乙方的自检内容后，组织乙方（必要时请有关专家）进行最终验收，验收时乙方应派员参加，共同对验收结果进行确认，并承担相关责任。验收合格后，填写政府采购项目履约验收单（一式伍份）作为对服务的最终认可。

（二）乙方向甲方提交服务实施过程中的所有资料，以便甲方日后管理和维护。

（三）验收依据:

1、招标文件、投标文件、澄清表（函）；

2、本合同及附件文本;

3、国家相应的标准、规范。

八、违约责任

（一）依据《中华人民共和国民法典》中的相关条款承担违约责任。

（二）未按本合同要求提供服务或服务质量不能满足本合同

要求，甲方应当将乙方违约的情况以及拟采取的措施以书面形式报政府采购监管部门，根据政府采购监管部门的处理意见，甲方有权依据《中华人民共和国民法典》有关条款及合同约定终止合同，并要求乙方承担违约责任。同时，政府采购监管部门有权依据《中华人民共和国政府采购法》及相关法律法规对乙方的违法行为进行相应的处罚。

（三）在本合同履行过程中，双方因违约造成对方损失的应当赔偿。

（四）甲方无正当理由逾期付款的，则每日以应付价款为基数，按照全国银行间同业拆借中心受权公布贷款市场报价利率(LPR)支付利息。

（五）乙方未能按照本合同约定时间提供服务或完成约定的项目服务内容的，从逾期之日起每日按本合同总价款 1 %的数额向甲方支付违约金；逾期 60 日以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。

（六）未经甲方书面同意，乙方不得擅自将本合同服务转包第三方承担。

（七）乙方在甲方提出故障通知时，未在本合同约定的响应时间内给予响应或未在约定的时间内派专业人员抵达甲方指定的用户现场提供技术服务的，每迟延一小时，应向甲方支付违约金 100 元人民币。该款项甲方有权从应付乙方的服务费中直接扣除，不足部分，由乙方补足。

（八）乙方未在本合同约定的服务时间内完成故障修复工作的，每迟延一小时，应向甲方支付违约金 100 元人民币，该款项甲方有权从应付乙方的服务费中直接扣除。

（九）如因乙方提供维保技术服务导致甲方设备、系统损坏的，乙方应赔偿甲方全部经济损失（包括直接损失和间接损失）。

（十）如果甲方因在乙方授权范围内使用乙方提供的软件、文件、资料等，而遭到的第三方就侵犯专利、商标、工业设计或其他知识产权而提出的索赔和诉讼，由乙方承担全部法律后果，如因该等情形导致甲方损失的，乙方应给予甲方全额赔偿。

九、保密

（一）乙方应遵守国家法律法规和行业规定，保守甲方的国家秘密及商业秘密。未经甲方同意，不得将承接政府服务项目获得的政府、公民个人等各种信息和资料提供给其他单位和个人。

如发生以上情况，甲方有权索赔。

（二）甲方有义务保护乙方的知识产权，未经乙方同意，不得将乙方交付的具有知识产权性质的成果文件、资料向第三方转让或用于本合同以外的项目。如发生以上情况，乙方有权索赔，但甲方依据相关法定职责对外公开的除外。

（三）本合同的保密信息包括所有商业秘密、技术秘密、通信或与该产品相关的其他信息，无论是书面的、口头的、图形的、电磁的或其它任何形式的信息，包括但不限于：数据、模型、样品、草案、技术、方法、仪器设备和其它信息。

（四）乙方应当按照甲方的要求采取有效的方法对该保密信息进行保密，所需费用由乙方承担。

（五）乙方对甲方的数据、软件、用户名、密码、系统结构、网络配置等不得泄露给任何第三方，如有违反，按违约处理。

（六）保密期限：本合同保密期限为永久保密。

（七）本条款为独立条款，本合同的无效、变更、解除和终止均不影响本条款的效力。

十、争议解决

（一）本合同在履行过程中发生的争议，由甲、乙双方当事人协商解决，协商不成的按下列第 1 种方式解决：

1、提交西安仲裁委员会仲裁；

2、依法向甲方住所地人民法院起诉。

（二）本条款为独立条款，本合同的无效、变更、解除和终止均不影响本条款的效力。

十一、合同变更

在本合同履行期限内，双方均不得随意变更或解除合同。如因项目需求情况发生变化，需要进行项目变更的，应双方协商后签订项目变更协议（如双方变更事项不能达成一致的，仍按本合同履行，否则视为违约）。

十二、合同生效

本合同一式 伍 份，甲方持 壹 份，乙方持 壹 份，西安市财政局政府采购管理处备案 叁 份，本合同经甲、乙双方法定代表人、负责人或授权代表签字并加盖公章之日起生效。本合同约定的服务期限届满后，本合同自动失效。

十三、其他

（一）西安市财政局政府采购管理处在合同的履行期间以及履行期后，可以随时检查项目的履行情况，对采购标准、采购内容进行调查核实，并对发现的问题进行处理。

（二）招标文件、投标文件、澄清表（函）、中标通知书、合同附件均构成本合同不可分割的部分。

（三）本合同未尽事宜，可由甲、乙双方协商确认后签订政府采购补充合同，补充合同与本合同具有同等法律效力。补充合同与本合同不一致的，以补充合同为准。

十四、合同附件

1、服务内容
2、维保方案
3、验收内容

附件 1：

服务内容

1、软件运维：主要包括系统和数据模块日常运维、系统安全管理、系统功能需求变更、软件系统各项目功能现场培训、服务台远程运维服务工作。

我司保障模块日常稳定运行，系统的安全更新、账号安全防护、安全事件记录。每日进行巡检；为系统运行随时提供技术保障。

为防止系统安全攻击，我司对平台服务、数据库进行日常维护以及可能如设备、人员操作不当引起的数据损失或设备问题，保障数据的完整性和可用性。

1.1 系统模块及数据日常运维

系统模块日常运维：对市级机关公务用车平台系统的运行情况进行巡检及重点技术保障，通过常态化的巡检监控、维护和管理，确保系统的高可用性、稳定性和安全性，同时优化性能、提高效率，提升整体运维服务质量和系统使用用户（各市级党政机关、事业单位）满意度。

保障模块日常稳定运行，每日进行巡检；为系统运行随时提供技术保障。为防止系统安全攻击对平台服务、数据库进行日常维护以及可能如设备、人员操作不当引起的数据损失或设备问题，保障数据的完整性和可用性，器进程与服务检查、磁盘空间检查、系统漏洞修补等，对数据库采用实时的增量备份，并进行每日业务低峰期全量备份，数据备份文件压缩后存放于当地环境，并做好访问权限防护，也用于必要的数据恢复。

数据模块日常运维：确保数据库系统的稳定运行和数据存储安全是系统数据日常运维的首要目标，从数据运维的范围、方式、流程和备份机制上。

数据日常运维内容主要包括数据库服务的资源监控、故障排查、备份文件检查和恢复、数据访问性能优化、数据处理、数据统计查询、数据共享同步等多个方面，旨在确保系统数据的安全存储和使用。

1.2 系统安全管理

我司提供系统及服务漏洞扫描与防护，如发现异常征兆，按照漏洞等级的修复时间整改完成，保障系统安全高效的正常运行。并每周提供系统安全情况报告。

主要对系统服务、 CPU、内存和磁盘等重要指标状态进行监控,对系统及服务漏洞扫描与防护。对操作系统进行安全加固。进行 7*24 小时日常监控维护，发现问题，按照问题的严重程度，确保在 24 小时内解决故障，保障系统稳定，每周提供维护报告和服务巡检报告。

1.3 巡检服务要求

从系统、数据模块日常巡检过程中，覆盖系统服务的环境资源占用和性能情况，以及系统应用客户端环境是否访问正常，是否存在兼容性问题，并检查运行环境的网络安全防护、病毒防护等是否需要完善。衡量系统应用是否正常运行的关键参数，主要包括平台服务器运行情况、应用服务情况、数据库备份情况、web 服务器运行情况、中间件运行情况、信息安全防护情况、数据库服务运行情况、防火墙运行情况、服务器存储情况等。每日出具运维日巡检单、按照运维日巡检单汇总出具周巡检单、按照每周汇总编写月度运维报告。

1.4 系统功能需求变更

在使用系统的过程中，我司针对西安市公务用车管理服务特点，保障系统持续系统功能需求变更迭代升级，在平台使用过程中可根据系统操作人员操作习惯、体验提出升级需求，维保单位根据需求信息定期进行升级开发、测试及平台安全检测、快速系统上线，随时响应采购人需求，始终保持采购人系统的安全性、行业先进性和易扩展性。

1.5 服务台远程运维服务

我司提供手机、微信群、微信等多种渠道的远程技术支持服务，为各使用单位提供 7×24 小时服务。配备专业客服人员，通过微信群、电话等实时处理各类咨询及系统平台问题。

远程技术服务无法解决问题的，如设备或系统发生故障，运维服务人员应在 10 分钟内响应，2 小时内到达现场解决问题。

1.6 项目管理与客户现场培训服务

我司负责运维过程中的报告编写及各单位的系统电脑端、APP 端、小程序的不定期培训。掌握项目运维动态，规范项目过程中突发事件及管理工作情况的报告行为，有效预防、及时协调、及

时发现项目运维中的问题，避免或者减少不确定因素造成的损失，确保安全、质量。运维项目经理负责所有人员的工作管理和监督，将综合运维服务的客户满意度损失降到最小。

2.硬件运维

我司对全市 3120 台车辆定位终端维修、定期巡检、维护保养、升级，保障全市 3120 台车辆北斗定位终端稳定运行，对终端设备进行调试、定期巡检、维护保养、改装、拆除、升级服务，每月进行北斗终端系统现场巡检及统计。负责 LED 无缝拼接大屏设备维修、更换。

3.物联网 SIM 卡

对 3120 张物联网 SIM 卡流量费，物联网卡移动数据通讯及流量，用于车辆定位监控系统、设备远程升级维护所有数据通讯服务。

4.平台短信服务

我司提供平台系统 10690 专用通道短信所有车辆申请、调度指派、驾驶员执行任务短信推送通知服务，便于我方用车部门、司乘人员、调度人员信息推送及会议通知等。通过短信及时告知对应节点工作人员及时响应业务，保障公车调度业务的高效率。

附件 2:

维保方案

1 系统模块及数据日常运维

对西安市公务用车信息化平台系统的运行情况进行运维及重点技术保障，通过常态化的运维监控、维护、和管理，确保系统的可用性、稳定性和安全性，同时优化性能、提高效率，提升整体运维服务质量和系统使用用户（各市级党政机关、事业单位）的满意度。

1.1 系统模块日常运维

系统模块日常运维服务主要对服务器 CPU、内存和磁盘等重要指标状态进行监控,对操作系统进行安全加固。我司安排 2 名中高级运维工程师进行 24 小时日常监控维护，发现问题 2 小时内解决，保障系统稳定并每周提供维护报告和服务器运维报告。

系统运行的服务环境资源占用情况和性能情况，以及系统应用客户端环境是否可以正常访问、是否存在兼容性问题，并检查运行环境的网络安全防护、病毒防护等是否需要完善，具体的运维内容如下:

平台服务运维：对系统的应用清单及部署服务地址清单，监控系统部署的各虚拟机性能指标、硬件资源占用情况，如CPU使用率、内存占用、磁盘使用率、端口访问等，检查系统运行日志，包括操作系统的自身运行日志及各系统应用的运行错误日志、警告信息和异常事件，对异常日志信息进行提取，由相应的技术运维人员进行分析，提前预知和解决问题。

平台服务（虚拟机）基础软件更新和安全补丁

西安市市级机关公务用车平台系统运行使用Liunx操作系统，客户端使用Windows 10/11操作系统及国产统信系统，浏览器以IE8以上版本为主，日常运维中需检查操作系统和基础应用软件的版本，并结合分析系统安全漏洞扫描结果，对操作系统进行应用安全补丁和更新、中间件漏洞的完善配置修改、系统业务功能的升级改造，提升系统部署环境的安全性。同时，对客户端电脑进行系统所需的基础运维软件版本进行检查，按需定期升级，并对部分电脑的系统应用兼容性进行分析解决。

（1）应用系统日常运维

西安市市级机关公务用车平台的各功能按使用对象不同，运行在互联网上，在日常于运维中需检查各系统应用是否可访问，如互联网页面是否可正常打开、系统登录入口是否可访问、接口服务是否可调用等；同时定期运维走访各市级单位对系统使用情况的反馈、问题收集，了解应用系统是否运行正常，确保业务的顺利开展，提升工作效率。

（2）清理临时文件

对虚拟机上部署的业务应用系统运行产生的临时文件、日志、缓存，按每个系统的保留周期，对已超期的临时文件进行及时清理，腾出资源，避免因存储空间不足导致系统异常。

（3）系统合规性和安全审计

根据信息化系统建设参照的法律规范和依据及国家、省市对信息化系统建设的规范性要求，遵照个人信息保护法、通信保密法，积极进行系统合规性评估和检查，如系统配置、安全策略、个人隐私、数据安全、访问控制、备份和恢复等方面，对不达标内容讨论整理解决方案，进行系统优化完善，确保系统符合相关的法规和标准要求。另外，系统建设内容、项目资料、过程文件，要及时整理归档更新，做好修订记录，配合进行安全审计，进一步提高系统建设的合规性。

（4）记录过程文档和检查报告

记录运维过程和结果，编写运维报告，为系统的运维管理提供文档支撑。

（5）系统功能模块页面日常运维

定期对用户登录、工作台、报警管理、全省一张网、监督分析、用车申请、车辆监控、车辆档案、驾驶员管理、第三方对接、系统设置等模块进行进行监督空运维工作。

1.2 数据模块日常运维

数据日常运维内容主要包括数据库服务的资源监控、故障排查、备份文件检查和恢复、数据访问性能优化、数据处理、数据统计查询、数据共享同步等多个方面，旨在确保系统数据的安全存储和使用。

（1）数据库资源监控

通过日常巡检，确保数据库的资源占用率（cpu、内存、存储），根据系统使用量，维持在性能稳定的指标内。

（2）数据库运行状态监控

运维人员定期对数据库自身的运行状态进行监控，包括数据库用户权限、数据库用户连接情况、数据库连接数、数据查询效率、运行日志、表空间文件大小情况等，及时对可能或已经存在的故障异常进行分析解决，并预测数据增长趋势，规划数据库的存储容量和硬件资源的扩展。

（3）定期检查数据备份文件可用性

配合管理人员完成数据备份，检查备份策略执行率、数据完整性、数据可恢复性，确保在进行应急响应时，能及时对数据进行恢复。

（4）数据查询性能调优

针对结构化数据，根据数据库运行日志及系统功能页面的数据写入和加载情况，对数据库 SQL 语句、存储过程、序列等，分析执行过程，提升查询效率。

针对非结构化数据，如业务中扫描上传的要件资料文件，存在 NFS 存储中，日常运维中需检查文件存储的占用大小、文件上传下载预览服务是否正常，定期归档清理垃圾文件、压缩文件。

（5）数据处理和统计需求处理

业务数据处理工单及统计需求，在符合数据安全管理的前提下，协调技术人员进行数据库脚本编写、验证，配合业务科室完成数据处理和数据统计，数据处理时做好原数据的备份，数据统计时不可影响线上业务系统的正常使用。

（6）定期清理业务备份临时表

在系统升级、业务查询统计、性能优化等需求处理时，会建立一些临时表、中间表、参照表、备份表，定期对这些表进行梳理，并与相应需求科室进行清理确认，部分临时数据直接删除、部分临时数据做好归档处理。

（7）数据安全与合规检查

实施数据加密、访问控制、审计日志等安全措施，确保数据不被非法访问、篡改或泄露，并符合相关法律法规的要求；在个人敏感信息写入、读取使用时，调用局内的安全加密服务，需做好加密、完整性校验、是否篡改校验。

（8）数据备份与恢复

除了常规的数据定期备份外，在业务系统升级、数据处理过程中，还要做好目标数据的备份恢复工作，不对库中的存量数据进行随意删减篡改，做好数据处理的过程文件记录。

（9）数据共享同步

检查业务数据同步到前置数据库是否正常，并按其他业务单位的数据共享需求，定制开发数据共享接口，发布到平台，供其他业务单位进行数据共享使用；同时，对局内业务科室对其他业务单位的数据共享需求，整理成数据字段明细，通过市平台发起数据共享需求，待其他业务单位发布数据共享接口后，负责进行接口对接联调，并集成各到业务系统中使用。

2 系统安全管理

我公司安排 5 名高级运维工程师进行每天 24 小时日常监测，如发现异常征兆，按照漏洞等级的修复时间整改完成，保障系统安全高效的正常运行。并每周提供系统安全情况报告。

安全防护服务、网络访问控制服务

在设备上进行必要的设置(如服务器、交换机的密码等)，防止黑客取得硬件设备的远程控制权。比如许多网管往往没有在服务器或可网管的交换机上设置必要的密码，懂网络设备管理技术的人可以通过网络来取得服务器或交换机的控制权，这是非常危险的。因为路由器属于接入设备，必然要暴露在互联网黑客攻击的视野之中，因此需要采取更为严格的安全管理措施，比如口令加密、加载严格的访问列表等。

安装和设置防火墙，现在有许多基于硬件或软件的防火墙，如华为、神州数码、联想、瑞星等厂商的产品。对于网络安全来说，安装防火墙是非常必要的。防火墙对于非法访问具有很好的

预防作用，但是并不是安装了防火墙之后就万事大吉了，而是需要进行适当的设置才能起作用。如果对防火墙的设置不了解，需要请技术支持人员协助设置。

入侵检测

系统平台运行中对系统进行防御入侵检测、漏洞扫描等安全检测，根据测试结果进行修复。

防御服务

通过以下五种方式提供安全防御服务:

1. 安装网络杀毒软件

现在网络上的病毒非常猖獗，这就需要在服务器上安装网络版的杀毒软件来控制病毒的传播，如瑞星、冠群金辰、趋势、赛门铁克、熊猫等推出的网络版杀毒软件；同时，在网络版的杀毒软件使用中，必须要定期或及时升级杀毒软件。

2. 账号和密码保护

账号和密码保护可以说是系统的第一道防线，目前网上的大部分对系统的攻击都是从截获或猜测密码开始的。一旦黑客进入了系统，那么前面的防卫措施几乎就没有作用，所以对服务器系统管理员的账号和密码进行管理是保证系统安全非常重要的措施。

系统管理员密码的位数一定要多，至少应该在 8 位以上，而且不要设置成容猜测的密码，如自己的名字、出生日期等。对于普通用户，设置一定的账号管理策略，如强制用户每个月更改一次密码。对于一些不常用的账户要关闭，比如匿名登录账号。

3. 监测系统日志

通过运行系统日志程序，系统会记录下所有用户使用系统的情形，包括最近登录时间、使用的账号、进行的活动等。日志程序会定期生成报表，通过对报表进行分析，你可以知道是否有异常现象。

4. 关闭不需要的服务和端口

服务器操作系统在安装的时候，会启动一些不需要的服务，这样会占用系统的资源，而且也增加了系统的安全隐患。对于完全不用的服务器，可以完全关闭；对于需要使用的服务器，应关闭不需要的服务，如 Telnet 等。另外，还要关掉没有必要开的 TCP 端口。

5. 定期对服务器进行备份

为防止不能预料的系统故障或用户不小心的非法操作，必须对系统进行安全备份。除了对全系统进行一次的备份外，还应对

修改过的数据进行每周一次的备份。同时，应该将修改过的重要系统文件存放在不同的服务器上，以便出现系统崩溃时(通常是硬盘出错)，可及时地将系统恢复到正常状态。

服务器的维护是一个非常烦琐的工作，最根本的一条原则就是“安全”二字，时刻把这个原则放在心里，维护服务器就会有章可循了。

3 系统功能需求维护

在系统功能需求维护开发过程中，我司将配备前端开发工程师 1 名，中级 Java 开发工程师 1 名，高级 Java 开发工程师 1 名，高级测试工程师 1 名，高级产品经理 1 名，共计 5 人，进行功能优化开发工作。

在使用系统的过程中，针对西安市公务用车管理服务特点，进行系统适配需求变更及系统升级，个性化需求进行专项开发及三方接口对接工作。在平台使用过程中可根据操作习惯、用户体验提出升级需求，产品经理及时收集需求，研发部门根据需求信息定期进行升级开发、测试及平台安全检测、快速系统上线，随时响应用户需求，始终保持系统的安全性、行业先进性和易扩展性。

根据西安市机关事务中心要求完成对外的数据、服务接口服务，实现数据共享与服务共享。

软件需求变更调研：角色应包括项目经理、高级软件工程师，应形成用户需求变更文档该文档需提交用户确认。产物为用户需求变更说明书文档。

需求分析;角色应包括项目经理、架构师、高级软件工程师，根据软件需求变更调研得到的用户需求变更说明书文档进行需求分析，应形成项目需求分析文档，该文档需提交项目组进行评审，主要是软件部分，对需求能否实现进行评估。产物为项目需求变更分析说明书文档。

原型设计：角色应包括项目经理、架构师、前端工程师、移动端工程师，根据项目需求变更分析说明书进行原型设计，根据需求分析变更文档进行 系统原型设计，主要包括利用界面原型制作工具设计图形类的功能模块，利用既有项目案例，制作实际项目案例参考，其中包括自己公司已有和市场上已存在的。连同项目需求变更分析说明书交由项目经理审核，最终由项目经理、架构师、前端工程师同用户完成原型的审核，最终形成第一次迭代开发的项目需求变更文档说明书。

详细设计：角色应包括项目经理、架构师及全体项目人员参与，应形成 软件概要设计、软件详细设计文档，该文档需提交项目组，主要是项目部，对设计是否符合用户需求进行评估。经多次修改与确认后形成最终的项目详细设计说明书文档（包括概要设计）。产物为：项目概要设计说明书，项目详细设计说明书文档。

原型开发：角色应包括软件开发人员，按照详细设计说明书进行原型开发;快速实现详细设计说明中的各项功能，细节问题放到二次或三次迭代时加入。内部测试完毕后交由测试部进行测试。

测试评审：角色应为测试部、项目组成员，测试只进行功能实现测试，不进行其他细节和边界条件等测试。测试通过后，交由项目组进行评审，修改。最后由项目经理、软件项目经理与用户就原型进行沟通，检验功能设计是否符合用户要求，用户是否还有其他需求。最后形成二次迭代开发新需求文档，到此一次迭代结束。

我公司新增（包括但不限于）以下明确功能，针对明确功能开发周期如下：北斗定位终端管理，自合同签订之日起 30 天内交付；申请购置管理，自合同签订之日起 60 天内交付；OCR 标识识别、VIN 信息识别，自合同签订之日起 180 天内交付。

4 项目运维管理服务

项目运维管理，报告编写及各单位的系统电脑端、APP 端、小程序的不定期培训。掌握项目运维动态，规范项目过程中突发事件及管理工作情况的报告行为，有效预防、及时协调、及时发现项目运维中的问题，避免或者减少不确定因素造成的损失，确保安全、质量。运维项目经理负责所有人员的工作管理和监督，将综合运维服务的客户满意度损失降到最小。

我公司为采购人和用户单位的相关管理员，审核员，调度员，驾驶及普通用户等进行系统化培训，培训内容基础信息维护，用车申请，调度派车，派车审核等，以确保人员能够独立进行管理、使用、故障处理及日常维护等工作，使平台能够得到正确的应用和良好的维护，保证整个信息系统可以健康、稳定的运行，保障多层次公务用车出行。

培训是为了让用户能更好的操作与维护，服务于整个公务用车信息管理服务平台，更好的进行科学有效的平台管理维护，保障出行用车。项目经理对项目的质量负全面责任，确定各级人员质量职责，对项目中的重大质量事项组织研究并作出决策，提出

质量要求。

项目主管负责有关技术文件的编制，对总体运维技术方案设计和详细设计质量负责，确保设计质量符合规范要求，满足客户需要；参加项目运维过程汇总技术问题的分析，提出解决方案；从设计上保证项目质量。

负责组织制订项目总体质量控制计划；负责项目质量方针和质量目标的贯彻落实；对项目各阶段、各环节质量进行监督管理；协助开展检验、测（调）试及验收工作；汇总并通报有关项目质量情况，对出现的质量问题坚持"四不放过"原则--即原因不清不放过，责任未落实不放过，问题未整改不放过，整改效果不合格不放过，并就项目质量有关事宜负责对外联络、协调、合作沟通工作，发现重大质量问题，及时向项目经理汇报。项目管理组负责从资源上为项目质量管理和保证提供必要条件，在保证项目质量的前提下，做好项目进度的控制管理工作，编制进度控制计划；负责项目对外联络工作，组织进度协调会，确保项目进度、运维效率。负责项目文档、技术资料的归档和管理。

5 硬件设备维护

我公司将按照招标文件要求为对西安市公务用车信息化平台内共监管市级机关公务用车 3120 辆（其中党政机关 2086 辆、事业单位 1034 辆）使用设备维护服务及平台系统运行维护服务，并确定单车平台系统维护标准，负责 LED 无缝拼接大屏设备维修、更换。安排 7 名中级安装工程师，保障事业单位 1034 台车辆和党政机关 2086 台车辆的定位终端安装调试、定期巡检、维护保养、升级。每季度对设备及系统运行状况进行一次全面巡检，如发现漏洞及时保养和升级，确保系统安全高效运行。

车载终端简介

产品名称：车载定位终端

产品型号：M11-BD

产品规格：L74mm*W55mm*H24mm

序号	项目	规格参数	备注
1	工作电压	DC 9V-36V	无
2	正常工作功耗	0.35W	无

3	工作电流	48～52mA@12V（休眠状态电流 18～21mA@12V）	
4	最大工作功耗	1.2W	无
5	最低功耗	0.24W	无
6	定位精度	<10 米 （2D RM）	此数据为公司实验室实测
7	定位方式	北斗定位	无
8	硬件架构	工业级芯片架构	无
9	通讯方式	TCP/UDP	
10	工作温度范围	-25℃ ~ +75℃	无
11	贮存温度范围	-40℃ ~ +85℃	无
12	数据协议	符合国家交通部 JT808 协议	
13	数据通信方式	GSM/GPRS 制式	
14	可靠性设置	电源高低压保护	
15	在线参数配置	可远程配置车载客户端参数，包括车牌号绑定、数据发送频率、远程主机地址、速度报警阈值。	
16	后备电池时间	电池充饱电的前提下，可连续工作 1.5h 左右；	

无缝拼接大屏规格：户内全彩屏 P1.875 全彩，共计 8.064 ㎡ 240mm*240mm 模组，宽 26 列*高 8 行，6.24mm*1.92mm 共计 208 张模组，分辨率 3328*1024。按照户内全彩屏参数要求，对 LED 无缝拼接大屏设备维修、更换。

6 服务台远程运维服务

我公司提供了手机、微信群、微信等多种渠道的售后服务，为各使用单位提供 7×24 小时服务。公司为西安市公务用车平台配备专业客服人员 2 人，通过微信群、电话等实时对各类北斗定位终端及系统平台使用问题进行处理和咨询答疑，如遇无法处理的需求或故障则转给相应的负责人进行处理，对整体过程进行跟踪。同时根据各单位实际需求，如电话远程指导效果不佳则协调安排培训讲师进行现场培训。针对各单位使用中提出的需求问题，转给研发运维组进行评审、开发、测试、上线，对其全过程进行

监控并反馈项目经理。

远程支持升级服务

我公司为用户提供400免费技术服务热线(4000-112-226)，在接到用户请求后，根据请求情况协调公司资源，第一时间给用户反馈并解决问题。

1.诊断故障并提交故障诊断报告

根据系统运行过程中出现的系统故障或其它异常情况，及时进行故障诊断，并提出故障诊断报告。故障诊断报告的主要内容包括：故障现场情况记录、故障的级别和紧急处理过程记录等。

2.制定系统维护和故障恢复的实施计划

根据提交的故障诊断报告，制定系统维护和故障恢复的实施计划。按照制定的计划实施系统维护工作。

3.管理、监督维护计划的维保

组成系统维护管理和监督工作组，全面负责管理和监督系统维护工作维保过程。并根据系统维护实施的各个阶段提交维护工作报告。

4.确认维护工作完成并提交维护报告

在系统维护工作完成后，由系统维护人员提交系统维护工作报告，由用户方项目组的技术人员对系统维护情况进行测试并予以确认。

5.提交成果

每次系统维护工作完成后，都应提交如下的报告、记录等文档等资料：

现场服务流程

优质的售后服务一直是我们公司在经营活动中最基本的原则。公司的技术支撑部门担负着专业的服务工作，无论是在系统的安装调试过程中还是在系统投入运行之后，无论发生任何问题用户都可以得到最快的响应，售后服务流程如下图所示：

7平台短信服务

公车系统中为保障对系统业务流转的快速响应，在公车申请、审批、派车、执行任务、收车等公车调度全流程节点、车辆告警、维保、年检提醒等均设置了短信通知，通过短信及时告知对应节点工作人员及时响应业务，保障公车调度业务的高效率，平均每个订单会产生6至10条短信,分别按照节点发送给车辆的申请人、调度人员、司机等。

短信平台的工作方式

短信平台对工作的帮助对用车单位：及时的发布订单状态，

与司机、调度的双方沟通更加及时便利。对公务用车中心：及时发送派车信息，与司机、调度的双方沟通更加及时便利。对单位员工：及时的发布单位通知、温馨提示等，降低无纸化办公，提升工作效率。

短信平台达成目标平台系统中所有车辆所有信息推送通知，便于用车部门、司乘人员、调度人员信息推送及会议通知等。达到信息推送及时、准确，达到互联互通。

8 物联网 SIM

物联卡基于物联网专网，采用物联网专属号段，通过专用网元设备支持短信、无线数据通信、语音等基础通信服务，并提供通信状态管理和通信鉴权等智能通道服务，默认开通物联网专用的短信接入服务号和物联网通用 APN。

物联卡业务是中国移动面向物联网用户提供的采用物联网专用的 10648 和 147 号段作为 MSISDN 的移动通信接入业务，通过专用网元设备支持短信和 GPRS 等基础通信服务，并提供通信状态管理和通信鉴权等智能通道服务，默认开通物联网专用的短信接入服务号和物联网专用 APN。

一、功能

1.基础通信能力：GPRS 通信能力和短信通信能力，短信可提供不同优先级服务（重发频次、储存时间），充分满足不同集团客户需求。

2.终端状态查询：向客户提供开关机信息、终端位置信息、终端 GPRS 上线、离线、IP、APN 等信息查询。

3.账务信息查询：向客户提供账户信息查询，提供账户欠费、流量超标等事件的提醒功能。

4.业务统计分析：向用户提供多维度的业务报表统计及分析等。

5.灵活计费功能：根据客户需求提供流量池、生命周期等多种计费方式。

二、优势

1.一点接入，全网服务：提供政企公司或各省公司一点进行业务受理，分省出卡的业务开通，各配合省根据客户需求进行卡的制作、配号和销售，直接为客户提供业务服务和网络服务，满足客户“一点拿卡”、“一站式服务”需求，避免客户与多个省进行业务对接，且无省间漫游结算，特别适合于全网业务应用的行业客户。

2.丰富的码号资源：拥有以 10648 开头的 12 位物联网专用号

段，支持短信和 GPRS 功能，容量一亿；以 147 开头的 11 位物联网专用号段，支持语音、短信和 GPRS 功能，容量一百万。物联网用户可以使用专门的号码，获取所需的丰富码号资源。

3. 灵活的计费方式：针对物联网业务的特殊性，提供了流量池计费方式和按生命周期计费方式，其中，按流量池计费即客户通过购买流量池，实现多张卡共用一个流量池的功能；按生命周期计费方式即终端硬件费加上终端整个生命周期包月费的总和，再通过一定的折扣率分摊到每个月，降低客户的总体成本。另外，在整个计费环节新增测试期和沉默期，满足客户测试期需求，并为客户免费提供测试流量及短信。

4. 高质量的网络：通过建设物联网短信中心、物联网 GGSN、物联网 HLR 等物联网专用网元，实现物联网用户与大众用户的网络分离，为行业客户提供可靠性和稳定性的网络。

5. 通信管理：采集网络信息，并通过物联网专网的运营管理平台为客户提供通信在网状态查询（开关机信息、PDP 激活状态、IP 地址查询、短信失败原因查询等）、流量信息查询、流量余额提醒等功能。

6. 终端管理：在终端管理方面为客户提供终端管理、远程控制、远程升级等，让用户时刻掌握终端状态，出现故障及时发现，并帮助用户快速故障定位。

附件 3:

验收内容

1、自检汇总表

公务用车信息化监管服务平台维保 自查报告			
类别	**检查项**	**情况描述**	**测试结果**
服务器登陆及权限设置	登陆密码设置及更新	对登录密码设置及更新、可登录账号检查	
	可登录账号检查	可登录账号进行检查，校验账号的安全级别	
服务器运行情	CPU 占用率	检查 CPU 使用情况，对占有率进行日巡检、周巡检确保系统稳定性。	

公务用车信息化监管服务平台维保
自查报告

类别	检查项	情况描述	测试结果
况	内存占用率	按照日巡检、周巡检情况，对服务器内存使用率、占用率进行检查，达到使用标准。	
	磁盘使用率	按照日巡检、周巡检情况，合理调整磁盘使用率，提升平台高效稳定运行。	
	I/O WAIT	对 I/O WAIT 进程跟踪，确保服务器进程不可中断睡眠，日巡检反馈情况，周巡检处理存在的异常，达到检查标准。	
	带宽/连接数	对服务器带宽、连接数进行检查，达到负载均衡。	
应用服务情况	tomcat 状态	主要检查 tomcat(升级后替换为 K8S)运行情况是否正常，每日、每周及时检查，存在问题及时处理。	
	mysql 数据库状态	系统运行过程中，数据库承载负荷，数据状态检查，确保数据链访问安全。	
	第三方 API 接口状况	存在三方 API 接口,不定期检查 API 接口情况，存在异常及时处理。	
	服务总体状态	主要对服务器的运行参数、运行状态、运行效率进行检查，确保非服务器稳定运行	
	平台总体响应状态	主要对系统访问的响应时间进行检查，在合理范围的时间确保系统访问有效，链路正常。	
备份容灾情况	数据文件大小	每周备份，每日巡检，对数据库文件进行管理，按项目标准要求，对数据文件进行存储，	
	备份文件状态	每日巡检，检查备份文件情况，确保备份文件安全、有效、数据完善。	

公务用车信息化监管服务平台维保 自查报告				
类别	检查项	情况描述		测试结果
	归档文件状态	平台所涉及的文件及时归档，不定期检查文件状态。		
服务器安全	病毒查杀	病毒库升级	对杀毒软件进行周期性升级，确保软件有效性。	
		病毒查杀结果/处理	日巡检、周巡检，对查杀的病毒及时处理，对处理结果进行分析，确保平台安全、网络安全。	
	漏洞扫描	何种漏洞扫描工具	洞鉴	
		漏洞扫描结果/处理	每周、每月对扫描出来的漏洞进行分类，按照级别进行处理，做到漏洞及时处理及时消除，确保服务器、数据库安全	
现场维修	天线	检查定位天线正常、异常		
	通讯	检查 SIM 卡开关状态正常，		
	OBD 数据	对 OBD 数据进行校验，检查 OBD 接线异常		
	终端	通电情况是否正常		
定位上线情况	定位位置	系统检查车辆定位准确性		
	定位轨迹	系统检查车辆轨迹是否完善、历史轨迹保留		
	实时跟踪	系统车辆实时跟踪、定位位置、时速是否正常。		
	定位通信	GPRS 数据流是否正常		
	短信平台	抄发送短信内容是否正常，查询设备指令是否正常。		

公务用车信息化监管服务平台维保 自查报告			
类别	检查项	情况描述	测试结果
定位离线情况	OBD 掉线	现场查看定位接线情况巡检。	
	终端绑定	平台终端状态情况巡检。	
车辆远程调试	发送指令	对绑定终端车辆、异常车辆进行指令发送并激活。	
	平台转发指令	车载终端应答状态进行检查，确认是否正常。	
自查结论：			

2、问题及需求记录表（需求、问题）

<table>
<tr><td>报修日期：</td><td colspan="2">示例：xxxx 年 x 月 x 日</td><td rowspan="2">服务类别</td><td rowspan="2">软件</td><td rowspan="2">□问题
□需求</td></tr>
<tr><td>维修日期：</td><td colspan="2">示例：xxxx 年 x 月 x 日</td></tr>
<tr><td>故障处理方式</td><td>□远程</td><td>□现场</td><td>故障处理结果</td><td colspan="2">□完成 □未完成</td></tr>
<tr><td colspan="6">故障基本信息</td></tr>
<tr><td>平台类型</td><td colspan="4">问题汇总描述</td><td>处理结果</td></tr>
<tr><td>需求 1：</td><td colspan="4">对客户使用中提出的需求项内容进行编写</td><td></td></tr>
<tr><td>问题 1：</td><td colspan="4">汇总本月度问题咨询情况。</td><td></td></tr>
<tr><td>处理过程</td><td colspan="5"></td></tr>
<tr><td>遗留问题：</td><td colspan="5">□有 □无 说明：</td></tr>
</table>

3、平台月巡检表

序号	巡检名称	维护巡检情况	巡检结果
1	服务器登录及权限设置	对登录密码设置及更新、可登录账号检查	
2	服务器运行情况	检查 CPU 占用率、内存占用率、磁盘使用率、I/O WAIT、带宽/连接数	
3	应用服务情况	Tomcat 状态、mysql 数据库状态、第三方 API 接口状况、服务总体状态、平台总体响应状态。	
4	备份容灾情况	数据文件大小、备份文件状态，规定文件状态	
5	服务器安全	防火墙策略，病毒查杀（安装何种杀毒软件，病毒库升级，病毒查杀结果处理），漏洞扫描（何种漏洞扫描工具，漏洞扫描结果）	
6	终端数据维修	包括天线、通讯、终端是否正常，OBD 数据进行校验，检查 OBD 接线异常。	
7	定位上线情况	定位位置准确性、轨迹是否完善、历史估计保留。、车辆实时跟踪、定位位置、时速，通信、短信平台等数据量、抄发送短信内容是否正常，查询指令是否正常。	
8	定位离线情况	OBD 掉线、终端绑定，现场查看接线情况、终端状态情况分析。	
9	车辆远程调试	发送指令、平台转发指令。对绑定终端车辆、异常车辆进行指令发送并激活。	
10	平台需求数量	平台功能优化，包括订单中心、车辆监控、用车申请、基础信息、系统设置。	

序号	巡检名称	维护巡检情况	巡检结果
11	平台故障数量	处理系统使用中故障问题	
12	培训及远程服务	对平台现场、远程方式培训及指导	

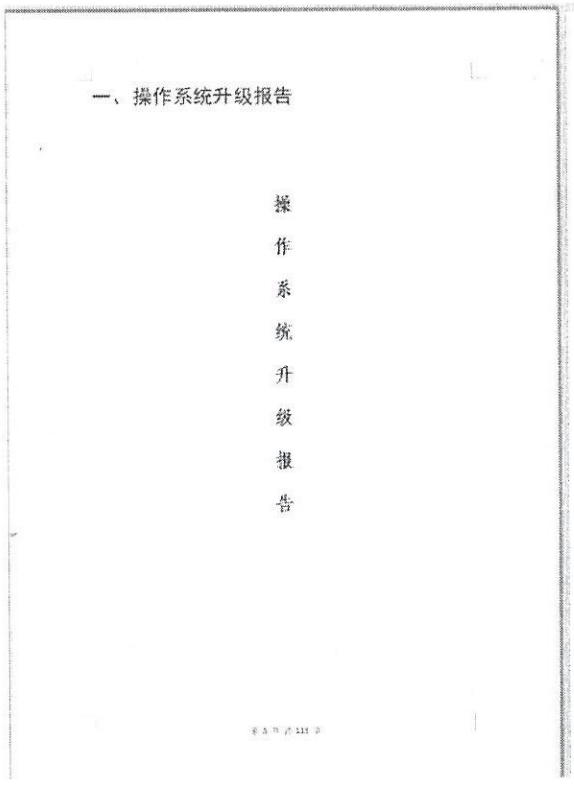
检测项目		检测内容	实测记录
现场维修	天线	检查定位天线正常	
	通讯	检查 SIM 卡开关状态正常	
	OBD 数据	对 OBD 数据进行校验，检查 OBD 接线异常	
	终端	通电情况是否正常	
定位上线情况	定位位置	系统检查车辆定位准确性	
	定位轨迹	系统检查车辆轨迹是否完善、历史轨迹保留。	
	实时跟踪	系统车辆实时跟踪、定位位置、时速是否正常。	
	定位通信	GPRS 数据流是否正常。	
	短信平台	抄发送短信内容是否正常，查询设备指令是否正常。	
定位离	OBD 掉线	现场查看定位接线情况巡检。	

线情况	终端绑定	平台终端状态情况巡检。	
车辆远程调试	发送指令	对绑定终端车辆、异常车辆进行指令发送并激活。	
	平台转发指令	车载终端应答状态进行检查，确认是否正常。	
检修人：　　年　月　日		检修单位：易迅通科技有限公司	
工程负责人：　　年　月　日			

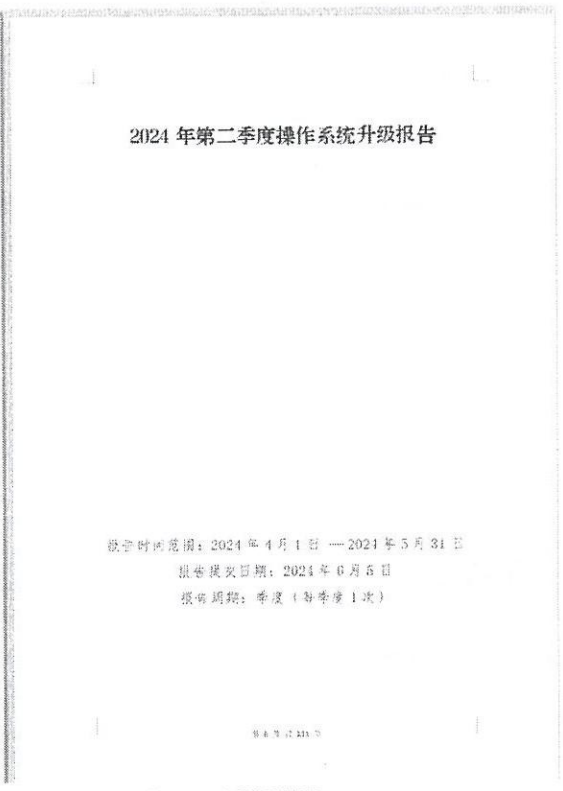
本月维保内容及问题汇总	示例： 1、本月对平台内 3120 台完成巡检工作，现场实际拆装、改装、调试总结 XX 辆，调试并完成上线工作 2、对平台日常、数据服务，数据库、应用服务器、服务器登陆情况巡检均正常。 3、防火墙、病毒查杀、漏洞扫描，每月扫描漏洞巡检发现低危 X 个，中危 X 个，高危 X 个，总计处理 X 个。 4、每日、每周、每月对服务器、应用服务器巡检工作。 5、维修过程中对 SIM 卡检测、全部开关机正常。
维保意见	示例： 1、车辆定位电源线在车辆检修时注意检查线路，防止拔掉。 2、对报废车辆的处置在车辆中心档案中修改状态，联系服务商处理车辆信息。

	3、车辆定期巡检上线，对车辆的电瓶并定期启动车辆。
下月维保及维修计划	示例： 1、列出下月巡检内容， 2、对平台运维、数据运维按照应用、数据服务、周扫描等进行罗列。总结月度扫描情况，列出佐证资料。 3、硬件终端类巡检、远程客户服务咨询工作量统计。

4、季度佐证材料：


一、操作系统升级报告

操作系统升级报告


2024年第二季度操作系统升级报告

报告时间范围：2024年4月1日——2024年5月31日

报告提交日期：2024年6月5日

报告周期：季度（每季度1次）

二、防火墙升级报告

防
火
墙
升
级
报
告

2024年第二季度防火墙升级报告

报告时间范围：2024年4月1日 —2024年5月31日
报告提交日期：2024年6月5日
报告周期：季度（每季度1次）

三、数据库升级报告

数
据
库
升
级
报
告

2024年第二季度数据MySQL升级报告

报告时间范围：2024年4月1日 —2024年5月31日
报告提交日期：2024年6月5日
报告周期：季度（每季度1次）

四、中间件升级报告

中
间
件
升
级
报
告

2024 年第二季中间件 kubernetes 升级报告

报告时间范围：2024 年 4 月 1 日 — 2024 年 5 月 31 日
报告提交日期：2024 年 6 月 5 日

5、项目周巡检单

巡检日期：	示例：xxxx 年 x 月 x 日	服务类别	□巡检 □其他
公务用车信息化监管服务平台巡检项目			
类别	检查项	情况描述	备注
服务器登陆及权限设置	登陆密码设置及更新	□正常□异常	
	可登录账号检查	□正常□异常	
服务器运行情况	CPU 占用率	□正常□异常	
	内存占用率	□正常□异常	
	磁盘使用率	□正常□异常	
	I/O WAIT	□正常□异常	
	带宽/连接数	□正常□异常	
应用服务情况	k8s 节点调度状态	□正常□异常	
	mysql 数据库状态	□正常□异常	
	mongodb 数据库状态	□正常□异常	
	kafka 消息队列状态	□正常□异常	
	nfs 存储状态	□正常□异常	
	nginx 代理服务状态	□正常□异常	
	第三方 API 接口状况	□正常□异常	
	服务总体状态	□正常□异常	
	平台总体响应状态	□正常□异常	
备份容灾情况	数据文件大小	□正常□异常	
	备份文件状态	□正常□异常	
	归档文件状态	□正常□异常	
服务器安全	防火墙策略		
	病毒查杀 / 安装何种杀毒		

		工具			
		病毒库升级			
		病毒查杀结果/处理		□已处理□未处理	
	漏洞扫描	何种漏洞扫描工具			
		漏洞扫描结果/处理		高危 个 中危 个 低危_个	
处理过程：					

佐证材料：

目录

右键此处文字->点击"更新域"，以显现目录。

1 综述信息

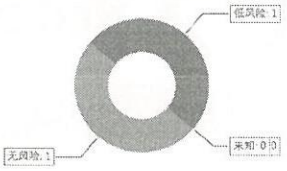
1.1 任务信息

任务名称	[redacted]
扫描策略	
启动时间	
结束时间	2024-04-05 16:04:
扫描耗时	36:35
存活主机数量/总扫描主机数量	1/1
发现漏洞数/存活主机数量	7/1
扫描的 URL 数量	1
发出的 HTTP 请求数	10297
任务风险等级	低风险

1.2 资产统计

1.2.1 资产风险分布

风险级别	目标数量	百分比
高风险	0	0.00%
中风险	0	0.00%
低风险	1	50.00%
无风险	1	50.00%
未知	0	0.00%
总计	2	100.00%



洞鉴 X-RAY

[redacted]的扫描任务报表

[redacted]

评估时间：2024-04-05 17:34:19

目录

右键此处文字-->点击"更新域"，以显现目录。

1 综述信息

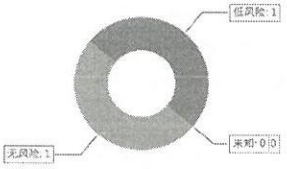
1.1 任务信息

任务名称	[redacted]
扫描策略	
启动时间	
结束时间	2024-04-05 16:04:
扫描耗时	36:35
存活主机数量/总扫描主机数量	1/1
发现漏洞数/存活主机数量	7/1
扫描的 URL 数量	1
发出的 HTTP 请求数	10297
任务风险等级	低风险

1.2 资产统计

1.2.1 资产风险分布

风险级别	目标数量	百分比
高风险	0	0.00%
中风险	0	0.00%
低风险	1	50.00%
无风险	1	50.00%
未知	0	0.00%
总计	2	100.00%



1.2.2 操作系统统计

序号	操作系统	主机数量	百分比
1	-	[redacted]	100.00%

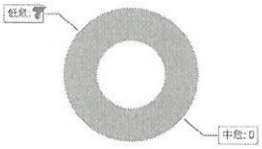
1.2.3 服务类型统计

序号	服务类型	服务数量	百分比
1	http	[redacted]	100.00%

1.3 风险结果统计

1.3.1 漏洞风险分布

1.3.1.1 漏洞风险分布总览



1.3.1.2 资产漏洞分布

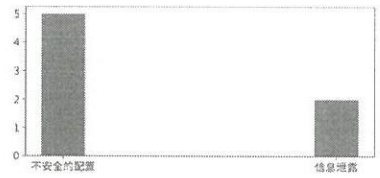
内容限制提醒：当前仅将主机和 web 各自风险最高的 top 5000 资产展示，无风险资产不列出展示。更多内容请前往子报告查看。

序号	任务目标	风险级别	漏洞总数	严重漏洞	高危漏洞	中危漏洞	低危漏洞
1	https://www.xxgwyc.com/	低风险	[redacted]	0	0	0	7
总计			[redacted]	0	0	0	7
比例			100.00%	0.00%	0.00%	0.00%	100.00%

1.3.2 漏洞 TOP5

序号	漏洞名称	漏洞类型	风险等级	漏洞总数
1	HTML 信息泄露漏洞	信息泄露	低危	1
2	HTTP 响应头 Server 泄露框架信息漏洞	信息泄露	低危	1
3	HTTP 响应头 Strict-Transport-Security 缺失漏洞	不安全的配置	低危	1
4	HTTP 响应头 X-Content-Type-Options 缺失漏洞	不安全的配置	低危	1
5	HTTP 响应头 X-Frame-Options 缺失（点击劫持）漏洞	不安全的配置	低危	1

1.3.3 漏洞类型 TOP5



2 资产探测结果

https://[redacted]/

1 Web 指纹信息

目标 Web 站点	https://[redacted]/
网站标题	vehicle-web-front
Web 框架	Default Universal Service,F5,Apache
URL 数量	1

3 漏洞列表

https://www.sxgwyc.com/(低风险)

HTML 信息泄露漏洞(低危) *1

漏洞权重	99%
漏洞类型	信息泄露
漏洞编号	CT-638341
漏洞描述	HTML 响应中注释可能存在敏感的内容，开发者应该在上线之前经过统一处理去除所有的注释，以防信息泄露。
漏洞首次发现时间	-
漏洞最近发现时间	-
漏洞危害	造成用户信息，站点配置信息等敏感信息泄露。
CVSS 评分	5.3
修复方案	如果非必要，将 HTML 内的注释删除

1) 漏洞位置: https://[redacted]

HTTP 响应头 Server 泄露框架信息漏洞(低危) *1

漏洞权重	99%
漏洞类型	信息泄露
漏洞编号	CT-638108
漏洞描述	在 HTTP 响应消息的头部中，其中通常会包含网站的框架信息，来表示网站使用了哪种框架、哪种语言、哪种 Web 容器等信息，还有可能暴露框架版本，攻击者可以利用这类信息发起进一步攻击。
漏洞首次发现时间	-
漏洞最近发现时间	-
漏洞危害	造成用户信息，站点配置信息等敏感信息泄露。
CVSS 评分	5.3
修复方案	修改配置文件，移除响应的 HTTP 响应头中包含的敏感信息 部署 Web 应用防火墙 可以避免受到网站服务器信息泄露的影响

1) 漏洞位置: https://[redacted]

HTTP 响应头 Strict-Transport-Security 缺失漏洞(低危) *1

漏洞权重	99%
漏洞类型	不安全的配置
漏洞编号	CT-638517
漏洞描述	现代浏览器提供了许多可选的安全相关功能等特性，这些功能等特性通常可以通过 HTTP 响应头来控制，使用这些功能，可以避免受到浏览器端的用户受到类似 CSRF、XSS、Click Hijacking 等前端黑客攻击的影响。
漏洞首次发现时间	-
漏洞最近发现时间	-
漏洞危害	通过专业的安全评估，如果被攻击者利用，可能会泄漏服务器敏感信息
CVSS 评分	6.5
修复方案	修改服务器中处理HTTP响应的配置文件。具体的位置和名称取决于您使用的服务器软件和操作系统。 示例： 1、如果您使用Apache服务器，配置文件可能是httpd.conf或apache2.conf。 在类似配置部分增加一行： Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" 这将在HTTP响应中添加一个名为"Strict-Transport-Security"的头，值为"max-age=31536000; includeSubDomains; preload"。这个头信息告诉浏览器只使用HTTPS连接访问该网站，并将该策略应用于包括子域名在内的所有页面。"max-age"参数指定了该策略的有效期。 保存配置文件并重新启动服务器，以使更改生效。

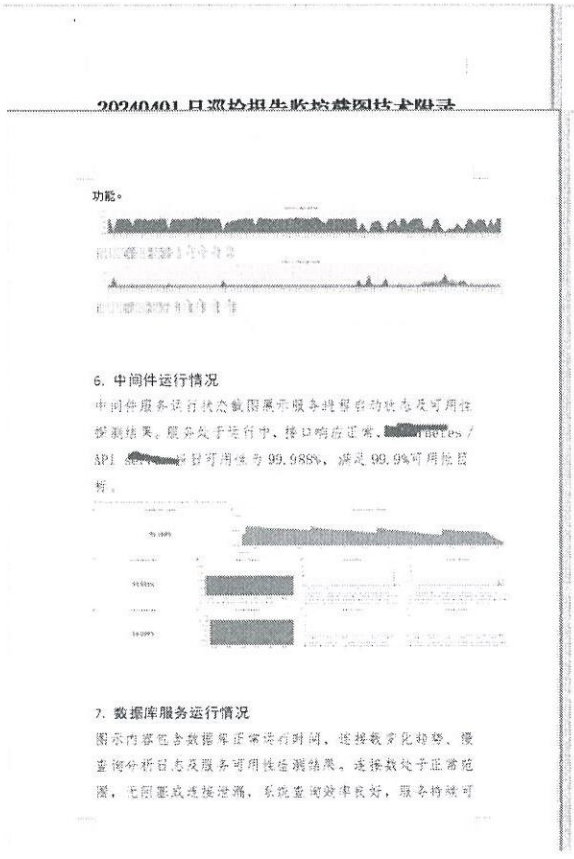
6、项目日巡检单

巡检日期：	示例：xxxx 年 x 月 x 日	服务类别	□巡检 □其他
1.数据库备份情况；2.服务器运行情况；3.中间件运行情况；4.服务器网络运行情况；；6.数据库服务运行情况；7.信息安全防护情况；8.防火墙运行情况；9.服务器存储情况。			

类别	检查项	是否正常/故障描述	备注
数据库备份情况	备份任务是否按时执行	□正常□异常 故障描述	
	备份日志有无报错	□正常□异常 故障描述	
服务器运行情况	CPU 占用率是否正常	□正常□异常 故障描述	
	内存占用率是否正常	□正常□异常 故障描述	
	分区使用率是否正常	□正常□异常 故障描述	
服务器网络运行情况	网卡状态是否正常	□正常□异常 故障描述	
	网络使用率是否正常	□正常□异常 故障描述	
web 服务器运行情况	Web 端口是否正常响应	□正常□异常 故障描述	
	黄金 API 是否可用	□正常□异常 故障描述	
中间件运行情况	中间件服务是否正常启动	□正常□异常 故障描述	
	中间件可用性是否正常	□正常□异常 故障描述	
数据库服务运行情况	数据库连接数是否正常	□正常□异常 故障描述	
	慢查询日志检查	□正常□异常 故障描述	
	数据库服务是否可用	□正常□异常 故障描述	
信息安全防护情况	防病毒软件是否已开启	□正常□异常 故障描述	
	病毒库是否更新为最新	□正常□异常 故障描述	
	是否发现入病毒木马入侵	□正常□异常 故障	

		描述	
防火墙运行情况	防火墙设备运行状态是否正常	□正常□异常 故障描述	
	是否发现病毒事件	□正常□异常 故障描述	
服务器存储情况	服务器存储是否正常运行	□正常□异常 故障描述	
	磁盘分区使用率是否正常	□正常□异常 故障描述	
处理过程： 示例：每日巡检完成后，平台运行正常。			

佐证材料


20240401日巡检报告监控截图技术附录

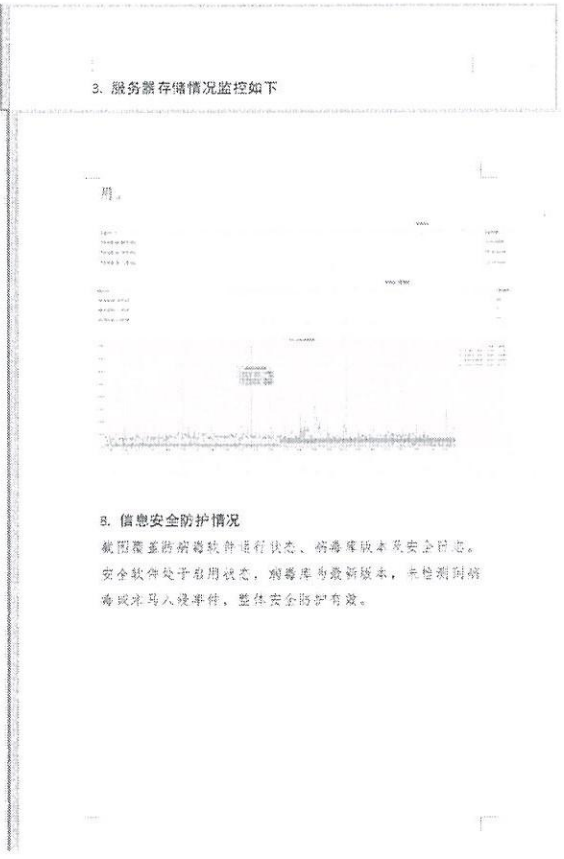
功能。

6. 中间件运行情况

中间件服务运行状态截图展示服务进程启动状态及可用性探测结果。服务处于运行中、接口响应正常、[redacted] / API [redacted]平台可用性为99.988%，满足99.9%可用性指标。

7. 数据库服务运行情况

图示内容包含数据库正常运行时间、连接数变化趋势、慢查询分析日志及服务可用性检测结果。连接数处于正常范围，无阻塞或连接溢满，系统查询效率良好，服务持续可


3. 服务器存储情况监控如下

用。

8. 信息安全防护情况

截图覆盖防病毒软件运行状态、病毒库版本及安全日志。安全软件处于启用状态，病毒库为最新版本，未检测到病毒或木马入侵事件，整体安全防护有效。

甲 方	乙 方
西安市机关事务服务中心 （盖章）：	易迅通科技有限公司 （盖章）：
住所：西安市凤城八路109号	住所：西安市经济技术开发区文景路以西乙方中港国际第2幢1单元16层11606号房
邮编：710016	邮编：710000
法定代表人（签字）：	法定代表人（签字）：刘玉华
被授权代表（签字）：徐湘民	被授权代表（签字）：
电话：86788579	电话：02986199603
	开户银行：中国建设银行股份有限公司西安凤城五路支行
	银行账号：61001753800052502766
日期：2015年7月2日	日期：2015年7月2日