2026 年度信息化项目运行维护服务采购项目合同

项目名称：2026 年度信息化项目运行维护服务采购项目

项目编号：YL-2026-000021-4.1B1

甲方：　　杨凌示范区公安局交通管理支队

乙方：　　陕西英广智能工程有限公司

2026 年 11 月

合同正文

甲 方：杨凌示范区公安局交通管理支队

地址：杨凌示范区常青路 1 号

法定代表人/负责人：权小虎

电话：029-87033306

乙 方：陕西英广智能工程有限公司

地址：陕西省杨凌示范区渭惠路西段博学嘉苑 19 幢 3 单元 309 室

法定代表人/负责人：解鹏军

电话：13992811040

根据《中华人民共和国民法典》《中华人民共和国政府采购法》等相关法律法规及本项目竞争性谈判文件（项目编号：YL-2026-000021-4.1B1）的要求，甲乙双方本着平等自愿、诚实信用的原则，就甲方的信息系统运行维护服务事宜协商一致，签订本合同，共同信守。

一、项目概况与服务期限

1.项目名称：杨凌示范区公安局交通管理支队 2026 年度信息化项目运行维护服务采购项目；项目编号：YL-2026-000021-4.1B1。

2.服务范围：甲方公安视频专网、公安信息网、互联网等网络内信息化系统的统一运维，涵盖前端路面所有智能设备（视频监控、卡口、电子警察、智能信号灯、雷视检测设备等）、甲方办公楼、车管所办公楼、大队办公楼、中队办公区域及警务室、执法站等场所，包

括内外场软硬件维护、网络安全、信息化系统平台运维、现场服务、培训服务、应急维护等内容，具体以本合同附件《运维服务清单》及《提升服务清单》为准。

3.服务期限：一年，自合同签订之日起一年内完成项目全部内容，并交付采购人验收合格，期满自动终止服务。

二、合同价款及结算

1.合同总价：人民币（大写）**壹佰零玖万叁仟伍佰元整**（小写：¥1,093,500.00元）。

此价格为固定包干价，包含人工、巡检、故障处置、耗材、配件更换等本合同项下全部运维服务及相关费用，以及服务费、税费和其他费用。合同总价一次性包死，不受市场价格变化因素的影响，甲方无需另行支付其他费用。

2.付款方式：银行转账。本合同生效后，甲方分段支付，服务周期年度过半，完成中期运维考核合格，支付合同总价 80%，整体运维年度服务期满，全部工作验收合格，无遗留问题、资料完整移交归档后，支付剩余 20%。。乙方应根据支付比例提交相应等额合规的增值税发票（□专票 ☑普票）。

3、乙方收款账户：

户名：陕西英广智能工程有限公司

开户行：中国银行杨凌农业高新技术产业示范区支行

账号：103228137823

四、运维服务内容及要求

1. **前端设备运行维护**：对所有道路交通技术监控设备前端进行运行检查、维护保养、设备调试、故障维修，包括补光灯和爆闪灯调试更换、软件升级、耗材更换、设备电源及内网纤路（除运营商线路外）线路维护等。每周或不定期开展外场巡视，每月或不定期开展外场设备清洁、检修、调试等日常维护保养，及时分析处理外场设备故障，并配合甲方完成前端点位迁改意见、设备检查标定及备案等工作。

2. **系统平台运行保障**：对机房服务器、PC 服务器、存储设备、交换机及操作系统、Oracle 数据库、中间件、数据备份系统等进行日常检查、故障响应与诊断排除，协助完成核心系统平台的优化调试、系统配置、漏洞修补、补丁升级及安全防护，硬盘损坏的予以更换。

3. **专业驻场服务**：提供不少于 4 名技术运维人员提供 7×24 小时现场驻场服务，驻场人员名单及排班表须报甲方备案，驻场人员请假或轮换的，乙方须提前 3 日通知甲方并安排同等资质人员顶替，不得出现岗位空缺。负责日常巡检、故障处理及服务需求响应。组建不少于 10 人的二线技术支持团队（涵盖项目管理、服务器、存储、网络、操作系统、数据库、备份、机房环境、强电等领域），提供定期或不定期的技术支持。

4. **日常监控巡检服务**：通过自主可控的一体化运维管理平台对各类业务系统、内外场设备的运行状态进行监控管理和运维管理；安排专职平台值守人员 7×8 小时值守，负责实时监控前端摄像头可用性、网络联通性和电源运行状态，跟踪反馈故障处理进度，每周进行故障

录入、汇总并完成故障处理报告，故障处理报告应于次周提交甲方，逾期提交的，甲方有权在月度考核中予以扣分；定期开展机房环境及系统工程硬件现场巡检。

5. **故障处理维护服务**：提供 7×24 小时运维服务响应，做好日常系统巡检、故障维护、视频图像调取、安全隐患排查及突发状况应急处置；从用户申告故障到服务响应时间小于 10 分钟；建立故障分级（Ⅰ-Ⅳ级）、定位上报、处理、记录汇总流程，Ⅰ、Ⅱ级故障须在 10 分钟内上报甲方运维管理部门并启动应急预案，III级故障处理完毕后三日内向甲方提交书面故障处理报告。

6. **维护保养巡查服务**：定期维护保养及清洁前端设备护罩、监控标识牌、机箱，修剪影响摄像机监控效果的枝叶，每季度至少一次。每季度至少对全部前端点位进行一次例行检查和维护，并对取电线路情况进行重点巡视检查；每季度对数据中心平台服务器、存储设备、操作终端、交换机等设备进行维护保养。

7. **重大活动保障服务**：重大节日及甲方重要活动期间，按要求加派维护人员和平台值守人员驻守指挥中心，事前制定保障方案并开展全面巡检，活动当天安排不少于 3 名专职工程师全时驻场，保证指定重点区域设备在线完好率达到 100%。

8. **应急演练安全服务**：乙方须积极配合甲方开展公安局交巡警支队信息化相关应急安全演练工作，覆盖网络安全、业务系统故障、外场前端设备大面积瘫痪等场景。

9. **人员安全**：针对公安局交巡警支队信息化运维外场作业场景，

乙方在开展路面路口设备巡检维修、高空登高调试监控、信号灯设备、线缆敷设、带电作业等工作过程中，若发生触电、高空作业坠落、道路路口施工作业磕碰及交通涉险等各类安全事故，乙方须第一时间按照应急预案组织抢险救援。凡是因乙方运维实施、现场防护、作业管理不到位引发的人身伤亡、第三方人身及财产损害，全部法律责任与经济赔偿责任均由乙方独立承担。乙方需为本项目全部运维作业人员足额投保保险、人身意外伤害等保险，保险额度匹配交管外场运维作业风险，保险有效期覆盖完整服务周期。

10. **安全服务：**每季度利用专业漏洞扫描工具对甲方全网关键业务应用进行全面安全扫描及加固（含系统漏洞、应用漏洞、WEB 漏洞、配置合规性检查），扫描和修复结束后 10 个工作日内提交《漏洞扫描和修复报告》并协助加固整改，扫描及加固时间须提前 5 个工作日书面通知甲方，经甲方确认后方可实施，每半年一次安全加固并提前提交《安全加固方案》；日常配合甲方工作人员处理安全事件。

11. **桌面系统维护服务：**负责公安信息网/视频专网/互联网及甲方各办公场所桌面系统的技术维护，负责各类应用系统和 PC 终端的防毒、杀毒、漏洞扫描、系统升级、各类高危信息发布等，维护各类网络数据安全。

12. **设备延保服务：**运维期内不在质量保证期的软件、硬件、设施设备、配套附件及工程质量等由乙方出资维修，确定无法维修的与甲方协商解决；在质量保证期内的由乙方无偿督促质保单位及时提供服务。

13. **备品备件与车辆工器具：**按甲方确认的运维设备总数量的 2%储备备品备件，备品备件清单及库存数量须于每月第 5 个工作日前提交甲方备案，甲方有权随时核查；备品备件消耗后，乙方须在 7 日内补足库存，确保备件储备率始终不低于 2%；建立备品备件库及完善的采购、申请、出入库、借用、盘点、报废管理制度，负责全部备品备件的免费维修并提供定期维护保养；高空作业车和维护工程车保证 7×24 小时全天候待命，手续齐全、足额投保且保险在服务期内持续有效；提供运维所需仪器仪表及维护工具并妥善保管使用。

14. **运维平台与资料流程管理：**乙方自带部署一套成熟、可用、自主可控的运维管理系统（平台），用于运维服务全流程管理（含事件管理、问题管理、配置管理、变更管理等流程），系统版权/使用权归乙方所有，甲方无需额外付费；服务期内乙方应免费提供升级、运维和技术支持，服务期结束后 10 个工作日内，乙方应按照甲方指定的通用、可读取、可使用、可迁移的数据格式，完整导出并向甲方移交全部运维数据及资料，并配合完成运维资料、账号密码、故障台账、配置文档等的完整移交。导出及移交内容应真实、完整、可用，且经甲方验收确认。未经甲方书面同意，乙方不得以平台版权或使用权归属为由拒绝、拖延、限制数据导出或资料移交。。

15. **服务交付成果：**按时提供年度服务方案和服务计划、年度服务总结报告，定期提供服务月报及重大故障专题报告，每次维护结束后详细填写维护报告并于 3 日内报送，报告须经甲方指定人员签字确认。故障处理填报《现场技术服务申请表》《故障处理报告》，巡检

填报《巡检服务申请表》《巡检报告》，均经双方签字确认。

16. **人员要求：**运维人员须经甲方政治审查合格后方可上岗，运维人员应政治素质可靠、责任心强、无前科及违法犯罪记录，具备扎实专业技能和对应岗位资格证书。合同履行期间，乙方应保障运维人员全员到位，未经甲方书面同意，乙方不得擅自更换或抽调驻场人员，人员调整须至少提前 7 个工作日书面报甲方审批，经甲方书面同意后方可实施。甲方对任一运维人员不满意或认为其不适合继续履职的，有权书面要求乙方在 7 日内予以更换，乙方应无条件配合。乙方应与甲方及运维人员签订保密协议，每年组织不少于 2 次安全及保密教育培训；乙方应严格遵守公安机关（交警）网络安全相关规定，坚决杜绝“一机两用”违规外联等安全事件。对有重大影响的运维作业，乙方应安排在夜间或业务停顿期间进行，并至少提前 5 个工作日将实施方案和应急预案提交甲方，经甲方书面批准后方可实施。

17. **服务团队要求：**建立完整可靠的项目组织机构（含运维管理组、驻场服务组、二线技术支持团队），高空登高作业应具备相关安全资质及设备；服务团队严格遵守甲方相关保密规定。

五、服务质量及考核

1. **运维质量指标：**全年运维服务事件响应率 100%，运维事件响应及时率≥95%，事件发现及时率和事件总体解决率≥98%；从用户申告故障到服务响应时间小于 10 分钟；驻场人员不能解决需远程人员现场支持的，到达现场时间不超过 2 小时，从用户申告到故障解决持续时长限制在 3 小时内；运维服务不满意投诉每半年不超过 2 次，全

年用户满意度调查≥85%。

2.**可用性指标**：机房温度 23±2℃、相对湿度 40%-60%；中心供配电系统动力输出连续稳定无闪断，输出电压保持 220±5V，机房 UPS 不间断电源可用；中心气体消防系统保持正常可用，中心安防系统可用率≥98%；网络系统连续工作无中断，骨干网络可用率≥98%；服务器、虚拟机、存储及核心平台软件运行正常，承载业务系统连续无故障，数据完整、安全可用；不因供配电等机房环境、动力或网络因素导致业务系统崩溃中断、数据丢失。

3.**规范性要求**：乙方组建由专业工程师组成的运维服务团队；机房环境干净整洁，专业工具齐备；设立明确的人员岗位职责，制定严格的管理制度和操作指南，人员持证上岗，工作日志准确详实；建立符合国家、陕西省运维服务标准的服务体系规范。

4.**安全性要求**：乙方建立常态化风险防范措施和安全保密制度，经常性开展安全保密教育和培训，制定专项应急预案并定期演练；对出入人员、托管设备、计算机终端、移动介质等管理办法切实可行；电子政务网络不因病毒、木马等因素发生大面积瘫痪，未发生敏感和涉密信息泄露等事件，信息安全事件投诉每年不超过 2 次。

5.**考核方式**：甲方实行分月履约考核，每月按自然周期核算服务内容；甲方每半年组织一次全方位运维服务质量考核（分别在合同签订后的第 6 个月和第 11 个月进行），考核内容包括服务绩效（占 50%）、服务能力（占 30%）和满意度（占 20%），每次综合评分满分 100 分，年度综合评分取各月度履约考核和半年运维服务质量考核结果的平

均值。

6.**考核结果运用**：综合评分≥90 分评定为优秀，乙方完成全部交付、整改及资料移交义务的，甲方按合同价款的 100%结算；综合评分≥75 分且<90 分评定为合格，甲方按合同价款的 90%结算；综合评分＜75 分评定为不合格，甲方按合同价款的 80%结算。对于评定为不合格的，甲方有权要求乙方在 7 日内完成整改；整改后仍不合格的，甲方有权解除合同，并要求乙方退还已付服务费中对应不合格期间的款项。上述考核结算不影响甲方要求乙方承担故障赔偿、数据或信息安全责任、人员及第三方损害赔偿、逾期整改违约金及其他合同责任。已经支付的款项超过最终应结算金额的，乙方应在甲方书面通知之日起 5 个工作日内返还差额，逾期未返还的，甲方有权从质保金中扣除。

7.月度考核、半年度考核及年度最终考核均不构成甲方对乙方服务的最终认可或对既有违约责任的放弃。甲方在考核或付款后发现乙方存在漏报、瞒报、虚假记录、隐蔽故障、重复故障、数据丢失、网络安全事件、保密违规、资料不完整移交或其他未被当期考核发现的违约事项，仍有权要求乙方整改、返还相应款项、承担违约责任并向质保金索赔。乙方的保修、保密、数据安全、损害赔偿及资料移交义务不因甲方付款、考核或服务期届满而终止。

六、其他要求

1.本次运维服务期限一年，分月履约考核，每月按自然周期核算服务内容。

2.服务起止时间以双方正式签订合同载明日期为准，合同履行期

限一年，期满自动终止服务。

3.服务到期前30日，乙方须按照甲方要求，完整移交运维资料、账号密码、故障台账、配置文档的完整移交及其他与运维相关的资料，移交内容、格式及完整性须经甲方书面确认。乙方拒绝、拖延或未按期、完整完成移交的，每逾期一日按合同总价款的0.2‰向甲方支付违约金，甲方有权从质保金中直接扣收相应违约金。

4.乙方运维服务遵循ITIL/ISO20000/ITSS等通用运维标准规范，以及《中华人民共和国网络安全法》、GB/T 28827系列、GB/T 22239-2019等国家、行业相关标准及甲方有关运维管理制度。

七、违约责任

（一）乙方未按本合同第四条约定履行运维服务义务，未达到本合同第五条约定的服务质量及考核指标，违反本合同第八条保密义务，未按约定提供备品备件或人员配备不足的；因乙方原因导致甲方信息系统中断、数据丢失或发生安全事故的；乙方均应赔偿甲方因此遭受的全部损失。乙方逾期提供服务或响应超时的，每逾期一日，应按合同总价款的0.02%向甲方支付违约金。

（二）乙方未按合同要求提供服务或服务不能满足合同要求的，甲方有权书面通知乙方限期整改，乙方应在收到通知后7日内完成整改；逾期未整改或整改后仍不符合要求的，甲方有权单方解除合同，从质保金中扣收违约金，并有权要求乙方返还已收取的预付款，同时要求乙方赔偿由此造成的全部损失，并将违约情况报送政府采购监管部门备案。

（三）依据《中华人民共和国民法典》《中华人民共和国政府采购法》的相关条款规定和本合同约定，乙方未全面履行合同义务或者除本条第（二）项以外其他违约的，甲方同采购组织机构有权终止合同，并从质保金中扣收应付违约金及相关费用，追偿因此遭受的全部损失。乙方应赔偿的损失包括但不限于甲方为恢复系统正常运行支出的费用、依法承担的第三方索赔损失、政府罚款以及甲方为实现债权支出的律师费、诉讼费、保全费等维权费用，甲方并可据此报请政府采购监管机关依法对乙方进行相应的行政处罚。甲方违约的，应当赔偿给乙方造成的经济损失。

八、保密条款

乙方及其运维人员应严守工作秘密，对服务过程中知悉的甲方事项及信息予以保密；甲方机型配置、IP 地址、生产经营数据、软件等信息不得向第三方泄露；维护过程中涉及甲方系统数据信息的，必须先经甲方相关负责人认可；维护工作的数据信息（无论打印或介质上的）不得带离工作现场，不得随意拍照、复制和传播；所有资料、技术文档、业务信息数据应妥善保管，不得遗失、转借、复印拷贝、修改、删除。乙方违反本合同保密条款或发生违规外联、数据泄露等安全事件的，除依法承担相应刑事、行政及民事责任外，还应按合同约定向甲方支付违约金，且甲方有权立即解除合同。违约金不足以弥补甲方实际损失的，乙方应就差额部分予以赔偿。

九、合同生效及其他

1. 本合同自签订之日起生效。

2. 如本合同有未尽事宜，以谈判文件为准，谈判文件未做要求的，由双方依法订立补充合同，补充合同与本合同具有同等法律效力。

3. 合同争议的解决：合同执行中发生争议的，当事人双方应协商解决，协商达不成一致时，可向咸阳市杨陵区人民法院提请诉讼。

4. 本合同一经签订，不得擅自变更、中止或者终止合同；对确需变更、调整或者中止、终止合同的，须经甲方书面同意并按规定履行相应的手续。

5. 本合同附件（附件一《运维服务清单》、附件二《提升服务清单》）为本合同不可分割的组成部分，与本合同具有同等法律效力。

6. 本合同纸质文本一式四份，甲乙双方各执二份，自双方签字盖章之日起生效。

甲方（盖章）：杨凌示范区公安局交通管理支队

法定代表人/负责人或授权代表：

[2026]年[11]月[18]日

乙方（盖章）：陕西英广智能工程有限公司

法定代表人/负责人或授权代表：

[2006]年[11]月[17]日

附件一：运维服务清单

序号	产品类型	产品描述	数量	单位	维保方式	服务级别	服务期限（月）
1	前端交通智能设备	对于前端电子警察，卡口抓拍机，各类补光灯，雷视设备，智能终端 ，红绿灯，信控主机，网络交换路彐产品等设备提供维护服务和定期巡检服务	1	项	人工服务	7*24 小时服务	12
2	后端设备维护	支队公安网，视频专网等网络中涉及到的所有软硬件产品和网络交换传输产品提供维保服务及定期巡检服务	1	项	人工服务	7*24 小时服务	12
3	机房设备维护	人员脏场服务，机房供电系统，空调系统，日常巡检维护	1	项	人工服务	7*24 小时服务	12
4	网络维护	对支队办公区域、两个大队、六个中队等所有场所内各种网络进行日常维护监控，提供一体化运维平台，完成机房服务器、网络、数据库、系统平台等关键指标的整合与标准化处理，实现智能统一的网络运维监控服务。	1	项	网络运维服务	7*24 小时服务	12
5	现场备品备件保障服务	为保障系统稳定运行，提供备品备件保障服务，包含补光灯，闪光灯，硬盘，内网收发器，卡口摄像机，电子警察，智能终端，信号机主板，雷视一体机，交换机，倒计时线路板等常用设备的备件储备、快速更换、故障替换、应急保障服务，确保设施持续正常运行。	1	批	保障服务	7*24 小时服务	12
6	运维耗材及配套施工服务	提供系统运维所需耗材供应及配套施工服务，包含含水晶头、网线、电源适配器、扎带、插板、PVC 线管、水泥砂浆垫层、铺装路面地砖、混凝土施工等耗材配送、安装铺设、现	1	批	施工服务	7*24 小时服务	12

			场施工、售发维护服务。				

附件二：提升服务清单

序号	服务名称	数量	单位	服务方式	服务级别	服务期限（月）	服务内容
1	网络安全威胁提升服务	1	项	平台服务	7*24 小时服务	12	安全威胁提升内容： 旁路镜像抓取网络流量，对 L4_L7 层协议深度解码，支持 HTTP、DNS、邮件、数据库、SSH、RDP、TLS 加密流量、[illegible]协议；完[illegible]会话重组、文件还原，提取五元组、访问[illegible]为、应[illegible]数据，可按[illegible]存储 PCAP 原始报文，用于事后取证溯源。 IDS 入侵检测：[illegible]、暴力破解、蠕虫、漏洞利用、DDoS 攻击检测：Web 攻击检测：SQL 注入、XSS、webshell、命令执行等 Web 漏洞攻击识别。 异常行为检测：识别内网横向移动、异常外朕、大量数据外传等可疑行为：从网络流量还原传输的附件、脚本、可执行文件，做静态检测：部分型号可集成轻量沙箱能力，对可疑样本做基础动态分析。 加密流量检测：基于 JA3 指纹、流量行为模型识别加密隧道、恶意加密通信，无需全部解密报文。

2	运维安全提服务	2	项	平台服务	7*24小时服务	12	第三方运维安全提升内容： 集中管理各类资产账号（服务器、交换机、防火墙、数据库），实现账号代填，运维人员不需要知道资产真实密码。 保管设备密码，支持密码定期自动改密，密码随机化，减少人工保管密码泄露风险 角色权限划分：管理员、运维人员审计员，不同人员分配不同资产、不同操作权限，最小权限原则。 所有运维人员必须通过堡垒机登录资产，禁止直连服务器 / 网络设备：支持 SSH、RDP、Telnet、VNC、FTP、数据库（MySQL/Oracle）等协议。 按用户-资产-账号进行授权：谁、可以访问哪台设备、使用哪个账号、允许什么时间登录。 实时查看运维人员正在操作的屏幕会话，看到输入命令、桌面操作。 命令黑白名单：禁止执行 rm -rf、格式化、删除数据库等高危命令；可以拦截、告警、记录。 记录登录人、登录时间、源 IP、访问资产、执行命令、操作结果，日志防篡改。 外部员工、外包人员通过客户端，互联网上加密访问内部服务器、

							业务系统、禁止暴露内网业务直接到公网。本地账号、AD/LDAP 域对接、短信、令牌、双因素认证，校验接入用户身份。 对经互联网传输的数据做加密，防止互联网传输过程窃听、篡改，传输数据加密，支持 AES、国密等加密算法，保证会议传输数据不被窃取篡改。 接入前检查终端安全状态：杀毒软件、系统补丁、是否存在恶意软件，不合规终端禁止接入为网。

3	互联网域安全提升服务	1	项	平台服务	7*24 小时	12	互联网域安全提升内容： 基于 IP 地址、端口、协议、用户，应用制定策略，允许 / 阻断网络访问。例如禁止外网访问内部数据库端口，允许内网访问互联网。 源 NAT：内网多主机共用公网 IP 上网，隐藏内网真实地址； 目的 NAT：把公网访问映射到内网服务器，实现服务器对外发布。 识别微信、视频、下载、游戏等应用，不只是看端口，可限制特定 APP 使用、管控带宽。 病毒过滤：对网络流量做病毒、恶意代码检测。 防恶意 URL，阻断访问钓鱼、恶意网站。 记录访问、攻击、策略命中日志：发生攻击、异常访问时产生告警，可导出日志用于安全审计。 支持按源地址、目的地址、应用、用户做策略，业务系统固定走专线链路；普通上网流量多链路分担；特定应用强制走某条线路。