安康市公安局智防管控平台建设项目合同

委托方：安康市公安局（以下简称甲方）

受托方：中移系统集成有限公司（以下简称乙方）

根据《中华人民共和国民法典》和其他法律、法规的规定，并按照公正、平等、自愿、诚实信用的原则，甲乙双方经友好协商，同意按照以下条款和条件，签署本合同。

第一条 合同内容

1、合同名称：

安康市公安局智防管控平台采购项目

2、合同内容：

序号	项目/设备名称	数量	单位	含税单价/万元	税率	含税总价/万元	备注
（一）智防管控平台开发							本项目基于中国移动5G网络+移动云+大数据能力，落地OneCity平台、城市大数据平台、集成平台，为甲方提供项目支撑工作。
A-01	基层基础管控平台	1	项	¥63.00	6%	¥63.00	
A-02	“两队一室”派出所主防平台	1	项	¥135.00	6%	¥135.00	
A-03	移动端APP	1	项	¥21.00	6%	¥21.00	
A-04	数据接入与上报	1	项	¥10.00	6%	¥10.00	
	小计					¥229.00	
（二）平台运行环境							
B-01	计算存储系统	1	项	¥18.00	13%	¥18.00	
B-02	安全防火墙系统	1	项	¥9.00	13%	¥9.00	
B-03	主机监控与审计系统	1	项	¥10.00	13%	¥10.00	
	小计					¥37.00	
（三）其他							
A-08	第三方软件测评	1	项	¥10.00	6%	¥10.00	
A-09	网络安全等级保护测评	1	项	¥10.00	6%	¥10.00	
A-10	密码应用安全性评估	1	项	¥12.00	6%	¥12.00	
A-11	系统集成	1	项	¥14.00	6%	¥14.00	
	小计					¥46.00	
	合计					¥312.00	

具体要求详见【附件一、建设内容】。

第二条 工期要求

合同签订后 30 天内完成

第三条 合同金额及支付

乙方依据双方签署的合同内容提供软硬件及相关服务，甲方需按照合同约定期限向乙方支付相关费用。

1、合同金额

本合同总金额 ￥3120000.00 （小写）元人民币（大写：人民币 叁佰壹拾贰万元整 ）

2、付款方式

（1）合同签订后一周内支付合同总金额的 60 %；

（2）安装调试完毕且初步验收合格后支付合同总金额的 20 %；

（3）项目审计完成后，以审定金额为准支付合同剩余金额；

3、双方结算相关信息如下：

（1）甲方结算信息：开户行名称：工行陕西安康汉滨支行，账号：2607060209096406455

（2）乙方结算信息：开户行名称：招商银行股份有限公司北京分行营业部，账号：8888015100002818

第四条 甲乙双方职责

1、甲方职责

1.1 甲方应配合乙方做好项目实施的组织协调工作，并配有专职工程管理人员对施工质量等进行全程监督的权利。

1.2 甲方应会同有关方面对系统性能进行检查，对项目质量进行监督，项目完工时应及时组织工程验收。

1.3 甲方应严格按照合同约定的付款时间及方式支付合同价款。

1.4 组织验收，并向乙方出具验收合格证明。

1.5 选派工作人员参加乙方组织的技术培训。

1.6 项目实施期间，甲方应明确一名联系人（甲方联系人姓名：刘亮，联系电话：19991529992），负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。甲方联系人如发生变更，需以书面形式通知乙方。

2、乙方职责

2.1 乙方应遵守甲方及有关单位安全管理制度，文明施工。

2.2 乙方应接受甲方委托的项目负责人对本项目建设的监督。

2.3 严格按照本合同要求开展项目实施，对项目工程涉及的质量、进度、售后服务等承担相关责任。

2.4 乙方提交的竣工资料的内容：项目技术资料、质量保证资料和竣工结算等。

2.5 乙方在项目实施过程中，不得随意更改本合同确定的内容、质量、技术要求。

2.6 乙方应与甲方积极配合，随时汇报工作情况，研究工作措施，及时解决项目实施过程中存在的问题。

2.7 按照合同规定组织对甲方相关人员的培训，使其能够基本掌握有关软硬件的使用和日常维护，具备排除系统简单故障的能力。

2.8 为保证项目高质量交付，可以在项目实施过程中引入合作伙伴，委托具备相应实施能力的单位负责项目的相应部分实施工作。

2.9 本项目基于中国移动5G网络+移动云+大数据能力，落地OneCity平台、城市大数据平台、集成平台，为甲方提供项目支撑工作。

2.10 项目实施期间，乙方应明确一名联系人（乙方联系人姓名：白如艾，联系电话：13684997151），负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。乙方联系人如发生变更，需以书面形式通知甲方，并征得甲方书面同意，并且替换人员必须与前期人员的资格和业绩相同或高于前期项目经理。

第五条 质量条款

1、乙方保证其提供的软硬件须符合国家现行的相关设计、安全、质量标准，如无相关国家标准，依次执行本行业设计、安全、质量标准有关规范及企业标准及招标文件的要求。

2、乙方承诺严格按国家相关标准、质量管理体系和技术标准组织实施，对质量进行严格检验，保证提供的项目质量符合国家标准。

3、乙方应负责并保证系统达到采购需求及正常运行。

第六条 项目验收

1、项目安装调试完毕后，乙方向甲方提交相关报验资料，甲方根据合同要求组织相关人员进行初步验收；

2、系统正常运行期限满2个月，乙方提交书面试用报告，经甲方同意后在7个工作日内组织最终验收。

3、验收依据：

3.1 本合同及项目有关招标文件、投标文件。

3.2 国家有关技术规范及法律文件。

4、系统自通过验收之日起进入系统维护期。

第七条 售后服务

1、项目质保期：本项目质保期为 1 年，质保期开始之日为工程验收合格之日起开始计算。

2、乙方的售后服务须符合国家的有关规定，因乙方拒绝提供售后服务，而使甲方增加的费用由乙方承担。

3、乙方设立维护热线电话， 2 小时响应，在质保期内出现甲方无法独立排除的故障时，乙方应派员在 4 小时内到达现场， 8 小时内修复。

4、如果乙方在收到通知后2天内没有弥补缺陷，甲方可采取必要的补救措施，但其风险和费用将由乙方承担，甲方根据合同规定对乙方行使的其它权力不受影响。

5、在质保期内无偿提供人员和技术支持，配合甲方进行技术改进；乙方应提供质保期内日常维护计划。

6、保修期内，因甲方使用、管理不当所造成的故障，乙方提供有偿服务。

第八条 知识产权

1、本次项目所使用软件，其相关知识产权归属安康市公安局。

2、在未经本次项目软件知识产权所有方书面允许的情况下，甲乙双方不得以任何方式将上述软件产品、文档及或软件的任何数据或程序向甲乙双方以外的任何第三方明示或暗示地披露、提供或以任何方式加以利用。

3、甲方不得将乙方提供的工程业务规范、标准和要求以及开发上述相关软件产品的过程中获悉的任何技术文档、相关的技术规范或技术标准明示或暗示地提供或透露给除甲方以外的任何第三方或以任何方式利用。

4、乙方保证其交付的任何产品、服务和文档等不侵犯第三方的知识产权，如因知识产权问题导致甲方遭受任何索赔、诉讼或损失，乙方应负责解决并赔偿甲方的全部损失，如因上游知识产权方政策调整、许可终止或其他客观原因导致服务无法持续，乙方有权据实顺延服务或免责，双方应协商妥善解决。包括但不限于：诉讼费、保全费、公告费、鉴定费等。

第九条 违约责任

1、乙方逾期提供服务的，乙方应按逾期提供服务总额每日万分之五向甲方支付违约金，由甲方从待付款中扣除。因甲方提供数据不全等不可抗力原因造成乙方逾期提供服务的，乙方不承担逾期责任。

2、除因不可抗力或任何一方不能预见、不能避免和不能克服的客观情况造成合同无法履行及其他法定、约定事由外，任何一方不得单方面解除合同。

3、任何一方造成项目延期或其他违约责任发生的，违约方应承担全部责任，同时守约方有权要求违约方赔偿全部损失。

第十条 争议解决

1、所有与合同及合同执行有关的争议将通过各方友好协商解决，如果在一方提出协商要求后的十天内，双方通过协商不能解决争议，则向项目所在地人民法院提起诉讼。

第十一条 通知与送达

1、本合同项下任何一方向对方发出的通知、信件、电子邮件等，均须采取书面形式。一方当事人变更联系方式的，应当在变更后3日内及时书面通知对方当事人，对方

当事人实际收到变更通知前的送达仍为有效送达，电子送达与书面送达具有同等法律效力。

甲方联系人：刘亮
联系电话：19991529992
联系地址：安康市高新区安康大道30号
邮编：725000
传真：0915-3181169
电子邮箱：921895458@qq.com

乙方联系人：赵永乐
联系电话：18702983996
联系地址：陕西省西安市团结南路11号国寿金融中心
邮编：710000
传真：0311-80998600
电子邮箱：zhaoyongle@cmict.chinamobile.com

2、双方将按如下规定确定通知被视为正式送达的日期；以专人递送的，接收人签收之日视为送达：

（1）以专人递送的，接收人签收之日视为送达；

（2）以传真方式发出的，以发件方发送后打印出的发送确认单所示时间视为送达；

（3）以特快专递形式发出的，发往本市内的，发出后第2日视为送达。发往国内其他地区的，发出后第3日视为送达。发往港、澳、台地区的，发出后第7日视为送达。发往境外其他国家或地区的，发出后第10日视为送达；

（4）以挂号方式发出的，发往本市内的，邮寄后第7日视为送达。发往国内其他地区的，邮寄后第15日视为送达。发往港、澳、台地区的，邮寄后第35日为视为送达。发往境外其他国家或地区的，邮寄后第45日为视为送达。

（5）以电子邮件发出的，自前述电子文件内容在发送方正确填写地址且未被系统退回的情况下，视为进入对方数据电文接收系统即视为送达。若送达日为非工作日，则视为在下一工作日送达。

3、本条第一款约定的联系方式亦为双方工作联系往来、法律文书及争议解决时人民法院和/或仲裁机构的法律文书送达地址。

4、合同送达条款与争议解决条款均为独立条款，不受合同整体或其他条款的效力的影响。即使本合同变更、撤销、解除、终止或认定无效的，该条款约定依然有效。

第十二条 合同生效

1、本合同一式肆份，甲乙双方各执贰份，经双方法定代表人或授权代表签字并加盖单位公章后生效，具有同等法律效力。

2、本合同执行日期为_____年_____月_____日至_____年_____月_____日止。

（以下无正文）

合同名称：《安康市公安局智防管控平台建设项目合同》

甲方（盖章）：【安康市公安局】

法定代表人/负责人：

签订日期：2025.11.10

乙方（盖章）：【中移系统集成有限公司】

法定代表人/负责人：

签订日期：2025.11.10

附件一、建设内容

（一）项目内容

本项目是以新一代公安信息网络为依托，在市局大数据平台搭建基层基础管控平台和派出所“两队一室”平台，采用市局、分县局、派出所分级应用的模式，实现派出所工作数字化以及数字“赋能”的应用，把辖区内所有的感知设备，特别是海量的社区资源探头在一张图上进行展示，并充分调动社会力量参与社会治理工作，真正实现“发案少、秩序好、人民满意”的目标。

（二）技术要求

1、基层基础管控平台

在市级建设“基层基础管控平台”，对各类警务工作的信息进行集成，统一开放数据服务，为派出所工作任务提供资源和保障，为基层基础工作赋能；同时根据派出所主防业务需求，优化各类业务流程，建立业务规范，形成业务标准件，指导基层基础工作规范开展；汇集上级指令和各警种的任务需求，统一下发、统一任务调度。

2、“两队一室”派出所主防平台

建立派出所“两队一室”平台。“两队一室”是一种新型的基层派出所内部组织结构，其中“一室”是指综合指挥室，主要负责派出所一屏总览、指挥一张图，巡逻防控、警情处置、视频巡查、勤务安排，“两队”是指案件办理队和社区警务队，案件办理队主要三高分析、案事件分析、分色预警、法律法规查询等。社区警务队主要负责电子台账、要素分析、一标三实、人员管理、网格管理等工作

3、移动端APP

围绕社区警务等派出所基础工作业务需求，构建警务通端APP应用，支撑社区民警、协辅警在移动端进行接单工作、信息报送、任务处置和任务流转等操作，实现赋能精准到业务、业务随势标准到表单、工作协同瞄准到个人、工作考核精细到任务。进一步提高基层移动作战能力与实时处置效能

4、数据接入与上报

基于省市相关系统业务规范与数据标准，依托省级治综平台、警综平台、情指行一体化平台等数据接口建立数据接入，实现数据赋能本地系统;同时，开放数据共享，为省级治综平台提供数据上报通道。

5、平台运行环境

包含计算存储系统、安全防火墙系统、主机监控与审计系统。

6、第三方软件测评

第三方软件测评由独立于开发方和使用方的专业机构执行，严格遵循相应认证标准，测试流程需涵盖测试计划与设计、测试实施及报告编制等环节。

7、网络安全等级保护测

由独立于开发方和使用方的专业机构执行开展测评工作，完整执行定级、备案、建设整改、等级测评及持续运维流程。测评需覆盖系统安全性、可用性、完整性、保密性及抗攻击能力，验证安全控制措施是否符合相应等级保护要求，并出具符合国家规范的测评报告。

8、密码应用安全性评估

密码应用安全性评估（密评）应依据标准，对网络与信息系统使用商用密码的合规性、正确性和有效性进行检测验证。评估需聚焦密码技术应用场景，确保其满足国家安全要求，并形成具备法律效力的评估报告。

9、系统集成

包含基础环境、硬件、软件及安全四个维度的集成实施，需制定分阶段实施方案，明确各子系统接口规范、兼容性要求及联动机制。安全集成需设计多层次防护架构，配置访问控制、数据加密等策略，并提供完整的实施方案、测试报告及运维文档，确保系统功能稳定、数据交换安全。

（三）技术参数

A-01、基层基础管控平台软件开发

1、任务管理

（1）基层基础管控平台任务管理为市县基管中心民警开放使用，依托大数据警务云资源，并利用大数据AI预警研判的能力，生成预警指令，任务运行管理接入预警指令信息，形成管控对象，对管控对象进行研判分析、风险标签标识，产生对应的工作任务清单。

（2）通过调度配置、任务配置，生成按照工作表单、赋能表单、考核要求的任务工作清单，调度给派出所或社区民警。

2、质效监督

（1）质效监督功能向市县基管中心民警、派出所综合指挥室民警开放，包括社区民警在线情况监督和工作成效监督两个阶段，其中在线情况监督主要包括登录情况、在线统计、和在线警力上图；

（2）工作成效监督主要包括：工作日志、日志看板、工作档案、任务处置质效统计分析、以及标准件下发情况统计等。

（3）通过在线情况监督、工作成效监督，实现任务处置的质效监督业务。

3、绩效考评

绩效考评由前期准备、考评规则配置、报表生成三个阶段。

（1）前期准备：市县基管中心考核民警根据考核方案要求展开考核项目分析、指标定义（到责任区）、指标数据生成、以及参评单位的设置，接着进入考核规则配置阶段；

（2）考评规则配置：逐步从考核方案、考核细项、及考核细项计分规则和考核方式配置完成考核规则配置阶段，系统根据考核项目的考核方式。

（3）报表生成：对于系统自动考核的细项，根据指标结果和计分规则生成细项得分，对于手工考核的细项，则考核民警应录入定性指标结果，并生成细项得分，系统根据考核细项得分累加，分别生成分县局排名、派出所单位排名、警务责任区排名结果，查看具体的考核细项得分情况。

4、系统配置

支持字典管理、指标配置、报表配置、台账配置、套打配置、通知通告、常用下载、卡片配置等系统配置。

5、权限配置

（1）权限配置主要给系统管理员开放使用。通过用户—岗位—角色—菜单或操作资源的关联关系，实现不同用户具备不同的菜单或操作资源的控制权限。

（2）一个用户可分配多个岗位，通过工作台进行岗位访问切换。

A-02、两队一室”派出所主防平台软件开发服务

1、工作台

支持个人信息维护，修改新增，查看相关工作指标及工作任务提醒及预警。

2、任务管理

（1）基层基础管控平台任务管理为市县基管中心民警开放使用，依托大数据警务云资源，并利用大数据AI预警研判的能力，生成预警指令，任务运行管理接入预警指令信息，形成管控对象，对管控对象进行研判分析、风险标签标识，产生对应的工作任务清单；

（2）通过调度配置、任务配置，生成按照工作表单、赋能表单、考核要求的任务工作清单，调度给派出所或社区民警。

3、标准地址

标准地址业务包括标准地址查询、标准地址登记两个部分，其中：

（1）标准地址查询：实现标准地址查询功能，找到某个具体标准地址，并进行标准地址入户访查，通过地址进入地址现场，房屋信息、单位信息、人员信息的展示和登记、变更、注销。

（2）标准地址登记：通过标准地址查询，找到某个具体门牌标准地址，单个或批量录入下级户室单元地址。

4、实有房屋

（1）实有房屋包括实有房屋登记、实有房屋变更、实有房屋注销、承租情况登记、和出租房检查等部分。社区民警通过查询实有房屋地址、或者房主信息进行信息查询，通过录入房屋基本信息、或者对已登记房屋进行信息变更或注销房屋；

（2）若房屋为出租房，则社区民警查询具体房屋信息后，可进行承租情况录入登记，同时根据出租房检查要求对接任务标准件定期生成出租房检查任务进行检查登记。

5、实有人口

社区民警通过入户访查进行实有人口核实登记，查询房屋具体地址，查询房屋及其居住人员信息，比对发现人员流入流出情况，可对已流出人员登记流出信息，或者登记新流入居住人员，通过省、部级人口信息查询服务，获取居住人员基本信息，核实登记人员流入信息，实现实有人口核实登记业务流程。

6、安全隐患

（1）派出所社区民警现场发现隐患，若安全风险隐患未违反治安处罚条例，则现场处罚并录入处罚结果，否则，责令隐患单位进行限期整改。

（2）若按期完成隐患整改，则录入整改情况，反之，对于未按期完成隐患整改的情况，则逐级上报分县局、市局进行责令整改处置，录入整改情况。

7、情报线索

社会群防力量发现情报线索，通过互联网移动应用上报情报线索，系统通过安全边界上传公安网社区警务平台，民警收到情报线索后，进行排查核实，进行情报线索处置。

8、安全防范

（1）安全防范针对专项任务开展社区民警检查，检查对象包括：校园、流动人口、不良未成年人、危爆品从业单位、寄递业、以及涉林要素。

（2）通过市县基管中心进行任务准入、调度、派发、任务标准化等流程，形成专项工作任务清单下发给社区民警执行处置，并反馈检查结果，系统生成统计报表展示。

9、群防群治

群防群治为派防范座谈：

（1）出所用户开放使用，采集辖区内群防群治组织、群防群治队员信息。录入群防群治组织信息检索条件，若未登记，则可发起群防群治组织信息登记；也可对已登记群防群治组织信息发起注销、变更登记。

（2）同时，群防群治组织可关联查询该组织的成员信息，发起群防群治成员信息登记，也可对已登记群防群治成员信息发起注销、变更登记。

10、防范座谈为派出所社区民警开放使用，采集社区民警开展的防范座谈信息，录入防范座谈信息检索条件，若未登记，则可发起防范座谈信息登记；也可对已登记防范座谈信息发起注销、变更登记。

11、安全宣传

安全宣传为派出所社区民警开放使用，采集社区民警开展的安全宣传信息，录入安全宣传信息检索条件，若未登记，则可发起安全宣传信息登记；也可对已登记安全宣传信息发起注销、变更登记。

12、巡逻防控

巡逻防控为派出所领导、社区民警开放使用，包括巡逻任务配置下发、现场巡逻两个阶段。

（1）派出所领导发起巡逻任务，通过巡逻路线录入、签到点管理设置、路线绘制、以及巡逻人员排班，向社区民警推送巡逻任务；

（2）社区民警通过移动端接收巡逻任务，巡逻过程中系统自动采集位置点，根据设置的签到点打卡签到，完成巡逻任务。

（3）整个巡逻过程路线轨迹，巡逻过程可通过地图可视化展示，接受派出所领导巡逻监督。

13、涉险公共区域摸排检查

（1）涉险公共区域针对社区民警开展日常检查，检查对象包括：涉险公共区域、涉险公共区域检查部位。

（2）通过市县基管中心进行任务准入、调度、派发、任务标准化等流程，形成涉险公共区域日常工作任务清单下发给社区民警执行处置，并反馈检查结果，系统生成统计报表展示。

14、矛盾纠纷排处

（1）矛盾纠纷排处为派出所民警、所领导和分县局领导开放使用，所领导和分县局领导进行风险评估审核，协助矛盾纠纷化解。包括矛盾纠纷建档采集和风险评估、干预化解、跟进回访三个阶段。

（2）派出所民警根据纠纷警情、现场工作登记进行矛盾纠纷信息核实登记，并进行现场调解，未化解矛盾纠纷进行风险评估，采集相关材料，提交所领导、分县局领导审批。所领导根据矛盾纠纷风险评估情况，进行审批，对于非警务类纠纷，则推送给政府其他部门进行化解，派出所民警跟进化解情况。

（3）系统定期对未化解矛盾纠纷发起干预化解，生成矛盾纠纷干预化解清单，推送派出所民警（社区民警）组织现场或所内调解，并对未化解矛盾纠纷发起风险评估，采集相关材料，提交所领导、分县局领导审批。

（4）系统根据已化解矛盾纠纷发起跟进回访，生成矛盾纠纷跟进回访清单，推送派出所民警（社区民警）进行现场回访，登记回访记录，确认矛盾纠纷风险情况，对于有风险矛盾纠纷，采集相关材料，提交所领导、分县局领导审批。

15、治安单位

（1）治安单位为派出所社区民警、所领导以及管理业务部门开放。包括治安单位管理、单位检查两个阶段。

（2）派出所社区民警通过查询辖区治安单位信息，可对已登记治安单位发起修改，包含：单位基本信息修改、管理部门修改、工商税务信息修改、从业人员信息修改、以及物/技/人防信息修改，也可以发起辖区治安单位信息登记，并提交所领导和管理业务部门审批。系统定期生成辖区治安单位日常检查工作清单，并与基管中心任务标准件对接，通过市县基管中心下发给社区民警执行处置，并反馈检查结果，系统生成统计报表展示。

16、辖区公共场所电子显示屏

公共场所电子显示屏为派出所用户开放使用，采集辖区内公共场所电子显示屏信息，录入电子显示屏信息检索条件，若未登记，则可发起电子显示屏信息登记，可根据实际需要，提交所领导进行审批审核；也可对已登记公共场所电子显示屏信息发起注销、变更登记。

17、帮扶救助对象

帮扶救助对象为派出所用户开放使用，采集辖区内帮扶救助对象信息，录入帮扶救助对象信息检索条件，若未登记，则可发起帮扶救助对象信息登记，可根据实际需要，提交所领导进行审批审核；也可对已登记帮扶救助对象信息发起注销、变更登记。

18、失物招领

失物招领为派出所用户开放使用，采集失物招领信息，录入失物招领信息检索条件，若未登记，则可发起失物招领信息登记；也可对已登记失物招领信息发起注销、变更登记。

19、工作登记

工作登记为派出所用户开放使用，采集工作登记信息，录入工作登记信息检索条件，若未登记，则可发起工作登记信息登记；也可对已登记工作登记信息发起注销、变更登记。

20、警格信息管理

派出所民警通过警务区登记，并对警务区划分居（村）委、责任区民警分配等操作，提交所领导审批审核，实现警务责任区管理业务。

A-03、移动端APP软件开发服务

1、社区警务智能工作台

统筹定制基层社区民警的职能工作桌面。社区警务智能平台使用对象为社区民警，根据社区警务室业务现状进行整理和分析，实现社区民警全面工作动态掌握和态势预警。

2、任务管理

根据业务警种的工作要求对各类社区民警业务标准件任务管理的工作平台。

3、标准任务

通过调度配置、任务配置，生成按照工作表单、赋能表单、考核要求的任务工作清单，调度给派出所或社区民警。

4、管理实有人口

支持标准地址，实有人口，实有房屋采集更新维护；支持严重/不良行为未成年人信息信息采集更新及维护；同时支撑对辖区实有人口信息进行抽查和抽查复核。

5、掌握社区民意

（1）实现安全隐患管理功能，实现辖区内安全隐患信息新增、修改、注销，包括发现时间、是否已化解、是否落实稳控措施、隐患内容、稳控措施、现场照片等内容。

（2）实现情报线索管理功能；

（3）实现辖区内情报线索信息新增、修改、注销，包括提供人信息、线索信息、评估信息、事件信息等内容；

（4）实现村干部信息管理功能，实现辖区内村干部信息新增、修改、注销，包括现任村书记和上一任村书记以及现任村长和上任村长的信息。

6、组织安全防范

（1），采集辖区内群防群治组织、群防群治队员信息。录入群防群治组织信息检索条件，若未登记，则可发起群防群治组织信息登记；也可对已登记群防群治组织信息发起注销、变更登记。

（2）同时，群防群治组织可关联查询该组织的成员信息，发起群防群治成员信息登记，也可对已登记群防群治成员信息发起注销、变更登记；支持巡逻防控签到、巡逻路线规划、巡逻小组管理、巡逻排班管理、巡逻轨迹可查；支持涉险公共区域针对社区民警开展日常检查，检查对象包括：实现涉险公共区域摸排检查管理功能，实现辖区内涉险公共区域摸排检查信息新增、修改、注销，包括部件信息、部件检查清单等信息。

7、管理社区秩序

（1）实现行业单位信息采集、录入、信息更新维护，支持日常检查任务下发执行；

（2）寄递业基于寄递业数据，通过数据建模的方式梳理出需要排查的对象数据，

转化为标准件任务通过工作指令的方式自动下达给基层民警，进行隐患摸排；

（3）矛盾纠纷信息采集登记、纠纷日调节、上报、处置、归档查询等；

（4）基于辖区公共场所电子显示屏数据提供查询功能，实现通过部署部位、显示屏名称等条件辖区内辖区公共场所电子显示屏查询展示。

8、服务辖区群众

帮扶救助对象为派出所用户开放使用，采集辖区内帮扶救助对象信息，录入帮扶救助对象信息检索条件。

9、其他常用功能

（1）支持民警相关工作登记；

（2）针对系统功能做出功能评价；

（3）提供假期申请管理功能，实现假勤情况的查询、登记功能，包括假勤类型、开始结束时间、申请天数、申请事由、照片等信息；日志查询功能，实现通过日志类别、所属单位、所属警务区、地址名称、起始截止日期、登记人等条件查询日志信息；

（4）支持涉林从业人员情况、林区作业审核审批情况、野生动物经营场所、森林防火风险区域情况、涉林企业信息、特许狩猎证件核发情况。

A-04、数据接入与上报软件开发服务

1、数据接入

基于省市相关系统业务规范与数据标准，依托省级治综平台、警综平台、情指行一体化平台等数据接口建立数据接入，实现数据赋能本地系统。

2、数据上报

开放数据共享，为省级治综平台提供数据抽取通道。

A-05、平台运行环境（计算存储系统）

1、处理器：配置≥2颗CPU；单颗主频：≥2.6GHz，核数：≥28；

2、内存：配置≥768GB，单根内存≥32GB；

3、系统盘：配置≥2块960GB SSD；

4、数据盘：配置≥12块8TB 7.2K SATA；

5、缓存盘：配置≥2块3.2TB NVMe SSD；

6、RAID卡：1块独立RAID卡，支持RAID0/1/10/5/6/50/60，4GB缓存；

7、网络：配置≥4个10GE光口，配置≥4个千兆电口；

8、电源：配置≥2000W冗余双电源；

9、超融合软件：配置适配现网的超融合计算节点软件和授权；

10、服务：提供介质保留服务；兼容现网超融合系统。

A-06、平台运行环境（安全防火墙系统）

1、标准机架式设备；8个千兆电口，4个千兆光口，4个万兆光口；2个扩展槽位，吞吐量≥20Gbps，最大并发连接数≥1500万，每秒新建连接数≥8万；

2、支持双栈.6to4隧道实现IPv6终端穿越IPV4网络的访问；

3、支持基于源和目的地址的连接排行，支持端口流量统计；

4、支持静态路由，动态路由（OSPF.RIP.BGP.ISIS等），VLAN间路由，单臂路由，组播路由等；

5、支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路；

6、支持基于 WEB地址URL的策略路由，可实现将不同类型的网站流量智能分配到不同的链路；

7、支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路；

8、支持链路聚合功能，支持 802.3ad 和静态轮询.热备等多种模式，MAC.MAC&IP.IP&Port多种聚合负载算法；

9、支持基于数据包的安全域.地址.用户及用户组.MAC.端口号.服务.域名等进行安全策略控制；

10、支持命中数追踪功能，可根据具体策略直接追踪到当前命中的会话。；

11、支持一体化安全策略配置，可以通过一条策略实现用户认证.IPS.AV.URL过滤.协议控制.流量控制.并发.新建限制.垃圾邮件过滤.审计等功能,简化用户管理；

12、支持同一个地址对象中可以包含IP.IP段.IPrange.排除地址等多种类型；

13、支持针对策略中的源.目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制；

14、支持主流ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD攻击防护，采用专业高效攻击防护算法，非采用简单的阈值进行攻击防护；

15、支持web界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度.报文数量.抓包时间及采样频率等基本参数；支持根据协议.源目的IP.端口等参数进行数据报文过滤；

16、支持全方位.多角度的风险趋势呈现。支持以曲线图形的方式呈现全网和核心资产的风险变化趋势。支持以柱状堆叠图形（按安全事件分类）的方式呈现全网和核心资产安全事件的趋势统计，每类安全事件是否参与统计可调节。支持以处理动作（如阻断/放行）的趋势统计；

17、支持日志中文化，可显示配置命令日志的操作人；

18、支持在三权分立模式下，对日志文件的加密导出/导入；

19、支持端口联动，支持上下行端口组的联动，可以实现单端口决定同组中的任意接口失效启动链路切换；

A-07、平台运行环境（主机监控与审计系统）

1、服务端支持在X86架构下欧拉24.03最小化系统中安装部署，也支持在飞腾ARM架构下银河麒麟V10操作系统中安装部署；产品客户端支持在常见Windows.Linux系统以及主流的国产化系统中部署；产品支持同一个服务端对安装在不同类型操作系统的客户端进行统一管理；

2、应具备多维度的态势大屏，至少包括资产态势大屏.运维态势大屏.威胁态势大屏.数据安全态势大屏。展示内容至少包括威胁告警统计.攻击阶段统计.威胁等级统计.漏洞信息Top5.终端威胁告警Top5.敏感信息Top5.敏感终端Top5.最新告警事件.威胁态势评分等信息

3、具备对全网终端资产进行统一管理和资产画像能力：可提供基于DeepSeek的智能分析，实现单个终端与全网终端的风险解读，直观展示终端资产的综合健康状态，并为用户提供合理的优化策略与处置建议；

4、具备资产运维和资产发现能力：可对终端资产进行关闭.重启.锁屏.结束进程.断开网络.远程协助等操作，同时可通过ARP.PING.NMAP三种方式对非法接入的终端资产进行探测，发现未安装客户端的终端资产；

5、具备资产清点能力，至少包括数据库.中间件.环境变量.内核模块.共享目录.Web应用.Web站点.安装包.证书等资产信息；

6、具备资产处置列表，可查看威胁告警的人工处置记录，并可解除处置，便于运维人员恢复处置操作；

7、具备对全网资产进行一键体检的能力，可一键完成漏洞风险.合规检查.弱密码检查.病毒查杀.Webshell检测.内存马检测.反弹shell等体检项目。同时，具备风险评估中心，能够根据终端威胁风险情况进行失陷终端分析.勒索风险评估.全网威胁统计.泄露防护统计等；

8、具备终端风险管理能力，至少包括漏洞检查.弱密码检查.暴露面管理能力；支持检测的漏洞类型应至少包括系统漏洞.应用漏洞.中间件漏洞.数据库漏洞等；弱密码检查应包含系统弱密码和应用弱密码，内置弱密码库，也可根据需要配置弱密码规则生成弱密码字典。暴露面管理能力应支持对全网资产进行网络暴露面检测.判定暴露范围，并能够根据检测结果引导用户进行暴露面收敛；

9、具备基线检查能力，能够对资产进行即时和定时基线检查，也能够直观的展示未通过项.检查项通过率.未通过主机数.主机通过率等结果信息；同时，内置通用基线模板和等保基线模板，并且支持自定义基线模板，通用基线模板支持自定义评分规则；

10、具备病毒查杀能力，可自行选择查杀效率.查杀位置.查杀引擎.处置方式等，并且应直观展示已处理和未处理的病毒数量，展示内容应至少包括已处理/未处理的全病毒数量.已处理/未处理的勒索病毒数量.已处理/未处理的挖矿病毒数量.已处理/未处理的蠕虫病毒数量；同时，针对Windows系统，具备勒索病毒专项防护能力，包括勒索诱捕.文件保险箱.数据备份等，实时检测勒索病毒，防止勒索病毒入侵；

11、具备威胁行为检测的能力，包括端口扫描.暴力破解.异常登录.主机蜜罐.异常行为等；具备敏感行为的检测能力，包括系统命令篡改.敏感文件访问.系统日志文件删除.自启动项添加.敏感命令执行等，全面的判断终端是否存在威胁行为；

12、具备行为基线检测能力，支持对进程行为.网络连接行为.端口监听行为.DNS访问行为.登录行为进行建模，并形成行为基线进行异常判断；

13、具备安全审计能力，应包括软/硬件变更审计.资源使用审计.账号变更审计.文件操审计作.注册表行为审计.命令行审计.打印行为审计.刻录行为审计.FTP访问行为审计.网站访问行为审计等，便于审计人员溯源违规行为；

14、具备系统加固的能力，支持对Windows系统的账户策略.本地策略.环境策略.注册表保护等项目进行安全加固，保证Windows系统的安全；具备外设管控能力，支持对U盘.光驱.软盘.手机平板.打印机.摄像头等外设进行使用控制；针对Windows系统，产品还应具备对移动存储介质的认证和加密功能，可实现对U盘的授权认证管理.专用目录加密认证管理以及全盘加密认证管理。此外产品还应具备身份鉴别的能力，包括准入认证.终端Ukey登录认证等多种方式，保障终端资产入网.登录系统的严格身份验证，防止非法身份入网；

15、具备对端口.进程.网络.文件等多方面的管控能力，并具备剧本式的全网自动响应能力，可根据告警事件类型编排响应动作.响应时间等。产品需支持与同品牌防火

墙设备深度联动实现应用准入控制，仅允许安装客户端且合规的终端访问受保护资源，对未装客户端用户提供浏览器友好引导自助安装，并对不合规终端实施访问阻断。；

16、具备微隔离功能，能可视化的展示全网资产的网络访问关系，形成安全的安全访问控制，缩小网络暴露面；

17、支持客户端运行环境需支持windows终端部署。

18、主机授权数量≥200个。

A-08、第三方软件测评

1、第三方软件测评由独立于开发方和使用方的专业机构执行，严格遵循相应认证标准，测试流程需涵盖测试计划与设计、测试实施及报告编制等环节。

2、测试内容应包括功能测试、性能测试及安全漏洞检测，确保报告具备独立性和客观性，全面反映软件质量与可靠性。

A-09、网络安全等级保护测

1、本系统应依据《信息安全技术网络安全等级保护基本要求》GB/T22239-2019、《信息安全技术网络安全等级保护定级指南》GB/T22240-2020等相关标准规范，确定非涉密信息系统网络安全等级，并根据等级的划分施行相应的安全防护措施。由独立于开发方和使用方的专业机构执行开展测评工作，完整执行定级、备案、建设整改、等级测评及持续运维流程。

2、测评需覆盖系统安全性、可用性、完整性、保密性及抗攻击能力，验证安全控制措施是否符合相应等级保护要求，并出具符合国家规范的测评报告。

A-10、密码应用安全性评估

1、按照信息系统已定的或初步拟定的网络安全等级保护级别，结合本项目实际情况与系统安全风险控制需求，以及《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）针对该系统网络安全保护等级提出的密码应用要求，对系统的密码应用需求进行分析。

2、密码应用安全性评估（密评）应依据标准，对网络与信息系统使用商用密码的合规性、正确性和有效性进行检测验证。

3、评估需聚焦密码技术应用场景，确保其满足国家安全要求，并形成具备法律效力的评估报告。

A-11、系统集成

1、系统集成应包含基础环境、硬件、软件及安全四个维度的集成实施，需制定分阶段实施方案，明确各子系统接口规范、兼容性要求及联动机制。

2、安全集成需设计多层次防护架构，配置访问控制、数据加密等策略，并提供完整的实施方案、测试报告及运维文档，确保系统功能稳定、数据交换安全。

附件二：保密协议

甲方：【安康市公安局】

乙方：【中移系统集成有限公司】

鉴于：

1、 乙方为甲方的合作商。在合作或交流中，乙方有可能接触到甲方及其下属使用单位系统中所涉及的知识、数据、绘图、专有技术、分析、计算、编辑、研究、数据、信息和其它材料。

2、 出于保护甲方合法的保密资料（定义见第一条）及有关权益之目的，乙方将遵守有关法律规定及行业准则，保守甲方之商业秘密。

为明确甲乙双方之权利义务，经友好协商，甲乙双方就上述保密事宜特订立以下协议：

第一条 保密资料

保密资料应包括但不限于甲方系统中所涉及的信息、知识、数据、人员信息和其它材料。由于乙方在提供服务过程中所涉及的资料（包括未注明"保密"的资料）可能直接影响甲方及下属机构的运营，因此乙方对于以上所提及的一切资料均有保密的义务。

第二条 资料的提供

甲、乙双方同意按照本协议的目的互相提供保密资料。双方均认识到保密资料是属于甲方的有价值的特殊的财产。双方同意，根据保密规范及相关法规约定的期限内，在没有取得甲方事先书面同意之前，乙方不向任何其他个人、商社、公司、联合体或其他团体，以任何理由或目的，披露甲方的保密资料。此外，双方同意保密资料可以提供给乙方的咨询者、代理人或顾问，但乙方需确保这些咨询者或顾问应当在与本协议条款相同的文件上签字承诺承担不披露保密资料的义务。双方还同意在没有获得甲方事先书面同意的情况下，乙方不以任

何形式为本协议目的以外的目的使用保密资料，包括但不限于和其他方竞争和/或获取其他的利益。

第三条 权属

乙方认识到甲方提供的所有保密资料是甲方的财产，并且该等保密资料不应该被视为向乙方授予了任何关于保密资料许可、专有或所有的权利。

第四条 披露和使用保密资料的限制

乙方应将保密资料限制在需要知道的公司雇员、咨询者或顾问的范围内，并且不会将保密资料披露给其他方。乙方不能以本协议目的以外的其他目的使用保密资料。

第七条 保密资料的返还

甲方可以在任何时候，以书面形式要求乙方返还或销毁任何依本协议而提供的书面保密资料及其复印件，并且乙方在返还或销毁时应附有书面陈述，该书面陈述应注明，此类返还或销毁时，乙方没有直接或间接地故意保留或控制任何保密资料及其复印件。乙方应在收到此类要求的14日内满足该等要求。

第八条 除外信息

本协议规定的保密资料不包括以下信息：

（1） 在从甲方处获得前，已经为乙方掌握的信息；

（2） 已经是为公众所知的信息，除非为公众所知是由于乙方违反本协议；

（3） 由乙方独立开发的信息；

（4） 乙方可按照有管辖权的法院、政府或其他有权机关（以下简称“有权机关”）的合法要求而披露的信息。但是，在此类情况下，乙方应在披露前书面告知甲方，使甲方有机会对在这

种情况下进行的交出信息或披露信息进行抗辩、限制或者保护。乙方应当只披露依法需要披露的那部分保密资料，并且乙方应运用合理的努力，从有权机关处取得可靠的保证或承诺：有权机关会以对待保密资料的方式对待需要披露的保密资料；

（5） 依甲方的书面授权而向第三方所披露的信息；

（6） 从第三方获得的信息，该第三方应当没有受到类似保密义务的限制。

第九条 违约责任

如乙方违反保密义务，故意、过错或过失泄密的，除应立即采取措施停止泄密行为，减小泄密造成的损失。乙方违反本约定的，乙方应向甲方作出赔偿，赔偿范围包括但不限于甲方因乙方行为而受到的索赔、费用支出、商业损失、法院或仲裁机构或任何其他权威机构作出的判赔或处罚。

第十条 期限

本协议自甲乙双方的法定代表人或授权代表签署并加盖公司有效印章后生效。不论双方合同或本协议是否解除或终止，乙方的保密义务将持续有效。

第十一条 公开宣布

双方同意，对双方间进行的任何讨论或协商的实质内容，任何提出的安排或协议的条款，以及任何与以上内容相关的其他信息进行严格的保密，并且不公开披露或向第三方披露。双方同意，双方均不能，也不允许任何双方的关联公司、子公司、个人、或其他实体，在没有事先征得双方同意并取得另一方的书面同意前，就此类安排或协议的讨论以及其他正在讨论或协商的商业和操作计划做任何公开宣布，无论是以新闻发布还是其他的形式。

第十二条 陈述和保证

（1） 每一方向另一方陈述并保证，该方为依其注册地法合法成立并存续的机构。每一方均表述，它有完整的权力及授权，能够签署本协议，并且能够从事为履行本协议而必须的各类事项。甲方保证，提供保密资料不会违反与其他第三方签订的任何其他协议。

（2） 双方均不对保密资料的准确性和完整性做任何陈述和保证，并且甲方不因为乙方使用保密资料或参与讨论和协商而有任何合同上的、侵权上的或其他的责任。

第十三条 一般条款

（1） 协议双方应签署并递交必要的文件，采取必要的行动，以实现本协议的条款和目的。

（2） 没有经过双方书面签字认可，任何对本协议任何条款的修订、解释或弃权是无效的。

（3） 任何一方延迟行使任何权利、权力或特权，并不是对这些权利、权力和特权的弃权。任何现在对该等权利、权力或特权的弃权，或任何单一或部分地行使权利、权力或特权，不会排除以后完全行使或对其它相同权利、权力及特权的行使。双方同意并认识到，甲方会因乙方的违约而受到难以修复的损害，并且甲方有权在发生违约事件时，获得司法救济。

（4） 所有段落的名称只是为了方便的目的，并不影响本协议内容的意思或解释。

（5） 本协议书作为双方合同的补充，与合同正文具有同等法律效力。

（6） 双方在本协议项下的义务对其合法继受人和被许可的受让人均具有约束力。

（7） 本协议和双方因本协议内容而产生的关系，依中华人民共和国法律解释。

（8） 所有本协议项下的通知、请求或其他往来信息均应使用书面形式。该等通知、请求或其他往来信息应当亲自送交，或者以挂号信或特快专递的形式寄出，或者以传真发出。寄出地址应为双方合同约定的送达地址。

（9） 本协议一式两份，双方各执一份，具有同等法律效力。

【以下无正文】

本页无正文，为《保密协议》签字页。

甲方（盖章）：【安康市公安局】

法定代表人/负责人：

签订日期：2025.11.10

乙方（盖章）：【中移系统集成有限公司】

法定代表人/负责人：王昀

签订日期：2025.11.10