用户需求书

注：本项目核心产品为全流量采集设备。

一、项目概述

1.建设目标

为深入贯彻落实国家《网络安全法》、《数据安全法》关于加强公民个人隐私保护的规定，根据公安部交管局《交警队伍顽瘴痼疾专项整治工作方案》、《公安交管信息安全隐患专项整治方案》要求，以“安全、合规、可信”为实现目标，提升科学实用的体系化安全防护能力，打造数据安全防护体系。实现全网安全态势敏锐感知，安全威胁快速检测与处置，确保业务访问全程可知可控，可管可查，最终达到加强数据安全保护的目的。

为落实以上相关要求，陕西省公安厅交警总队将开展陕西省公安交管网络应用信息安全管控系统项目建设，加强交管六合一应用系统的网络访问监管。通过采集网络流量数据，与信息系统日志数据结合进行分析，建立异常行为分析模型，对存在的访问风险进行分析与告警，降低出现信息泄露的隐患和风险。

2.建设内容

根据建设目标以及交警总队网络建设的现状，本项目具体实现以下建设任务：

2.1 建设安管系统，提供多层次、全方位的信息系统安全监管。

2.2 以网络数据流量分析为依据，对操作行为进行审计并进行异常行为访问的告警追溯。

2.3 对访问行为进行约束，对异常访问进行阻断，从源头上保障数据访问，防范数据泄密，保护机密数据的安全性。

2.4 采集访问网络应用的全流量日志，实现对交管网络应用系统访问的安全审计和网络操作审计。

2.5 对加密系统进行日志对接；对非加密系统，支持业务操作还原以及业务访问追溯。

2.6 建设资产可视化管理系统，对 IT 资产进行自动扫描、分析和识别。

2.7 可以与省公安厅的应用日志安全审计平台进行对接，提供审计数据。

二、项目要求

序号	建设项目	主要性能指标	数量	备注

序号	建设项目	主要性能指标	数量	备注
1	网络安全审计系统	▲1、应用日志审计：可按照系统预设的审计策略通过系统日志对用户的访问行为、数据查询记录等进行审计。系统可自动识别业务系统各种操作行为和内容，支持按角色、时间、地点、人物、区域等多维度自动对每个用户的登录、浏览、回放等操作行为进行收集、分析和报告，并形成用户日志，且无法被删除、修改或覆盖。并支持日志的统计、查询、分析及报表功能。包括正向搜索、反向追溯、操作轨迹分析等功能； ▲2、协议日志审计：支持 HTTP、FTP、TELNET、SMTP/POP3 协议日志审计。包括 HTTP 日志查询、FTP 日志查询、TELNET 日志查询、SMTP/POP3 日志查询等功能； ▲3、SIP 信令审计：支持 SIP 协议日志审计。根据流量自动还原成对摄像头的操控命令，支持国标 GB/T 28181。可以对所有网络摄像机的信令进行解析和统计分析，也可以查询指定 IP 的网络摄像机在选定时间范围内的访问控制命令。包括：网络操作类型统计、操作功能统计（例如云台控制、预览、视频下载等）等； ▲4、操作页面还原：系统可对操作日志进行快照还原，准确还原操作场景和页面，完整记录应用系统的所有操作行为和内容，对操作场景进行复现，为审计分析提供线索和依据； ▲5、操作行为追溯：实现操作日志的反向追溯，按照关键字对操作行为进行追溯，找出所有涉及到关键信息的操作行为，从而进一步排查相关人员、时间范围、业务系统等的相关操作，锁定违规事件的线索范围，准确还原业务系统用户对关键信息的操作； ▲6、操作轨迹分析：系统支持秒级的时间轴还原，将操作人员对业务系统的访问和操作轨迹复现在时间轴上； ▲7、流量指标分析：支持流量趋势分析、应用流量趋势分析、协议流量趋势分析、区域流量访问排序等； ▲8、网络流量查询：网络流量查询功能，可实现对网络流量进行统计、分析，可按流量梯度、时间范围、IP 段、业务系统、源 IP 所在区域、所属单位/部门、操作名称、连接方式、协议类型等多维度展现监测结果； 9、访问活跃度排名：用户终端网络访问活跃度排名； 10、服务活跃度排名：应用服务（被访问）活跃度排名； 11、区域流量访问排序：显示出某个时间段内每个区域流量访问的排序顺序。 12、与省公安厅的应用日志安全审计平台进行对接，提供审计数据	1	软件
2	资产管理系统	▲1、资产总览：用可视化图表方式，多维度、全方位的展示设备资产情况，包括资产总数、资产类型分布、资产注册占比、设备厂商统计、部门资产统计、资产告警分布等；	1	软件

序号	建设项目	主要性能指标	数量	备注
		▲2、资产管理：包括设备信息维护、视频设备维护、交换机信息维护等功能。实现对各类 IT 硬件设备、软件服务等的信息维护、设备查询、和注册管理。支持资产批量导入和导出。可管理的资产包括服务器设备、视频摄像头设备、操作终端、网络设备、存储设备等； ▲3、设备发现：可实现对网络中的各类设备的扫描发现，可查看当前发现设备列表和历史发现情况。支持主动扫描探测，流量采集分析等多种方式实现资产设备的发现，发现方式可以灵活配置，组合使用； ▲4、设备识别：支持对设备类型的分析识别，通过检测设备操作系统、端口状态、设备厂商等多种信息，可准确分析出设备类型。系统预置交换机设备、服务器设备、数据库服务器设备、视频 IPC 设备、操作终端设备等多种特征模型。支持设备类型分析模型的自定义配置，可按照设备属性和运行参数等多种信息配置特征模型，包括设备端口、操作系统、系统版本、设备厂商等内容； ▲5、设备指纹：通过对设备基础信息、配置信息、行为信息的分析识别，对设备 IP、MAC、端口、行为基线等信息进行建模，生成设备二维码指纹作为设备唯一的表征信息。支持对设备指纹的实时监测，当发现设备指纹发生变化，可及时告警处置。		
3	全流量采集设备 **（核心产品）**	硬件参数： 内存：不小于 32GB DDR4 硬盘：不小于 240G SSD， 管理接口 1 * 千兆，业务接口 1 * 千兆，数据接口 4 * 千兆 + 2 * 万兆。 功能： 1.支持旁路镜像部署方式； ▲2.支持对视频监控操作行为日志进行采集；支持对网络视频操作行为流量数据进行采集；支持获取视频操作行为的网络交互流量； ▲3.支持命令行和 B/S 管理方式；支持网络 L2 层全流量采集；支持网络 L3 层 IPv4 流量独立采集；支持网络 L3 层 IPv6 流量独立采集；支持实时导出流量统计数据到指定收集器；支持 IPFIX 网络流量监测标准协议； ▲4.支持最大 20Gbps 的实时流量采集。 ▲5.支持多维度对网络流量进行统计、分析；对全网流量变化趋势的综合分析。 ▲6. 实时在线分析 L2-L7 层网络协议，提取元数据，支持日志、协议、数据包全字段索引。 ▲7.支持 HTTP、UDP、SIP 协议解析 ▲8.支持 HTTP 操作还原，可以还原为操作快照 9.支持 IPv4、IPv6、IPv4/IPv6 双栈	1	硬件

序号	建设项目	主要性能指标	数量	备注
		▲10.支持数据包深度检测。支持最大 20Gbps 的实时流量检测，支持网络 L2 层全流量深度数据包检测，支持网络 L3 层 IPv4/IPv6 流量独立深度数据包检测 ▲11.支持流量协议识别。支持 SSL、SSH、Telnet 等 30+种常用应用协议识别，支持协议规则自定义 ▲12.支持应用特征识别。支持 SSL 和 HTTP 应用特征自动学习功能。支持 100+种常用应用特征识别，支持自定义应用识别特征 ▲13.自定义识别规则库。支持应用识别规则库自定义，预置 30 种应用协议和 100 多种应用特征，为后续流量管控提供丰富的样本集。 14.数据共享。支持实时导出应用识别结果到全流量存储分析设备。 15.可同时采集多路镜像流量 ▲16.支持基于接口的网络分流，可将指定接口的流量按照分流算法分流至一到多个目标接口 ▲17.支持基于接口的网络汇聚，可将多个指定接口的流量按照算法汇聚至目标接口 ▲18.支持基于接口的网络镜像，可将指定接口的流量镜像至目标接口 ▲19.支持基于分类器的网络分流和汇聚，可根据 L2-L4 层信息将流量分流或汇聚（支持按源 MAC、目的 MAC、源 IP、目的 IP、传输协议、源端口、目的端口分流和汇聚）至目标接口 ▲20.支持基于应用识别的分流和汇聚功能，可根据应用名称分流或汇聚流量至目标接口		
4	协议解析设备	硬件参数： 内存：不小于 64GB； 硬盘：不小于 240G SSD；数据存储：不小于 8T； 管理接口 1 * 千兆，业务接口 1 * 千兆，2*万兆网卡。 功能： 与全流量采集设备直连，实时解析分析流量数据，支持重要的业务系统操作访问还原追溯，追溯异常操作，杜绝违规越权访问。支持 WEB 方式配置管理。 ▲1.操作日志审计，支持按时间、地点、区域、操作类型等多维度自动对用户的登录、修改、查询等操作行为进行收集、分析和报告，并形成用户日志。 ▲2.业务操作回溯，对于非加密的系统，采用智能监测、页面还原技术，准确还原应用系统操作界面，对操作场景进行复现。 ▲3.支持对操作内容的反向追溯功能。 ▲4.支持多维度对网络流量进行统计、分析；对全网流量变	2	硬件

序号	建设项目	主要性能指标	数量	备注
		化趋势的综合分析。 ▲5.支持多种应用识别，多种协议分析。 6.通过与流量采集设备级联，支持本地化存储 ▲7.与系统的日志进行对接,对流量审计结果和操作日志进行对比审计 ▲8.支持 HTTP、UDP、SIP 协议解析，还可以对摄像头的私有协议进行审计 ▲9.支持 HTTP 操作还原，可以还原为操作快照 ▲10.支持 20G 网络流量采集存储和审计还原 ▲11.通过旁路实现日志还原，日志符合公安部日志审计数据规范 12. 支持流量数据存储，提供 8T 存储空间，可扩展至 32T 13.支持 IPv4、IPv6、IPv4/IPv6 双栈 14.采用旁路方式部署，避免串接造成的单点故障 ▲15.支持展示全网各采集点的链路指标，包括流量、流速、网络性能等； ▲16.支持全文搜索，以即时查询的方式，根据关键字进行全文搜索，有强大的搜索逻辑 17.支持告警策略管理，包括告警转发、告警存储、告警管理预警源管理以及告警处理策略定义 18、部署方式灵活，支持透明模式和旁路模式部署，后期可根据业务量动态扩容，自带设备、系统日志监控各节点的运行状况。		
5	安全风险评估	安全等级保护测评 在系统正式上线运行前,聘请第三方等保测评机构对即将上线的系统进行安全等级保护测评。等级保护测评按照国家等级保护标准对本系统进行测评，编制等级保护差距测评报告，制定建设整改方案，提供等保测评验收报告，完成终评验收，取得系统备案证书。	1	其他

注：“▲”项属于重要功能指标，须提供原厂的功能截图并加盖原厂公章。

三、项目实施、培训及服务要求

1.项目期限要求

合同签订后 3 个月完成项目建设，计划 2023 年 7 月底前完成验收。

2.项目验收

（1）中标供应商按照项目需求完成项目后，由用户方组织验收。

（2）系统功能：按照需求书的要求，检查系统功能是否达到设计要求。

（3）系统性能：按照需求书的性能指标，测试系统指标是否达到设计要求。

（4）文档资料：检查系统设计文档是否齐全、是否合格。

3.服务要求

（1）中标供应商必须拥有一套切实可行的质保保证体系，确保项目的实施及服务质量。

（2）为保证系统的正常运行，中标供应商必须承诺保障本项目的本地化服务能力，中标后于项目所在地设立常驻服务和技术支持机构，并配备较强的专业技术队伍，能提供快捷的售后服务响应。

（3）服务内容包括现场服务、定期巡检、故障服务。

（4）中标供应商应建立运行维护团队，故障响应要求：

（5）提供断电保障，保障系统稳定运行。

（6）故障在 1 小时内响应，如电话、网络等不能解决问题，2 小时到现场，24 小时解决问题，紧急状况 1 小时到现场，4 小时解决问题。

（7）如遇紧急、重大服务事项，需在保证提供多人、快速服务响应的情况下配合管理方协调产品的研发单位进行现场应急事件处理。

（8）中标供应商在完成项目后，应提供终验合格后 3 年的免费质量保证服务。

（9）中标供应商应有完善的文档管理制度，保证运行维护过程中产生的文档。

（10）在提供服务的过程中，获悉的一切资讯需严格遵守保密协议，严禁自行使用或向他人传播，泄漏或擅自使用或允许他人使用上述信息，由此造成的损失应承担相应的法律责任。

七、付款方式

1.合同签订后向中标供应商支付合同总价款的 40%；

2.验收合格后，采购人向中标供应商支付合同款总额的 60%；

3.中标供应商承诺在采购人办理以上各期付款的支付手续前，为采购人出具等额的符合国家规定的发票；

4.上述时间不包括采购人正常办理支付报批手续的时间。