最高限价：154.50 万元

九、投标分项报价表

（一）采购设备和软件部分						
序号	名称	规格、技术参数	单位	数量	全费用综合单价（元）	合价（元）
1	智能防护终端	1.采用 ARM 架构，核心芯片采用国产化芯片，CPU：主频≥2.4GHz，核心数≥八核，内存≥4G，存储≥32G，算力≥6TOPS。终端支持串口协议对接；支持对输入的音视频信号进行视频信号与音频信号分离输出，提供≥1×AUDIO 接口，≥1×HDMI 输入接口，≥1×HDMI、≥1×DP 输出接口；终端支持多种网络环境运行：支持有线网络环境，提供≥2×LAN 口；支持无线网络环境，提供≥2×Wifi 天线接口；支持 SIM 卡网络环境，提供≥1×SIM CARD 口；支持通过指示灯查看运行状态，指示灯配置：≥1×WIFI 信号灯，≥1×LAN 信号灯，≥1×PWR 信号灯；提供≥1×TYPE-C 接口，支持通过接口方式对终端进行调试、维护和注册。 2.具备对 Android、Windows、Linux、iOS、统信 UOS、银河麒麟 Kylin、深度 Deepin 等主流操作系统所输出的播放内容（包括但不限于主画面、画中画、应用弹窗、弹幕等所有内容）进行实时内容安全检测与审核。 ★3.具备系统运行状态自检测与系统自动恢复运行能力，终端实时检测系统运行状态，若终端出现系统宕机时，将会触发重启功能，此时终端将自动重启系统，恢复正常运行状态。（需提供具有 CMA 或 CNAS 标识第三方权威检测机构出具的检测报告及全国认证认可信息公共服务平台查询截图，并加盖送检制造商公章佐证） ★4.支持检测画面录制，录制时间≤20 小时，可通过可视化界面对已录制画面进行回放查看，支持下载录制画面内容功能，实现对播控事件过程中播出的内容进行溯源与取证。（需提供具有 CMA 或 CNAS 标识第三方权威检测机构出具的检测报告及全国认证认可信息公共服务平台查询截图，并加盖送检制造商公章佐证） 5.支持横屏与竖屏模式检测输出，输出分辨率最大支持 4K 分辨率 60 赫兹，终端 HDMI 输出支持自定义分辨率与刷新率，自定义分辨率包含但不限于 3840×2160、2560×1600、1920×1080、1600×900、1024×768、2160×3840、1600×2560、1080×1920、900×1600、768×1024 等，支持修改输出填充模式。 6.终端需内置多套检测模型，模型包含：暴恐模型、色情模型、旗帜模型、人脸模型、文字模型，原始样本库≥500 万，支持对模型调优，提高检测识别准确率。	台	14	25600	358400

		★7.终端需支持 4G 物联网联网模式，在联网状态下可通过标准 API 接口协议与公共场所电子显示屏监管前端进行通信，实现配置下发与数据交换；无网络时，终端可自动切换至离线检测模式，实时对视频内容进行智能审核，并对识别出的违规内容执行播放阻断。 8.终端支持将检测到的违法违规内容信息报送至公共场所电子显示屏监管前端，报送信息包含：告警类型、终端名称、位置、告警画面图片等信息，形成完善的告警统计、告警查询、告警详情等审计溯源日志，并可将溯源日志导出生成报表。 ★9.终端文字检测敏感词库应支持 20000 条以上，每个敏感词字数最高可支持 20 字；终端应能满足在不低于 20000 次识别敏感词、敏感人脸、涉黄、涉政旗帜、暴恐视频或图像或文本测试中，识别准确率≥99.99%；终端应能满足在不低于 20000 次正常图像测试中，图像中均无敏感词、敏感人脸、涉黄、涉政旗帜、暴恐视频或图像或文本信息，误识别率≤0.01%；（需提供具有 CMA 或 CNAS 标识第三方权威检测机构出具的检测报告及全国认证认可信息公共服务平台查询截图，并加盖送检制造商公章佐证） ★10.终端具备毫秒级视频源内容同步能力，支持设置延时播放，延迟播放时间最低可设置到 500ms，当检测出违规内容时，阻断反应时间应小于延迟播放时间，实现毫秒级阻断，避免违法违规画面播出。（需提供具有 CMA 或 CNAS 标识第三方权威检测机构出具的检测报告及全国认证认可信息公共服务平台查询截图，并加盖送检制造商公章佐证）				
2	公共场所电子屏显示监管前端	1.前端须具备统一的综合监管能力，核心功能包括事件告警数据汇总与分类、违规内容预览、事件处置、终端状态监控、检测规则与数据版本管理及应急措施管理。前端应提供直观的事件监管应用，通过首页仪表盘动态展示终端矩阵概览（如接入总数、在线/离线状态）、告警统计、类型分布及趋势分析，并运用图表等可视化工具清晰呈现业务数据，以辅助用户快速决策和响应。 2.前端须支持多台终端同时接入，并能汇总展示全部告警信息，列表需包含处置状态、风险级别、终端名称、位置、告警图片与时间等关键字段，支持按终端或告警类型筛选，并可直接对关联终端执行关屏、复位等远程操作。同时，前端应提供详细的终端全生命周期记录查看功能，包括告警记录、操作日志、任务日志、升级日志等，并能实时监控终端健康状态（如网络信号、终端温度、HDMI 连接状态及故障情况），实现精细化运维管控。 3.前端应提供完善的检测策略与智能模型管理模块。支持对识别模型（如涉黄、暴恐、特殊旗帜、人物库、敏感词等）进行版本的新增、编辑、删除、启用/禁用等升级操作。支持对检测策略进行灵活的新增、编辑、删除及内容（识别类型、范围阈	套	1	162000	162000

		值）开关配置。此外，前端还需具备样本管理功能，支持对单图或多图轮询内容进行新增、查看、审核（同意/拒绝）、删除等操作，确保所有预设内容合法合规后方可投入使用。 4.前端应支持应急联系人管理功能，支持管理各分组的应急联系人，支持扩展告警推送，将告警信息实时推送给对应应急联系人；推送方式包括但不限于：SMS 推送、邮箱推送、企业微信推送。 ★5.前端应支持对访问前端 IP 和账号进行限定访问，可设置允许访问前端 IP 地址和账号。（需提供具有 CMA 或 CNAS 标识第三方权威检测机构出具的检测报告及全国认证认可信息公共服务平台查询截图，并加盖送检制造商公章佐证）。 6.前端须支持对所有内容安全监管终端进行统一集中管控，可远程执行关屏、开屏、复位、重启、关闭检测、固件配置及审核策略更新等操作，并实时查看终端运行状态（如正常、关屏、离线等）。前端须具备应急插播管理功能，支持对插播内容进行新增、审核（同意/拒绝）、下发及删除等操作，并可设置多图循环播放次数，确保内容合法合规方可使用。 7.前端应提供特定人物与特定词汇的阻截管理功能。支持对人物库和词汇库进行分组，允许批量导入或手动添加数据；支持为同一人物添加多张人脸图片以提高识别准确率，并可基于名称或备注精准查询词汇。同时，前端需具备完善的检测开关与复位机制：授权账号可临时关闭检测以放通所有内容；当视频源恢复正常后，可通过复位操作解除持续阻截状态，恢复正常播放。 8.前端需内置待办、已办事项管理模块，支持查看待办事项的发起人、接收时间、流程状态及具体内容，并可执行审核（同意/拒绝）操作；已办事项可查询审核人、审核意见及操作时间等信息，实现审核流程的可追溯与规范化管理。前端需支持特定场景的识别管理，可对场景库进行分组及数据批量导入或手动维护，并据此实现内容的放通或阻截。同时，前端应具备完善的检测统计功能，能按终端、时间、地址等多维度条件筛选并统计检测时长、告警次数、处置情况等信息，并支持报表导出。此外，前端必须记录所有账号的登录日志与详细操作日志，确保所有操作可追溯、可审计。 9.前端需具备多用户权限与集中化管控展示功能，应提供基于角色的多用户管理体系（如系统管理员、应急管理员等），并为不同角色分配差异化功能权限。前端需具备集中管控能力，能远程配置终端的接入参数（IP、端口、网络类型等），并具备内容展示功能，集中展示终端状态、告警态势、实时画面等关键信息。当触发违规告警时，终端应能自动调用前端预设画面（支持多图轮播，可设置数量与间隔）进行覆盖，并提供对应的功能界面截图证明。				

		10.前端属于自主研发设计，非 OEM 产品，（需提供原厂或原制造商软件著作权证明）。 ★11.支持接入第三方公共场所电子显示屏智能防护终端相关视频、图片及告警等数据，相关开发工作由投标方承担。（投标方提供确保接入书面承诺书）				
3	智能防护插件	1.智能防护插件需支持在 Android、Windows、Linux 等主流操作系统上部署运行，并具备良好的显示适配性，可自动匹配终端的横屏/竖屏模式，实时上报画面内容。软件须具备高兼容性的分辨率检测能力，支持从 1024×768 至 8K（7680×4320）范围内的标准及非标准分辨率，确保对视频、图片等内容的全覆盖检测。 2.智能防护插件应提供清晰的实时运行状态监控界面，可直观展示检测、通信、运行及绑定状态。同时，软件界面需支持查看与配置终端地址、服务器地址及端口等关键网络参数（需提供终端地址、服务器地址及端口查询截图证明）。为保障系统安全，软件须采用账号密码管理机制，绑定后任何配置更新操作均需验证密码，防止人为恶意篡改。智能防护插件完成部署后，能够自动生成管控终端终端 ID，通过终端 ID 快速定位出现违规内容的管控终端，支持看终端 ID、版本等信息。 ★3.智能防护插件完成部署后支持对终端的运行信息查看，方便现场调试与问题排查。当开启调试信息查看时，可在管控终端屏中显示连接信息、传输速率、传图分辨率等信息。（需提供具有 CMA 或 CNAS 标识第三方权威检测机构出具的检测报告及全国认证认可信息公共服务平台查询截图，并加盖送检制造商公章佐证） 4.智能防护插件须具备开机自启动及后台静默运行能力，实现对终端播放内容的实时监测，并以典型时间＜200ms 的毫秒级速度将画面回传至智算中心检测服务器。所有与服务器的通信必须采用 SSL 加密技术，确保传输安全与完整。当检测到违规内容时，软件能立即将屏幕画面切换为经前端审核的预设画面（支持多图轮询播放），待内容合规后自动恢复。同时，智能防护插件须支持接收公共场所电子屏显示监管前端的应急视频插播指令，可强制替换当前画面，并支持设置循环播放次数。 5.智能防护插件应具备初步保护能力，普通用户无法通过软件界面直接关闭软件，导致相关服务停用，若对防护插件配置进行调整，需要通过对应权限账号登陆才可进行调整，确保防护插件配置正常。	个	8	5200	41600
4	公共场所电子屏智算中心	1.智算中心需采用软硬一体化部署 CPU：主频≥2.0GHz，核心数≥12 核，内存≥256G，存储≥5T。算力卡≥2 块，单算力卡≥16384 个 CUDA 核心，配备≥24GB GDDR6X 显存，显存位宽≥384bit，显存带宽≥1 TB/s。 ★2.智算中心须支持违规画面的毫秒级检测与阻截通	套	1	88000	88000

		知，在同时对多个终端画面内容处理时，典型阻截时间＜900ms。（需提供具有 CMA 或 CNAS 标识第三方权威检测机构出具的检测报告及全国认证认可信息公共服务平台查询截图，并加盖送检制造商公章佐证） 3.智算中心须支持管理页面查询日志信息，设置页面可通过选择对应的日志文件，进行对日志内容的查看，并具备向公共场所电子显示屏监管前端上报任务日志和升级服务日志。 4.智算中心支持一屏一策功能，支持通过公共场所电子显示屏监管前端对不同防护插件设置不同策略，可以根据不同区域的终端屏，制定专属策略。 5.智算中心须具备高并发处理能力，至少同时支持对 20 个安装智能防护插件的终端进行 7×24 小时的画面内容实时分析检测。检测模型需覆盖涉黄（含不同肤色及动漫人物）、涉政、暴恐、敏感词、涉毒、涉赌等多种违规类型，并支持 OCR 文本识别，确保不受字体、字号、旋转等变形因素干扰。检测到违规内容时，应立即通知终端防护插件进行拦截替换。为保障系统安全稳定及兼容现有开源技术栈，智算中心须基于 Linux 系统部署(支持如 CentOS7+ 或 Ubuntu 20.04+ 或 openEuler22.03+等主流发行版)。公共场所电子显示屏监管前端应实时显示检测、运行、通讯连接等运行状态，并支持查询终端型号、终端序列号、IP 地址、策略名称等详细信息。 6.智算中心应支持灵活的场景化检测策略，可通过公共场所电子显示屏监管前端对特定内容配置放行或阻截规则，实现按需执行检测与通知。同时，系统需提供对原有模型进行升级与调优功能，通过公共场所电子显示屏监管前端对智算中心模型进行优化，达到提升对违规内容的识别准确率，确保检测能力持续有效。 7.千兆交换机 1 台，需支持≥24 个 10/100/1000Mbps 自适应 RJ45 端口，背板带宽≥48Gbps，包转发率≥35.7Mpps。				
5	公共场所电子显示屏终端安全终端	1.标准 1U 机架式，含 3 年硬件维保服务。性能：扫描 IP 数 1536（6 个 C 类），监管 IP 数 500 个。内存≥16G，存储≥128G，网口≥6 千兆电口，电源 60W 单电源。 2.安全终端应具备资产自动识别能力。针对识别过程中可能出现的资产品牌误判，系统须提供自定义品牌匹配规则功能，允许管理员为指定资产类型设置品牌匹配关键词并与正确品牌关联，实现对此类识别错误的自动化、批量校正，提升资产信息准确率。（投标时须提供该功能配置界面截图，并加盖原厂公章予以证明） ★3.安全终端须提供完善的资产档案管理功能。除预置标准档案字段外，应支持管理员根据管理需求，自定义扩展档案字段（包括字段名称、数据类型等）。自定义字段需能自动集成到对应资产类型的	台	1	33000	33000

		详细信息展示中，实现资产“一机一档”的精细化、集中化管控。（投标时须提供档案管理配置界面及建档后的效果截图，并加盖原厂公章予以证明） ★4.安全终端须具备网络风险检测能力， 支持终端的仿冒资产检测、弱口令检测及漏洞检测，（提供各项功能的原厂截图证明且加盖公章）				
6	日志采集解析终端（专网侧）	1.标准 2U 机架式硬件一体机，日志源个数≥350 个，数据峰值处理能力≥5500EPS；国产品牌 CPU，CPU 主频≥2.7GHz，CPU 核心数≥8 核 8 线程，CPU 数量≥1，国产操作系统，内存≥16G，硬盘实际存储空间≥6T；电源：双电源，网口≥千兆电口×8（包含管理口×1，HA 口×1，业务口×6），≥千兆光口×4（含 2 个千兆 SFP 多模光模块）。 ★2.支持通过在目标主机上安装 Agent 程序，监测目标主机的 CPU 利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。（提供产品功能截图并加盖公章） 3.支持以下对象的性能监控：操作系统：Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris；数据库：MySQL、Oracle；应用服务器：Weblogic、Tomcat；Web 服务器：Apache。 ★4.按照盐城市公安局关键信息基础设施安全保卫平台接口对接要求，支持 Syslog 等协议，推送日志采集解析终端接收的告警日志，为监测预警提供必要的数据支撑。（提供承诺函并加盖公章）	台	1	95000	95000
7	日志采集解析终端（互联网侧）	1.标准 2U 机架式硬件一体机，日志源个数≥1000 个，数据峰值处理能力≥25000EPS，国产品牌 CPU，CPU 主频≥2.6GHz，CPU 数量≥2，CPU 总核心数≥24 核 24 线程，国产品牌操作系统，内存≥64G，硬盘实际存储空间≥32T，电源：双电源，网口≥千兆电口×6（包含管理口×1，HA 口×1，业务口×4），≥千兆光口×4（含 2 个千兆 SFP 多模光模块）、≥万兆光口×2（含 2 个万兆 SFP 多模光模块）。 ★2.支持通过在目标主机上安装 Agent 程序，监测目标主机的 CPU 利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。（提供产品功能截图并加盖公章） 3.支持以下对象的性能监控：操作系统：Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris；数据库：MySQL、Oracle；应用服务器：Weblogic、Tomcat；Web 服务器：Apache。 ★4.按照盐城市公安局关键信息基础设施安全保卫平台接口对接要求，支持 Syslog 等协议，推送日志采集解析终端接收的告警日志，为监测预警提供必要的数据支撑。（提供承诺函并加盖公章）	台	1	155000	155000
8	安全访问认证网关	1.标准 2U 机架式硬件一体机，最大并发用户数≥1200；CPU 主频≥2.4GHz，CPU 数量≥2，CPU 总核心数≥6 核 12 线程；内存≥32G；硬盘实际存储空间≥2T；电源：双电源；网络接口：网口≥千兆电口	台	1	185000	185000

		×4（包含管理口×1，HA 口×1，业务口×2），≥千兆光口×4（含 4 个千兆 SFP 多模光模块）；接口扩展槽≥2 个。 ★2.集成现有的 B/S 应用系统、C/S 应用系统、移动 APP 等，提供统一认证门户，统一认证门户界面内容支持按照采购人需求进行个性化设置，用户认证通过后推送统一的应用入口，通过引导访问应用系统。统一认证门户提供客户端下载。（提供产品功能截图并加盖公章） ★3.支持认证因子的管理，内置支持：本地账号密码、动态口令认证；支持标准化对接：钉钉扫码、企业微信、飞书扫码、AD 认证、短信验证、邮箱验证；支持证书对接：标准国密认证、商密认证、CA 认证。（提供产品功能截图并加盖公章）				
采购设备和软件部分合计						1118000
(二)、租赁设备部分						
序号	名称	规格要求	单位	数量	**全费用综合单价（元）**	**合价（元）**
1	互联网威胁与失陷监测设备硬件配置	1.软硬一体 2U 标准机架式；CPU≥16 核心 32 线程×2；内存≥256GB；存储≥2×1.2T SAS, 1.92TB NVME ×2 块，硬盘插槽配置≥10 个；配备企业级远程管理卡；≥2 个万兆 SFP+ 网口(含光模块)；≥4 个千兆网口；满配冗余热插拔电源、含导轨等附件。硬盘免返还，原厂 1 年服务质保及特征库升级，设备过保或授权到期后其余设备归还。 ★2.租用重点单位 DNS 流量分析设备（满足全量接入 2.4G 重点联网单位 DNS 全量数据需要，如实际量大于该数值，设备分析能力要同步匹配）。	项	1	25000	25000
2	设备性能	★要求单台设备对 DNS 流量的处理能力不低于 15 万 QPS 且要求单台设备至少可以存储 6 个月的告警数据。	项	1	50000	50000
3	威胁情报数据能力	★1.情报本地化要求：能将所有情报指标进行本地化；提供自动化情报更新能力。出站情报支持小时级更新，IP 信誉数据实现天级更新。 ★2.本地出站情报要求：准确率超过 99.9%，情报库指标不少于 100 万条；本地情报包含丰富的上下文，至少包括：是否 APT、针对行业、关联样本、注册人信息、解析 IP、关联组织等。 ★3.海量数据关联分析溯源能力：可对所有情报数据提供附加情报分析能力，支持分析的网络基础数据要求至少包含 10 年以上 Whois 注册信息历史数据、5 年以上 PDNS 历史数据等。	项	1	100000	100000
4	威胁监测与分析能力	1.安全监测服务	利用多种检测手段，发现传统僵木蠕、勒索病毒、挖矿木马、APT 等威胁事件，以及针对重点行业的高级持续性攻击，并触发告警。并围绕威胁事件展示事件攻击者 IP、具体攻击行为、被攻击的单位，以及攻击者所属团伙的背景信息。为通报预警、快速处	项	1	25000	25000

			置、侦查调查、案件溯源提供监测数据支撑。				
		2.威胁态势监控	以网络安全事件与威胁告警为元数据，对网络空间安全相关数据进行汇聚分析，形成针对人、物、地、事、时多维视图，从不同视角出发感知网络安全态势。呈现的态势信息包括整体安全态势、安全事件与等保单位态势、黑客画像概览、受害者画像概览、初步案件线索等。支持对最近 24 小时、最近 7 天、最近 30 天的告警数据的分析展示。	项	1	20000	20000
		3.重点单位监测	以重点单位为维度，对重点单位网络进行持续监测，发现并统计各类威胁事件，并详细识别被攻击 IP，结合资产数据，告警信息，协助定位被攻击主机或设备。并可以自动化生成针对重点单位的威胁报告进行下发通报，并对处置整改进行跟踪。	项	1	25000	25000
		4.资产信息录入	支持录入资产信息，将发现的威胁事件、分析数据，以及情报信息与资产信息关联分析。	项	1	20000	20000
		5.案件线索	利用威胁情报能力，对海量告警数据建立分类、筛选模型，对告警次数多、持续时间长、影响范围广的本地黑客发动的网络攻击事件进行案件线索提取。通过侦查调查，还原包括受害者、攻击者以及攻击过程等信息，形成案件证据链条，进而指导针对攻击者真实身份的追踪溯源工作。可利用先进的威胁情报理念、溯源分析技术，结合案件线索中的木马、域名、IP、哈希、字符串等信息进行自动化拓展关联分析，进而深层次挖掘攻击者真实身份，定位地理位置，实现从网络虚拟信息到真实身份信息的追溯，填补案件收网所需完整证据链的最后一环。	项	1	20000	20000
		6.本地黑客档案库	对筛选出的需要现场取证的案件线索，利用威胁情报对案件线索归属黑客团伙进行分析，并对该团伙攻击者背景信息进行丰富，包括攻击者背景描述，标签、目标区域、目标行业，攻击手法和特征等等，并支持对相关信息进行自定义。将提取的黑客画像数据在本地形成本地的黑客画像数据库，为以后的案件侦查调查和分析溯源提供支持。	项	1	22000	22000
		7.情报管理	提供命中情报检索、管理、自定义添加情报的能力。帮助用户检索和查看当前系统中的命中的情报，分析命中情报详情，并可禁用/启用相应的情报，帮助用户去管理针对于组织自身的特有情报库。此外提供了自定义情报功能扩展了用户的检测能力，用户可自己录入单条或者批量录入情报，自定义的情报可实时进入流量检测流程中。自定义情报支持域名、ip 、威胁标签、严重级别等情报信	项	1	26000	26000

			息相关字段。				
		8.输出威胁分析报告	按照周、月、季度、半年、全年或自定义时间周期导出分析报告；以及导出重保期间的分析报告；报告需要包含：（1）总体威胁态势，APT 攻击、黑产攻击、个人攻击概述；（2）告警详情分析，整体失陷趋势、整体威胁类型、不同严重程度的告警、APT 威胁分析、各地市失陷分布；（3）总体安全态势总结及建议；（4）重点单位失陷统计表。	项	1	70000	70000
租赁设备部分合计							403000

序号	分部名称	单位	数量	单价（元）	合价（元）	备注
1	采购设备和软件部分	项	1	1118000	1118000	/
2	租赁设备部分	项	1	403000	403000	/
合计					**1521000**	/

投标人：（单位盖章）中电鸿信信息科技有限公司

法定代表人或授权委托人：（签字或盖章）

日期：2026 年 2 月 3 日