# 襄城县疾病预防控制中心

## 关于采购智慧卫监建设项目的请示

**县卫健委：**

接河南省财政厅、河南省疾病预防控制局，关于提前下达2025年医疗服务与保障能力提升，豫财社【2024】214号、许财社【2024】119号提前下达资金（35万元）用于卫生监督机构能力提升。

我单位响应上级文件精神，使卫生健康监督规范化、信息化（智慧卫监），更好的服务襄城人民，我单位为了此项目更加完善，在资金不足的情况下，力争在2025年底完成，此项目大约需要41万元。疾控中心积极筹措资金，目前单位资金已到位，计划开展采购工作。

妥否，请批示。

襄城县疾病预防控制中心

2025年6月24日

| 智慧卫监建设项目 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 系统名称 | 序号 | 名称 | 描述 | 单位 | 单价 | 数量 | 合计 |
| 互联网识别监管平台系统 | 1 | 互联网识别监管平台系统 | 用先进的人工智能深度学习技术和图像监测自主算法，利用监控摄像头云端传输的实时监控画面，有效检测放射卫生场所人员穿戴防辐射用品的情况，将异常情况上报，实现放射卫生非现场监管。主要功能包括：1、监控台：展示区域内所有智能识别设备的地理位置及最新监测信息。2、设备管理：设备管理内展示设备关联的管理相对人及对应的设备信息，可对所连接设备的序号、所在位置、设备类型、型号、编号等信息进行编辑设置。3、预警中心：预警中心可以设置放射卫生AI智能识别的结果，及时通知到监督员或医疗机构管理者。可以自定义预警类型，如放辐射服穿戴的件数少于1件就通知，以及设置APP、短信等通知的方式。4、AI智能识别：<br>1）对所有医疗机构的放射卫生监控设备的管理，能够点击查看现场实时视频。<br>2）定义放射卫生违法行为，关联AI人工智能网络摄像机的所处科室、环境。<br>★3）对违法行为进行智能识别行为训练。根据训练结果不断调整识别成功率。<br>★1）支持机器深度学习功能，使用AI智能算法实现智能识别、动态标注、自动抓拍、自动录像保存等操作。<br>5）支持通过短信、微信等方式自动推送预警信息到卫生监督人员手机，提醒卫生监督人员及时处理。卫生监督人员监督检查后，在该系统对预警信息进行反馈，实现闭环管理 | 套 | 222300 | 1 | 222300 |
| | 2 | 系统调试服务费 | 系统调试服务费 | 次 | 500 | 12 | 6000 |
| 机房基础配套服务 | 1 | 机房基础配套服务 | 本服务包含：机房动环系统的搬迁及安装服务、同时满足机房内配套设备的安装服务，包括：防静电地板的安装、机房内综合布线等；部署UPS主机集中监控系统，支持MODBUS-RTU协议，可实现UPS远程监控，最大200台UPS集中监控。 | 套 | 11713 | 1 | 11713 |
| | 2 | 系统调试服务费 | 系统调试服务费 | 项 | 1200 | 1 | 1200 |
| 消防系统 | 1 | 消防系统 | 消防系统：系统支持80个点位联动，可连接WiFi，支持APP无线调试及云端报警功能带打印、联网功能；满足机房内2个感烟点位数据联动并实现报警；满足机房内2个感温点位数据联动并实现报警；室内温度过高时系统会触发声光报警器，室内烟气过高时系统会触发七氟丙烷开关，同时触发声光报警器和气体喷洒指示灯，实现短时间内灭火；系统可通过紧急启/停按钮实验紧急情况的开关。 | 套 | 30511 | 1 | 30511 |
| | 2 | 系统调试服务费 | 系统调试服务费 | 项 | 2000 | 1 | 2000 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 防火墙系统 | ★1、含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN、SSL VPN功能模块；≥3年硬件维保服务，≥3年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。<br>2、性能要求：网络处理能力≥5Gbps，并发连接≥180万，每秒新建连接≥5万/秒。<br>3、基础网络功能：支持IPv4和IPv6双协议栈，具备DNS、DHCP、MAC、静态路由、策略路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP、IPSec VPN、SSL VPN、GRE VPN、DS-Lite、6in4隧道、VXLAN、BFD、接口联动、802.1x认证等功能。<br>★4、抗拒绝服务攻击功能：能够抵御ICMPFlood、UDPFlood、SYNFlood、TearDrop、Land和Ping of Death等基本的拒绝服务攻击，渗透成功的包数量小于5%，正常连接建立大于90%，提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明并加盖原厂商公章。<br>★5、协同防护功能：支持与其他安全产品联动构建联防联控的网络安全防护体系，包含终端管控类系统联动、威胁监测与分析类系统联动、态势感知与安全运营类平台联动、蜜罐联动等功能，提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明并加盖原厂商公章。<br>6、蜜罐诱捕功能：支持对接蜜罐产品，基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN等因素将匹配的数据流量引流至蜜罐设备进行攻击诱捕。<br>★7、SSL解密功能：解密后的数据会进入到高级功能中进行扫描，用以实现加密流量的安全防护，提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明并加盖原厂商公章。<br>★8、网络攻击防护功能：包含木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑IP、Flood攻击防护等功能，提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明并加盖原厂商公章。<br>9、网络诊断功能：支持ping检测、traceroute检测、TCP端口检测、UDP端口检测等网络诊断检测工具，可基于抓包数量、接口、源地址、源端口、目的地址、目的端口和表达式设置抓包策略。 | 套 | 21000 | 1 | 21000 |
| | | | 1.最大日志分析能力≥6000条/秒，含300个日志源授权；<br>2.支持对多种设备以及多种采集方式的日志和事件的采集，提供强大的日志和事件处理、统计、分析、查询及告警等功能同时以图形化、可视化技术将识别到的各种事件和异常通过多维度方式直观的展现给用户；<br>3.支持日志基本信息概览，可查阅日志总数、预计可存天数、已存日志天数、已用容量，可对当前日志源数量进行统计，用户可根据日志基本信息全面了解当前系统的使用情况；<br>4.提供统计分析功能，包括但不限于日志统计、审计统计、告警统计，对审计事件风险等级分布、审计事件风险趋势、审计事件类型占比、审计事件日志源占比等提供详细的图形化统计；<br>5.提供日志查阅功能，支持日志合并查阅，可按照一定组合条件将日志进行合并查询，能够查阅事件分类、事件子分类、日志源、主机名、源IP、目的IP等详情；<br>6.*提供审计记录功能，支持审计记录查询，可按照登录审计、操作系统审计、账户审计进行分类查询，能够查询审计主体、审计客体、动作、动作结果、来源IP等详情；<br>7.支持审计策略配置，可根据审计对象配置审计策略，默认审计策略全部启用，包括但不限于登录审计、操作系统审计、账 | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 户审计等规则分类；<br>8.*提供报表管理功能，可根据时间周期定义报表内容，包括但不限于当天、当月、最近7天、最近30天，可支持报表在线查看，通过报表名称即可在线查看报表，可支持扫码下载，通过扫描二维码即可下载报表；<br>9.支持定时报表功能，可根据每周、每月、每日定时将生成的报表自动发送，支持自定义报表标题，以HTML、Word等通用格式输出；<br>10.*提供日志源管理，可支持日志源自动解析配置，无需手动添加任何日志源即可实现自动解析，同时提供自动解析日志源的总接收日志数、实时接收日志速率的实时统计；<br>11.*提供采集服务管理，可支持snmp-trap、syslog等协议，要求具有文本格式E文本的接入能力，支持TCP、UDP协议；<br>12.*提供告警中心配置，系统告警具有CPU温度告警，提供CPU温度告警值，同时具有多种告警方式，必须包括内置告警、企业微信、钉钉、邮箱、Syslog、SNMPTrap等方式； | | | | |
| 二级等保测评服务 | 2 | 综合日志审计系统 | 13.提供告警发送记录，能记录每一个告警信息的发送过程，内容包括告警方式、告警时间、告警内容、告警结果、操作等；<br>14.*提供多种部署模式，支持旁路部署、集群部署、虚拟化部署，网卡配置可提供管理口、镜像口等多种属性，可同时配置IPv4和IPv6地址，网卡配置可提供虚拟IP配置；<br>15.提供通用网络配置，可提供不低于3种DNS服务配置，可同时配置IPv4和IPv6地址，并且能够检测出当前DNS服务的联通性是否正常，保证DNS服务的有效性；<br>16.提供系统重启、系统关机、系统复位管理，可提供不低于2种系统复位方式，在复位过程中要求使用登录密码安全保护，避免产生误操作；<br>17.提供日志配置，可提供日志清理，要求日志保留时间不低于6个月，具有日志合并周期，能够对不超过30秒内的日志进行合并处理，并且支持地理位置识别，能够记录当前设备所在地理位置；<br>18.提供配置备份和恢复，可提供配置文件本地备份，可详细记录当前备份配置文件的时间、版本、文件大小，可选择对已备份的配置文件进行下载和还原，并且支持对配置文件进行导入操作，在导入过程中要求使用文件密码安全保护，避免产生误操作；<br>19.*提供存储管理能力，可提供新加入磁盘发现，支持识别磁盘类型、序列号、厂家、磁盘状态、磁盘大小，并能够将磁盘加入到当前数据存储中，同时具备数据存储切换能力，将日志数据切换至大容量存储，对数据存储进行动态扩容；<br>20.*提供设备自身防护，能够发现并自动锁定攻击者，系统能够生成详细的防护记录，提供自定义高危端口，锁定时间不少于七天；更多安全管理包括但不限于远程调试、DEBUG日志下载、访问白名单；<br>21.提供集群管理对接，可对加入节点设备进行统一升级管理，可提供对集群内所有设备进行固件升级、规则升级，可统一上传升级包进行固件或规则升级操作，可提供集群内所有设备升级成功的日志记录；<br>22.*提供双因子认证对接，具有内置双因子认证，可使用手机APP、微信小程序进行扫码绑定，并提供手机验证工具下载；可与第三方双因子认证对接，对接信息包括但不限于接口地址、设备名称、共享密码、服务器ID、登录设备IP； | 套 | 33000 | 1 | 33000 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | 终端杀毒 | 1、软件规格：控制中心支持Windows Server、CentOS、Redhat、麒麟V10、统信UOS等服务器操作系统部署安装<br>2、客户端支持Windows XP SP3及以上、Windows 7、Windows 8、Windows 10、windows 11、Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019、Windows Server 2022、CentOS 5~8、Red Hat Enterprise Linux 5~8、Ubuntu1610、macOS X 10.15、macOS 11.1、macOS 12.0.1、macOS 12.1、macOS 12.2、macOS 12.3、macOS 12.4、macOS 12.5、macOS 12.6、macOS 12.7、macOS 13、macOS 14、macOS 15、中标麒麟、银河麒麟、麒麟V10、统信UOS v20等操作系统部署<br>3、病毒防护策略功能：病毒防护策略支持强制策略，隔离区可设置空间大小、是否静止终端用户从隔离区恢复文件、隔离区文件保存天数等参数，病毒处理方式支持由程序自动处理、询问用户、不处理仅上报日志等方式，压缩包扫描支持20层，并可设置超过指定大小的压缩包不扫描。<br>4、主动防御支持进程防护、注册表防护、驱动防护、键盘记录防护、系统账户防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护、Win7加固、XP加固、远程登录防护、网络入侵防护、僵尸网络攻击防护、网络攻击防护、ARP攻击防护、DNS防护等，高级威胁防御支持无文件攻击防护、文档攻击防护、横移渗透攻击防护、内存攻击防护等，支持从IM软件、下载、邮件接收文件为恶意时弹窗提示用户。<br>★5、病毒防护能力：支持对主机磁盘、主机内存、主机引导区、移动存储介质等的病毒检测，病毒检测类型包含文件感染型病毒、宏病毒、蠕虫、木马程序、间谍软件、脚本恶意程序、后门程序、僵尸程序、勒索软件、RootKit 恶意程序、BootKit 恶意程序等，病毒处理动作包含阻止、删除、隔离、清除还原等，提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明并加盖原厂商公章。<br>6、防逃逸功能：支持逃避检测防护，包含压缩文件检测、加壳文件检测、格式混淆检测、捆绑文件检测等防护方式。<br>★7、主机防火墙 支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标IP，支持输入IP范围。开标现场需进行以上功能演示，可以通过控制中心下发主机防火墙策略。<br>8、硬件资产管理功能：能够准确采集终端硬件信息，采集的硬件信息包含硬件型号、厂商等，能够实时显示插入、拔出硬件后的硬件资产信息，能够实时监测到硬件资产安装、拆卸和更换等变更情况，并进行实时响应，响应内容包含日期时间、终端名称、硬件名称、变更事件描述等内容，提供CNAS认可检测机构出具针对软件功能的检测报告关键页证明盖原厂商公章。<br>9、弹窗防护 支持对不同类型主流软件的弹窗进行拦截，终端可定期更新云端弹窗规则库。<br>★10、病毒查杀能力：产品为一级品，内存占用≤0.4GB，CPU | 套 | 120 | 10 | 1200 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 占用≤10%，病毒库扫描时间≤1分钟，病毒样本基本库检测率≥99.7%，特殊格式病毒样本库检测率≥99.9%，误报率≤0.1%，提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明并加盖原厂商公章。<br>11、终端管理功能：能够对USB接口、串口、并口、1394、PCMCIA、USB存储设备、存储卡、冗余硬盘、软驱、打印机、扫描仪、键盘、鼠标、红外、蓝牙、摄像头、手机/平板、移动数据网卡、MODEM设备、ISDN设备、ADSL设备、手机/平板盘符等外部接口和设备进行有效管理<br>★12、补丁分发功能：能够按照补丁分发范围、分发时间、安装情况和终端类型等方式进行补丁分发，支持补丁静默和用户提示安装两种方式，可显示终端已安装和未安装补丁信息，提供CNAS认可检测机构出具的针对软件功能的检测报告关键页证明并加盖原厂商公章。<br>13、垃圾清理：支持手动扫描和清理软件安装残留文件以及系统历史记录文件。<br>14、启动项管理：支持检测系统启动项、服务项、计划任务，并支持启动项的优化。<br>15、配置要求 本次项目实际配置控制中心软件（Windows Server版）≥1套；Windows PC终端实配授权含病毒防护（不含第三方扩展引擎）、补丁管理、主机防火墙、终端管控功能、安全小助手（弹窗防护、垃圾清理、启动项管理）等功能。支持主流Windows PC客户端操作系统，包含3年更新服务。 | | | | |
| | 4 | 系统调试服务费 | 系统调试服务费 | 项 | 1285 | 1 | 1285 |
| | 5 | 等保测评 | 参照国家等级保护2.0技术标准对信息系统按照等级保护第二级标准开展测评和差距分析，出具整改意见和测评报告，协助完成系统定级专家评审工作，完成本次测评报告在网安部门的备案工作，并协助取得有效的备案证明。 | 项 | 28000 | 1 | 28000 |
| 宽带服务 | 1 | 千兆宽带 | 上行带宽80M，下行带宽1000M | 条 | 1360 | 12 | 16320 |
| 合计： | | | | | | | 407529 |