

合同编号: PYS-2025-12-30-001

汝州市医疗保障局

医保局内网安全防护项目

销

售

合

同

需方: 汝州市医疗保障局

供方: 河南杉铭信息科技有限公司

签订日期: 2026 年 1 月 7 日

合 同

需方（甲方）：汝州市医疗保障局

供方（乙方）：河南杉铭信息科技有限公司

供、需双方根据《中华人民共和国采购法》、《中华人民共和国合同法》等法律法规的规定，就竞争性磋商项目名称：汝州市医疗保障局医保局内网安全防护项目按照公正、平等、自愿、诚实信用的原则经友好协商，同意签订本合同。

一、本合同总价：

小写：¥765800.00 元（人民币）大写：柒拾陆万伍仟捌佰圆整。

供货范围、数量及分项价格详见一下列表，单位：人民币/元

序号	设备名称	品牌、型号及技术参数	规格	数量	单价（元）	合价（元）
1	Web 防火墙	<p>品牌：奇安信、型号：NSG2800-Web-SM-WL8</p> <p>1、标准 1U 机箱，单电源；板载 6 个千兆电口，2 个千兆光口，2 个扩展插槽，1 个 Console 口，2 个 USB 接口。</p> <p>2、网络层吞吐量 5G，并发连接 300 万，每秒新建连接数 7 万；默认含 16 个 IPsecVPN 标配并发隧道数。包含 3 年 WAF 软件特征库服务，3 年硬件维修服务。</p> <p>3、部署模式功能：支持透明传输模式、反向代理模式部署，并支持两台设备形成主-备冗余部署模式，能够将 WEB 访问负载均衡到多台 WEB 服务器上。</p> <p>4、支持产品页面一键断网（禁止访问）功能，在特殊情况下，实现对特定网站的快速下线。</p> <p>5、支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP 并发请求及实时事件的动画统计。</p> <p>6、攻击防护功能：支持 CC 攻击、SQL 注入、XSS、第三方组件漏洞、目录遍历攻击、Cookie 注入、CSRF、文件包含攻击、盗链、OS 命令注入、WEBshell、反序列化攻击等 WEB 攻击防护功能，能够防护应用扫描、漏洞利用工具等自动化工具发起的攻击，并支持攻击逃逸防护能够检测并</p>	台	1	39700	39700

		<p>阻断经逃逸技术处理的攻击行为。</p> <p>7、支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护。</p> <p>8、支持检测并清洗的攻击类型：IP 攻击，TCP 攻击，UDP 攻击，ICMP 攻击，DNS 攻击，HTTP 攻击等 20 多种 DDoS 攻击类型。</p> <p>9、支持入侵防护功能，并提供入侵防护特征库，特征库需要提供 22 种类型并提供至少 14000 条入侵检测特征库</p> <p>10、日志与告警功能：安全审计日志记录内容包括：事件发生的日期和时间、主体、客体、描述、协议类型、源地址、目标地址、源端口和目标端口等，告警信息包括事件发生的日期和时间、主体、客体、描述、危害级别等，能够对高频发生的相同告警事件进行合并告警，能够按照 IP 地址、时间段和应用类型条件和以上条件组合对应用流量进行统计，能够以报表形式输出统计结果。</p> <p>11、支持轻量级蜜罐防御功能，提供伪造的后台管理系统页面，主动诱使黑客进行攻击，记录攻击行为</p> <p>12、支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间。</p> <p>13、产品具备资产探测功能，提供自动识别资产系统类型和开放端口。</p> <p>14、支持非法 URL 外联检测功能，针对特定外联 URL 进行监控或阻断，并且支持自定义 URL 地址。</p> <p>15、支持移动端管理功能，不需要安装 APP 和第三方插件，通过手机浏览器即可管理设备，并可查看设备 CPU、内存使用情况；支持移动端对资产的一键断网功能，提供网站一键下线以及批量下线的应急措施。</p>				
2	互联网 防火墙	<p>品牌：奇安信、型号：NSG2800-SM-WL68</p> <p>1、标准 1U 机箱，单电源；板载 8 个千兆电口，2 个千兆光口，2 个万兆光口，1 个扩展插槽，1 个 Console 口，2 个 USB 接口，默认含 16 个 IPsecVPN 并发隧道数(最大 500)和 16 个 SSLVPN 并发用户数（最大 300）。</p> <p>2、网络处理能力 7Gbps，并发连接 180 万，每秒新建连接数 7 万；含 3 年特征库升级（应用识别特征库、病毒防护</p>	台	1	43590	43590

	<p>特征库、入侵检测特征库、URL 分类特征库升级服务)、威胁情报订阅服务。含 3 年硬件维保服务。</p> <p>3、部署模式：产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。</p> <p>4、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。</p> <p>5、地址转换：所投产品必须支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。</p> <p>6、IPv6 支持：所投产品支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 服务器或手动方式获取 AFTR 参数。</p> <p>7、访问控制：所投产品支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略推荐可以指定策略流量，分析后自动生成源地址精度更高的安全策略。</p> <p>8、共享上网检测：所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。</p> <p>9、入侵防御：所投产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNVDID、CWEID 等信息在漏洞攻击特征中体现）详细信息。</p> <p>10、病毒防护：所投产品能够支持 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀；本地病毒库规模大于 3000 万。</p> <p>11、SSL 解密功能：解密后的数据会进入到高级功能中进程扫描，用以实现加密流量的安全防护。</p>			
--	--	--	--	--

		<p>12、策略与处置：产品支持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置；基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等。</p> <p>13、蜜罐策略：产品支持IPv4和IPv6流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。</p> <p>14、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。</p> <p>15、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%。</p>				
3	上网行为管理与审计系统	<p>品牌：奇安信、型号：NBM-SM-WL18</p> <p>1、标准1U机箱，单电源；标准配置6个千兆电接口（其中含1个管理接口和1个HA接口），1T机械硬盘；含网页过滤、用户认证、应用控制、内容审计、带宽管理、行为监控分析等功能；提供物理硬件bypass按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。</p> <p>2、网络带宽200M，1500人以下网络环境使用；最大并发连接数为16万，最大新建连接数为3500/秒；含3年应用协议库、URL特征库和审计特征库升级授权，3年标准维保服务。</p> <p>3、部署模式：支持网关模式、镜像模式和网桥模式部署。</p> <p>4、IPV6支持：能够支持IPv6环境下的网址访问审计、生成分析报表等功能；能够在IPv6环境下，正确审计显示用户的IPv6地址；</p> <p>5、可视化风险呈现：提供可视化的首页风险面板及监控中心，可集中呈现上网行为风险等级状态以及行为状态，并可展示特征库规模详情。</p> <p>6、网络状态：能够实时提供在线用户趋势、设备流速趋势、</p>	台	1	32550	32550

		<p>用户流量排名、应用流量排名、用户实时流量和应用实时流量等信息。</p> <p>7、病毒查杀：支持配置病毒查杀策略，检查网络中传输的文件是否是病毒，支持记录日志、病毒过滤；</p> <p>8、应用管理：可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制。</p> <p>9、网页管理：根据 URL 库及 URL 关键字进行网址访问管理，一条策略实现阻断、记录、告警，方便维护。</p> <p>10、资产管理功能：支持通过主动探测和被动识别的方式实现网络中设备资产以及数字资产的发现与管理。</p> <p>11、流量管理：支持多级虚拟通道，可以将物理带宽分成至少 7 级虚拟通道，合理分配物理带宽资源。</p> <p>12、带宽控制：可以限制 P2P、视频等大流量应用的最大带宽上限，减少带宽的浪费。</p> <p>13、共享接入：可识别网络中的私接路由或共享 wifi 的网络行为并配置阻塞策略；阻塞条件支持基于终端总数量、PC 数量、移动终端数量分别配置；</p> <p>14、访问质量监测功能：支持 Web 访问质量监测功能，可对监测对象的 Web 访问质量实时监测，对当前网络诊断的结果进行评级。</p> <p>15、日志统计：可生成网页访问、论坛发帖，webmail、邮件收发、应用访问、应用流量、通道分析等各种统计报表。</p>				
4	日志审计	<p>品牌：奇安信、型号：LAS-R11P-QDFX-PA</p> <p>1、硬件规格要求 标准 1U 机架式设备，配置 6 个千兆电口，2 个扩展插槽，1 个 Console 接口，2TB 硬盘。</p> <p>2、性能规格要求 日志采集处理均值 7000EPS，综合日志处理性能 2600EPS；包含 60 个日志源授权，含 3 年软件升级服务和 3 年硬件维保服务。</p> <p>3、支持审计各种网络设备、安全设备、主机操作系统、数据库、中间件、应用系统以及用户自己的业务系统的日志、事件、告警等安全信息。</p> <p>4、日志采集功能：支持通过 syslog/syslog-ng、文件或目录读取、SNMP Trap、WMI、JDBC、Netflow、Kafka、WebService 等多种方式完成各种日志的收集功能。</p> <p>5、日志解析规则定义功能：支持对接入日志进行正则进行</p>	台	1	33980	33980

		<p>解析，并能自动生成正则表达式来提取日志属性，支持对接入日志进行 JSON、Key-Value、分隔符或数组解析。</p> <p>6、等保大屏展示功能：等保大屏界面支持查看设备运行天数、日志源数量、原始日志数、关联事件数、告警总数、等保合规情况、本地最早日志产生时间、已保存日志天数、平均每天日志存储量、存储空间情况、日志源列表、登录失败用户分布等信息。</p> <p>7、商用密码功能：日志审计平台支持使用国家商用密码算法对日志进行完整性保护，未被篡改的日志验签结果为成功，被篡改的日志验签结果为失败。</p> <p>8、长日志审计功能：日志审计平台能采集接收 4/8/16/32/64KB 长日志，且日志无截断现象，日志完整。</p> <p>9、日志加密转发功能：日志审计平台可根据字段需求选择性转发并转发日志可加密。</p> <p>10、事件可视化展示功能：日志审计系统具备丰富的事件可视化展示能力，具备多种展现手段，至少包括曲线图、面积图、柱状图、水平柱状图、饼状图、环状图、桑基图、关系图、数值图、地图(世界地图、中国地图)、3D 地球等等。</p>				
5	合规一体机	<p>品牌：奇安信、型号：NSG9800-SM-WL18M</p> <p>一、硬件规格要求</p> <p>2U 机架式硬件，标配 6 个千兆电口，4 个千兆光口，2 个扩展插槽，1 个 Console 口，2 个 USB，8T 硬盘。</p> <p>二、防火墙部分</p> <p>1、网络处理能力 8Gbps，标配应用管控、入侵防御、防病毒、URL 管控、威胁情报功能模块。默认自带 32 个 IPSEC VPN 和 32 个 SSLVPN，最大可支持 2000 个 IPSEC VPN 和 1000 个 SSLVPN。支持液晶屏，含 3 年硬件维保和特征库升级；</p> <p>2、基础组网 支持 VTEP (VxLan Tunnel EndPoint) 模式接入 VxLAN 网络，并可作为 VxLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI (VxLAN Network Identifier)、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定；</p> <p>3、网络协议支持 MTU9000byte 的巨型帧 Jumbo Frame；</p>	套	1	95600	95600

	<p>4、VNF 功能 显示所有可支持的 VNF，包括防火墙、终端安全、日志审计、堡垒机等；</p> <p>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。</p> <p>三、终端安全部分</p> <p>1、终端许可管理 实配 100 终端数，标配防病毒模块，可扩展补丁管理、主机防火墙、安全小助手（弹窗防护、垃圾清理、启动项管理）等功能，支持常规 windows PC 客户端，最大支持 500 个终端授权；</p> <p>2、产品全功能支持简体中文/繁体中体/英语自由切换；</p> <p>3、基础功能 客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察；</p> <p>4、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。</p> <p>5、终端防病毒防护 支持不少于三个杀毒引擎混合使用，提高病毒检出率。</p> <p>四、日志审计部分</p> <p>1、综合日志处理性能 1000eps；包含 35 个日志源，三年维护服务。</p> <p>2、更好的应对等保合规检查，内置等保大屏展示。等保大屏界面必须包含（设备运行天数、日志源数量、原始日志数、关联事件数、告警总数、本地最早日志产生时间、已保存日志天数、平均每天日志存储量、存储空间情况）等 9 大界面效果展示。</p> <p>3、日志加密转发功能：日志审计平台可根据字段需求选择性转发并转发日志可加密。</p> <p>4、系统提供页面可视化编辑归一化策略，对页面查看的日</p>				
--	--	--	--	--	--

		<p>志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化，不需修改系统程序。</p> <p>5、日志交互式分析 可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。</p> <p>五、堡垒机部分</p> <p>1、最大图形并发为 20，最大字符并发为 20；授权 20 个资源；含三年产品库升级和维保服务；</p> <p>2、支持多因子认证，包括手机令牌、手机短信、动态令牌等方式；</p> <p>3、支持使用微信小程序生成动态口令，用于用户双因子认证，实现通过账号密码+动态口令的方式登录堡垒机；</p> <p>4、不限操作系统类型，无需安装任何客户端插件，使用浏览器通过 H5 方式即可直接运维 SSH、RDP、Telnet、VNC 和 SFTP 资源；</p> <p>5、统计分析功能：支持按照事件的来源、类型、发生总数进行统计，并将统计的事件信息转换成统一格式，以便于理解的方式显示。</p>				
6	防火墙	<p>品牌：奇安信、型号：NSG2800-SM-WL28A</p> <p>1、标准 1U 机箱，单电源；板载 8 个千兆电口，2 个千兆光口，2 个万兆光口，1 个扩展插槽，1 个 Console 口，2 个 USB 接口，默认含 16 个 IPsecVPN 并发隧道数(最大 500)和 16 个 SSLVPN 并发用户数（最大 300）。</p> <p>2、网络处理能力 5Gbps，并发连接 180 万，每秒新建连接数 7 万；含 3 年特征库升级（应用识别特征库、病毒防护特征库、入侵检测特征库、URL 分类特征库升级服务）、威胁情报订阅服务。含 3 年硬件维保服务。</p> <p>3、部署模式：产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。</p> <p>4、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。</p> <p>5、地址转换：所投产品必须支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在</p>	21	台	24780	520380

	<p>地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。</p> <p>6、IPv6 支持：所投产品支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 服务器或手动方式获取 AFTR 参数。</p> <p>7、访问控制：所投产品支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略推荐定可以指定策略流量，分析后自动生成源地址精度更高的安全策略。</p> <p>8、共享上网检测：所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。</p> <p>9、入侵防御：所投产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNVDID、CWEID 等信息在漏洞攻击特征中体现）详细信息。</p> <p>10、病毒防护：所投产品能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀；本地病毒库规模大于 3000 万。</p> <p>11、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。</p> <p>12、策略与处置：产品支持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置；基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括 1 天、7 天、30 天、90 天、永久等。</p> <p>13、蜜罐策略：产品支持 IPv4 和 IPv6 流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN 的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。</p> <p>14、网络攻击防护功能：包含木马后门、勒索软件通信防</p>			
--	---	--	--	--

	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。 15、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%。				
总价	小写: ¥765800.00 元 大写: 柒拾陆万伍仟捌佰圆整				

二、质量要求及供方对质量负责条件和期限

供方应提供全新未拆封产品（包括零部件、附件、备品备件等），如确需拆封的，应在供货前征得采购人同意，否则视为不能交货。供方保证全部按照合同规定的时间和方式向需方提供货物和服务，并负责可能的弥补缺陷。需方对货物规格、型号、质量有异议的，应在收到货物后 2 日内以书面形式向供方提出。

三、售后服务承诺

1、质保期限：设备硬件（含特征库升级服务）三年。

售后服务响应时间：30 分钟之内响应，1 小时现场支持。

售后服务机构名称、地址及联系方式：河南杉铭信息科技有限公司、河南省信阳市平桥区平安大道北区市场 96-5 号、联系方式：13283768177。

四、合同履行地点及进度

合同生效后，供方应于 7 个工作日（含安装调试）内按需方要求在汝州市医疗保障局（需方指定的地点）完成本项目的交货及安装调试。货物运送的费用由供方负责。需方应在货物到达指定地点后，提供符合安装条件的场地、环境等。

五、培训

供方在货物交付及安装调试完成后，应组织对需方提供货物的使用培训及使用说明、合格证书及其它相关资料，否则按不能交货对待。

六、验收要求

- 1、供方履约完毕及时向需方提出验收申请。
- 2、需方在收到供方验收申请后内组织验收。

2、需方在收到供方验收申请后内组织验收。

七、付款程序、期限及方式

1、合计总金额：小写：¥765800.00 元 大写：柒拾陆万伍仟捌佰圆整

2、付款方式：合同签订后，需方一次性付清全额货款，即小写：¥765800.00 元 大写：柒拾陆万伍仟捌佰圆整

八、违约责任

1、本合同生效后，双方应本着诚实信用原则，不得违反。

2、售后不及时违约责任，甲方有权利对乙方每次扣除相关货款 0.3%元。

九、保密条款及相关约定

1、甲方应对乙方产品成交价格及产品的技术性能、参数、程序、结构、使用说明或其他技术资料等实行保密措施，不得将产品技术资料等转达或泄露给第三方。

2、本合同项下的硬件安全产品为加锁密封产品。在使用过程中，如甲方未经乙方事先书面允许，自行开锁启封，则乙方不再对产品以及与产品相关的任何问题负责。

十、其他约定

1、本合同经甲乙双方代表或授权代理人签字盖章后生效。

2、本合同经双方签字并盖章既行生效，本合同一式陆份，甲方执肆份，乙方执贰份，均具有同等法律效力。

甲 方（盖章）：汝州市医疗保障局

法定代表人或委托代理人（签字）：李华

电 话：

地 址：河南省汝州市洗耳北路洗耳小区南侧 150 米

乙 方（盖章）：河南杉铭信息科技有限公司

法人代表或委托代理人（签字）：王三三

账 号：1679 3101 0400 1807 6

开户行：中国农业银行股份有限公司信阳胜利路支行

电 话：13283768177

签订日期：2026 年 1 月 7 日