信阳市住房公积金管理中心网络安全设备更新采购项目采购合 同

合同签署地：信阳市

甲方：信阳市住房公积金管理中心

地址：羊山新区新五大道太古广场A栋5楼

电话：

联系人：

乙方：信阳明众电子科技有限公司

地址：河南省信阳市浉河区成功南路190号门面房

电话：13526076088

联系人：张艳

为了明确双方的权利和义务，甲、乙双方在平等协商的基础上，就如下条款达成一致意见，特签署本合同。

第一条　产品（货物）名称及规格

产品（货物）名称及规格：设备采购

（产品描述详见附件。除本合同另有所指外，“产品”、“货物”为同义词。）

第二条　交货时间和地点

乙方应根据甲方书面通知，在甲方指定的时间将货物送至指定地点交由甲方指定收货人代表（详见附件），并自行承担为完成交付义务而发生的运输费、装卸费、保险费、税金、安装调试费等各项费用。

第三条　价款

本合同项下的货物价款为人民币（大写）：壹佰壹拾叁万玖仟玖佰捌拾元（小写：1139980.00元）。前述货款包含了乙方为履行本合同项下的全部义务而收取的全部费用，如增值税、营业税、所得税等各种税项以及软件许可使用费、运输费、装卸费、安装费、材料费、包装费、培训费等各项费用。

第四条　付款方式

1、签订合同后，甲方分两次支付费用，第一次付款：签订合同并出具发票之日起10个工作日内支付合同总金额的70% 即柒拾玖万柒仟玖佰捌拾陆（ ￥797986.00 ）；

第二次付款 ：设备安装调试完毕经甲方验收合格后 10 个工作日内支付合同额的 30% 即叁拾肆万壹仟玖佰玖拾肆（ ￥341994.00）。

2、乙方要求甲方将货款支付到以下账户：

开户银行：中原银行股份有限公司信阳申城支行

账户信息：411517010180050701

第五条　　包装和运输

1、乙方所交货物的包装必须是生产厂家的原厂包装。但在运输和交付过程中，为保护货物的安全，根据必要和适当的原则，乙方应采取符合国家标准或货物性质的措施，对货物进行适当的再包装，这种包装应适于长途运输，符合防潮、防震、防锈、防腐、防尘和防野蛮装卸等要求，以确保货物安全无损地交付给甲方。

2、因乙方未采用充分的、适当的包装和防护措施而造成货物的任何损坏，乙方应承担因此产生的一切费用和损失。

3、乙方负责办理货物的运输事宜并支付相关运费，承担货物的运输风险。

第六条　　交付、签收和验收

1、乙方交付货物时，应将货物装箱单提交给甲方；乙方未将装箱单交付甲方的，视为未完成交货义务。

2、乙方送货至约定地点后，甲方应在 3 个工作日内完成对货物的签收。签收之日视为货物交付之日，自交付之日起，货物的所有权和风险由甲方承担。甲方签收时，应根据本合同和装箱单对乙方所交货物的质量、规格、型号、数量、随附技术文件等方面进行检验。如发现货物的质量、规格、数量与合同和装箱单规定不符的，甲方有权拒绝接受并向乙方提出调换、退货，直至索赔。

3、甲方签收货物后，双方可以进入安装、调试、检验等后续阶段。货物根据其性质不需要安装，或甲方认为没有必要由乙方进行安装、调试的，则甲方应在 15 个工作日完成签收，且签收的完成即意味着验收完成，甲方逾期签收的，视为验收通过。

4、根据货物的性质或甲方的要求，货物需要进一步安装、调试的，乙方应根据甲方的要求，在指定的时间内派遣合格的工程技术人员赴现场完成安装、调试工作。货物安装和调试完成后 5 个工作日内，甲方应完成货物的验收工作。在验收过程中，如发现货物质量不符合质量标准，乙方应根据货物的实际情况负责补齐、退换、修理，直至验收合格，并承担因此给甲方造成的损失。

5、乙方同意，货物验收合格并不免除乙方对货物所应当承担的责任。

第七条　　质量与保证

1、乙方保证交付的合同货物符合国家标准、行业标准或生产厂家的企业标准，上述标准不一致的，以严格的标准作为所交付货物的质量标准。乙方交付的货物还应符合甲乙双方认可的乙方产品说明书所规定的功能、性能以及其他质量标准。

2、如果没有上述可参照的标准，则乙方保证提供的货物能够实现甲方的合同目的，满足最终用户的实际需要。

3、乙方保证所提供的货物是通过正常渠道销售的行货产品，为原厂生产、制造和包装，是未曾投入使用过的全新产品，没有设计上或制造上的缺陷。货物为软件产品或包含软件产品的，则乙方保证软件无病毒、无恶意代码、无明显错误，能够充分实现货物说明书中描述的功能。

4、乙方保证对其提供的货物享有合法的所有权，在货物上不存在任何未曾向甲方透露的担保物权、司法扣押、行政扣押以及其他任何妨碍甲方或甲方的最终用户获得货物所有权的法律障碍或权利瑕疵。

5、乙方保证其出售的货物没有侵犯任何第三人的知识产权。

第八条　　售后服务

1、硬件货物自验收合格之日起，乙方提供 3 年的原厂标准维保服务。

2、软件货物自验收合格之日起，乙方提供 3 年的软件维护和升级服务。

3、除双方另有约定外，乙方承诺提供 7×24（即每周 7 天、每天 24 小时）的热线电话技术支持；货物出现系统故障后 24 小时内赶赴现场处理。

4、有关售后服务乙方委托第三方进行的，乙方应对第三方的服务质量负责。

5、甲方认为需要对其进行必要的培训的，乙方应安排合格的专业人员组织相应的培训活动。具体培训事宜，双方可以附件或补充协议的形式予以明确。

6、由于乙方原因致使甲方购买的货物未能享受本合同约定的售后服务，乙方视为违约，应赔偿因此给甲方造成的损失。

第九条　　保密

1、甲乙双方对本合同的存在、内容，以及在合同履行过程中获悉的对方商业秘密和专有信息（包括但不限于甲方所购买货物的数量、价款、配置，以及用户名单、甲方的客户关系）负有保密义务，不得对外披露；根据有关法律的要求，一方依法履行信息披露义务披露前述信息的除外。

2、本合同无论因何种原因变更、解除或终止，均不影响本条款的效力。

第十条　　违约责任

1、甲方未按合同约定付款，每延迟一日须向乙方支付应付款项的 3‰作为违约金，延迟违约金不超过本合同总金额的 5%。

2、乙方未按合同约定交货（包括因交货不符导致的迟延交货），每延迟一日须向甲方支付迟交货物总值的3‰作为违约金，延迟违约金不超过本合同总金额的5%。

4、乙方交付的货物不符合合同约定的质量标准，经更换或修理后，仍不符合合同约定的，甲方有权退货，解除本合同，乙方应退还已收取的款项，并支付5%的违约金。

5、本合同其他条款对违约责任另有约定的，从其约定。

第十一条　不可抗力

1、本合同中，不可抗力是指不能预见、不能避免并不能克服的客观情况，包括：战争、火灾、洪水、台风、地震、政策变化或其他人力不可抗拒之事件。

2、因不可抗力事件导致本合同无法履行或迟延履行，双方均免责，但遭受不可抗力事件的一方应及时通知另一方，并在事件发生后15日内提供法定机构出具的有效证明。

3、不可抗力事件解除后，双方将积极配合，继续履行本合同，但合同的履行已无必要的除外。

第十二条　合同的终止

1、本合同履行完毕，则自动终止。

2、乙方逾期30天交货，甲方有权解除本合同。

第十三条　争议的解决

因本合同而发生的一切争议，甲乙双方应协商解决；协商不成的，任何一方可向甲方所在地的人民法院提起诉讼。

第十四条　其他事项

1、乙方确认，乙方根据本合同对甲方承担的义务，同样适用于甲方的最终用户。

2、本合同自双方盖章之日起生效。未尽事宜，由双方友好协商解决。

3、本合同一式肆份，甲、乙双方各执贰份，每份具有同等的法律效力。

（以下为签署页）

甲方：

授权代表签字：

甲方签章：

日期：2024.6.14

乙方：

授权代表签字：

乙方签章：

日期：2024.6.14

附件一：

序号	安全产品	型号	参数	单位	数量	备注
安全区域边界						
1	外联防火墙	NSG3300-1860-Z	（KA 替代工程名录限价内容包含：产品主机、36 个月维保服务；不包含扩展板卡、升级授权、光模块以及超过限价内容的维保、安装服务）网络层吞吐量 3.94G（名录内数据，增配接口板卡之后，整机最高可达 10G）；并发连接≥600 万；每秒新建连接数 11.99 万；标准 2U 机箱；冗余电源；板载 1 个 MGT 管理接口；1 个 HA 接口；4 个 10/100/1000M 自适应电口和 8 个 SFP 插槽；另外还支持 1 个接口板卡扩展插槽；1 个 Console 口；2 个 USB 接口；默认含 1TB 硬盘；含三年硬件维保服务，防火墙基础组件：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 等功能。3 年全功能模块升级订阅服务包（威胁情报数据订阅服务、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）含三年硬件维保服务。	台	1	
2	WAF 防火墙	W3300-GB10	国产化 Web 应用防火墙系统；网络吞吐量为 2.4Gbps；应用层处理能力为 0.6Gbps；网络并发连接数 100 万；HTTP 并发为 70 万；HTTP 新建连接数大于 13000/s。标准 2U 机箱；标准配置 6 个千兆电口；12 个千兆 SFP 插槽；2 个万兆 SFP+插槽；1TB 硬盘；冗余电源；1 个 Console 口；2 个 USB 接口。含 3 年 WAF 软件特征库服务；3 年硬件质保服务。	台	1	
3	入侵防御	P3300-1610-F	网络层吞吐量 4G（名录内数据），网络层吞吐量 12G（真实整机吞吐），入侵检测吞吐 1Gbps，并发连接≥400 万，每秒新建连接数 10 万，标准 2U 机箱，冗余电源，板载 1 个 MGT 管理接口，1 个 HA 接口，8 个 10/100/1000M 自适应电口（支持 2 对 Bypass）和 4 个 SFP 插槽，另外还支持 1 个接口板卡扩展插槽，1 个 Console 口，2 个 USB 接口，默认含 1T 硬盘；入侵防御系统基础组件；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 等功能，含三年入侵防御特征库升级服务。含三年硬件维保服务。	台	1	
4	入侵检测	D3300-1610-F	满检速率为 8G，并发连接≥900 万，每秒新建连接数 14 万，1 个管理网口，1 个 HA 接口，板载 4 个千兆电口和 4 个千兆光口插槽，另有 2 个扩展槽，1T HDD 存储；标准 2U 机箱；冗余电源；液晶屏；默认含 1T 硬盘；含三年硬件维保服务；含三年 IDS 特征库升级授权	台	1	
5	网闸	GZ3000-FT20	产品性能：网络层吞吐≥1Gbps，应用层吞吐≥950Mbps，应用层并发性能≥10 万条，视频并发数≥400 路（2M 码流）；硬件配置：2U 机箱，	台	1	

			内、外主机配置分别如下 CPU：飞腾腾锐 D2000（2.3GHz，8 核），操作系统：银河麒麟操作系统 V10（内核版本 4.19.90），内存 ：8GB，硬盘：64GB +4TB，内、外主机分别配备显示屏，冗余电源；内网接口规格：6 个 10/100/1000Base-T 端口（含 1 个管理口，1 个 HA 口，4 个业务口），4 个 SFP 插槽,2 个扩展插槽，1 个 Console 口，2 个 USB 口；外网接口规格：6 个 10/100/1000Base-T 端口（含 1 个管理口，1 个 HA 口，4 个业务口），4 个 SFP 插槽,2 个扩展插槽，1 个 Console 口，2 个 USB 口； 功能模块：数据库同步、文件交换、数据库访问、邮件访问、安全浏览、安全 FTP、定制模块、工控访问等；可增配集中监控与数据分析中心（MDA）统一管控；质保年限：默认包含三年维保			
安全计算环境						
6	数据库审计系统	DBA3300-G-1000Z	兆芯硬件平台和中标麒麟安全操作系统，内置 4TB 磁盘存储空间。标准 2U 机箱，双电源；板载：1 个 RJ45 接口,2 个 USB 接口，6 个千兆电口，4 个千兆光口。报价中包含三年软件升级和硬件维修服务	台	1	
安全管理中心						
7	运维审计系统	BH3300-G-1000Z-GM	采用兆芯多核硬件平台和中标麒麟服务器版操作系统。外观：标准 2U 机架式，标配 6 个千兆电口、4 个千兆光口,支持 1 个扩展插槽，内置国密密码卡，4TB 企业级硬盘，冗余电源。支持液晶屏，最大可选 500 授权许可 。提供 50 个被管资源数授权。提供支持 SM1、SM2、SM3、SM4、SM7、SM9 等密码算法的智能密码钥匙，具有设备管理、应用管理、容器管理、证书存储、权限控制等功能。提供一套个人 CA 认证。提供三年标准维保服务。	台	1	
8	日志审计系统	LAS-PKQ2M	性能：综合日志处理性能 2000EPS。硬件规格：飞腾 CPU，麒麟操作系统，标准 2U 机箱，6 个千兆电口，4 个千兆光口，2 个扩展插槽（可选 4 万兆光），1 个 Console 接口，冗余电源，4TB 硬盘。包含 60 个日志源授权，3 年硬件维保服务和 3 年软件升级维护服务	台	1	
网络接入区						
9	接入交换机	S5560X-58C-HI	传输速率：10/100/1000/10000Mbps 交换方式：存储-转发 背板带宽：2.4/24Tbps 包转发率：513/705Mpps MAC 地址表：支持黑洞 MAC 地址 端口结构:非模块化 端口数量:56 个	台	4	

			端口描述:48 个 10/100/1000Base-T 电口,6 个 1G/10GBase-X SFP Plus 端口,支持 2 个插槽 VLAN:支持基于端口的 VLAN;支持基于 MAC 的 VLAN;基于协议的 VLAN;基于 IP 子网的 VLAN;支持 QinQ，灵活 QinQ;支持 VLAN Mapping;支持 Voice VLAN;支持 MVRP QOS:支持 L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP(IPv4/IPv6)地址、目的 IP(IPv4/IPv6)地址、TCP/UDP 端口号、VLAN 的流分类;每端口支持 8 个队列;支持对端口接收报文的速率和发送报文的速率进行限制，最小粒度为 64Kbps;支持报文的 802.1p 和 DSCP 优先级重新标记;支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持 SP、WRR、SP+WRR 三种模式 网络管理:支持 STP/RSTP/MSTP 协议;支持 STP Root Protection;支持 BPDU Protection;支持 G.8032 以太网环保护协议 ERPS,切换时间≤50ms,可兼容其他支持该协议的产品;支持 RPP			
安全服务						
10	漏洞扫描服务	定制	安排网络安全人员进行漏洞扫描服务。漏洞扫描主要是通过评估工具以本地扫描的方式对安全检查范围内的系统和网络进行安全扫描，从网络内部和外部两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。同时会辅以人工检查做到全局扫描。 服务频次：服务周期内，每年 4 次，共 12 次。	项	1	
11	重保值守服务	定制	安排专业的安全服务人员，进行现场值守，在服务期间对客户网站及业务系统进行的安全监测，对网络中的流量进行实时威胁分析，及时发现网络中黑客的攻击渗透行为并及时阻断。同时配备应急响应服务，能够快速地发现并处置安全事件，防止安全事件对重大活动或者会议造成影响。在重保值守结束后，将提供《重保值守总结报告》，总结重保值守期间发现网络中存在的风险并提出加固建议。 服务频次：服务周期内，每年提供不超过 3 人/天。	项	1	
12	应急响应服务	定制	中心业务系统发生安全事件，并产生重大影响时，需提供应急响应服务时，提供应急资源支持和应急人员支持，评估影响范围、事件抑制、溯源分析和复盘安全事件，协助开展业务恢复工作，并针对安全事件提供有效的整改意见。 服务频次：应急响应覆盖整个服务周期。	项	1	