设备采购合同

甲　　方：铜川市人力资源和社会保障局

法定代表人/负责人：辛治国

地　　址：铜川市新区齐庆路 2 号

联系方式：　0919-3185565

乙　　方：陕西卓为信息技术有限公司

法定代表人/负责人：李方成

地　　址：陕西省西安市高新区南三环西辅道 34 号融城东海 A 座 506-507

联系方式：029-83645478

依据《中华人民共和国民法典》及相关法律法规的规定，甲乙双方就甲方采购乙方的防火墙、堡垒机、日志审计、入侵检测等硬件设备事宜，经友好协商，达成如下协议：

一、设备采购明细

序号	产品名称	品牌型号	产品参数	单位	数量	单价（元）	总价（元）
1	省市防火墙	绿盟科技 NFNX3-HF200	1.标准 1U 机架尺寸，国产飞腾 E2000Q CPU，国产银河麒麟 V10 操作系统，8G 内存，数据硬盘为 1TB 固态硬盘，管理口为 1 个 GE 管理口和 1 个 RJ45 串口，2 个 UEB 接口，千兆电口 10 个，combo 口 4 个，接口扩展插槽 2 个，整机网络层吞吐量 4G，整机应用层吞吐量 2G，新建 TCP 连接数 4 万/秒，TCP 并发连接数 100W，含 3 年系统升级服务及 3 年原厂质保。 2.产品在多项安全防护能力开启后的实际防护性能，产品采用多核分布式安全操作系统，充分发挥硬件的并行计算能力，提供对应的计算机软件著作权登记证书。 3.支持通过 ICMP、TCP、UDP 协议，完成对目的 IP 地址（支持 IPv6）可达性的探测，支持在策略路由、GRE 隧道、DNAT 策略、HA 中设置链路探测。 4.为高效编辑策略，支持对多条策略的源/目的地址、协议/端口、应用、时间等进行批量修改，实现一次修改覆盖多条策略。	台	2	71000	142000

			提供原厂盖章的证明材料。 5.黑白名单内容支持IP地址(可直接写入或通过文本智能提取)、协议TCP/UDP/ICMP和端口进行设置，且支持配置双向地址。 6.文件传输协议，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制。提供原厂盖章的证明材料。 7.支持XFF解析功能，针对Web应用代理场景，可以解析出报文中真实客户端的IP地址。提供原厂盖章的证明材料。 8.支持基于域名的防火墙策略，一条策略中支持不少于配置128个域名（支持IPV6），支持通配符格式的域名如*.test.com，支持10级域名且层级可配置。提供原厂盖章的证明材料。 9.基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。提供原厂盖章的证明材料。 10.产品符合国内权威机构的《防火墙产品检验方案》的要求，能力成熟度达到三级，提供检验通过证明。 11.产品厂商具备符合GB/T 27922-2011的售后服务认证和符合GB/T31863-2015、GB/T 33718-2017的履约能力服务认证。				
2	横向防火墙	绿盟科技NFNX3-HF200	1.标准1U机架尺寸，国产飞腾E2000Q CPU，国产银河麒麟V10操作系统，16G内存，数据硬盘容量为4TB，管理口为1个GE管理口和1个RJ45串口，2个UEB接口，千兆电口10个，combo口4个，接口扩展插槽2个，整机网络层吞吐量4G，整机应用层吞吐量2G，新建TCP连接数4万/秒，TCP并发连接数100W，配置防火墙、流量管理、IPSEC VPN、应用管理、入侵防护、病毒防护、URL过滤功能，含3年系统升级、特征库升级、病毒库升级服务及3年原厂质保。 2.产品在多项安全防护能力开启后的实际防护性能，产品采用多核分布式安全操作系统，充分发挥硬件的并行计算能力，提供对应的计算机软件著作权登记证书。	台	2	71000	142000

			3.支持通过 ICMP、TCP、UDP 协议，完成对目的 IP 地址（支持 IPv6）可达性的探测，支持在策略路由、GRE 隧道、DNAT 策略、HA 中设置链路探测。 4.为高效编辑策略，支持对多条策略的源/目的地址、协议/端口、应用、时间等进行批量修改，实现一次修改覆盖多条策略。提供原厂盖章的证明材料。 5.黑白名单内容支持 IP 地址(可直接写入或通过文本智能提取）、协议 TCP/UDP/ICMP 和端口进行设置，且支持配置双向地址。 6.文件传输协议，支持基于 HTTP、FTP、POP3、SMTP、IMAP 协议的进行多线程下载以及有密码压缩包下载限制。提供原厂盖章的证明材料。 7.支持 11000+种入侵规则（支持 IPv6）过滤并提供服务器、内网等多种规则模板。 8.支持 2500 万文件病毒库，病毒查杀率高，支持 ZIP/ARJ/CAB/RAR/GZIP/BZIP2/TAR 等不少于 20 层压缩文件的病毒查杀。提供原厂盖章的证明材料。 9.支持 XFF 解析功能，针对 Web 应用代理场景，可以解析出报文中真实客户端的 IP 地址。提供原厂盖章的证明材料。 10.支持基于域名的防火墙策略，一条策略中支持不少于配置 128 个域名（支持 IPV6），支持通配符格式的域名如 *.test.com,最多支持 10 级域名且层级可配置。提供原厂盖章的证明材料。 11.基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。提供原厂盖章的证明材料。 12.产品符合国内权威机构的《防火墙产品检验方案》的要求，能力成熟度达到三级，提供检验通过证明。 13.产品厂商具备符合 GB/T 27922-2011 的售后服务认证和符合 GB/T31863-2015、GB/T 33718-2017 的履约能力服务认证。				
3	终端准入防御	启明星辰天清入侵防御	1.标准 1U 设备，双电源，标配 8 个千兆电口（含 3 对 bypass），4 个千兆光口，	台	1	98600	98600

	网关（IPS）	系统 V6.0 NGIPS8000-P-G2320-DNR	1 个扩展槽位，128G SSD;增加硬件板卡 8 千兆电口（含 4 对 bypass）一块；默认支持 IPSecVPN 和 SSLVPN 模块(200 个并发用户);默认开通入侵防护功能. 2.产品为专业性入侵防御设备而非 NGAF、NGFW、UTM 设备；厂商是《GB/T 28451-2023 信息安全技术 网络入侵防御产品技术规范》起草单位。系统内置入侵防御特征库，覆盖勒索、挖矿、webshell、僵尸网络、木马后门、蠕虫、信息泄漏、权限绕过、未授权访问、SSRF、XXE、CSRF、代码执行等；（提供第三方权威检测报告证明，包含但不限于 CNAS 或 CMA 检测报告复印件并加盖厂商公章。） 性能要求：最大网络层吞吐量 30G，在入侵防御和防病毒功能开启下，每秒新建 HTTP 连接数 20 万，最大并发连接数 500 万。 准入功能：系统可与现行终端安全管理系统联动，实现终端准入功能，提供加盖厂商公章的可行性测试报告复印件。 授权及质保：3 年入侵防御特征库授权，终端准入联动功能永久开启，至少支持 2000 点终端。3 年原厂维保服务。 安全能力:系统应默认内置不少于 11 种规则集，至少包括严格检测模板、物联网检测模板、WEB 服务器模板、僵木蠕检测模板等。 支持根据特征名称、攻击类型、协议类型、操作系统、来源、严重程度、影响软件、发布年份、流行程度等分类对 IPS 特征库特征信息进行查询（截图证明）;支持入侵防护引擎检测模式设置，包括智能检测或深度检测。可对数据采取不同的处理模式，包括应用优先或安全优先两种模式，用户可根据实际需求灵活选择；（截图证明） 网络部署：系统应支持 HA，包括主主模式和主备模式。支持 DNS 代理设置，可支持 DNS 协议漏洞攻击防护、DNS 反射放大攻击防护、DNS 缓存投毒攻击防护。（截图证明） 安全运维：策略路由支持下一跳 IP 探测，探测的协议类型至少包括（ICMP、TCP、FTP、HTTP、HTTPS、DNS、LDAP、SMTP、POP3、				

			ARP 协议）。（截图证明） 设备运维： 支持基于文件类型的策略路由，可实现将不同文件类型进行智能选路。(截图证明)； 支持针对 HTTP、HTTPS 应用的 URL 控制、网页防篡改、请求体检测、web 表单关键字过滤、文件上传限制、外链防护、盗链防护、CSRF 攻击防护、爬虫等 WEB 安全防护能力。 产品资质：具有中国信息安全测评中心颁发的国家信息安全测评信息技术产品安全测评证书，级别 EAL4+ 产品通过浪涌（冲击）抗扰度测试、雷击抗扰度测试，提供报告复印件及盖公章 具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》 产品制造商具备 GB/T 27922-2011 售后服务认证证书 产品制造商需具备国家信息安全测评中心颁发的信息安全服务资质证书-安全工程类，三级资质。				
4	VPN 接入防火墙	绿盟科技 NFNX3-HF200	1.标准 1U 机架尺寸，国产飞腾 E2000Q CPU，国产银河麒麟 V10 操作系统，8G 内存，数据硬盘为 1TB 固态硬盘，管理口为 1 个 GE 管理口和 1 个 RJ45 串口，2 个 UEB 接口，千兆电口 10 个，combo 口 4 个，接口扩展插槽 2 个，整机网络层吞吐量 4G，整机应用层吞吐量 2G，新建 TCP 连接数 4 万/秒，TCP 并发连接数 100W，含 3 年系统升级服务及 3 年原厂质保。 2.产品在多项安全防护能力开启后的实际防护性能，产品采用多核分布式安全操作系统，充分发挥硬件的并行计算能力，提供对应的计算机软件著作权登记证书。 3.支持通过 ICMP、TCP、UDP 协议，完成对目的 IP 地址（支持 IPv6）可达性的探测，支持在策略路由、GRE 隧道、DNAT 策略、HA 中设置链路探测。 4.为高效编辑策略，支持对多条策略的源/目的地址、协议/端口、应用、时间等进行批量修改，实现一次修改覆盖多条策略。提供原厂盖章的证明材料。 5.黑白名单内容支持 IP 地址(可直接写入	台	2	71000	142000

			或通过文本智能提取）、协议TCP/UDP/ICMP和端口进行设置，且支持配置双向地址。 6.文件传输协议，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制。提供原厂盖章的证明材料。 7.支持XFF解析功能，针对Web应用代理场景，可以解析出报文中真实客户端的IP地址。提供原厂盖章的证明材料。 8.支持基于域名的防火墙策略，一条策略中支持不少于配置128个域名（支持IPV6），支持通配符格式的域名如*.test.com,最多支持10级域名且层级可配置。提供原厂盖章的证明材料。 9.基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。提供原厂盖章的证明材料。 10.产品符合国内权威机构的《防火墙产品检验方案》的要求，能力成熟度达到三级，提供检验通过证明。 11.产品厂商具备符合GB/T 27922-2011的售后服务认证和符合GB/T 31863-2015、GB/T 33718-2017的履约能力服务认证。				
5	安全运维审计堡垒机（核心产品）	绿盟科技OSMSNX3-HF190	1.标准1U机架尺寸，国产飞腾E2000Q 4C 2.0GHz CPU，国产银河麒麟V10 内核5.4操作系统，内存16G，硬盘4TB+ 32G EMMC，管理口1个，千兆电口10个，combo口4个，接口扩展插槽2个，配合可管理资产授权数量100个，字符并发会话数800，图形并发会话数300，含三年原厂质保及系统升级服务。 2.系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约，缺省用户账号密码遗失后仅能被重置，防止密码泄露不支持找回。 3.用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP认证、RADIUS认证、USBKEY认证、OTP、短信认证等身份认证方式；支持可知因素和不可知因素的双因素认证。提供原厂盖章的证明材料。 4.支持通过堡垒机直接代理HTTP/HTTPS	台	1	83600	83600

			协议，无需前置机。提供CMA或CNAS资质的检测机构出具的检测报告扫描件或复印件。 5.支持Oracle、MSSQL、MySQL、PostgreSQL、Informix、达梦、人大金仓、南大通用、高斯、DB2、MongoDB、Sybase、OceanBase、TDSQL For MySQL、TDSQL-C For MySQL、PolarDB For MySQL、SequoiaDB For MySQL等数据库协议代理，支持调用本地工具运维，保留运维习惯。提供CMA或CNAS资质的检测机构出具的检测报告扫描件或复印件。 6.支持基于用户、用户组、组织机构、角色和用户属性的静态授权，通过不同授权模型满足运维管控要求。 7.支持RDP、X11、VNC、SSH、TELNET、RLOGIN、SFTP、FTP、SAMBA协议的HTML5运维，无需本地运维客户端；支持通过H5文件运维的方式上传和下载文件。提供原厂盖章的证明材料。 8.支持可通过参数配置开启或关闭字符、图形、文件、数据库等协议的审计范围，但不影响对应协议的基础会话审计。 9.支持自动化运维，支持自定义自动化脚本。支持设定任务为手动、定时和周期执行方式。支持登录后自动执行脚本，执行完后堡垒机保存运维记录。 10.支持自动化运维功能，支持window bat脚本、windows ps脚本、linux shell脚本、python脚本等脚本类型。提供原厂盖章的证明材料。 11.支持页面风格个性化配置，可以自定义“系统名称”、“系统标签”、“系统图标”、“登录页logo”、"网站ico"、“登录页风格（浅色或深色）”、“登录页背景图”、“登录页logo”、“系统主题色（浅色或深色）”、“导航栏颜色（浅色或深色）”、“系统布局（上下，左右，混合）”、“是否展示页脚”等，无需额外定制。 12.支持堡垒机系统定义为控制器模式和网关模式，控制器模式支持单机或HA部署，网关模式支持单台或多台分布式部署。 13.定制内置的前置机，确保内置前置机能				

			够兼容电围、2/3G 警口、电查、机主等业务系统，以及对应数据库的运维工具，确保全网软硬件资产的运维过程均能够在审计范围内。 14.产品拥有《网络安全专用产品安全检测证书》，符合“增强级”“互联互通”并符合 GB/T45409-2025《网络安全技术运维安全管理产品技术规范》（增强级）要求。 15.产品厂商具备符合 GB/T 27922-2011 的售后服务认证和符合 GB/T 31863-2015、GB/T 33718-2017 的履约能力服务认证。				
6	业务专网入侵检测设备	绿盟科技 NIDSNX3-HH2000	1.标准 1U 机架式设备，交流冗余电源，配置国产化银河麒麟 V10（内核版本 5.4.18）操作系统和国产化海光 3330（3.0GHz，4 核）CPU，内存 16G，2*USB 接口，1*RJ45 串口，2*RJ45 管理口，6 个千兆电口，4 个千兆光口，2 个接口扩展插槽，数据盘容量 4TB，系统盘容量 128GB SSD，整体吞吐量 15Gbps，应用层吞吐量 10Gbps，TCP 并发连接数 400 万，每秒新增会话数 20W，含 3 年的特征库升级授权，3 年硬件维保。 2.产品为专业 IDS 系统，并通过工业和信息化部审核，符合电信设备进网要求。 3.系统提供入侵规则分类，更便捷的制定检测策略，如勒索、挖矿、SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等，攻击特征库数量至少为 15000 种以上。 4.系统提供服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警。 5.系统提供关键文件检测功能和攻击快照功能，能够识别关键文件，以防止非法外传行为。 6.系统能够有效检测 SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁。 7.支持自定义报表模板，可设置报表封面、logo 等信息；可选报表日志类型、可配置过滤条件、可设置执行周期、数据统计区	台	1	81600	81600

			间、并可配置报表格式和输出方式（如本地存储、邮件外发或FTP外发）；支持设置手动报表、自动报表；支持预置至少5种报表模版，报表类别数量不少于50类。提供原厂盖章的证明材料。 8.支持与本次采购的防火墙进行联动，实现针对检测到的入侵攻击进行针对性防护。提供原厂盖章的证明材料。 9.投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，优选市场占有率排名靠前的品牌。 10.产品厂商具备符合GB/T 27922-2011的售后服务认证和符合GB/T31863-2015、GB/T 33718-2017的履约能力服务认证。				
7	互联网入侵检测设备	绿盟科技NIDSNX3-HH2000	1. 标准1U机架式设备，交流冗余电源，配置国产化银河麒麟V10（内核版本5.4.18）操作系统和国产化海光3330（3.0GHz，4核）CPU，内存16G，2*USB接口，1*RJ45串口，2*RJ45管理口，6个千兆电口，4个千兆光口，2个接口扩展插槽，数据盘容量4TB，系统盘容量128GB SSD，整体吞吐量15Gbps，应用层吞吐量10Gbps，TCP并发连接数400万，每秒新增会话数20W，含3年的特征库升级授权，3年硬件维保。 2. 产品为专业IDS系统，并通过工业和信息化部审核，符合电信设备进网要求。 3.系统提供入侵规则分类，更便捷的制定检测策略，如勒索、挖矿、SQL注入、XSS注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等，攻击特征库数量至少为15000种以上。 4.系统提供服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警。 5.系统提供关键文件检测功能和攻击快照功能，能够识别关键文件，以防止非法外传行为。 6.系统能够有效检测SQL注入、XSS注入、webshell等多种常见的应用层安全威胁。	台	1	81600	81600

			7.支持自定义报表模板,可设置报表封面、logo等信息;可选报表日志类型、可配置过滤条件、可设置执行周期、数据统计区间、并可配置报表格式和输出方式(如本地存储、邮件外发或FTP外发);支持设置手动报表、自动报表;支持预置至少5种报表模版,报表类别数量不少于50类。需\提供原厂盖章的证明材料。 8.支持与本次采购的防火墙进行联动,实现针对检测到的入侵攻击进行针对性防护。提供原厂盖章的证明材料。 9.产品是被广泛应用的成熟产品,在国内市场具有较高的市场份额,优选市场占有率排名靠前的品牌。 10.产品厂商具备符合GB/T 27922-2011的售后服务认证和符合GB/T31863-2015、GB/T 33718-2017的履约能力服务认证。				
8	日志审计设备	绿盟科技LASNX3-HH1000	1、标准1U机架尺寸,交流冗余电源,国产Hygon3250 CPU,国产银河麒麟V10操作系统,内存32G,系统盘256G SSD,数据硬盘4TB,管理口1个,HA口1个,USB口2个,千兆电口6个,千兆光口4个,接口扩展插槽2个,配置日志源接入授权100个,日志处理性能5000eps,含日志收集、日志查询、日志存储、报表管理、事件管理、资产管理、用户管理、系统配置等功能,含三年原厂质保及系统升级服务。 2.系统支持的数据采集方式包括但不限于SYSLOG、RSYSLOG、SNMP Trap、FTP、JDBC、NetFlow V5、NetFlow V9 、KAFKA、WMI、专用Agent等方式采集日志。 3.系统支持规则自适应日志接入,仅输入端口即可自动匹配相应规则,完成日志自动接入。提供CMA或CNAS资质的检测机构出具的检测报告扫描件或复印件。 4.系统支持采集国产化操作系统日志,包括但不限于:银河麒麟、中标麒麟、openEuler、中科红旗、统信、龙蜥、BC-Linux、凝思、中科方德等。 5.系统支持界面配置即可完成未识别日志接入,无需编写xml。提供CMA或CNAS资质的检测机构出具的检测报告扫描件或复印件。	台	1	83600	83600

			6.系统内置对主机日志展开深度分析，分析场景包括但不限于登录情况、用户核心文件/文件夹监控、敏感操作及异常外联等。提供通过中国国家认可机构 CNAS 的第三方检测报告。 7.系统内置对 WEB 服务器日志展开深度分析，分析内容包括但不限于发起请求的地址及浏览器情况、响应结果、访问趋势等。提供 CMA 或 CNAS 资质的检测机构出具的检测报告扫描件或复印件。 8.系统支持日志源监控能力，包括采集器维度及资产维度的监控，资产维度支持展示资产详细信息。 9.系统支持对资产进行监控配置，包含资源监控、采集监控、采集限速等。提供 CMA 或 CNAS 资质的检测机构出具的检测报告扫描件或复印件。 10.系统支持将产生硬件故障但能 WEB 访问设备上的数据备机到新设备上，备机数据应包含日志数据、事件告警、报表管理、数据采集、资产管理等。提供 CMA 或 CNAS 资质的检测机构出具的检测报告扫描件或复印件。 11.系统支持多源事件关联分析能力，包括单源过滤模式、多源时序模式和多源关联模式，并支持规则嵌套。 12.系统能够按照多种维度统计日志信息，包括但不限于攻击日志、审计过滤、恶意程序、防火墙、主机报表、应用服务器、网络设备、Windows 审计、Linux 审计、终端审计、SOX 合规、PCI 合规、ISO 27001 合规等多种场景。 13.产品厂商具备符合 GB/T 27922-2011 的售后服务认证和符合 GB/T 31863-2015、GB/T 33718-2017 的履约能力服务认证。				
9	核心区防火墙	绿盟科技 NFNX3-HF200	1. 标准 1U 机架尺寸，国产飞腾 E2000Q CPU，国产银河麒麟 V10 操作系统，8G 内存，数据硬盘为 1TB 固态硬盘，管理口为 1 个 GE 管理口和 1 个 RJ45 串口，2 个 UEB 接口，千兆电口 10 个，combo 口 4 个，接口扩展插槽 2 个，整机网络层吞吐量 4G，整机应用层吞吐量 2G，新建 TCP 连接数 4 万/秒，TCP 并发连接数 100W，含 3 年系统升级服务及 3 年原厂	台	2	71000	142000

			质保。 2.产品在多项安全防护能力开启后的实际防护性能，产品采用多核分布式安全操作系统，充分发挥硬件的并行计算能力，提供对应的计算机软件著作权登记证书。 3.支持通过 ICMP、TCP、UDP 协议，完成对目的 IP 地址（支持 IPv6）可达性的探测，支持在策略路由、GRE 隧道、DNAT 策略、HA 中设置链路探测。 4.为高效编辑策略，支持对多条策略的源/目的地址、协议/端口、应用、时间等进行批量修改，实现一次修改覆盖多条策略。提供原厂盖章的证明材料。 5.黑白名单内容支持 IP 地址(可直接写入或通过文本智能提取）、协议 TCP/UDP/ICMP 和端口进行设置，且支持配置双向地址。 6.文件传输协议，支持基于 HTTP、FTP、POP3、SMTP、IMAP 协议的进行多线程下载以及有密码压缩包下载限制。提供原厂盖章的证明材料。 7.支持 XFF 解析功能，针对 Web 应用代理场景，可以解析出报文中真实客户端的 IP 地址。提供原厂盖章的证明材料。 8.支持基于域名的防火墙策略，一条策略中支持不少于配置 128 个域名（支持 IPV6），支持通配符格式的域名如 *.test.com,最多支持 10 级域名且层级可配置。提供原厂盖章的证明材料。 9.基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。提供原厂盖章的证明材料。 10.产品应符合国内权威机构的《防火墙产品检验方案》的要求，能力成熟度达到三级，提供检验通过证明。 11.产品厂商具备符合 GB/T 27922-2011 的售后服务认证和符合 GB/T 31863-2015、GB/T 33718-2017 的履约能力服务认证。				
合计：人民币：997000 元，大写（玖拾玖万柒仟元整）							997000

设备总价款为人民币［玖拾玖万柒仟］元整（小写：￥997000元），乙方提供增值税专用发票（13%）此价格包含设备价款、运输费、安装调试费、税费等一切费用 。

服务内容：

1、乙方针对供货设备为甲方提供不少于5人的CISP培训服务，培训内容按照CISP考试标准严格执行，40个课时，合同签订后一年内完成所有培训内容，并提供CISP考试培训课件。

2、乙方针对甲方现有的8个业务系统提供安全检查服务，服务内容包括“两高一弱”检查、配置基线检查等，每个季度一次，每年四次。

3、乙方针对甲方网络机房内现有资产提供现场服务，每个季度一次，每年四次，服务内容包括但不限于设备状态巡检、漏洞管理、补丁修复、日志分析、安全加固等。

4、如遇重大安全事件，乙方提供应急响应支持，包含应急响应人员支持、应急响应设备支持等，并承诺2小时内响应，8小时内提供解决方案，24小时内完成应急响应事件处置，48小时内输出应急响应处置报告。

5、乙方负责本次采购设备以及网络机房现有不同品牌设备的集成和联调联试。

6、乙方在施工过程中造成甲方现有设备故障且无法及时修复或修复时间大于2小时的，提供满足现有需求的备件并调试正常运转。

7、乙方提供应急回退方案，在施工过程中遇到问题，且距工作时间不足6小时的，采取回退措施，不得影响业务办理。

二、质量标准

1.乙方提供的设备应符合国家、行业现行的质量标准及双方约定的技术参数要求。

2.设备应是全新未使用过的，且具备完整的包装、配件及技术资料。

三、交付及验收

1.交付时间：乙方应在合同签订后15日历天前将设备设备运送至甲方指定地点。

2.交付方式：乙方负责设备的运输、装卸，运输过程中的风险由乙方承担。

3. 验收期限：甲方应在设备交付后的［10］个工作日内进行初步验收。验收内容包括设备数量、外观、质量、技术参数等，超过［5］个工作日未能完成验收的，视为初验合格。设备联调联试后试运行，试运行合格后进行终验（竣工验收）。

4. 验收标准：依据本合同约定的质量标准及设备技术参数进行验收。若验收发现设备存在质量问题或与合同约定不符，乙方应负责在 5 日内无偿更换并验收合格，逾期更换的甲方有权终止合同，并拒付合同款项。

四、双方权利义务

（一）甲方权利义务

1. 有权要求乙方按照合同约定的时间、质量标准交付设备。

2. 按照合同约定支付设备采购款。

3. 在乙方交付设备时，配合乙方进行设备的交接及验收工作。

4. 对验收合格的设备，按照设备使用说明进行合理使用和维护。

（二）乙方权利义务

1. 有权要求甲方按照合同约定支付设备采购款。

2. 按照合同约定的时间、地点、质量标准交付设备，并提供设备的相关技术资料、售后服务等。

3. 质保期自设备验收合格之日起计算，期限为 3 年。在设备质保期内，乙方对设备出现的质量问题，负责免费维修或更换。

4. 乙方负责对甲方使用人员进行必要的设备操作培训，确保甲方人员能够正确使用设备。

五、付款方式

1. 第一笔：合同签订后财政拨付资金到账后 30 个工作日内，乙方提供合法的发票后支付合同总金额的 40.0%，即人民币 ￥398800.00 元；

2. 第二笔：供货联网调试完成，财政资金拨付后，30 个工作日内，支付合同总金额的 50.0%，即人民币 ￥498500.00 元；

3. 第三笔：项目验收合格后，达到付款条件起 30 个工作日内，支付合同总金额的 10.0%，即人民币 ￥99700.00 元。

2. 乙方指定的收款银行及账户

乙　　方：陕西卓为信息技术有限公司

账　　号：61001930041052515625

开 户 行：中国建设银行股份有限公司西安经济技术开发区支行

六、违约责任

1.交付违约：若因乙方原因造成服务交付延迟，乙方应主动告知甲方并加急整改。逾期情形轻微的，双方友好协商免责；确造成甲方实际损失的，乙方不仅要承担给甲方造成的损失，还要承担不低于合同总价5%的违约金。

2.付款违约：甲方应按约及时付款。若出现短期逾期，双方友好协商顺延，互不追责。若无故逾期超过30个工作日、且经乙方提醒仍未履约的，乙方可单方解除合同，甲方仅需赔偿乙方实际产生的直接损失。

3.其他违约：双方在履约过程中出现轻微违约情形的，优先沟通整改、互不追责。若一方过错造成对方实际损失的，违约方仅需赔偿守约方实际直接损失。

4.违约赔偿以弥补对方实际直接损失为原则，秉持公平友好原则处理，不重复、超额追责。

5.合作过程中出现违约争议，双方坚持友好协商、互谅互让为先，积极化解问题。协商无果的，可按本合同争议条款合规处理。

6.若乙方交付的设备质量不符合合同约定，乙方应负责无偿更换、直至设备验收合格。如因此导致甲方损失的，乙方应承担赔偿责任。若产品存在严重质量问题，需承担违约金，标准为合同总价的20%。

七、保密条款

双方在合作期间，应对知悉的对方商业秘密、技术信息、涉密资料予以妥善保管、善意使用。合同终止后，仍需保持保密义务。若因疏忽造成轻微泄密且及时整改、未造成损失的，互不追责；若故意泄密造成对方损失的，需赔偿实际直接损失。

八、不可抗力

1、不可抗力指不能预见、不能避免、不能克服的客观情况，包括自然灾害、战争、疫情、政府政策重大调整、行政管制、系统全域故障等法定情形。

2、遭遇不可抗力一方应及时书面通知对方，并于30个工作日内提供有效证明文件，双方可相应顺延履行期限，互不承担违约责任。受影响方应积极采取措施降低损失。

3、不可抗力持续超过90日，导致合同无法继续履行的，任一方均可书面通知对方解除合同，双方据实结算，互不追责。

九、争议解决

本合同在履行过程中如发生争议，双方应首先友好协商解决；协商不成的，任何一方均有权向甲方住所地有管辖权的人民法院提起诉讼。

十、其他条款

1. 本合同自双方签字（或盖章）之日起生效。

2. 本合同未尽事宜，双方可签订书面补充协议，补充协议与本合同一致。

3. 本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。

甲方（盖章）：铜川市人力资源和社会保障局

法定代表人或授权代表（签字）：

签订日期：2026 年 8 月 20 日

乙方（盖章）：陕西卓为信息技术有限公司

法定代表人或授权代表（签字）：

签订日期：2026 年 8 月 20 日