报价唯一性

分项报价表

项目编号/包号：常采公[2023]0248 号
项目名称：常州市钟楼区人民检察院检察工作网安全体系建设项目
报价单位：人民币元

序号	分项名称	品牌商标	规格型号	技术参数	数量	单位	投标价格	
							单价	合价
1	防火墙	深信服	FW-1000-GA640	网络层吞吐量≥9.5Gbps，应用层吞吐量≥1Gbps，并发连接数≥220 万，新建连接数≥10 万； 标准 2U 设备；国产 CPU，CPU 核数≥4，CPU 主频≥2.0GHz，中标麒麟操作系统；内存≥8GB；标配≥6 个千兆电口+4 个千兆光口；3 年软硬件维保，3 年特征库升级。 产品须开启 IPS 模块，具备入侵防御功能。 产品须开启 web 应用防护模块，具备 web 应用防护功能。 产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 产品支持策略路由负载来支持基于服务、ISP 地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，总共需要支持加权流量、带宽比例、线路优先等负载均衡调度算法。 产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求 产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制。 产品支持源地址转换 SNAT，目的地址转换 DNAT 和双向 NAT 等功能， 支持一对一、一对多、多对一等形式的 NAT。支持 IPv4 / v6 NAT 地址转换。 产品内置应用特征识别库，支持不少于 2980 种应用规则，支持对游戏、下载工具、IM 聊天工具、视频软件、股票软件等类型应用进行检测与控制。 产品具备Web 应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含 SQL 注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL 后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为，安全特征规则超过 3320 种。 具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵。需提供国家权威机构出具的关于“漏洞防扫描”的相关证书。 支持对服务器和客户端的漏洞攻击防护，支持 XSS 攻击、SQL 注入等 WEB 攻击行为进行有效防护；	1	台	128000	128000

				支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等 DoS/DDoS 攻击防护；支持 IP 地址扫描和端口扫描防护； 支持 Land、Smurf、WinNuke、Tear Drop、IP 数据块分片传输、超大 ICMP 数据攻击等攻击基于数据包攻击防护；支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 支持对常见应用服务（FTP、SSH、SMTP、IMAP、POP3、RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间；（提供相关证明材料） 产品支持僵尸网络检测功能，防止失陷主机威胁内网扩散。需提供国家权威机构出具的关于“僵尸网络检测”的相关证书。 产品支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 产品支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便安全策略管控。需提供国家权威机构出具的关于“安全策略管理”的相关证书。 要求所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。 所投产品需具备《计算机软件著作权登记证书》，提供有效的证书复印件。 所投产品具备中国国家信息安全产品认证证书，提供有效证书复印件。 提供产品生产厂家出具的叁年质保承诺书原件并加盖供应商公章				
2	路由器	华为	AR3260-2X100E-AC	采用无阻塞交换架构 交换容量≥640Gbps 双主控双电源，千兆光口*8，千兆电口*6，千兆 combo 口*4，三年维保 模块插槽≥10 个； 包转发能力最高可达 40Mpps 支持 FE、GE、EPON/GPON、同异步串口、E1、T1、3G、4G/LTE 等接口 支持 4G LTE 接口，LTE 可向下兼容 3G 支持静态路由，策略路由，动态路由协议：RIP、OSPF、BGP、IS-IS 支持 IPv6 静态路由；支持 RIPng、OSFPv3、IS-ISv6、BGP4+等动态路由协议； 支持组播协议：IGMP V1/V2/V3，IGMP-Snooping V1/V2/V3，PIM SM，PIM DM，MSDP 支持 LDP，MPLS L3 VPN，静态 LSP，动态 LSP，MPLS TE，IP FRR，LDP FRR，TE FRR	1	台	45000	45000

				支持 MAC、802.1x、Portal 认证、广播抑制、ARP 安全等，支持本地认证、AAA 认证、RADIUS 认证等 支持包过滤防火墙、ASPF，支持防火墙安全域 支持 IPS 安全功能，特征库可在线升级，可以防范木马，蠕虫，病毒等攻击 支持 URL 过滤功能，可以过滤指定域名的网站，并可远端查询; 所有业务板卡支持直接热插拔 支持接口备份功能，VRRP 等可靠性技术 支持 BFD 功能，包括 BFD for 静态路由/RIP/OSPF/ISIS/BGP/RSVP/PIM 等 支持智能策略路由（SPR）或者类似技术，可根据多个链路的网络质量，动态选择最佳链路 支持 NetStream 或类似的流量采集功能；须与现有设备组成双机热备模式。 支持 Console、telnet、SSH 等登陆方式;支持 mini-usb console 接口 支持 SYSLOG、SNMP V1/V2/V3、RMON、WEB 网管、CWMP 功能; 提供产品生产厂家出具的叁年质保承诺书原件并加盖供应商公章				
3	核心交换机	H3C	S5560-54C-EI	交换容量≥598Gbps，包转发率≥252Mpps。 提供不低于 48 个千兆电口，4 个万兆光口；双电源。 支持 802.1X 认证/集中式 MAC 地址认证; 支持 IRF2 智能弹性架构，分布式设备管理，分布式链路聚合，分布式弹性路由。 支持基于端口的 VLAN、支持基于协议的 VLAN、支持基于 MAC 的 VLAN 支持流镜像、N:4 端口镜像、本地和远程端口镜像; 支持静态路由、RIPv1/v2，RIPng、OSPFv1/v2，OSPFv3、BGP4，BGP4+ for IPv6、IS-IS、等价路由，策略路由、VRRP/VRRPv3 等 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 支持 GE 端口聚合、10GE 端口聚合、40G 聚合、静态聚合、动态聚合、跨设备聚合。 支持 RMON 告警、事件、历史记录，支持 iMC 智能管理中心，支持电源的告警功能，风扇、温度告警，支持 VCT（Virtual Cable Test）电缆检测功能，支持 DLDP 单向链路检测协议。三年质保。	1	台	21500	21500
4	堡垒机	深信服	OSM-1000-GA640 V3.0	标准 1U 设备，国产 CPU，国产操作系统；内存≥16G，硬盘≥64GB SSD+1TB SATA，至少提供 6 个 1000M 电口，4 个 1000M 光口。 可管理资源数≥50 个，支持 licence 扩容物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构系统各模块支持以 B/S 方式管理，采用 https 加密方式访问全面支持 Windows、linux、国产麒麟系统、	1	台	115800	115800

				Android、IOS、Mac OS 等客户端操作系统下的 H5 页面一站式运维，实现跨终端适应性 BYOD（Bring Your Own Device）字符协议：SSHv1、SSHv2、TELNET 图形协议：RDP、VNC 文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板支持通过协议前置机进行协议扩展，至少支持扩展 KVM、Vmware、数据库、http/https、CS 应用等支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期支持对用户指定限制登录 IP、登录时间段（可循环，如每周一到周五 9：00-17：00 时）等规则，以确保可信用户登陆系统支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度符合密码策略要求支持 unix 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开支持命令黑命单，对字符型设备（如 linux/unix/网络设备）的高危命令执行进行阻断，如 rm、shutdown、reboot 等支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人支持配置资源访问时间规则，即使授权范围内的资源，需在指定时间范围内才可发起访问，确保运维在可信时间范围支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP 等客户端工具实现单点登陆，不改变运维人员操作习惯支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放支持对 FTP/SFTP 传输的原始文件进行完整记录，并提供下载取证支持提供系统内部操作审计，包括管理员和运维用户的登录、登出、对系统的配置操作、账号属性修				

				改等系统管理操作全面支持 IPV6，设备自身可以配置 IPV6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登陆和审计公安部《计算机信息系统安全专用产品销售许可证》；国家版权局《计算机软件著作权登记证书》				
5	入侵检测系统	奇安信	网神 P3300-1610-F	国产操作系统以及国产芯片；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，4 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 口所投产品设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；所投产品支持 IPv6 环境下的静态路由及动 OSPFv3 动态路由所投产品支持配置基于 IPv6 地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL 过滤、应用识别、反间谍软件等安全功能；所投产品支持路由模式、透明模式的 HA 高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA 高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA 高可靠性部署支持配置接口权重；支持链路探测所投产品支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查所投产品比如支持基于 IPv4/v6 地址、应用的会话限制，限制动作包每 IP 新建、每 IP 并发、所有 IP 新建、所有 IP 并发，且可以基于安全域指定限制方向所投产品支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 2800 种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类所投产品支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件五种分类；所投产品支持上传、下载、双向的文件内容过滤，内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持 html、doc、docx、xls、xlsx、ppt、pptx、chm、7z 等 30 种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别所投产品支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片等；并可在设备页面显示每种攻击类型的丢包统计结果所投产品支持自定义基于 TCP、UDP、HTTP 协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围所投产品支持防御基于安全域	1	台	118500	118500

				的 IP 地址欺骗攻击，指定 IP 或网段从特定安全域流入能够检测包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、物联网漏洞攻击等在内的网络攻击行为所投产品支持自定义 TCP、UDP、HTTP 协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的 CVE 编号或 CNNVD 编号。 所投设备提供统计分析面板，可展示威胁统计、恶意 URL、恶意域名、恶意地址所投设备支持自定义一个或多个过滤条件，日志可以进行模糊检索或指定条件的精确检索，快速定位特定目标当前行为是否存在异常，网络中是否存在异常等问题，并可记录一个或者多个自定义过滤条件历史。 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 所投设备支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询产品具备公安部《计算机信息系统专用产品销售许可证》提供产品生产厂家出具的叁年质保承诺书原件并加盖供应商公章				
6	终端安全	奇安信	WS-ESM-XC-FL-AVS	支持：麒麟 v10 服务器（龙芯 3B3000、鲲鹏 920、FT2000+、兆芯 C/E）、UOS20 sp1 服务器（龙芯 3B4000、兆芯 C/E）、中科方德（龙芯、飞腾、申威、X86） 本次配置≥100 点授权，支持：银河麒麟 V10(龙芯、飞腾、X86)、银河麒麟(龙芯、飞腾、X86)V10.1、UOS20 sp1(龙芯、龙芯 3A5000、鲲鹏 920、麒麟 9006C、飞腾、X86、兆芯)、中科方德（龙芯、飞腾、申威、X86），TencentOS Server3 单机客户端在接入控制中心后，自动转换为网络工作模式 支持跨平台统一管理，控制中心可统一接入管理网络中的 WINDOWS 系统终端防病毒、类 LINUX 系统终端防病毒、国产通用终端(AK)、国产专用终端防病毒(ZYJ)；控制中心支持多级级联部署，并支持病毒查杀日志上报；支持病毒库从上级升级；支持上级控制中心对下级控制中心自动动态授权分配或手动自定义分配授权点数 支持控制中心数据库的备份及还原；支持定时备份；支持备份到指定 FTP 服务器 设置客户端到控制中心下载的并发数和带宽限制，可灵活设置每周或者每天具体限速时间段 服务器升级设置 - 可以设置病毒库自动更新的频率和时间，更新源支持互联网升级、从上级控制中心升级或从指定的控制中心升级，支持断点续传，支持设置升级使用的 HTTP 代理服务器 可以设置服务器访问的白名单 IP 地址段，只有在白名	1	套	20000	20000

				单范围内的 IP 可以访问控制中心，增强安全性 支持创建策略模板，模板可复用，可作为基准创建新模板；添加策略时按场景关联模板，使用更灵活 支持策略模板优先级，策略可以关联多个模板，模板中策略存在冲突时，可以自动处置策略冲突，按照优先级高的执行； 支持生效规则和生效时间条件设定，策略可以根据生效规则下发到不同范围类型的终端上去，同时可针对多个策略设置的不同的生效时间条件，确保策略在管理员指定的时间和条件范围内生效； 支持单点策略下发，可以针对特定终端下发不同的策略 支持分组策略下发，可以针对不同的终端分组（部门）下发不同的策略； 终端密码防护：支持防退出密码保护和防卸载密码保护，支持静态密码和动态密码。 升级策略：支持可选自动升级策略和非自动升级策略 支持终端使用情况统计，包括安装率、部署率、实名率、操作系统分布、cpu 分布等 可查看全网或特定分组内终端的安全情况，包括计算机名、IP 地址、病毒数、病毒库更新时间，支持通过自定义标签、终端类型、操作系统、在线状态、计算机名称、IP、MAC、使用人等多个条件的与/或组合进行终端筛选，支持保存筛选条件；支持对终端进行分组转移和手动删除终端操作 支持注册终端的概览信息、策略信息、病毒查杀日志； 支持通过分组或条件筛选对指定范围的终端下发快速扫描、全盘扫描、强力查杀、隔离区文件恢复； 支持隔离区锁定，锁定后用户无法操作。支持隔离区文件过期自动清除。 支持对指定范围的终端下发升级病毒库任务； 病毒分析统计报表：支持终端病毒分析趋势分析和统计，包含病毒查杀趋势、病毒种类占比、触发方式趋势、病毒排行榜；支持报表导出； 统计分析方式：支持按分组统计、按终端名统计、按病毒统计多种统计方式；支持各类统计导出 支持病毒日志详情中按病毒名搜索，便于追查网内是否已有外部安全事件暴露的病毒； 黑白名单添加方式： 支持通过填写文件 MD5、SHA1 值上传；支持通过导入文件的方式上传，适合黑白名单较多的情况；支持根据客户端上报的扫描结果添加黑白名单 文件实时监控：针对文件复制粘贴、移动、重命名等操作实时监控，发现威胁文件及时告警并隔离； 监控文件执行操作，发现有恶意进程启动时，及时告警并拦截阻止程序运行 支持文件监控、文件右键手动扫描、定时扫描，以及全盘扫描、快速扫描和自定义扫描等，对恶意代码进行清除、删除，并支持备份。 支持客户端软件程序、恶意代码特征库的在线和离线				

				升级，支持客户端手动和自动升级。 病毒库离线升级：支持通过客户端离线升级工具导入最新的病毒库，完成本地病毒库升级； 服务端一键升级：支持管理员通过升级管理功能对指定的分组、终端或全网进行一键下发升级任务，完成批量终端本地病毒库升级； 支持自动升级和手动升级选择设定，手动升级默认主程序和病毒库都不自动升级，也可选择不升级主程序但升级病毒库； 实时防护开启：支持文件系统实时防护的开启和关闭； 病毒发现处理：实时防护过程中发现病毒时处理方式可选择杀毒软件自动处理病毒，并将原始文件隔离备份，也可选择发现病毒后通知终端用户，由终端用户选择处理； 支持防护级别设置，支持监控文件类型设置。 扫描类型设定：支持扫描所有文件、仅扫描程序及文档文件选择； 病毒发现处理：发现病毒时处理方式可选择杀毒软件自动处理病毒，也可选择用户选择处理； 资源占用选择：终端病毒扫描时，资源占用选择不限制、低资源、平衡型； 目录白名单：加入白名单的目录在病毒扫描和实时防护时将被跳过，如果路径在终端未被匹配到，该条目将失效； 扩展名白名单：带有白名单中扩展名的文件，在病毒扫描和实时防护时将被跳过； 压缩包层数设置：支持压缩包扫描设置，可以设定最大扫描多少层的压缩包文件； 压缩文件跳过设置：支持跳过文件大小大于阈值设定的单个压缩文件； 支持扫描跳过文件大小超过阈值设定的单个大文件，提高扫描性能； 实时防护锁定：实时防护是否允许终端用户开启或关闭； 扫描任务锁定：扫描时是否允许终端用户暂停、停止扫描任务； 定时扫描查杀锁定：是否允许终端用户自行修改本地定时查杀设置 支持客户端杀毒软件防非授权退出和软件自保护，可以做到防止用户私自退出安全防护，防止用户或第三方软件对安全防护软件的强退破坏； 国产专用机终端恶意代码检出率不低于 99.5% 国产专用机终端恶意代码误报率不高于 0.1% 具备产品软件著作权，提供国家版权局颁发的《软件著作权登记证书》 提供公安部颁发的《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（增强级）资质证书。 要求提供产品生产厂家出具的叁年质保承诺书原件并加盖供应商公章				
7	数字化安	中电鸿信	定制	（1）基础设施运维管理:根据本次采购清单中列明的系统设备及相关设备提供维护、技术支持服务和运维	1	项	140000	140000

	全运维服务			管理服务，通过对设备定期进行规范化的预防性巡检，并提供巡检报告；对存在问题及突发故障提供及时有效的技术支持、完善的解决方案和事后防范机制，减低故障对生产的影响，使系统与设备保持或迅速恢复其良好的工作状态，消除产生故障的薄弱环节，使系统与设备更趋于稳定、安全、合理和高效，同时提供相关巡检报告。 （2）资产数字化管理：加强信息化资产包括应用系统资产整理能力，实施数字化资产整理服务，将目前所有的软硬件资产、外围线路资源、拓扑结构、系统架构、端口、应用数据信息梳理清楚。对大量基础设施进行统一管理、统筹分配形成专有信息资产库，结合完整的信息化资产整理规范，综合查看所有（机房、机柜、设备等）的软硬件配置、工作配置文件、质保时间、维修记录、服务工单、日常维护记录、巡检记录、运维知识库等，并能提供各种安全便捷的方式查看相关资料（电脑终端、微信端等），从而提高基础设施安全运维效率，保障整体网络的安全平稳运行。 （3）信息化基础架构整体优化部署：结合采购人现有的所有业务应用系统、实际业务需求，需不断优化现有基础设施软硬件设备的运行模式，并根据业务系统实际运行情况提出安全优化部署建议，根据采购人相应实施方案对信息化基础设施进行部署，重点对工作网内重要系统或设备进行安全性、功能性优化，在保障基础设施重要设备得到充分利用的前提下，进一步保障网络基础架构的高可用性，避免业务中断，增加网络稳定性及可靠性，同时，还须配合采购人做好服务期内机房及弱电井内线路整理工作，保证物理线路也得到充分优化及保障，使采购人的信息化基础设施安全保障工作达到一个更高的标准。 （4）通讯链路检查排障：网络的健康状况整体运行状态、各项硬件资源开销状况、链路健康状况如端到端时延变化、链路端口工作稳定性、链路负载百分比、部署路由策略情况下端到端选路变化、路由条目变化、管理权限用户的行为审计、设备软件配置变动审计、设备日志审计、安全事件审计等，需根据采购人要求定期提供各种机房、系统、设备对应的数字化巡检报告，积极配合采购人进行网络构架调整和故障处理，减少网络变更的风险。 （5）基础设施资源排障及安全加固：在服务期内对采购人所有业务终端、硬件设备、各业务应用系统等通过专业的系统巡检工具及安全扫描工具，并结合人工检测的方式进行多方位扫描，并提供对应稳定性修补文档。通过安全运维专业人员的技术支持服务，协助采购人信息化应用人员做好各种日常安全维护管理工作。 （6）信息化安全事件统一处理：配合采购人将各种系统事件、安全事件的相关处理结果全部记录在案，并提出相应改进建议及方案，方便事后分析，不断提高采购人的网络安全运行防护系数，及时避免和降低安				

				全事故，提高整网信息化系统的安全性和稳定性。协助采购人对指定系统实施对应的系统、安全整改/加固工作。 （7）安全运维应急演练：协助采购人制定各种符合常州检察系统实际情况的基础设施安全运维事件应急演练方案，进行各种系统/安全突发事件的故障解决演练及技术演练，根据演练成果，不断改进安全运维管理方式。 （8）数字化安全运维培训：通过对采购人设备实施数字化资产整理服务后，依据现有的系统及安全运维内容，并结合现有的实际业务环境部署优化需求，将数字化安全运维中的数字资产管理、指标化巡检服务、系统优化调整、安全运维服务等内容给用户定期培训，或根据用户需求，对安全运维范围内的各类技术和标准进行培训，不断优化数字化安全运维服务内容及规范。 （9）安全运维建议：通过对采购人基础设施情况的具体了解及需求分析，结合投标方自有项目实施能力、规划经验，为采购人提供更符合实际情况的软硬件基础设施管理目标、软硬件安全运维方案，在现有资源基础上，加大利用率，进一步提高采购人在基础设施安全运维方面的绩效及目标，发挥出基础设施资源的最大效能。				
8	数字化安全运维平台	中电鸿信	定制	数字化安全运维管理平台应采用二维码化与知识化的核心目标，利用“数据收集”、“码上运维”、“知识统一”三大理念及为多种专业定制的用户视图提供“扁平化”数字安全运维服务。并通过各种运维服务不断收集处理各种运维数据及知识，为用户及运维团队提供实时决策数据支持。平台包含数字化设备资产查询（机房/机柜/设备等）、机房巡检、设备巡检、日常事件管理、服务工单管理、运维服务管理等功能模块。	1	项	20000	20000
合　　计							608800	608800

注：1.本表应按包分别填写。
2.如果不提供分项报价将视为没有实质性响应招标文件。
3.本表行数可以按照项目分项情况增加。
4.上述各项的服务内容如表格中填写不下的，可以逐项另页描述。

投标人名称（加盖公章）：中电鸿信信息科技有限公司
日期：2023 年 11 月 1 日