采购需求

一、项目概况

本项目为人民检察院检察工作网综合运维服务，覆盖检察工作网核心网络、中心机房、网络安全设备、业务终端及专线链路等全范畴运维保障（涉密部分除外），严格遵循政法网络安全及检察信息化建设相关规范，通过专业化、标准化的运维管理与安全加固服务，实现现有运维服务的无缝、平稳承接，保障核心业务系统安全、合规、连续运行。同时推进安全平台国产化升级改造，全面加固工作网安全防线，强化系统安全纵深防御能力。

二、服务区域

渭南市人民检察院本级及所属各区、县人民检察院。

三、实施目标

1.业务连续性目标：核心业务系统全年可用率不低于99.9%，无因运维服务失误导致的业务中断或数据丢失；建立完善的故障应急响应机制。

2.运维服务延续性目标：完成现有运维工作的平稳交接，建立完整的运维服务台账、知识库与应急方案，实现运维服务无脱节、无空档。

3.安全加固目标：按要求完成安全平台国产化升级，升级后系统安全防护能力符合网络安全等级保护要求，安全漏洞整改率100%，构建完善的纵深防御体系。

4.合规性目标：所有运维操作、安全改造工作均符合检察信息化管理规定、网络安全相关法律法规及保密管理要求。

5.检察工作网承载非涉密业务与办公，须与涉密网、互联网物理隔离，严禁交叉、数据互通，按等保分级管理。

四、主要服务范围（涉密除外）

1.安全平台升级及运维服务

（1）核心设备配置的定期备份、版本化管理及合规性检查（安全网关、安全探针等20余个设备定期登录、相关特征库/规则库实时更新与策略调优服务、配置信息数据定期更新维护等）；

（2）全系列安全设备须按要求定期进行更新维保；

（3）对软硬件进行漏洞扫描服务，及时发现漏洞，并进行安全加固服务。

（4）安全平台升级：原入侵防护（NIPSNX3-CH3330）、防火墙（NFNX3-CH3330）、网络安全漏洞扫描（RSASNX3-X）三台设备维保到期且退服，全面升级为信创平台。综合考虑本项目实际情况,为覆盖本项目全部资产及未来扩展需求,系统配备具体应满足如下参数要求：

服务名称	参数需求	单位	数量
网络入侵防护系统	1、采用国产处理器架构及国产操作系统，满足信创环境适配要求，网络层吞吐量≥10G，应用层吞吐量≥2G。标准1U机架式设备，配置交流冗余电源；USB接口≥2个，RJ45串口≥1个，RJ45管理口≥1个,电口（3路bypass）≥6个，千兆光口≥4个；接口扩展槽位≥2个；硬盘≥256G SSD+4T SATA。 2、▲系统攻击特征库数量不少于15000条，支持定期更新，具备针对主流网络攻击、漏洞利用、恶意代码等威胁的识别能力，可覆盖常见攻击场景。 3、攻击告警和攻击频率设置支持关联模版规则进行检测，	台	1

	支持高、中、低不同级别的检测灵敏度设置，支持设置诱饵 IP 的识别机制。 4、通过 X-Forwarded-For、X-Real-IP 等字段来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务的客户端最原始/真实的 IP 地址，并可自定义 IP 识别字段的优先级顺序。 5、▲系统首页支持以可视化方式展示威胁事件分布、攻击类别分布与趋势、TOP 入侵事件、TOP 攻击源/目的 IP、攻击源地理分布等信息；支持对威胁事件进行下钻分析，关联查看对应日志分类及详细信息。 6、▲支持与日志审计系统进行联动，同时支持通过标准协议（如 Kafka）与第三方平台进行数据对接；通过 Kafka 服务器与第三方联动。 7、▲系统具备 DoS/DDoS 攻击防护能力，可识别并防护常见的 Flood 攻击（如 SYN Flood、UDP Flood、DNS Flood、HTTP Flood 等）、端口扫描（TCP/UDP 端口扫描、PING Sweep）及 ARP 欺骗等攻击行为。 8、对高危漏洞、高危端口、弱口令进行有效识别，支持场景化配置与展示，支持关联高频高危漏洞、关联高危端口配置，支持关联漏洞动作自定义设置，支持开启高危端口访问拦截。 9、系统支持系统状态告警规则配置，可设置温度、电源、证书、升级管理、高可靠等告警项的规则与阈值，支持告警信息推送至消息中心。 10、▲提供软件著作权证明（代理商须提供软件厂商授权+权属证明），证明有效、合格，且与产品名称、内容匹配，否则佐证无效。 以上参数、功能需提供有效佐证（指定要求的除外）：厂商向社会公开的功能截图/产品说明书/具备 CNAS/CMA 资质的第三方检测机构出具的检测报告（依据标准现行有效，检测结果满足要求）等。		
防火墙系统	11、标准 1U 机架式设备，网络吞吐量≥10G，应用层吞吐量≥3G，最大并发连接数≥250 万，新建连接数≥3 万，千兆电口≥16 个，千兆光口≥8 个，万兆光口≥4 个，接口卡扩展槽≥1 个，配置双电源，支持 SSL VPN 功能，并发用户授权≥15 个。提供入侵防御、防病毒、应用识别、URL 过滤、Web 应用防护等安全特征库升级授权，服务期不少于 3 年。 12、支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等分类展示，并给出总体安全评分。 13、支持僵尸网络分析，攻击链推导及资产安全风险等级的可视化呈现。	台	1

	14、支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，支持配置多维度过滤条件，包括源/目的安全域、源/目的地址、用户、服务等，支持配置多条匹配规则。 15、▲支持流量自学习功能，可设置自学习时间，并自动生成 DDoS 防范基线及防范策略。支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。 16、▲支持基于应用层协议设置流控策略，可设置最大带宽、保证带宽、协议流量优先级等,支持带宽通道独占以及共享管理模式。 17、支持对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的差异化防护策略。支持自动黑名单管理功能。 18、支持超过 16000+种特征的全面攻击检测和防御能力，可识别并防护主流网络攻击、漏洞利用、恶意代码等威胁。 19、▲提供软件著作权证明（代理商须提供软件厂商授权+权属证明），证明有效、合格，且与产品名称、内容匹配，否则佐证无效。 以上参数、功能需提供有效佐证（指定要求的除外）：厂商向社会公开的功能截图/产品说明书/具备 CNAS/CMA 资质的第三方检测机构出具的检测报告（依据标准现行有效，检测结果满足要求）等。		
网络安全漏洞扫描系统	20、系统支持虚拟化部署，可适配主流虚拟化平台；支持授权 IP/域名资产扫描，授权规模不低于项目实际资产需求（为覆盖本项目全部资产及未来扩展需求，授权可扫描总数量≥1000 的 IP 地址或域名，最大并发主机数≥60,最大并发任务数≥10）；支持多任务并发扫描，可配置合理的并发主机数与并发任务数，满足本项目扫描效率要求。 21、系统具备全面的漏洞检测能力，支持主流漏洞标准（如 CVE、CNNVD、CNVD 等），可覆盖常见的系统漏洞、应用漏洞、配置漏洞等。 22、▲支持风险告警与闭环管理，可配置告警内容、方式及资产范围，支持邮件、平台告警等多种通知方式；支持风险状态的批量或单个管理。 23、▲支持可视化风险分析，可展示资产风险分布、风险等级、风险趋势等信息，支持详情查看。 24、支持自定义报表功能，可配置报表标题、页眉页脚、章节内容等。 25、支持弱口令/口令猜测检测，可针对主流操作系统、数据库、中间件、网络设备等常见协议进行口令安全检测；支持自定义用户字典、密码字典。 26、支持国产操作系统、国产数据库及国产应用软件的漏洞检测，具备针对国产环境的漏洞识别能力。 27、▲支持漏洞验证功能，可对扫描发现的漏洞进行验证，输出漏洞利用过程与风险分析报告。		

	28、支持资产探测功能，可实现主机资产、Web 资产的自动探测与识别。 29、▲提供软件著作权证明（代理商须提供软件厂商授权+权属证明），证明有效、合格，且与产品名称、内容匹配，否则佐证无效。 以上参数、功能需提供有效佐证（指定要求的除外）：厂商向社会公开的功能截图/产品说明书/具备 CNAS/CMA 资质的第三方检测机构出具的检测报告（依据标准现行有效，检测结果满足要求）等。
★网络入侵防护系统、防火墙系统、网络安全漏洞扫描系统须经四部委（国家网信办、工信部、公安部、国家认监委）授权的机构进行网络关键设备和网络安全专用产品的安全认证或安全检测（结果合格且符合要求，同时提供该认证机构或检测机构在四部委授权机构的名单截图）。	

2.云平台升级及运维服务

（1）平台、软件定义存储与网络的日常监控、故障处理、性能优化及补丁升级服务；

（2）38 台物理服务器（品牌：锐捷 RG-CS5020 等）、3 套超融合一体机硬件状态监控，并进行故障诊断、备件更换及性能优化等服务。

（3）云平台（品牌：深信服等）升级，麒麟内核 OS 授权、虚拟桌面接入管理软件授权。

3.机房运维服务

（1）动力环境运维（机房空调、UPS、配电、精密列头柜等动力系统）；

（2）环境监控与预警、定期巡检、维护保养(安防监控、硬盘录像、硬盘、消防报警、烟感、温感、气体灭火装置、LED 显示系统)；

（3）容灾备份系统维护。

4.网络与通信服务保障服务

（1）12 条骨干线路维护（含各区县）；

（2）对核心、汇聚及接入层交换机（共计 26 台，品牌：华为 S5735-S48S4X、CE6881-48S6CQ-B 等）进行配置管理、性能监控及故障排查；

（3）各单位桌面终端及接入层信息点的系统维护及故障排查。

5.交付资料

（1）系统运行操作说明书、维护手册、软件著作权、安全认证证书/检测报告等；

（2）试运行报告、定期运维报告、漏洞扫描报告、性能分析报告、备份报告等；

（3）人员培训记录表、相关专业证书、派驻人员服务日志等。

五、主要服务内容

（一）日常巡检值守服务

1.实行 7×24 小时电话+远程响应，工作日安排驻场运维工程师在岗值守。

2.每日全网设备在线状态、链路带宽、机房温湿度、UPS 负载、动环告警巡查。

3.每周全覆盖网络配置、安全策略、服务器运行巡检。

4.每月出具巡检报告、隐患整改清单。

5.建立运维台账：设备资产清单、配置备份、巡检记录、故障工单、整改记录、值班日志等，全程可追溯。

（二）网络设备运维

1.负责工作网所有网络、安全设备日常配置维护、固件版本升级、配置定期备份、异常告警处置等。

2.网络卡顿、环路、IP 冲突、端口宕机、跨网访问异常等故障快速排查修复等。

3.配合完成网络拓扑调整、VLAN 划分、权限隔离、路由策略优化，严格落实工作网与互联网物理隔离要求。

（三）中心机房运维

1.机房环境、供电、制冷、消防、安防、动环系统日常维护，及时处理断电、温湿度超标、设备告警等问题。

2.服务器操作系统、数据库日常监控、启停维护、磁盘空间清理、资源负载优化。

3.每季度机房全面安全体检，排查线路老化、机柜布线混乱、接地不规范等隐患并整改。

（四）终端及系统运维

1.工作网终端系统重装、软件安装、病毒查杀、账号权限配置、密码重置、外设故障调试。

（五）网络安全运维

1.定期开展漏洞扫描、弱口令核查、恶意行为监测，及时安装安全补丁、封堵安全漏洞。

2.防火墙、网闸、安全审计设备策略常态化优化，定期导出安全日志、留存审计记录。

3.配合完成网络安全等级保护测评、涉密信息检查、上级网信及检察系统安全督查整改。

4.重大节假日、重大会议、专项检察工作重保专项值守，落实7×24小时零间断保障。

（六）应急故障处置

1.一般故障：1小时内响应并到场，2小时内处置完毕。

2.重大故障：30分钟内响应并到场，4小时内处置完毕。

3.故障处置完成后形成专项处置报告，分析原因、制定预防措施，杜绝同类问题重复发生。

（七）其他服务

1.提供现场技术指导、信息化建设咨询、网络改造方案建议、设备升级替换技术论证服务。

2.整理年度运维总结、资产盘点报告、安全合规自查报告，配合采购人完成验收及上级检查。

3.检察工作网承载非涉密业务与办公，须与涉密网、互联网物理隔离，严禁交叉、数据互通，按等保分级管理。

4.服务期间采购人要求的其他相关服务。

六、服务考核与验收要求

1.按月提交运维工作简报、工作记录，按季度提交巡检及整改报告，年末提交全年运维总结报告。

2.建立故障工单闭环管理，响应时效、故障处置率、隐患整改完成率纳入月度考核。

3.按采购需求、服务台账、故障记录、培训及重保保障情况进行考核验收，验收不合格按合同约定扣减服务费用、限期整改。

七、工作场景：检察系统工作网运维

八、其他要求

1、运维单位须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受采购人、政府和社会的监督，承担社会责任。

2、网络运营服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

3、运维单位应制定详细的内部运维管理制度、安全管理制度和操作规程。组建科学合理的运维团队，明确团队人员的岗位职责和责任义务，合规合法用工。

4、按照网络安全等级保护制度的要求，履行安全保护义务，制定防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

5、提供的网络产品应当符合相关国家标准的强制性要求，与现有设施设备匹配，不得设置恶意程序，发现安全缺陷、漏洞等风险时，应当立即采取补救措施，在规定或者当事人约定的期限内，不得终止为其提供的产品、服务持续提供安全维护。

6、运维单位须制定网络安全事件应急预案，有明确的响应、到场、处置时间和措施方案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

7、协助开展网络等保测评、安全认证、检测、风险评估等活动，配合有关部门依法实施的监督检查，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息时，应当遵守国家有关规定。

8、运维服务期间，不得从事非法活动或为非法活动提供帮助，不得侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动。

9、设置专门安全管理机构和通过安全审查的安全管理负责人；定期对从业人员、检察人员进行网络安全教育、技术培训和技能考核。

10、应当采取技术措施和其他必要措施，建立健全信息保护制度，设置专人负责对其收集的各种信息严格保密，防止信息泄露、毁损、丢失。若发生或者可能发生信息泄露、毁损、丢失时，应立即采取补救措施。

11、运营单位应当自行或者委托网络安全服务机构对其运营管理的网络安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关采购人或负责关键信息基础设施安全保护工作的部门。

12、运维单位应当建立网络信息安全投诉、举报制度，及时受理并处理有关网络信息安全的投诉和举报。

13、定期与采购人组织会议，沟通阶段服务成果及工作中存在的问题和后续的改进计划，完整记录服务过程和结果。