

政府采购项目 采购需求

项目名称：平顶山尼龙新材料开发区管理委员会电子政务外网暨办公业务资源网系统购买服务

采购单位：平顶山尼龙新材料开发区管理委员会

编制单位：平顶山尼龙新材料开发区管理委员会

编制时间：2026年6月17日

编制说明

一、采购单位可以自行组织编制采购需求，也可以委托采购代理机构或者其他第三方机构编制。

二、编制的采购需求应当符合《财政部关于印发政府采购需求管理办法的通知》（财库〔2021〕22号）要求及政府采购的相关规定。

三、斜体字部分属于提醒内容，编制时应删除。

四、对不适用的内容应删除，并调整相应序号。

一、需求清单

（一）项目概况

采购内容：采购主要包括政务外网机房环境使用服务、政务外网通信中心网络和安全服务、政府门户网站群系统服务、平顶山尼龙新材料开发区管委会电子政务外网运维服务、办公业务资源网机房环境及使用服务、办公业务资源网通信中心网络和安全服务、办公业务资源网业务应用系统平台使用服务、平顶山尼龙新材料开发区管委会办公业务资源网运维服务、平顶山尼龙新材料开发区管委会政府门户网站等级保护三级测评服务。具体内容详见竞争性磋商文件。

（二）采购项目预（概）算

总 预 算：120 万元

（三）采购标的汇总表

包号	序号	标的名称	品目 分类编码	计量 单位	数量	是否 进口
1	1	平顶山尼龙新材料开发区管理委员会电子政务外网暨办公业务资源网系统购买服务	C16080000	项	1	否

（四）技术商务要求

（1）项目概况：采购主要包括政务外网机房环境使用服务、政务外网通信中心网络和安全服务、政府门户网站群系统服务、平顶山尼龙新材料开发区管委会电子政务外网运维服务、办公业务资源网机房环境及使用服务、办公业务资源网通信中心网络和安全服务、办公业务资源网业务应用系统平台使用服务、平顶山尼龙新材料开发区管委会办公业务资源网运维服务、平顶山尼龙新材料开发区管委会政府门户网站等级保护三级测评服

务。具体内容详见竞争性磋商文件。

三、服务清单

序号	名称	内容	服务期限
1	政务外网机房环境及设施服务和机房运维服务	提供开发区政府电子政务外网机房装修及空调、视频监控、配电系统、不间断电源系统和消防门禁系统等设施的服务，以及核心机房环境相关软硬件设施的运维服务。机房按照国家 C 类标准提供服务。	2 年
2	政务外网网络核心设施及配套网络安全设施服务和运维服务	提供政务外网基础网络、安全服务，该服务所需至少包括核心路由、核心交换、防火墙等，提供政务外网骨干核心网络运维服务。	2 年
3	平顶山尼龙新材料开发区管委会电子政务外网运维服务	提供对平顶山尼龙新材料开发区管委会电子政务外网的基础网络运维服务，保障网络的稳定运行；定期的日常运维服务，日常至少 1 月进行一次例行运维保障巡检。出现故障即时响应，2 小时内安排人员到现场处理。	2 年
4	办公业务资源网机房环境及服务	提供开发区政府办公业务资源网机房装修及空调、视频监控、配电系统、不间断电源系统和消防门禁系统等设施的服务，以及核心机房环境相关软硬件设施的运维服务。机房按照国家 C 类标准提供服务。	2 年
5	办公业务资源网核心网络接入和安全服务	办公业务资源网核心网络相关的安全服务，包含核心路由器、核心交换机、安全防火墙等。	2 年
6	平顶山尼龙新材料开发区管委会办公业务资源网运维服务	提供对平顶山尼龙新材料开发区管委会办公业务资源网的中心机房网络运维服务，保障网络的稳定运行；定期的日常运维服务，日常至少 1 月进行一次例行运维保障巡检。出现故障即时响应，2 小时内安排人员出现场处理。	2 年
7	政府政务办公云平台软硬件基础支撑服务	提供政府政务办公云平台运行所需的软硬件支撑服务，服务包括计算、存储、运行内存、数据库、中间件等软硬件基础支撑资源，其中，基础支撑软硬件要按照相关国家标准要求，符合国产化的适配要求。	2 年
8	政府政务办公云平台应用软件服务	遵照平顶山市政府政务办公云平台统一设计要求，提供功能模块服务，服务包括公文流转审批和签发、阅办文的传阅签批、内部考勤、用车申请等流程审阅和签批等功能。并与市政府政务办公云平台完成对接，保障与政府公文的在线签批和流转。	2 年
9	政府政务办公云平台移动办公服务	遵照平顶山市政府政务办公云平台统一设计要求，保障移动端与电脑端的协同办公数据一致，服务包含移动端 OA 个人办公的工作桌面、消息推送、待办事宜处理、协同 OA 信息查看、日程提醒、移动签到，支持图片、语音、位置上传等功能。	2 年

10	政府政务办公云平台电子签章系统服务	遵照平顶山市政府政务办公云平台统一设计要求,满足印章加密体系要求,实现与市级电子印章加密体系的认证和对接,实现电子印章的制作、保存、查询和统计等功能,使用高强度加密算法或国家机要管理单位认可的硬件加密设备对印章进行加密。服务包括对印章进行制作和发放,对印章进行日常维护和更新,保证印章的数据安全。	2 年
11	政府政务办公云平台短信平台服务	遵照平顶山市政府政务办公云平台统一设计要求,提供符合政务办公流程的短信中心,实现各类办公流程的短信提醒以及通知提醒,会议通知时的短信回复和综合分析统计的短信平台服务。	2 年
12	政府门户网站群系统服务	平顶山尼龙新材料开发区管委会政府门户网站群服务、政府门户网站群系统符合国办新要求网站检测改版要求。	2 年
13	平顶山尼龙新材料开发区管委会政府门户网站等级保护三级测评服务	按照《网络安全等级保护条例》要求,对平顶山尼龙新材料开发区管委会政府门户网站系统进行等级保护三级测评,并将取得相关部门的备案证书。	2 年

技术参数要求

序号	服务名称	服务要求
1	政务外网网络核心设施及配套网络安全设施服务和运维服务	提供政务外网基础网络、安全服务，该服务所需至少包括核心路由、核心交换、防火墙等，提供政务外网骨干网核心网络运维服务。
		一、不少于 1 台核心路由器
		至少配置双主控、双电源、≥8 口千兆电口、≥8 口千兆光口
		支持路由引擎、业务板卡完全物理分离。
		采用全分布式转发处理架构，业务槽位支持子母卡分离设计。
		支持交换容量≥35.84Gbps。
		支持包转发率≥6000Mpps。
		整机业务插槽数量≥2 个（不含路由引擎、业务子卡插槽）。
		支持并配置内置的交流/直流电源模块，支持 N+1 冗余。
		支持路由引擎、业务载板/模块、电源/风扇等关键部件的高可用性热插拔设计。
		要求路由引擎（主控板）外置提供 USB Console 接口、AUX 口、管理口及 SD 卡插槽。
		支持高速同步串口、E1/CE1、FE、GE、10GE、155M/622M/2.5G POS、CPOS、155MATM 等广域网接口。
		支持并实配支持不少于 200 万条 NAT 功能。
		全部业务板卡支持并实配 Netflow（如 Netstream、IPFIX 等）功能。
		支持并实配支持 L2TP、IPSec VPN、GRE VPN 功能。
		支持并实配防火墙功能，可提供状态检测、URL 过滤等多种安全特性。
		支持并配置广域网传输优化技术
		支持并配置静态路由、等价路由、策略路由；支持并可配置 RIPv1/v2、BGPv4、BGP4+等路由协议。
		支持并配置 MPLS VPN。
		支持并配置 Telnet、SSH 管理模式；支持并配置 CLI、SNMP v1/v2/v3、RMON 1/2/3/9；支持并配置 Syslog 日志功能。
		二、不少于 1 台核心交换机
		74.18Tbps/295.41Tbps
		8,400Mpps/72,000Mpps
		至少配置双主控、双电源、≥48 口千兆电口
		支持增强以太网特性（DCB）：
		802.1Qbb: Priority-based Flow Control (PFC)，基于优先级的流控。
		802.1Qaz: Enhanced Transmission Selection (ETS and DCBX)，增强传输选择
		802.1Qau: Congestion Notification (CN/QCN)，拥塞通告
		支持统一交换特性：FCoE（Fibre Channel over Ethernet）
		支持 VXLAN 二层网桥
		支持 VXLAN 三层网关
		支持 VSU3.0(Virtual Switch Unit, 虚拟交换单元)
		支持虚拟化带宽≥2.56Tbps
		支持 VSD(Virtual Switch Device, 虚拟交换设备)
		支持纵向虚拟化
		支持 TRILL 透明交换网络

	支持 L2GRE
	支持 VEPA（虚拟以太网端口聚合）
	支持虚拟机策略自动迁移
	支持 OpenFlow 1.3
	支持 Jumbo Frame
	支持 802.1Q
	支持 STP、RSTP、MSTP
	支持 Super VLAN
	支持 GVRP
	支持 QinQ、灵活 QinQ、QinQ 终结
	支持 LLDP
	支持 ERPS（G.8032）
	支持静态路由、RIP、OSPF、IS-IS、BGP4
	支持 VRRP
	支持等价路由
	支持策略路由
	支持 GRE 隧道
	支持静态路由 OSPFv3、BGP4+、IS-ISv6、MLDv1/v2
	支持 VRRPv3
	支持等价路由
	支持策略路由
	支持手工隧道、自动隧道、ISATAP 隧道、IPv4 over IPv6，支持 GRE 等隧道技术
	支持 IGMP v1, v2, v3
	支持 IGMP Snooping
	支持 IGMP Proxy
	支持 PIM-DM、PIM-SM、PIM-SSM 等组播路由协议
	支持 MLD
	支持 MLD Proxy
	支持组播静态路由
	支持 MPLS 转发
	支持 MPLS MIB(RFC1273, 4265, 4382)
	支持跨域 OPTION A/B/C 三种模式
	支持 MPLS VPN/VPLS
	支持 VPWS
	支持标准、扩展、专家级 ACL
	支持 ACL 80
	支持 IPv6 ACL
	支持 802.1p
	支持 SP、WRR、DRR、SP+WRR、SP+DRR 等队列调度机制
	支持 RED/WRED
	支持基于出端口/入端口的限速
	支持 HqoS
	每端口 8 个优先级队列

	独立的交换网板与独立的主控板设计，实现转发与控制平面完全分离
	主控板支持 1+1 冗余备份
	交换网板支持 N+1 冗余备份
	电源、风扇支持 N+M 冗余备份
	背板无源设计，避免单点故障
	各组件支持热插拔
	支持热补丁功能，可在线进行补丁升级
	支持 ISSU
	支持 GR for OSPF/IS-IS/BGP
	支持 BFD for VRRP/OSPF/BGP4/ISIS/ISISv6/MPLS/静态路由等
	支持 NFPP（基础安全保护策略）
	支持 CPP（CPU 保护）
	支持 DAI，端口安全，IP Source Guard
	支持 802.1x/Portal/Mac 等多种认证方式
	支持 RADIUS 和 TACACS+ 用户登录认证
	支持 uRPF
	支持登录认证、口令安全
	支持未知组播不送 CPU、支持未知单播抑制
	支持 SSHv2，为用户登录提供安全加密通道
	支持 Console/AUX Modem/Telnet/SSH2.0 命令行配置
	支持 FTP、TFTP、Xmodem、SFTP 文件上下下载管理
	支持 SNMP V1/V2c/V3
	支持 RMON
	支持 NTP 时钟
	支持故障后报警和自恢复
	支持系统工作日志
	支持 IPFIX 流量分析
	三、不少于 1 台出口防火墙
	2 个千兆 Combo 接口（光电复用），10 个千兆电接口，2 个千兆光接口，1U 高度，2G 内存，19 寸机箱，标配 500G 硬盘 配置三年防病毒、防攻击、上网行为管理、Web 安全防护等增强特性授权；
	网络层吞吐量≥1Gbps，最大并发连接数≥130 万；
	支持多种控制策略的匹配条件配置，支持用户、接口、源地址/区域、目的地址/区域、源目的地理、应用、服务、终端类型等维度；
	支持一体化控制策略的配置，在一条策略中，可开启入侵防御、病毒防护、URL 过滤、应用控制、邮件控制、web 关键字、虚拟账号、文件类型过滤、协议过滤、终端公告提醒等 10 余种策略；
	系统定义超过 8500+条主流攻击规则，包含 Backdoor、bufferoverflow、dosddos、im、p2p、vulnerability、scan、webcgi、worm、game，入侵防御特征库 BPS 检出率为 85% 以上；
	支持自定义 IPS 特征，支持针对 8 种协议自定义入侵攻击特征，包括 IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP 等协议；可拓展协议字段，设置数据包中的匹配内容；支持选择包含、等于、不等于、大于、正则匹配等匹配方式；可选择多种匹配条件，支持设置“与”

	和“或”的匹配顺序；
	支持网络黑名单,支持 IP/域名/MAC 匹配,支持匹配 HTTP 协议报文中的 X-Forwarded-For 字段内的 IP 地址；
	支持 HTTP, FTP, POP3, SMTP, IMAP 协议的病毒查杀；支持 ZIP、TAR 等压缩打包文件的病毒查杀,压缩最大支持 20 层；（需提供带有系统登录地址的功能页面截图）
	支持 HTTP 协议的精确访问控制,可针对 IP、URL、Method、Referer、User-Agent、Cookie、Url-args 等字段设置内容,匹配内容包括但不限于：包括、不包含、等于、不等于、属于、不属于、长度小于、长度等于、长度大于、正则匹配等；日志级别包括但不限于：不记录、危急、告警、严重、错误、警告、通知、信息等；
	支持针对 IP、端口进行端口扫描,可选择立即执行或定期执行；支持呈现扫描结果,包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息,支持导出功能；（需提供带有系统登录地址的功能页面截图）
	支持展示风险级别、IP、用户、部门、风险级别、操作系统、重要程度、受攻击总数、风险来源等内容；
	支持数据下钻至单资产风险详情,可自动关联该资产所有安全信息,安全信息包括但不限于：入侵防御、威胁情报、WEB 防护、病毒防护、防暴力破解、非法外联防护、弱密码防护、扫描攻击防御和行为模型等,支持以趋势图方式按时间展示各类安全事件的趋势,方便管理员快速了解资产安全状况,以便进行准确的进行安全防护；
	支持终端准入管理功能；检测规则包括杀检查规则、登录域检查规则、操作系统规则、进程检查规则、文件规则、注册表规则、补丁检测规则、Windows 账号规则、防篡改检查规则、软件检查规则、外联检查规则等；管控规格包括计划任务、外联控制、外设管控、端口管控等；
	支持 802.1x 认证,可对接本地和 AD 域用户源进行用户名密码认证,实现内网强管控；
	支持 MySQL、PostgreSQL、Oracle、Informix、SQL Server、Sybase、DB2 等多种数据库审计,包括：SQL 语句操作内容、SQL 会话起始时间等；
	支持故障监控,可通过系统执行单用户检测、网络故障排查、解密策略故障排查、用户认证故障排查、WEB 访问质量监控等操作,提高故障排查效率；（需提供带有系统登录地址的功能页面截图）
	产品需有国内软著；具有由公安部颁发的《计算机信息系统安全专用产品销售许可证》或安全检测证书；
	产品具备 IPv6 Ready Logo 认证
	四、不少于 1 个上网行为管理功能
	支持非法外联学习和防护特性,可有效保障服务器安全,可定义外联白名单地址和端口；支持通过流量自学习能获得服务器合法的外联行为,检测流量中的异常访问流量,可以自动拦截。学习时长可选择 1 小时、12 小时、一天、一周等；
	应用特征数不少于 7000 个,规则数不少于 13000,移动应用不少于 2000 个；
	支持 vpn 翻墙应用检测,可自定义检测宽松度,可识别常见如 SOCKS5、WEB 代理、红杏出园、自由门、无界浏览等 120 种以上 vpn 应用；（需提供带有系统登录地址的功能页面截图）

	支持终端准入管理功能；检测规则包括杀检查规则、登录域检查规则、操作系统规则、进程检查规则、文件规则、注册表规则、补丁检测规则、Windows 账号规则、防篡改检查规则、软件检查规则、外联检查规则等；管控规格包括计划任务、外联控制、外设管控、端口管控等；
	支持 802.1x 认证，可对接本地和 AD 域用户源进行用户名密码认证，实现内网强管控；
	支持防翻墙检测，支持识别网络代理应用不少于 180 中；翻墙行为分析代理服务器所属地域分布、代理服务器所属地域排名、翻墙用户排名、翻墙用户组排名、翻墙应用排名，详细展示出源地址、用户、用户组、代理应用、风险级别、翻墙次数、时间、操作等信息；
	五、不少于 1 个网络负载均衡功能
	支持 7 元组的链路负载均衡策略，负载均衡接口支持接口和接口组，支持基于域名进行链路负载，负载算法包括但不限于优先级和权重等；
	六、不少于 1 台 VPN 防火墙
	系统应采用标准机架式设备，而非插卡式设备，不需要业务卡即可实现下一代防火墙业务；
	为保证防火墙运行的稳定性和处理能力，要求设备采用非 X86 架构对各项安全功能进行加速优化处理；
	系统具有良好的可扩展性，能够扩展支持病毒防御、入侵防御、应用识别、垃圾邮件过滤、文件防泄漏、上网行为管理、APT 防御、僵尸主机检测、IPSEC VPN 与 SSL VPN 等功能；
	要求固化千兆电口数量 ≥ 10 个；为保障接口稳定性，所投产品必须是固化接口，而非板卡接口。
	三层网络吞吐 $\geq 2\text{Gbps}$ ，IPS 吞吐量 $\geq 500\text{Mbps}$ ，最大并发连接 ≥ 100 万，最大新建连接 ≥ 10000 ；
	IPSEC VPN 隧道数 ≥ 200 ，设备本身要求自带 200 个 IPSec VPN 授权；SSL VPN 并发用户数 ≥ 100 ，设备本身要求自带 100 个 SSL VPN 授权；
	支持路由模式、透明（网桥模式）、混合模式；
	要求支持虚拟防火墙，支持同一个网口用于多个虚拟防火墙支持虚拟系统技术，且每个虚拟防火墙独立管理
	为保障不同业务不同安全策略，要求支持单独为每个虚拟防火墙设置会话数、策略数、用户数、IPSECVPN 隧道数、硬盘空间使用量等，进行按需分配
	支持 SD-WAN 功能，支持基于用户、用户组的 SD-WAN 策略，包括带宽质量监控、链路优化、一键配置上线等
	支持主-备和主-主 HA 方案。双机热备要能支持多种组网形式，确保可靠性，并且数据接口和心跳线支持冗余，支持双机会话同步，实现无感知切换
	支持策略路由、组播路由、静态路由、BGP、RIP、RIPNG、OSPF、OSPFv3、ISIS、ISISv6 等动态路由协议（非透传）；
	支持 802.1Q Trunk，支持不同 VLAN 之间的数据隔离。
	内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户/用户组、应用、URL 类型、接入类型、地理位置、终端类型、设备组、服务、时间、安全引擎（入侵、URL 过滤、病毒过滤、垃圾邮件过滤、SSL 代理）的识别与控制
	支持服务器的负载均衡，提供加权轮询、最小连接数、最小 RTT 等多种负载均衡方式

	支持 SYN Flood、UDP Flood、ICMP Flood、LAND 攻击、Smurf 攻击、Fraggle 攻击、Winnuke 等攻击防护；具备硬件 TCP SYN FLOOD 防护加速能力
	支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换
	为解决公网 IP 地址资源问题，支持 NAT 的端口扩展技术，实现单个公网 IP 的无限地址转换。
	可自动检测互联设备及连接终端信息，自动生成逻辑拓扑，并基于拓扑展示终端指纹信息和网络连接信息
	为保障语音系统效果，支持 VoIP 防护，可基于 SIP 与 SCCP 协议防护，可限制 SIP 的注册请求，可限制 SCCP 的呼叫建立
	支持对 HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、MSSQL、ORACLE、NNTP、DHCP、LDAP、VoIP、NETBIOS、TFTP、SUNRPC 和 MSRPC 等常用协议及应用的攻击检测和防御
	支持旁路和在线两种模式
	支持自定义 IPS 特征
	具备 12000 种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、严重程度、特征名称、应用类型等方式的查询。
	支持对 HTTP、FTP、SMTP、POP3、IMAP 协议的应用进行病毒扫描和过滤
	支持深达 10 级以上的文件压缩。可以限制过滤文件的大小，对超大文件采取“通过”或“阻止”动作。
	支持对 VPN 传输隧道内容进行病毒过滤；
	支持 IPsec VPN、SSL VPN、L2TP VPN、GRE VPN、L2TP over IPsec VPN、GRE over IPsec VPN 等 VPN 组网
	IPSEC VPN 支持阶段二下的 DH 组的密钥交换方式，支持 DH group 21、27、28、29、30、31 的类型
	IPsec 隧道支持多 CA 数字证书导入功能，同一台主机建立多个 IPsec 隧道时，支持不同的隧道导入不同的 CA 数字证书
	支持对登录 SSL VPN 的用户端系统进行端点安全检查
	支持完备的 IPv6 的 IPsec 能力，包括 Site-to-site、远程接入 VPN 和动态 DNS 的 IPv6 接入方式，IPv6 下的 Aggressive 协商模式。
	七、不少于 1 台政务外网 NAT 防火墙
	下一代防火墙。含基本网络防火墙功能、访问控制、入侵防御、病毒防护、用户认证、负载均衡、流量控制、资产识别、IPsec VPN，SSL VPN 等功能。
	八、不少于 1 台堡垒机
	1、纳管全网 IT 资产，统一运维入口，阻断资产直连访问。
	2、精细化身份权限分级管控功能，分级管控人员权限，托管账号密码，防范越权非法访问。
	3、全流程运维行为审计溯源功能，全链路运维留痕，日志防篡改，支持安全事件溯源取证。
	4、生成合规审计报告，自动化运维，闭环工单审批流程。
	九、不少于 1 个日志审计
	1、异构设备全域日志采集，兼容全网设备日志接入，多协议采集各类系统运行日志。
	2、日志标准化存储管理，统一格式化日志数据，大容量存储，日志防篡改防删除。

	3、安全威胁智能分析告警，联动规则研判异常行为，实时告警内网攻击违规行为。
	4、安全事件溯源关联分析，多维关联研判日志，快速定位攻击链路，支撑事件溯源取证。
	5、合规审计报表自动输出，适配等保审计标准，一键生成台账报表，满足监管核查需求。
	十、不少于 1 套服务器安全软件
	提供 5 个服务器防病毒授权。
	身份认证：用户管理、机构管理、用户组管理、认证策略、认证方式、密码策略；
	访问控制：web 应用、服务器资源、资源组、设备信任列表、设备黑名单；
	可信应管理：终端应用自动采集、可信应用黑白名单设置；
	终端检测：防泄露水印；
	系统管理功能：服务监控、角色权限、网络配置、存储管理、logo 设置、日志外发；系统监控、故障诊断；
	终端兼容列表：支持 Windows 7/8/10、；MacOS 10 及以上版本；Linux ubuntu 20；Android 5.0 及以上版本；IOS 10.0 及以上版本；
	部署方式：支持单机部署
	提供自主知识产权的防病毒引擎；
	对于恶意文件处理措施至少支持三种以上，包括厂家推荐措施、统一处理措施、以及针对不同类型病毒/恶意软件提供不同处理措施，同时不同病毒/恶意软件类型不少于 5 种分类；
	具备机器学习能力；
	具备爆发阻止功能，管理端可配置爆发阻止策略，封堵共享目录；
	支持指定单个或多个客户端做为更新代理，并可指定某特定 IP 地址段的客户端从其他客户端获取更新；
	十一、不少于 1 台安全域管理网关
	符合电子政务外网的标准体系，满足相关协议和认证的要求，实现跨域切换和认证服务。实现电子政务外网分时分域访问的规划设计，实现网络鉴权的准入控制和安全访问控制。
	十二、不少于 1 套网络管理软件
	本项目提供 10 个设备使用授权
	B/S 架构，无需安装客户端，
	全中文图形化界面，支持 Windows 平台，采用 C/S 架构同时支持 B/S 应用模式。
	系统应具备自身监控功能，能够监控自身服务、组件的可用性、端口、连续运行时间、JVM 线程数、分配内存量、使用内存量，当有故障时，能够及时告警。
	业务系统的可用性、健康度、繁忙度等关键指标支持自定义计算规则，可通过与、或、优先级、权重等计算规则灵活定义。
	为更方便扩展未来资源管理的需求，系统应提供调用外部脚本监控的方式对监控对象进行个性化指标采集。调用外部脚本的方式指通过远程执行方式定时调度脚本，获取执行结果
	系统应站在业务管理的角度管理 IT 资源，能够根据业务系统所关联的物理资源、权重和关联资源之间的关联关系等进行业务建模，支持业务拓扑视图，当业务系统所关联的资源出现异常时，应能够高亮显示资源告警及故障的传递关系。
	为了减轻系统运维人员的重复工作，系统应提供设备自动巡检功能。1、巡检内容包括服务器、网络设备、应用、无线、虚拟化、存储、机房环境等所有管理对象。2、巡检应支持自定义多个巡检任务面向不同的管理对象，设定巡检时间。巡检结束后应生成巡检报告以邮件方式发送给运维人员。

		数据中心机房是信息化最为关键的场所，3D 可视化是扩展运维范围及效率的重要手段，场景会随着业务的需要而进行变更及维护，所以 3D 场景需具备灵活的可维护编辑特性。
		支持无需定制及二次开发，即可创建建筑内部的户型结构，支持对墙、门、柱、窗、办公家具、文字、机柜、动力、环境、安防等 3D 模型的拖拽和编辑；2、支持设计图可直接导入 3D 仿真机房进行呈现，导入的机柜和动力、环境、安防 3D 模型可关联机房动环数据指标，并在 3D 机房中呈现告警和数据指标值。
		因管理对象厂商众多、软硬件型号众多，运维管理系统要求支持多厂商多类型的综合管理。包括主流的网络设备、安全设备、无线设备、服务器、虚拟化资源、存储设备、应用、机房环境等。
		系统自动呈现网络的真实拓扑图，支持三层网络拓扑、二层物理拓扑、VLAN 子网拓扑等不同的呈现方式，通过不同的拓扑多角度管理网络。
		实现普通用户通过自助的方式发起服务申请和故障报修，并能够跟进请求的处理进度。1、支持微信的方式在线提交服务请求和故障报修。2、为让用户能快速识别所需要申请的服务类型，系统支持平铺卡片方式显现服务类型，卡片内容包括服务名称、服务简介及自定义的图标，各种服务类型支持收藏功能，方便用户快速使用常见服务。3、支持对已提交工单的评论功能，可以实时对已提交工单补充信息并发布自己的意见。
		为从宏观和整体角度掌握所有 IT 系统的运行情况，系统应提供 IT 整体健康指数的量化指标，使运维部门的管理人员清晰了解当前整体 IT 系统的好坏，以及 IT 整体健康情况的历史走势。通过分析 IT 整体健康指数了解其影响因素是哪些业务系统。
		系统自运维管理
		系统应具备足够的稳定性，必须具备自监控和异常通知的能力：自熔断，针对本地代理方式，当代理占用操作系统资源超过一定配额后，自动将自身占用高的进程进行熔断处理，提供证明截图。
		为了能实时分析用户访问应用的真实体验情况，系统应能具备采集网络中的流量
		1、可实时捕获并保存网络中的全量通讯数据包并以专用格式存储，原始数据包与统计数据分别存储互不干扰。能够根据原始数据包进行体验指标的统计，支持 1 分钟精度的汇总统计，并可汇总为 30 分钟、1 小时的颗粒度的统计数据。支持调整原始数据包存储和统计数据的存储周期。
		2、支持数据包采集过滤器配置，IP 地址范围、MAC 地址、VLAN、MPLS VPN、VxLAN 设置过滤条件等多种条件对流量进行精细化过滤。需提供系统功能截图。
		为了支撑告警的规则灵活性，适用于不同的故障场景，系统应能支持基于函数的方式定义产生和恢复条件，需能提供以下方式：
		1、系统应能支持判断指标返回值符合阈值的次数；
		2、系统应能支持判断指标连续返回值符合阈值；
		3、系统应能支持判断指标最后一次返回值符合阈值；
		4、系统应能支持判断最后一次值与上一次值是否相同；
		5、系统应能支持判断指标环比增长率(值)、下降率(值)符合阈值的次数；
		6、根据所选用的指标返回值类型，函数中的阈值判断的运算符应能包含但不限于：“>、<、>=、<=、!=、包含、in、区间 (>X 且 <Y) ”等。需提供系统截图。
		十三、不少于 1 台运维服务器
		2 颗 CPU 主频≥2.0GHz 内存≥128 3 块 4T 硬盘 冗余电源
2	办公业务资源网核心网络接	一、不少于 1 台核心交换机
		配置≥24 个电口，实现终端数据二层转发，具备 VLAN 划分、端口隔离、链路聚合功能，支持环路检测与端口安全，保障局域网稳定传输。

入和安全 服务	二、不少于 1 台核心路由器
	配置三层口数量 ≥ 4 ，至少包含 2 个 Combo 光电复用接口
	配置二层千兆以太网电口数 ≥ 24 个
	转发性能 $\geq 3\text{Mpps}$
	内存 $\geq 1\text{GB}$ ，Flash $\geq 256\text{MB}$
	支持冗余电源模块（非 RPS 电源）
	冗余电源支持热插拔（模块化）
	无风扇设计
	可用扩展模块插槽 ≥ 4 个（非 SFP 模块插槽），可扩展 TDD/FDDLTE 全制式 4G 模块，E1/CE1 模块、同步/异步串口模块等
	配置 USB 接口 ≥ 1 可用于零配置上线，SD 卡接口 ≥ 1 ，多功能复 FUNC 键，为便于设备管理，便于紧急情况下的设备状态恢复，需提供主机图片。
	支持静态路由、RIPv1/v2、OSPF、BGP4 等路由协议
	支持 IGMP、PIM-SM、PIM-DM、DVMRP 等组播协议
	支持状态防火墙功能
	支持并内置 MPLSVPN、IPv6 等组网功能
	支持 web 管理界面、TR-069 网管协议、SNMPv1/v2c/v3 网管协议
	三、不少于 1 台防火墙
	为保证防火墙运行的稳定性和处理能力，要求设备采用非 X86 架构对各项安全功能进行加速优化处理。
	要求固化千兆电口数量 ≥ 10 个；为保障接口稳定性，所投产品必须是固化接口，而非板卡接口。
	设备最大吞吐量 $\geq 2\text{Gbps}$ ； 设备最大 IPS 吞吐量 $\geq 500\text{Mbps}$ ； 最大并发连接数 ≥ 100 万； 每秒新建连接数 ≥ 10000 ； IPSEC VPN 吞吐量 $\geq 2\text{Gbps}$ ； IPSEC VPN 隧道数 ≥ 500 ，设备本身要求自带 500 个 VPN 授权； SSL VPN 并发用户数 ≥ 100 ，设备本身要求自带 100 个 VPN 授权；
	支持路由模式、透明（网桥模式）、混合模式
	要求支持虚拟防火墙，且每个虚拟防火墙独立管理；
	为保障不同业务不同安全策略，要求支持每个虚拟防火墙能进行路由表、策略、VPN 等设置；能够在虚拟系统中应用所有安全特性。
	支持不同虚拟防火墙之间数据路由和透明转发模式；
	支持等值路由（ECMP），并支持链路权重设置。
	支持主-备和主-主 HA 方案。双机热备要能支持多种组网形式，确保可靠性，并且数据接口和心跳线支持冗余。
	支持策略路由、组播路由、静态路由、RIP(v1/v2)、OSPF、BGP、IS-IS 等；
	支持 802.1Q Trunk，支持不同 VLAN 之间的数据隔离。
	支持状态检测、包过滤、深度应用层检测；
	支持 SYN Flood、UDP Flood、ICMP Flood、LAND 攻击、Smurf 攻击、Fraggle 攻击、Winnuke 等攻击防护；
	策略具备接口、地址、服务、时间、用户、带宽等的配置。

		支持基于特定源地址、目的地址、应用端口组合的会话数限制。
		支持 SSL 深度检测功能
		为保障语音系统效果，支持 VoIP 防护，可基于 SIP 与 SCCP 协议防护，可限制 SIP 的注册请求，可限制 SCCP 的呼叫建立
		支持用户自定义攻击特征
		支持对特定文件类型阻断；
		入侵检测特征库≥5000 种
		支持 HTTP、FTP、IMAP、POP3、SMTP、IM、HTTPS、IMAPS、POP3S、SMTPS 协议病毒过滤
		支持深达 10 级以上的文件压缩。可以限制过滤文件的大小，对超大文件采取“通过”或“阻止”动作。
		支持对 VPN 传输隧道内容进行病毒过滤；
		支持基于代理模式、流模式的垃圾邮件检测过滤
		防垃圾邮件功能支持 IP 地址过滤、邮件地址过滤、MIME 头信息、邮件内容过滤、RBL 实时黑名单、域名解析等多种方法。
		支持防数据泄漏功能，能对 HTTP、FTP、SMTP、POP3 等协议中的敏感内容进行过滤和阻断。
		要求支持文件指纹识别、文件水印检测，要求提供功能截图。
		要求对 HTTP 信息进行保护，HTTP 可检测 GET/POST、html 头、URL、CGI、Cookie、内容和用户等
		支持 Web 分类和 Web 页面过滤，要求 URL 数量≥2.5 亿个
		要求支持 URL 地址/域名黑白名单，并支持基于代理模式、流模式、DNS 模式的 URL 过滤
		能对 HTTP 对象进行控制，包括阻断 Java Applet，Cookies，Active X 等
		应用程序列表数量大于 2900 种；
		支持基于应用防御、入侵防御、恶意软件防御的统计结果定义用户的信誉值
		支持僵尸主机、C&C 客户端检测功能
		支持 0-day 恶意软件变种、可疑文件等 APT 高级可持续威胁的统计功能，要求提供功能截图。
		为了支持业务扩展，要求支持 IPv4/IPv6 双栈
		为更好的支持 IPv6 业务，要求支持基于 IPv6 的策略设置、内容过滤、IPS 检测、代理、流控和 VPN 功能
3	政府政务办公云平台软硬件基础支撑服务	提供政府政务办公云平台运行所需的软硬件支撑服务，服务包括计算、存储、运行内存、数据库、中间件等软硬件基础支撑资源，其中，基础支撑软硬件要按照相关国家标准要求，符合国产化的适配要求。
4	政府政务办公云平台应用软件开发服务	遵照平顶山市政府政务办公云平台统一设计要求，提供功能模块服务，服务包括公文流转审批和签发、阅办文的传阅签批、内部考勤、用车申请等流程审阅和签批等功能。并与市政府政务办公云平台完成对接，保障与政府公文的在线签批和流转。 1. 政务办公云平台是完全依托全市办公业务资源网和政务办公统一技术平台标准而设计和开发的，满足各类政务办公需要，实现政务办公的信息化和自动化，提升政务办公效率，降低政务办公成本。

	2. 其主要功能和各子业务系统有：公文审批系统、公文交换系统、阅办文签批系统、请假审批系统、公车管理系统、出差申请管理系统、会议通知系统、人事管理系统、督察督办系统、信息采编系统、电子邮件系统等政务办公所需的各类业务子系统。平台支持领导手写签名，原笔迹签批，任务交办以及全流程进度监控等功能。
	4. 根据平顶山市政府关于政务办公平台国产化适配的相关要求，办公业务资源网中一体化政务协同办公平台须适配国产服务器，同时支持国产化和非国产化的终端设备，平台支持银河麒麟等各类国产化服务器操作系统和各类国产化和非国产化终端操作系统，适配支持国产化中间件和国产化数据库以及办公软件等，系统功能以及相关组件均兼容国产化的建设要求，且通过国家相关适配认可证书，能确保通过市政府政务办公统一技术平台对接时的标准验收，实现与市级政务办公统一技术平台的无缝对接。
	5. 可实现与市政务办公云平台的无缝对接，可实现与各县区以及市直各接入单位的流程对接，实现市直各单位与县区垂直和管理单位的文件等传送，实现公文报送以及公文签收等业务协同办公。
	6. 在政务办公平台基础上部署移动办公平台软件模块，提供独立 APP，支持主流的安卓和 IOS 操作系统，提供最核心的服务帮助领导抓住零碎时间，充分满足其随时随地办公的需求。手机移动办公系统界面采用宫格式的界面风格、操作便捷简洁、提示明确，几乎不用培训就能上手。手机移动办公支持收发及时消息，审批流程、门户信息阅读，写工作日记、阅读员工日记，布置任务、汇报任务，安排日程、查看日程等日常移动办公业务。
	7. 政务协同办公系统是通过信息技术、网络以及电子通讯等高科技手段，对各类办公中所形成的信息进行数字化，通过网络环境，实现各类信息有机整合与信息分布式共享，使工作人员可以通过各种办公工具（PC 机、手机、Pad 等相应的工具）进行办公。达到简化业务流程，随时随地处理业务，加快业务处理过程，提高办公效率的目的。
	8. 统一工作门户系统政务门户，根据信息内容不同可以分栏目发布，通常栏目有政府动态，内部信息，内部刊物，报刊杂志，政策法规，资料文档，党、团、工会工作，党办、团委、工会的工作信息可在内部网上发布。资料检索个人门户即我的办公页面，个人门户主要的办公组件有：登录入口，快捷工作，通知通告，待办工作，已办工作，日程安排，政策法规，内部论坛，综合查询。
	9. 全文检索，系统应提供了以下的检索功能：
	支持字、词、长句子的混合检索。
	中英文(全角/半角)混合检索、英文和数字的混合检索。
	布尔查询。具有多个检索词逻辑运算（与、或、非、差、优先、相临、异或）功能。
	高级检索。除了向用户提供基于全文的关键词句的检索外，系统还向用户默认提供按照标题、日期、作者、分类和文章关键词的综合检索。
	渐近检索。用户可以在检索结果中检索，不断缩小检索范围，提高检索精度。
	临近检索。用户即使无法回忆起整个句子，也可通过相邻或者相近关键词的查询查找到准确的结果。
	模糊查询。支持使用通配符“*”的模糊匹配查询，并支持“?”号的单字符匹配查询。
	强大的检索功能
	在数据量较大时支持多库并行检索技术，以提高检索和数据加载速度。
	支持对 MS OFFICE 文档（Word/Excel/Powerpoint）和 PDF 文件自动建立索引，不需加工。支持 Native-XML 全息索引。
	内嵌汉语自动分词系统，支持按词索引、按字索引、按关键词索引等多种索引策略。
	检索系统核心支持 GB2312/GBK/GB18030，BIG5 和 UTF8，可支持多语言的检索。

		提供词典维护功能，可以设定和维护行业专用的词典，实现行业专业检索。
		全文检索应具有较高的安全性，支持系统级、数据库级、记录级和字段级四级安全控制机制，支持数据库远程镜像功能。
		检索系统支持集群架构的检索结构部署，可以随着系统数据量的增长平滑扩展系统检索能力。
		10. 即时通讯将系统中的人员组织信息同步到即时通讯工具；也可以实现在即时通讯工具传送文件并存储到文档库；待办流程推送到即时通讯工具，建立为相关人员提供在线沟通平台。应用人员可以以消息方式通知下一环节协作人员，协作人员可以在信息门户上以消息对话框方式接收到消息通知，能够实现资料的简便、快捷、有序地传输。
		11. 用户系统管理和设置，通过简单的方式即可实现政务办公平台个人登录页面的系统配置，个人系统管理主要功能包含：密码设置、用户组管理、主题管理、常用批注管理、工作流提醒及显示设置等等，
		政务协同办公系统个人办公模块作为日常办公的首页，整合用户日常办公所涉及的主要操作模块和信息，包括日程安排、待办公文、任务安排、消息提醒、通知等等。
		12. 公文主要是发文、收文、签报、请示等。不同的公文类型，流程表单格式、公文样式管理要求都不同。一个发文，发文单主要由表头、表单、正文、附件组成。最后形成发文单要实现国家规范的发文文件，要把表头、表单中的内容加入正文，最终形成一定格式的发文文件。所以在通过协同政务办公平台系统来实现发文管理的时候需要可以灵活自定义公文的类型，并需要可以实现每种类型公文的格式可以对应多个自定义模板，以此达到“规范公文形式、减少纸质公文、提高公文质量”的公文管理要求。
		公文管理是以公文流转为核心，实现机关公文处理和管理的电子化。支持电子公文及纸质公文扫描件的流转管理，实现公文的电子起草、审核、会签、签发、分发、登记、拟办、批阅、传阅等工作，自动处理反馈、催办、流程跟踪与统计、查询和归档等任务。
		要求支持公文单自定义和文单模拟，收文支持 PDF、OFD 格式公文；能够实现自动对外发布功能，能够将公文单中的信息自动带入公文中。
		公文管理须实现与电子档案系统的数据集成对接；与政府信息公开系统相关栏目的数据集成对接。公文能够按年度/组织机构进行分类。
		公文管理系统要求能够对所有的红头文件及非红头文件（内部请示报告、汇报材料等）进行管理，支持加签、转办、签批、修改留痕、智能表单、流程自定义及跟踪等功能。非红头文件可以由发起人自由定义流程。
		13. 请假管理。主要半酣请假单模板预置，设计请假单并预置进系统进行管理，请假单录入管理，请假单分类管理，请假单审核管理，请假单归档管理，请假单统计分析，签到管理，签到数据对接，签到数据分析，签到数据报表。
		14. 人员外出管理是政务办公云平台中的辅助管理功能。为了便于叶县人民政府内部人员相互联系，了解人员去向，防止因人员外出而影响办文、办事，需要加强对人员外出的管理。外出管理模块具备的功能如下：一、具有查询功能。二、具有权限管理功能。三、具有统计分析功能。四、具有人员去向告示牌的功能。五、具有提醒功能。在录入人员去向时，在“发送提醒给”中选择要提醒的对象。选取“同时保存到日程安排”即可将此保存到日程中。外出信息登记信息展示
		15. 车辆管理主要包含车辆登记，用车申请，车队调度，司机管理，保养记录，车辆信息统计查询。
5	政府政务办公云平台移动办	遵照平顶山市政府政务办公云平台统一设计要求，保障移动端与电脑端的协同办公数据一致，服务包含移动端 OA 个人办公的工作桌面、消息推送、待办事宜处理、协同 OA 信息查看、日程提醒、移动签到，支持图片、语音、位置上传等功能。

	公服务	1. 根据市政府对办公业务资源网的技术规范要求，实现统一的政务文件的数据交换，依托市级统一移动办公总出口和整体解决方案标准，实现我县统一的移动办公出口管控，数据与政务办公云平台保持时时同步，解决政务办公时间及空间上工作处理困难的问题，实现随时随地办公。
		2. 移动办公平台与政务办公云平台无缝集成，同时满足和符合国产化的各项要求，终端客户端支持平板、手机等移动办公，支持独立的客户端，同时适配鸿蒙操作系统，适配和支持安卓系统等。
		3. 平台功能支持移动办公的高安全标准设置，支持终端的硬件序列号锁码、手机号绑定、以及账号和硬件设备的一体化设定、颗粒级的权限控制等综合性安全管控，实现与核心区安全设备的联动监测和提醒，保证移动办公的高度安全。
		4. 平台集成了服务级别的在线转码技术，实现国产化格式 OFD 以及其他版式文件和流式文件在线转码阅办，无需移动终端设备安装其他三方客户端，依托市级转码服务器和转码要求，直接在线转码查看文件，无需下载，确保政务办公数据的安全以及隐私保护。
		5. 在政务办公平台基础上部署移动办公平台软件模块，提供独立 APP，支持主流的安卓和 IOS 操作系统，提供最核心的服务帮助领导抓住零碎时间，充分满足其随时随地办公的需求。手机移动办公系统界面采用宫格式的界面风格、操作便捷简洁、提示明确，易操作。手机移动办公支持收发及时消息，审批流程、门户信息阅读，写工作日记、阅读员工日记，布置任务、汇报任务，安排日程、查看日程等日常移动办公业务。
		6. 统一门户设计。以政务办公自动化平台为基础建设移动办公系统，建立应用系统用户界面的统一归口平台，该系统将应用系统中各个功能模块有机地结合在一起，形成统一的应用平台。同时根据授权规则对各账号进行功能的权限设置，实现不同权限的用户登录移动端之后看到的功能模块不等，同时实现门户自定义设置功能，无需每次更改调整都要进行移动端的升级，自动加载配置的方式实现灵活的移动终端 APP 的设置。
		7. 灵活安全的规则定制。移动办公平台可以对终端设备进行各种综合性安全验证防护，通过对移动终端设备硬件序列号以及短信、二维码登陆验证等方式实现交叉验证，提升安全性，同时为了便于使用，对终端登陆设备可以实现多台绑定机制，便于领导有多台移动终端设备。
		8. 自定义表单设计。为了后期更好的兼容性，表单设计和制作支持对 HTML5 模式，同时表单设计支持灵活的处理笺设计，设计操作简单，支持常用的 Word 导入导出，同时设计的效果运行在不同终端和打印表单都可以达到理想的控制的样式和兼容效果，便于灵活设计移动终端与传统 PC 端对于表单的设计制作。
		9. 协同办公数据同步：待办事宜 与协同办公数据同步，处理需要待办的工作事宜；
		已办事宜 与协同办公数据同步，查看已经办过的工作事宜；
		办结事宜 与协同办公数据同步，查看已经办结的工作事宜；
		会议通知 与协同办公数据同步，处理与回复或查看会议通知内容；
		交办管理 与协同办公数据同步，对领导或其他人员交办工作的处理和跟进；
		安全管控 支持对移动设备硬件级绑定、手机号绑定、准入绑定、网络绑定等；
		系统配置 系统支持灵活的功能配置以及功能模块的权限调整，支持不同人员不同岗位移动终端界面和功能模块显示；
6	政府政务办公云平台电子签章系统服务	遵照平顶山市政府政务办公云平台统一设计要求，满足印章加密体系要求，实现与市级电子印章加密体系的认证和对接，实现电子印章的制作、保存、查询和统计等功能，使用高强度加密算法或国家机要管理单位认可的硬件加密设备对印章进行加密。提供电子印章的授权服务，服务包括对印章进行制作和发放，对印章进行日常维护和更新，保证印章的数据安全。

	1. 符合全市统一印章加密认证体系，在办公资源网上实现了电子签章处理后全市办公体系的标准对接以及公文印章的双认证（指国产化和非国产化终端签章后统一的认证标识），电子签章管理中心平台支持基于国产化的硬件服务器架构及国产化的服务器操作系统，也支持非国产的基础平台部署，同时数据库完全实现了国产化数据适配。 2. 含服务控制中心平台一套，实现与市级电子印章加密体系的认证和对接，以及 CA 证书的互认，终端客户端支持各类国产化终端设备和非国产化终端设备（注：国产化和非国产化支持统一签名认证，但授权机制各自独立不互通）。电子密钥产品符合国家保密标准 BMB52—2020《安全保密产品 电子签章产品技术要求》。 3. 电子签章管理系统 （1）签章系统严格遵照公安部相关技术标准与国家法律法规，满足电子签章的法律合规性需求 （2）审计日志：提供对签章日志的查询、导出等功能。其中日志内容包含密钥盘序号、单位名称、签章名称、日志描述、操作 IP 等信息。同时能导出到 Excel 表格，包含的功能应该包括单位名称、签章名称、用户名称、日志类型、加盖类型、日志分类、日志时间、操作 IP 等。 （3）统计报表：支持签章统计明细报表、密钥盘统计明细报表、持章人用章统计汇总表、持章人用章统计明细报表、日志时间段等。支持将统计后的 Excel 报表文件保存到本地。 （4）签章控制：可以对签章日期、签章次数、星期设置、允许 IP 段、禁止 IP 段、使用期限等进行控制。 （5）打印管理：提供 Word/Excel/pdf 等格式文档进行打印控制功能，控制内容主要包含控制打印机、控制打印电脑、控制打印份数。签章状态打印方式包括：签章空白打印、签章黑白打印等。 （6）升级服务：提供客户端升级模块和服务器端升级模块，客户端升级模块，上传客户端升级包，所有连接到签章服务器的客户端自动下载升级更新；服务器端升级模块，上传服务器端升级包输入管理员密码，自动完成升级。 （7）信息校验：检测数据库中的用户密钥信息、签章信息、日志信息是否被第三方直接从数据中恶意篡改，实现数据安全性验证。校验后将显示已篡改的密钥记录。 （8）多语言支持：支持简体中文、繁体中文、英文等其他语言模式。 （9）支持多种环境：支持 MYSQL、ORACLE、SQLSERVER 多种数据存储方式保存签章数据，以及 Windows、Linux 操作系统部署。 4. 电子签章客户端 （1）以 PKI/PMI 技术为基础，采用 COM/ActiveX 技术开发，应用，将电子印章和数字签名技术完美结合为一体。电子签章加密采用国际标准算法及国内商用密码算法，产品安全可靠。 （2）全面支持 Microsoft Word\Excel\HTML\PDF 电子文档格式应用上的电子签章。支持对微软 word/excel，金山 wps 文字/wps 表格文档进行电子签章且微软 office 文档用金山打开可以做到签章互签互验，反之亦然； （3）支持文字批注、手写签名功能，实现业务系统在 Word 文档上的联合审批要求，兼容 Office2003\2007\2010\2013\2016 等版本，同时实现以上版本之间的互验。 （4）签章验证：可验证单个印章或批量验证多个印章的有效性，检测被签名的文件名称、授权单位、用户名称、签章时间、签章唯一序列号、计算机 IP 等信息，同时验证文档的内容是否被篡改，篡改后文档的签名自动失效。
--	---

		(5) 签章显示：支持 OFFICE 签章在有电子签章环境下可以显示红色印章，一旦离开签章环境，看到的则是黑章或无章，保证红章文件的安全性。
		(6) 盖章模式：支持多模式盖章方式，包括光标定位、鼠标定位、鼠标连续盖章、鼠标连续多页盖章。
		(7) 支持文档打印控制，可以控制到打印计算机、打印机、打印份数，打印控制支持盖章人手工设置和签章服务器集中设置两种模式。
		(8) 签章对文档锁定功能：包括：文档锁定模式，锁定后文档无法修改无法复制；批注锁定模式，锁定后文档无法修改，但是内容可以复制。
		(8) 支持打印签章水印功能，包括设置文字水印和图片水印方式。
		(10) 支持 OFFICE\PDF 签章在加盖印章时同时在印章下方显示印章加盖时间。时间位置包括居中、居上、居下、左上、左下、右上、右下。
		(11) 支持签章雾化，防止签章图片被截图，打印时，签章图案为正常显示。
		(12) HTML 签章支持多种主流浏览器，包括 IE、Google、Firefox、Safari 等，方便用户在多种操作系统环境中不同浏览器中做网页盖章操作。
		(13) 后台服务器自动批量盖章功能,实现无人值守大批量 PDF 文档自动盖章：自动 PDF 盖章、PDF 数字签名、PDF 加密、PDF 域签名和 PDF 水印等
		(14) 支持多 key 多 CA 技术：支持多家 CA 的数字证书和多家硬件 key 厂商的对接和电子签章。
		(15) 提供必要的的数据交换接口和二次开发服务，可与第三方业务系统实现无缝集成。
7	政府政务办公云平台短信平台服务	遵照平顶山市政府政务办公云平台统一设计要求，提供符合政务办公流程的短信中心，实现各类办公流程的短信提醒以及通知提醒，会议通知时的短信回复和综合分析统计的短信平台服务。
		1. 依托全市办公业务资源网的统一出口管理要求，实现各类办公事项和会议通知的短信提醒，通过该平台实现全市办公业务资源网统一短信提醒。
		2. 支持会议通知时的短信回复和综合数据分析统计。采用政务级别的短信专属通道，支持移动、联通、电信三家运营商号码的短信接收。
		3. 支持多业务系统对接
		政府都有自己的业务系统，很多业务信息都是通过系统生成后发送，这就要求短信平台能够与业务系统之间对接来实现数据交互，尽量减少二次开发，缩短项目时间。
		4. 千万级信息的处理能力
		对于政府来讲，不仅需要提交千万级的信息量，而且还对短信的及时性要求也是极高，尤其是会议通知类动帐短息，及时性都要求控制在 1 秒左右；为了避免信息的丢失和延时，这就要求短信平台具备大规模短信的处理能力和发送能力，既要保证信息的安全与完整，又要有条不紊的将信息及时发送出去。
		5. 状态报告及时返回
		通过短信平台提交大批量的信息后，有多少条是成功到达客户手机是大都会关心的问题，所以平台需要能及时看到短信的发送的状态，从短信提交、处理过程及成功到达手机后发回的状态报告都能查看。
		6. 管理方面功能支持。机构及权限管理，信息安全管理，通讯资料导入与管理，通道的智能调配及流量的均衡处理，费用及业务统计报表。
		7. 运维方面的优势。系统稳定性，系统安全性状态报告功能，多通道动态负载均衡，通道热拔在线，通道切换平台业务监控，自动预警高性能高健壮性。

四、技术需求描述

（一）政务外网机房环境及设施服务和机房运维服务

由承建方根据国家 C 类机房的标准提供配套机房服务、后期运维管理服务、设备更新维护等。

基本要求

机房配套服务不仅仅是一个计算机网络服务，更重要的是一个集系统集成、建筑配电、建筑消防、建筑装饰、暖通净化专业、计算机专业、弱电控制专业、接地防雷专业等多学科、多领域的综合服务。在配套服务中应包含供配电方式、空气净化、安全防范措施以及防静电、防电磁辐射和抗干扰、防水、防雷、防火、防潮、防鼠等诸多方面的设施，以确保计算机系统长期正常运行工作。

依据国家有关标准和规范，结合所需系统运行特点进行总体设计。业务完善，技术规范，安全可靠为主，确保系统安全可靠的运行。根据功能及服务要求区别对待，在满足用户的基本要求的同时，做到服务有重点，效率有保障，并保证场地工作人员的身心健康，延长系统的使用寿命。为设备和工作人员创造一个安全、可靠、美观、舒适的服务场所。

本次机房配套服务应包括以下几个方面：1. 机房基础装修环境； 2. 机房市电供配电系统； 3. UPS 不间断电源系统； 4. 接地系统； 5. 防雷系统； 6. 空调系统； 7. 门禁系统； 8. 视频监控系统； 9. 机房消防系统； 10. 新风系统； 11. 照明及应急照明系统等。

（二）政务外网网络核心设施及配套网络安全设施服务和运维服务

（1）提供互联网出口管控服务

国家电子政务网管中心对电子政务互联网出口的安全防范有统一的要求和规范。根据具体需求，需提供出口防火墙等服务设备。

网络的大量应用会带来系统的高速运转，为了提供稳定及时高效的网络基础环境，为了对多条互联网出口线路进行有效和充分的利用，并且方便对后续线路的扩充，需要提供网络负载均衡功能，进行合理的访问和线路统一调度。

（2）建设统一的互联网出口平台

根据国家和省、市有关文件要求，须建设中央、省、市、县 四级统一互联网出口，原则上各局委不再单独建设互联网出口，应通过电子政务外网城域网接入本级电子政务外网平台，通过电子政务外网城域网连接本级电子政务外网统一互联网出口访问互联网。

电子政务外网统一互联网出口应通过相应的网络安全逻辑隔离措施，部署本级政务外网互联网出口。

对于统一互联网出口的解决方案应根据电子政务外网的应用现状，解决多运营商链路的接入问题，解决流量控制问题、智能路由选路、多链路负载与备份功能、智能 DNS 解析、精细化的上网行为控制问题，并且为各接入委办局提供统一互联网出口服务，对互联网出口做统一的规划。互联网统一出口带宽应具备后期进行进一步扩展的能力。

互联网出口区域须部署逻辑隔离设备，将政务外网互联网出口区域和互联网隔离，互联网出口区域的管理和安全须符合公安部有关技术要求和标准。提供防火墙等安全服务。提供 VPN 接入功能。

（3）电子政务外网网络交换平台设计

电子政务外网网络交换平台包括骨干传输网交换平台和城域网交换平台。

随着电子政务建设的深入开展，以建设电子政府为目标的政府信息系统建设，需要融合多种网络应用，应该综合考虑电子政务外网网络交换平台的稳定性、多业务融合性。

完成本级电子政务外网与上级政务外网平台的对接，实现政务外网相应区域的协同对接。

政务外网城域网交换平台由核心传输网路由器、核心交换机、局委接入设备组成。作为电子政务外网网络交换核心平台，承载电子政务外网相关业务，电子政务外网核心路由器、交换机须支持 MPLS VPN 功能。

本级政务外网区域规划须依据电子政务外网有关规范和要求，以电子政务外网“2+N”结构为基础，对本级政务外网进行安全局划分，具体划分应包含公用网络区、互联网区、专网区等区域。各个区域之间须通过 MPLS VPN 技术进行隔离，并依照政务外网有关标准，实现不同 VPN 区域之间的数据交换。

（4）政务外网运维区

电子政务网络基础设施跨越几代的技术发展，政务外网管理单位负责运维的网络和应用系统不断增加，信息管理的难度逐步加大，而业务部门对 IT 服务的要求不断提高；同时，随着数据集中和各个业务区的规范设计，外网管理中心承担了很多重要业务应用系统的运维工作，面临的运维压力越来越大。这就需要一套完整先进的运维监控和服务体系，可以自动监控、自动更新、自动实现流程管理，为电子政务外网的整体 IT 信息化系统的建设和运行提供有力的保障，同时将费用和风险降低到最小。

要求对 IT 信息环境及各项业务系统，尤其是重要业务系统的运行情况进行监控，才能事前防范。

须在政务外网的管理中心建设高度自动化的、集中的运维中心，承担起全 IT 系统的监控和管理，实现全面的实时监控、自动告警和预警、智能统计和分析，结合运维与管理手段，最大程度地保证业务系统的稳定运行。提供运维服务器、堡垒机服务、网管软件授权服务、日志审计服务、

服务器防病毒服务等。

(5) 局域网安全接入

终端同一时间只能访问政务外网的一个区域。

根据《GW0206-2014 接入政务外网的局域网安全技术规范》等国家、省、市有关要求，应实现终端不能“同一时间”访问电子政务外网的多个区域的需求，防止终端被恶意控制，作为“肉鸡”、“跳板”对电子政务外网进行非法访问和攻击，保证电子政务外网内终端可安全访问各个业务区域的系统。

局域网接入终端的身份鉴别

局域网内的终端在接入政务外网时，需要对终端进行身份鉴别。接入局域网终端能够进行注册，注册信息至少要包括 MAC 地址、用户信息等其他信息，同时使用者口令应采用强口令。

局域网接入终端的准入控制

局域网内的终端在接入政务外网时，需要对终端进行准入控制。局域网接入终端在进行用户注册时，管理员应能够管理和分配终端用户访问区域的权限，可实现电子政务外网的可控访问，没有访问某一区域权限的用户无法访问该区域。

终端访问认证架构

局域网接入终端访问政务外网时，应采用 B/S 架构进行终端认证。实现终端用户在安装专用软件的情况下，可以进行终端认证。终端认证同时需要支持单点登录功能，实现终端用户在不同业务区域之间切换时，不需要重新进行身份认证，仅需重新选择区域即可。

权限管理

局域网终端准入系统应具备分角色管理的能力。用户注册及其他管理权限可根据实际需求分为多种，例如超级管理员角色、局办委普通管理员角色等。超级管理员：拥有所有用户注册权限，可管理其他普通管理员，并且拥有其他所有权限；局办委普通管理员：仅可管理由超级管理分配的，本级单位终端用户的注册及其他本级权限。

(6) 电子政务域名及 IP 地址资源规划

1. 国家、省地址规划、2. 域名规划、3. AS/MPLS VPN 规划，根据以上要求，做出开发区 IP 地址规划详表及实施方案。

(三) 平顶山尼龙新材料开发区管委会电子政务外网运维服务

电子政务外网的网络基础设施和交换中心的日常运行、维护工作由供应商提供专职工程师进行售后运行维护服务。

运行维护服务包括，信息系统相关的网络链路、交换设备、安全设备及其他信息系统的运行

维护与安全防范服务，保证用户的信息系统的正常运行，降低整体管理成本，提高网络信息系统的整体服务水平。同时根据日常维护的数据和记录，提供用户信息系统的整体建设规划和建议，更好的为用户的信息化发展提供有力的保障。

通过运行维护服务的有效管理来提升用户信息系统的服务效率，协调各业务应用系统的内部运作，改善网络信息系统部门与业务部门的沟通，提高服务质量。结合用户现有的环境、组织结构、IT 资源和管理流程的特点，从流程、人员和技术三方面来规划用户的网络信息系统的结构。将用户的运行目标、业务需求与 IT 服务的相协调一致。

信息系统服务的目标是，对用户的信息系统基础资源进行监控和管理，及时掌握网络信息系统资源现状和配置信息，反映信息系统资源的可用性情况和健康状况，创建一个可知可控的 IT 环境，从而保证用户信息系统的各类业务应用系统的可靠、高效、持续、安全运行。

(四) 办公业务资源网机房环境及服务

提供开发区政府办公业务资源网机房装修及空调、视频监控、配电系统、不间断电源系统和消防门禁系统等设施的服务，以及核心机房环境相关软硬件设施的运维服务。机房按照国家 C 类标准提供服务。

(五) 办公业务资源网核心网络接入和安全服务

办公业务资源网核心网络相关的安全服务，包含核心路由器、核心交换机、安全防火墙等。

(六) 平顶山尼龙新材料开发区管委会办公业务资源网运维服务

提供对平顶山尼龙新材料开发区管委会办公业务资源网的中心机房网络运维服务，保障网络的稳定运行；定期的日常运维服务，日常至少 1 月进行一次例行运维保障巡检。出现故障即时响应，2 小时内安排人员出现场处理。

(七) 政府政务办公云平台软硬件基础支撑服务

提供政府政务办公云平台运行所需的软硬件支撑服务，服务包括计算、存储、运行内存、数据库、中间件等软硬件基础支撑资源，其中，基础支撑软硬件要按照相关国家标准要求，符合国产化的适配要求。

（八）政府政务办公云平台应用软件服务

目前，信息化的发展已充分展开，单位内部的业务应用系统很多，各系统间没有什么联系，且需要通过多个账户和密码登陆到不同的系统，极不方便。要求提供基于 SSO 单点登录、统一身份管理和统一信息发布的政府政务办公云平台解决方案。

根据市政府要求，政府协同办公平台应依托全市办公业务资源网进行建设，应符合省、市相关建设规范和平顶山市关于办公业务资源网和协同办公平台建设的有关要求。县办公业务资源网业务应用软件系统要求按照平顶山市人民政府办公室《关于推进全市政府系统电子政务建设工作的通知》（平政办[2011]11 号）、《平顶山市人民政府办公室〈关于促进全市电子政务协调发展的实施意见〉》（平政办[2015]115 号）、《平顶山市人民政府办公室〈关于在全市政府系统升级推广启用新版政务办公云平台系统的通知〉》（平政办明电[2018]209 号）、《平顶山市人民政府办公室关于规范推进全市政府系统办公业务资源网及政务办公业务系统平台建设的通知》文件的要求进行建设；

实现公文收发、公文阅办、文件审批、公文交换等一体化的政府文件审批流转办理，支持可视化流程在线编辑，实现灵活的自定义流程智能办理，提供公文流转审批和签发、阅办文的传阅签批、内部考勤、用车申请、财务报销等流程审阅和签批等功能。与市政府政务办公云平台完成对接，保障与政府公文的在线签批和流转。

发文管理：对流程发文的管理，如起草，审核，签批，归档等发文文件的处理，支持流程自定义可视化设置，能够支持较复杂的流程定义等功能。

收文管理：对收文阅办的管理，如拟稿，阅办，转办，转发，归档等功能。接受上级部门文件，自动进行内部公文的转发，无需下载导入。

公文传输：对正式公文文件的下发，上报，签章，打印控制等，依托全市办公业务资源网实现全市单位授权范围内的文件传输交换（含县市区单位）。

电子邮件：政务办公专网邮件系统。依托全市办公业务资源网实现全市单位授权范围内的文件传输交换（含县市区单位）。

文档知识库：对业务系统中的文档进行的分类管理以及授权分享查看打印等功能。

系统设置：业务系统的相关流程配置，门户配置，接口配置，组织结构及人员信息配置等系统设置功能。

（九）政府政务办公云平台移动办公服务

待办事宜，与协同办公数据同步，处理需要待办的工作事宜；

已办事宜，与协同办公数据同步，查看已经办过的工作事宜；

办结事宜，与协同办公数据同步，查看已经办结的工作事宜；

会议通知，与协同办公数据同步，处理与回复或查看会议通知内容；

交办管理，与协同办公数据同步，对领导或其他人员交办工作的处理和跟进；

安全管控，支持对移动设备硬件级绑定、手机号绑定、准入绑定、网络绑定等；

系统配置，系统支持灵活的功能配置以及功能模块的权限调整，支持不同人员不同岗位移动终端界面和功能模块显示；

提供移动端 OA 个人办公的工作桌面，消息推送、待办事宜处理、协同 OA 信息查看、日程提醒、移动签到等功能，并支持图片、语音、位置上传等功能。

在政务办公平台基础上部署移动办公平台软件模块，提供独立 APP，支持主流的安卓和 IOS 操作系统，提供最核心的服务帮助领导抓住零碎时间，充分满足其随时随地办公的需求。手机移动办公系统界面采用宫格式的界面风格、操作便捷简洁、提示明确，几乎不用培训就能上手。手机移动办公支持收发及时消息，审批流程、门户信息阅读，写工作日记、阅读员工日记，布置任务、汇报任务，安排日程、查看日程等日常移动办公业务。

实现与市政府协同办公云平台无缝对接，实现公文文件的上传下达，与市政府以及市直各单位文件流转的无缝对接。

(十) 政府政务办公云平台电子签章系统服务

市政府办公室[2011]11 号文件要求，全市要采用统一的电子签章验证系统。我县直接采购市政府电子签章验证管理平台分中心管理授权及县级区域内的有关单位的签章客户端来组建县级电子签章管理系统，以达到县和市电子签章管理系统之间数据统一、互联互通的目的，实现集中控制、分级管理。市电子签章验证管理系统功能描述如下：

电子签章管理系统是一个独立的管理系统。能实现公章的制作、保存、查询和统计等功能，同时使用高强度加密算法或国家机要管理单位认可的硬件加密设备对公章进行加密。上级主管机关负责公章的制作和发放，进行公章的日常维护，保证公章的数据安全。

系统支持使用多个公章管理系统构成一套分布公章管理体系，实现集中控制、分级管理，以适应多级的公文传输要求。上级的公章服务器可根据需要将盖章和打印许可的验证权限发放到其它公章服务器，使公章及公文服务器的部署更为灵活。支持数字签名证书的信任体系，使分布式公章体系的安全性得以保障。

电子公章的存储应该与移动设备硬件信息进行绑定，防止公章文件被非法复制；电子公章使用时，实现可视化盖章，并在预览时显示虚化的公章，防止通过拷屏或照相等方式获得公章印模，

而在打印时，在纸质上公章则是全真显现；电子公章使用时，应该满足服务器端在线验证的模式，充分保证公章使用的安全性。

电子公章系统应支持各级行政单位多级互联架构,支持多级分布式部署， 电子公章系统支持 PKI 体系，并实现打印控制。

（十一）政府政务办公云平台短信平台服务

支持多业务系统对接，短信平台能够与业务系统之间对接来实现数据交互，尽量减少二次开发，缩短项目时间。千万级的信息量，而且还对短信的及时性要求也是极高，尤其是会议通知类动帐短息，及时性都要求控制在 1 秒左右；避免信息的丢失和延时，短信平台具备大规模短信的处理能力和发送能力，既保证信息的安全与完整，又有条不紊的将信息及时发送出去。通过短信平台提交大批量的信息后，有多少条是成功到达客户手机是大都会关心的问题，平台能及时看到短信的发送的状态，从短信提交、处理过程及成功到达手机后发回的状态报告都能查看。

（十二）政府门户网站群系统服务

1、提供门户网站服务功能描述

根据平顶山市人民政府办公室“关于做好政府网站与政务新媒体存在问题整改工作的通知”以及国务院办公厅和省、市政务信息公开办公室相关文件要求，是对原有网站建设和管理的补充，采用“统一规划、协同建设、分级管理”的建设模式，依托全市政府门户网站群架构为政府各部门提供统一的系统平台,把平顶山尼龙新材料开发区管委会门户网站建设成为功能齐全、内容丰富、更新及时、 服务到位、 制度健全、考核机制完善的统一平台。本次应用软件建设的主要任务如下：

软件平台的使用授权：要求提供完整的软件平台使用权限，如内容管理、栏目管理、内容审核、内容回收站、信件处理、用户管理以及权限管理等。

网站开设报备、ICP 备案、网警备案等协助办理：要求协助办理网站各类备案工作以及所需材料的报送。

网站前端模板定制设计、页面开发制作：根据要求进行网站前端模板的设计制作，符合《国务院办公厅关于印发政府网站发展指引的通知》国办发（2017）47 号文件中“网页设计规范”的要求并达到用户满意。如有阶段性专题页面，需要专人进行设计制作。专题的页面风格原则上应与网站整体风格一致，具体页面展现可根据需要灵活设计。

基础的技术支撑及运维服务：要求在相关技术领域给予用户免费的系统知识层面的普及、咨询答复、培训和帮助。除不可抗力造成的服务中断外，因为其它问题导致服务中断的需要在规定

时间负责修复。应按照国家有关部门涉及信息系统安全的有关规定，进行网络安全服务和信息安全等级保护。同时负责网站除内容发布之外的技术运维工作以及网站安全防护工作。

功能优化：服务期内网站后台的故障修复及平台性能优化调整。

网站培训：网站建设完成后需要针对信息保障人员进行操作培训。

等级保护测评：需要按照要求对网站进行三级等保测评。

用户中心对接：根据国办政府网站发展指引和考评细则建设统一的用户中心功能,实现一站式登录,同时结合我省政务服务平台对数据的要求,要求全省政府门户网站用户中心要依托全省统一身份认证平台进行注册和登录认证。

数据同源对接：按照市政府检测平台的对接要求，实现与市政府门户网站群平台的检测数据及信息发布数据的同源对接。如：互动交流信件数据、依申请公开信件数据及相关信件的办理流程监管对接、栏目更新情况的数据对接等，实现全站数据的办理/管理/监测的对接，实现数据源的唯一性和完整性。

IPV6 平台改造：对网站平台系统进行协议改造，使之对 IPV4 和 IPV6 双栈支持。

页面标签标准化改造：根据国办网站发展指引要求，对门户网站的模板标签进行标准化改造调整，对网站首页、栏目页、内容页等页面的 meta 标签进行标准化改造。

无障碍浏览：根据《中国残疾人联合会 国家互联网信息办公室关于加强网站无障碍服务能力建设的指导意见》和 2017 国办下发的政府网站发展指引以及最新的政务门户网站和新媒体考评细则等文件的要求，增加网站无障碍浏览工具条模块，如页面放大缩小/阅读/辅助线等功能，满足残疾人对浏览政务门户网站的需求。此功能要求在服务期内免费升级和调整，满足考评的技术标准，同时进行与网站主题设计的适配和优化。

全文（智能）检索：根据国办印发的政府网站发展指引要求,以及最新的政务网站考评细则要求,对政府网站实现全文检索功能,支持检索时间/检索效率/检索分类/检索内容等功能支持,以及实现与各类业务数据接口的扩充,实现基于大数据服务的全文检索,以及对版式文件和格式文件的检索。

智能机器人（智能问答）：根据国办印发的政府网站发展指引要求,以及最新的政务网站考评细则要求,增加智能机器人功能,实现智能客服的问答操作,要求机器人要有自我学习能力,通过不断的优化升级,进行自我学习提升。同时要求与全文智能检索实现接口对接,智能机器人服务端要支持前端词条的记录和分析,自动生成报表,不断实现自我学习和灵活的词条维护,同时支持与市级站群平台机器人管理系统的数据对接实现数据词语的共享。

空栏目/长期不更新/错别字检测提醒：对网站运维中栏目运维的空栏目检测和长期不更新检测进行提醒和督办,对信息发布的错别字和敏感词进行检测提醒。

死链接检测提醒：对网站全站链接进行检测提醒，并深度检测链接状态和信息，防止暗链。

短信提醒：对网站各类检测数据以及信件办理过程中的消息进行提醒和短信推送。

安全检测扫描：定期对网站进行安全检测和扫描，并根据用户需要导出检测报告。协助用户完成日常关于网站运维的表格统计和数据报表与上级主管部门的上报工作。

移动微门户：根据技术要求和指标，对门户网站的前端进行移动设备的适配升级，支持手机、平板等设备界面，要求界面美观，功能丰富。同时与网站数据无缝对接，在服务期内不断升级迭代，优化移动终端的访问效果。

健康运行检测平台：根据以上各类检测数据的汇总分析，形成检测平台，并根据要求实现各类检测数据与市政府检测平台数据的对接和传输。

(十三) 平顶山尼龙新材料开发区管委会政府门户网站等级保护三级测评服务

按照《网络安全等级保护条例》要求，对开发区政府门户网站系统进行等级保护三级测评，并将取得相关部门的备案证书。

(十四) 其他说明

1、供应商的方案须报平顶山市电子政务外网运维中心等有关部门备案通过后方可执行。本次项目相关服务，由中标方负责承担服务期内服务升级的相关费用，用户方在服务有效期内不承担任何更新和升级费用，需出具承诺书；

2、办公业务资源网业务应用系统平台需与市政府政务办公云平台完成对接，保障与政府公文的在线签批和流转，需出具承诺书；

3、供应商须承诺与市级电子政务外网网络运维管理平台实现无缝对接，并承担其产生的相关对接费用，需出具承诺书。

(2) 服务要求：合格，满足采购人要求。

(3) 质量标准：满足采购人要求。

(4) 服务期限：2 年

(5) 付款方式：合同签订后 30 日内，甲方向乙方支付服务费用的 40%。乙方向甲方提供网络维护服务满 180 日后，甲方对乙方所提供服务质量无异议，且乙方不存在其他违约的情况下，30 日内向乙方指定银行账户支付服务费用的 40%。合同期满，30 个工作日内支付剩余 20%。