一、项目总体情况

（一）项目名称：芦山县人民医院 5G 定制网及等保项目

（二）项目所属年度：2024 年

（三）项目所属分类：服务

（四）预算金额（元）：870000.00 大写（人民币）：捌拾柒万元整

（五）项目概况：为了满足芦山县人民群众的健康需求，提高县域医疗服务水平，加快建设健康芦山，本项目拟对芦山县人民医院和各乡镇卫生院进行设备投资改造。

服务内容及要求如下：

1、5G 定制专网服务：为加快 5G 在智慧医院领域的创新应用，结合《关于促进“互联网+医疗健康”的发展意见》中要积极开展远程医疗等服务的要求，消除空间障碍，促进医疗资源下沉，提高 4G/5G 信号覆盖范围和质量为医院内部通信、远程会诊、远程监控等提供支撑。

2、医院内外网改造服务：通过对医院网络整治，实现医院内网外隔离，同时兼顾医院病房多媒体电视业务（IPTV）部署。

3、三级等保服务：按照国家《网络安全法》及医院相关管理要求，对医院信息集成平台、众阳云健康系统进行三级等级保护服务。

（六）本项目是否有为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商：否

二、项目需求调查情况

依据《政府采购需求管理办法》的规定，本项目不需要需求调查，具体情况如下：

（一）需求调查方式

（二）需求调查对象

（三）需求调查结果

1.相关产业发展情况

2.市场供给情况

3.同类采购项目历史成交信息情况

4.可能涉及的运行维护、升级更新、备品备件、耗材等后续采购情况

5.其他相关情况

三、项目采购实施计划

（一）采购组织形式：分散采购

（二）预算采购方式：非公开招标

采购方式：竞争性磋商

（三）本项目是否单位自行组织采购：否

（四）采购包划分：不分包采购

（五）执行政府采购促进中小企业发展的相关政策：

本项目不专门面向中小企业采购

（六）是否采购环境标识产品：否

（七）是否采购节能产品：否

（八）项目的采购标的是否包含进口产品：否

（九）采购标的是否属于政府购买服务：否

（十）是否属于政务信息系统项目：否

（十一）是否属于高校、科研院所的科研仪器设备采购：否

（十二）是否属于 PPP 项目：否

（十三）是否属于一签多年项目：否

四、项目需求及分包情况、采购标的

（一）分包名称：合同包一

1、执行政府采购促进中小企业发展的相关政策

1)不专门面向中小企业采购

本项目不专门面向中小企业采购

注：监狱企业和残疾人福利单位视同小微企业。

2、预算金额（元）：870000.00 大写（人民币）：捌拾柒万元整

最高限价（元）：870000.00 大写（人民币）：捌拾柒万元整

3、评审方法：综合评分法

4、定价方式：固定总价

5、是否支持联合体投标：否

6、是否允许合同分包选项：否

7、拟采购标的的技术要求

1	**采购品目**	信息化设备零部件	**标的名称**	芦山县人民医院 5G 定制网及等保项目
	数量	1	**单位**	项
	合计金额（元）	870000.00	**单价（元）**	870000.00
	是否采购节能产品	否	**未采购节能产品原因**	无
	是否采购环保产品	否	**未采购环保产品原因**	无
	是否采购进口产品	否	**标的物所属行业**	软件和信息技术服务业

标的名称：芦山县人民医院 5G 定制网及等保项目

<table>
<tr><th>参数性质</th><th>序号</th><th>技术参数与性能指标</th></tr>
<tr><td></td><td>1</td><td>
<table>
<tr><th>序号</th><th>服务名称</th><th></th><th>数量</th><th>单位</th></tr>
<tr><td>1</td><td>5G 定制网络</td><td>5G 技术网络性能要求：
●1、5G 网络可靠性：5G 核心网、承载网、UPF/MEC 等重要组建采用设备冗余、链路备份等技术保障。
●2、5G 室外频谱资源带宽：5G 室外可用 4GHz 以下连续频谱资源大于等于 200M。
●3、5G 室内频谱资源带宽：5G 室内可用频谱资源大于等于 240M。
5G 定制专网参数要求：
数据传输速率要求：
●4、单位逻辑区域（小区）内平均吞吐率，满足下行 450Mbps，上行 45Mbps。
●5、单位逻辑区域（小区）下行峰值速率大于等于 500Mbps
并发用户数要求：
●6、单位逻辑区域（小区）满足至少 400 个终端数</td><td>1</td><td>套</td></tr>
</table>
</td></tr>
</table>

				据并发。 网络时延要求： ●7、从医疗终端到本地医院医疗应用平台之间，双向端到端的平均网络时延不超过 100ms。 ●8、从医疗终端到区域或者跨区域医疗应用平台之间，双向端到端平均网络时延不超过 100ms。 5G 网络移动性要求： ●9、数据平均丢包率不超过 5‰。 ●10、移动业务掉话率不超过 8‰。 网络接入可靠性： ●11、终端接入成功率不低于 98%。 ●12、无线射频单元设备故障率全年不超过 2%。 ●13、网络系统可靠性不低于 99%。 ●14、采用专业的 pioneer、phu 等测试软件，对指定覆盖区域内的任何区域进行网络指标测试，并对测试结果的真实性进行承诺。 5G 定制网运营管理服务平台： ●15、需提供对应的设备组网管理平台，平台提供设备机卡绑定和解绑、设备重启、设备状态查询、流量查询、在线查询、WiFi 配置、在线升级、恢复出厂组网变更、自定义性能告警等功能。 ▲16、管理平台安全等级保护满足三级或以上等级要求。（投标时需提供管理平台信息系统安全等级保护备案证明并加盖供应商公章） ●17、支持可视化 VXLAN 二层组网，灵活管理各分支设备隧道。 ●18、支持泛资产告警监控及告警推送，通过对终端、号卡、组网等对象建立监控规则，生成告警，支持短信或邮件推送。 ●19、支持一键判障，对终端、号卡进行诊断。 ●20、支持号卡自助管理，如：达量断网、流量告警、流量使用情况、流量包查询、网络保障服务等。 ▲21、支持用户自主免审批调整套餐，包括变更和新建、退订流量包，以及自己调整机卡绑定关系、Qos 加速等。（投标时需提供产品功能截图证明并加盖供应商公章） ●22、支持分权分域，可设置多种角色、多级账号，对不同账号分配不同的数据权限。 ▲23、支持号卡激活，一键完成出账信息变更及业务 IP 签约。（投标时需提供产品功能截图证明并加盖供应商公章） ▲24、支持拨测测速，通过平台远程进行 ping、TCP 测速，测试网络连通性及速率带宽。（投标时需提供产品功能截图证明并加盖供应商公章）		

<table>
<tr><td></td><td></td><td></td><td></td><td>●25、支持隧道启停，允许在完成的组网中临时对分支终端的隧道进行关闭和开启。关闭后，分支终端与中心终端的网络通信断开。有需要时还可再重新开启。</td><td></td><td></td></tr>
<tr><td></td><td></td><td>2</td><td>5G 物联网网关</td><td>●1、CPU≥4 核，内存≥4GB，存储≥16GB，支持 5G/4G/3G，Wi-Fi 双频，千兆独立电口≥5 个，USB3.0 接口≥1，RS232 接口≥2，Console 口≥1。
●2、支持物联网、复杂组网、智能选路、双发选收、工业协议适配。
●3、Wi-Fi 最大连接数≥30 个，Wi-Fi 覆盖范围≥30 米，配套 5G 流量卡。
★4、提供不少于 8 台 5G 物联网网关才能满足建设需求。</td><td>1</td><td>套</td></tr>
<tr><td></td><td></td><td>3</td><td>医院内外网改造服务</td><td>★（一）组网内容
<table><tr><th>序号</th><th>组网内容</th></tr><tr><td>1</td><td>需要新建 AP 覆盖点 144 个，其中内网 65 个 外网 79 个</td></tr><tr><td>2</td><td>康复楼康复楼，住院楼 WIFI 和各内外网建设 1 套汇聚交换机。共 4 台，（每栋内网 1 台，外网 1 台）。门诊楼有有线业务安全冗余角度和负荷分担，采用全光万兆汇聚，和接入交换机全光万兆双上下行直联。</td></tr><tr><td>3</td><td>核心交换机内外网各一套</td></tr><tr><td>4</td><td>汇聚交换机全光（康复，住院）</td></tr><tr><td>5</td><td>AC 控制路由器内外网各一套，分别接入内外网</td></tr><tr><td>6</td><td>存量老旧网线整治 264 条</td></tr><tr><td>7</td><td>康复楼和住院楼的 16 口 POE 交换机和本栋汇聚交换机全光千兆互联。</td></tr></table>（二）相关服务要求：
数据接入交换服务
●1、支持 802.3ad 链路聚合、802.1x 、端口镜像测试、广播风暴抑制。</td><td>1</td><td>项</td></tr>
</table>

				▲2、支持 STP/RSTP、IGMP Snooping、DHCP Snooping（投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） ●3、支持静态路由、策略路由、RIP、OSPF、RIPng、OSPFv3。 ▲4、设备工作温度-10℃~+55℃，温度变化率≥1℃/min,高低温持续时间 20min，循环周期≥100 次，运行不丢包。（投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） ●5、支持用户访问控制、Telnet 访问安全、网管—SNMPv3 协议。 ▲6、支持支持丰富的 IPTV 特性，通过 IPTV 的部署，可对不同用户实施不同的 CAC(channel access control）规则。（投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） ●7、支持环网保护机制（以太环网保护技术 ZESS）、ERPS 以太网环保护协议 G.8032，可实现以太网环路 50ms 级的保护。 ▲8、地址缓存能力≥16K、设备支持防雷等级≥6KV。（投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） **全光汇聚数据交换服务** ●9、支持 URPF、802.3ad 链路聚合功能、802.1x 功能。 ●10、支路由协议安全 、IGMP Snooping、DHCP Snooping。 ●11、支持用户访问控制、Telnet 访问安全测试、网管—SNMPv3 协议测试。 ●12、支持横向虚拟化。		

				▲13、支持丰富的 IPTV 特性，通过 IPTV 的部署，可对不同用户实施不同的 CAC(channel access control) 规则。(投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） ●14、支持环网保护机制（以太环网保护技术 ZESS、ZESR)，支持 ERPS 以太网环保护协议 G.8032，可实现以太网环路 50ms 级的保护。 ▲15、支持地址缓存能力≥65K、设备支持防雷等级≥6KV 。(投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） ●16、支持设备 MAC 地址表大小≥65K、支持 VLAN 数量≥4K。 ▲17、支持用户访问控制、Telnet 访问安全测试、网管—SNMPv3 协议测试、设备带承载业务运行，240 小时运行无丢包、设备工作温度-10℃~+55℃，温度变化率≥1℃/min,高低温持续时间 20min，循环周期≥100 次，运行不丢包。(投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） **无线组网数据交换服务** ●18、支持 POE/POE+ ●19、支持 802.3ad 链路聚合、802.1x 、端口镜像测试、广播风暴抑制。 ▲20、支持 STP/RSTP、IGMP Snooping、DHCP Snooping。(投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告加盖供应商公章） ●21、支持静态路由、策略路由、RIP、OSPF、RIPng、OSPFv3。 ▲22、设备工作温度-10℃~+55℃，温度变化率≥1℃		

				/min,高低温持续时间 20min，循环周期≥100 次，运行不丢包。（投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告扫描件加盖供应商公章） ●23、支持用户访问控制、Telnet 访问安全、网管—SNMPv3 协议。 ▲24、支持支持丰富的 IPTV 特性，通过 IPTV 的部署，可对不同用户实施不同的 CAC(channel access control）规则。（投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告扫描件加盖供应商公章） ●25、支持环网保护机制（以太环网保护技术 ZESS）、ERPS 以太网环保护协议 G.8032，可实现以太网环路 50ms 级的保护。 ▲26、地址缓存能力≥16K、设备支持防雷等级≥6KV。（投标时提供具有资质的检测机构出具的 CNAS 或 CMA 的检测报告扫描件加盖供应商公章） ●27、支持设备 MAC 地址表大小≥16K、支持 VLAN 数量≥4K。 **无线终端控制服务** ●28、投标设备必须为硬 AC 架构，整机本地转发方式支持管理 AP 数量不少于 512 个 AP 的管理能力，本体默认自带 512 个 License 授权。 ●29、支持多 WAN 接入、DPI 流量控制、上网行为管理、多种认证方式、防火墙、VPN 应用、AC 控制器等功能，网关模式下带机数量≥300 台。 ●30、支持实时显示设备概况：接口状态，CPU 温度感知，CPU 使用占比，内存占比，上行下行速率等。 ●31、支持显示近 1 天内各协议流量分布情况，如视频、游戏、下载、文件传输等，可实时展示相应协议		

				的上行下行速率图表。 ●32、支持设备状态监控功能，可监控展示线路、终端、协议、策略、负载、分流等状态信息。 ▲33、支持智能流控功能，依据上网用户数量自动分配走向；并可基于线路负载、应用协议、源目端口、域名、上下行进行线路分流；支持终端限速功能。（投标时需提供相应功能的 WEB 界面截图证明加盖供应商公章） ●34、支持可基于信道、信号强度以及无线频段的无线射频优化功能。 ▲35、支持基于 DPI 七层数据识别技术，支持基于交通旅游、休闲娱乐、体育健身、购物网站、金融理财等多种分类进行上网行为管理控制，并可基于 IP 组及时间进行控制。（投标时需提供相应功能的 WEB 界面截图证明加盖供应商公章） ●36、支持对 AP 定位、重启、升级、周边信道扫描，无线干扰分析。 **上网行为管理服务** ●37、支持 DHCP server，DHCP relay，IPV4 路由协议，策略路由，NAT，IPSEC VPN，SSL VPN；系统内置电信、移动、联通、教育网四大 ISP 地址表，用户也可以自定义 ISP 地址库。 ●38、支持基于带宽、优先级的链路负载均衡、支持黑名单，扫描攻击防护，异常包攻击防护， Flood 攻击防护。 ▲39、支持基于接口的上下行带宽管理，支持高、中、低优先级通道设置，支持应用、服务、用户、源地址、时间的通道匹配，保障带宽，限制带宽，每 IP 限速，自动支持流量整形，通道化 HQOS，时间选择支持基		

				于日计划、周计划、月计划、单次计划等。(投标时需提供相应功能的 WEB 界面截图证明加盖供应商公章） ▲40、支持 Radius 认证，LDAP 认证，Radius/LDAP 服务器组主备和集群，短信认证实现 WIFI 认证上网，微信认证实现 WIFI 认证上网，支持防私接路由。(投标时需提供相应功能的 WEB 界面截图证明加盖供应商公章)。 ●41、支持应用控制及审计：支持根据应用/应用类来区分不同的应用行为，支持根据应用行为来区分不同应用的审计内容，根据应用行为确定审计内容，支持基于关键字或者数字的内容审计，包括 P2P 类，IM，搜索引擎，股票软件，网络游戏， Webmail，BBS 社区类，发件人过滤，非加密邮件，如可以在识别出 IM 即时通讯软件是 QQ 还是微信等客户端的基础上，准确识别到用户正在进行正常通信（文字或视频）还是刷朋友圈和逛 QQ 空间等，从而有目的和针对性地加以阻断和限制。 ▲42、支持 URL 过滤策略：支持恶意 URL 过滤，支持预定义和自定义 URL 分类过滤，支持 URL 阻断和审计支持对匹配 URL 的文件内容进行缓存加速，需缓存文件可手动上传及更新；可查看缓存可用空间和命中次数。(投标时提供相应功能的 WEB 界面截图证明加盖供应商公章） ●43、支持基于源、目的、规则集的入侵检测，支持 5 种自定义动作，支持软件 bypass，DDOS 防护，系统定义超过 2200 条规则特征库。 ●44、支持 HTTP，FTP，SMTP，POP3，IMAP 协议的病毒查杀，查杀邮件正文/附件、网页及下载文件中包		

				含的病毒，支持 300 万余种病毒的查杀，病毒库定期与及时更新。 ●45、系统资源信息，实时流量（设备），接口信息状态，应用流量统计，用户流量统计，设备流量统计，支持对设备转发流量统计，CPU 使用率，内存、会话、转发流量等统计趋势图。 **无线终端部署服务** ●46、双频吸顶无线 AP 支持 802.11a/b/g/n/ac/ax ，内置天线，1 个 10M/100M/1000M 以太网口。 ●47、支持 4 条空间流，整机最大接入速率≥1775Mbps。 ▲48、在 MCS10/ MCS11 调制下，2.4GHz 设备所有天线接口的总输出功率应能达到 17dBm，同时 5GHz 设备所有天线接口的总输出功率应能达到 17dBm。（投标时需提供第三方检测机构出具的检测报告扫描件并加盖供应商公章） ▲49、在 802.11ax 协议下，单个用户的上行/下行吞吐量大于 2Mbps 的情况下，设备支持同时工作的用户数量≥120。（投标时需提供第三方检测机构出具的检测报告扫描件并加盖供应商公章） ●50、工作温度：0℃~45℃，工作湿度：10%～90%RH（无凝结），支持 POE 供电：IEEE802.3af/at。 ●51、支持加密方式：WPA-PSK、WPA2-PSK、WPA-PSK+WPA2+PSK。 ●52、最大支持 SSID 数 8 个，支持隐藏 SSID，支持基于 SSID 的最大用户接入设置，支持不同 SSID 可配置单独的加密机制、VLAN 属性。 ●53、支持对接入用户的信息数据统计，支持定时开启，支持定时重启。		

				▲54、提供投标设备型号无线电设备发射型号核准证。 **集成服务** ★55、包含配套光缆布放、网线布放、电源线布放、设备箱安装、网线整治等。		
		4	三级等保测评服务	★1、按照国家《网络安全法》及医院相关管理要求，对医院信息集成平台、众阳云健康系统进行三级等级保护测评。	1	套
		5	云上安全产品（三级等保服务）	安全管理中心 ●1、与云平台紧耦合，可实现云平台一键下单，自动交付。（投标时需提供产品截图证明并加盖供应商公章） ▲2、提供虚拟下一代防火墙、IPS、WAF、恶意代码检测、网页防篡改、终端微隔离、终端防入侵、防病毒、补丁检测等安全防御能力。（投标时需提供产品截图证明并加盖供应商公章） ●3、支持集中展示业务系统的风险状态，包括业务风险分布、风险级威胁趋势、安全事件列表、安全评分、已具备的安全能力列表等。 ▲4、组织架构统一管理，安全组件统一认证，用户可通过控制台单点登录安全专区平台及所有安全组件。安全组件集中授权，集中监控、集中管理。从安全管理中心可管理所有安全组件。（投标时需提供产品截图证明并加盖供应商公章） ●5、可识别租户用户资产，可对资产进行分组管理，结合安全组件数据进行风险分析。 ●6、提供时间轴视图进行安全事件溯源，并生成资产安全报告。 ●7、集中展示资产的基线、补丁病毒、安全告警等数据，方便安全管理员评估特定资产的安全运行情	1	套

				况。 ●8、可对租户主机/应用进行安全漏扫，并可生产漏扫报告。 ●9、威胁分析中心对全网资产的安全事件及告警进行分类，至少按照风险等级、事件类型、影响标签、来源、状态等维度来分类。 ●10、提供事件 Top10 统计，受影响的 IP 云图，同时能够针对特定事件，详细分析风险和影响、展示事件发生的趋势。 防火墙 ●11、支持基于区域、IP 地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。 ●12、支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 ●13、支持对 HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP 协议进行病毒检测和查杀，支持最大 16 层的压缩文件查杀。 ▲14、具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。（投标时需提供产品截图证明并加盖供应商公章） ▲15、产品内置 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，支持超过 3000 种 Web 服务器漏洞特征规则。（投标时需提		

				供产品截图证明并加供应商盖公章） ●16、支持基于源 IP、Referer、URL 等多种组合条件对 CC 攻击进行检测，检测指标为检测时间和触发阀值。 ●17、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。 ●18、支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞。 ●19、支持内容敏感数据防泄露功能，对传输的文件和内容进行检测,支持对银行卡号、手机号码等类型数据防护。 ●20、支持网站防篡改功能，可防止攻击者非授权修改网站目录文件。 ▲21、支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用。（投标时需提供产品截图证明并加盖供应商公章） 堡垒机 ●22、支持 windows 系统、linux/unix 系统、网络设备。 ●23、支持从 windows AD 域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式。 ●24、支持 Windows AD 域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号。 ●25、支持 windows 系统、网络设备、linux/unix 系统、数据库等设备账号的收集功能。 ●26、支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权。		

				●27、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。 ●28、支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容。 ●29、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。 ●30、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。 ●31、支持自定义多级审批流程，可设置一级或多级审批人，每级审批流程可以指定通过投票数。 ●32、支持紧急运维流程，当运维人员需对目标设备进行紧急运维时，可通过紧急运维流程直接访问目标设备，同时记录为紧急运维工单，便于相关审批人事后对该流程进行确认以及审计员事后查看。 ▲33、支持双人复核登陆，登录时必须经过第二人授权后才能登录，第二人可通过远程授权或同终端授权两种方式实现授权。（投标时需提供产品截图证明并加盖供应商公章） ●34、支持用户访问时间策略、资源访问时间策略、用户 IP 地址策略。 ●35、具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚。 ●36、支持 NTP 系统时间同步配置，保证审计日志拥有可靠的时间戳。 ●37、支持告警对外转发，转发方式支持 syslog、S		

				NMP 等方式。 日志审计 ●38、支持添加、修改、删除资产。 ●39、支持对资产的基本属性进行维护。 ▲40、资产支持组织、地域等各类视图的管理。（投标时需提供产品截图证明并加盖供应商公章） ●41、支持拓扑管理，并能够支持拓扑维度展示整体安全、事件分布、告警分布等。 ●42、系统支持对 IP 对象的自动发现功能，支持 IPv6，对自动发现的设备可以转资产或删除。 ●43、系统支持从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段。 ●44、支持审计对象的定义，包括：审计目标对象、审计行为对象、审计行为执行者对象、审计来源对象、审计时间段对象等。 ●45、支持日志文件备份到外部存储设备，包括 FTP/NFS 等。 ●46、支持按时间范围进行数据备份。 ●47、系统支持以 FTP 上传方式将归档文件存储到第三方存储系统中。 终端安全 ▲48、支持全网风险展示，显示当前未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell 后门数量、高危漏洞及其各自影响的终端数量。（投标时需提供产品截图证明并加盖供应商公章） ●49、支持僵尸网络监控，对发现的恶意域名链接进行一键处置。 ●50、提供勒索病毒整体防护体系入口，直观展示最		

				近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。 ●51、支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等。 ●52、支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组。 ●53、资产登记功能，终端用户可以录入本终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，并可设置哪些为必填项，以便于进行终端资产管理。 ●54、全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示。 ●55、对安装了指定版本操作系统、特定应用软件、开放了高危端口的风险主机进行统计，具备对风险主机进行漏洞扫描、安装高危软件的主机列表信息统计导出、高危端口一键封堵的能力。支持对在线终端下发实时通知消息。 ●56、据统计周期、终端名称、IP 地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志的查询和检测。 ●57、导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议。 ●58、持针对管理控制中心性能，安全事件，勒索病毒事件等邮件告警。		

				●59 灰度升级，可以先指定部分终端或终端组进行更新，避免全网终端一次升级带来的流量风暴。 ●60、客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴。 ●61、持对 zip， rar， jar， cab， 7z 等常见压缩文件的扫描检测。 ●62、持压缩文件层级进行策略配置，最大可配置检查 10 层压缩文件。 ●63、支持配置跳过一定大小的文件，大小范围支持 1M~100M。 数据库审计 ▲64、支持 Hadoop 架构下的数据仓库 HIVE 的审计，能审计到 Hive sql 创建数据库、建表、删除表、修改表结构、创建 / 删除视图、向数据表内加载文件、将查询结果插入到 Hive 表中、基本的查询等操作。（投标时需提供产品截图证明并加盖供应商公章） ●65、支持全文检索数据库 solr 的审计，能审计到 solr 的查询、插入行为的操作信息。 ●66、支持 Hadoop 架构下的大数据库 Hbase 审计，能审计到 JDBC、Native Java API 等接口的调用操作。 ●67、支持 Caché的后关系型数据库的审计，支持 Sqlmanager/WinSql、Studio、 Portal、Terminal、Medtrak 工具的审计，能够审计到 M 语言操作以及返回结果。支持的版本包括：Caché 5.2.4/2010/2015/2016。 ●68、支持对实时数据库 IP21 的审计，可审计到 WEB 操作指令及 API 调用的指令，并且可审计到返回的		

				位号。 ●69、支持数据库嵌套、函数审计(sum 求和函数等)、返回结果、脚本等审计。 ●70、绑定变量：可以审计通过隐藏用户名的绑定变量，包含动态和静态变量的方式访问数据库行为。 ●71、对图形界面运维工具检索后再删除检索出的记录，能够审计到删除的具体记录内容。 ●72、支持端口重定向审计，在服务器端口变化动态协商为其他端口时同样能精确审计。 ●73、支持 B/S 三层架构 http 应用系统 100%精准关联审计，可提取包括应用系统的人员工号（应用层账号）、数据库帐号、操作系统用户名、客户端主机名、客户端 IP、客户端 MAC 在内的“六元组”身份信息，精确定位到人，并可获取 XML 返回结果。 ●74、支持框架：tomcat、apache、weblogic、jboss。 ●75、支持带 COM、COM+、DCOM 组件的三层架构应用审计，可提取包括应用层工号（账号）之内的“六元组”身份信息，精确定位到人。 ●76、支持添加系统语句规则来过滤系统语句，根据系统语句定义规则进行应用层过滤。 ●77、支持白名单管理，根据白名单（条件为 IP/MAC/数据库账户/审计对象/操作语句）定义规则进行应用层过滤）。 ●78、支持 HTTP、FTP、Telnet、SMTP、pop3、nfs 等网络协议的审计。 ●79、支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警。		

				●80、支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警。		
	2	（一）项目技术、实施方案 1、供应商需针对本项目提供项目技术方案，包括但不限于以下内容：①项目的需求分析②重难点分析③5G 组网和内外网改造服务方案④等级保护建设方案⑤网络安全防护建设方案⑥无线组网方案⑦网络运行和业务保障等。 2、供应商需针对本项目提供实施方案，包括但不限于以下内容：①配套设施安装实施方案 ②项目实施组织形式③项目阶段划分及工作结构分解④进度保障措施⑤质量管理措施⑥风险规避措施⑦保密措施⑧售后服务等。 （二）履约能力 1、网络服务能力保障: 供应商能在四川省境内从事相关增值电信和基础电信业务： ①具有《中华人民共和国增值电信业务经营许可证》; ②具有《中华人民共和国基础电信业务经营许可证》或与具有基础电信业务经营许可资质的机构签订的合作协议。 2、供应商 2020 年 1 月 1 日至今类似项目履约经验。 （三）人员要求 1、项目负责人（1 人）：项目负责人具备人社部和工信部颁发的信息系统项目管理师证书。 2、信息安全负责人（1 人）：具有注册信息安全专业人员（CISP）证书，同时具备由国家相关行政主管部门颁发的网络通信安全管理员证书。 3、运维人员（1 人）：具有人社部和工信部颁发的信息系统项目管理师证书。			