政府采购项目采购需求

采购单位：内江市第一人民医院

所属年度：2023年

编制单位：内江市第一人民医院

编制时间：2023年10月27日

一、项目总体情况

（一）项目名称： 内江市第一人民医院更换和增补新老区网络安全设备和安全服务采购项目

（二）项目所属年度： 2023年

（三）项目所属分类： 货物

（四）预算金额（元）：3,000,000.00元 ， 大写（人民币）：叁佰万元整

（五）项目概况：更换和增补医院网络安全设备及安全服务

（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：

·本项目属于以下应当展开需求的情形

·本项目属于以下可以不再重复开展需求调查的情形

（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：竞争性谈判

（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

注：监狱企业和残疾人福利单位视同小微企业。

（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）是否省属高校、科研院所科研设备采购：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

2、预算金额（元）：3,000,000.00，大写（人民币）： 叁佰万元整

最高限价（元）： 3,000,000.00，大写（人民币）： 叁佰万元整

3、评审方法：最低评标价法

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**	信息安全设备	**标的名称**	更换和增补新老区网络安全设备和安全服务
	数量	1.00	**单位**	批
	合计金额（元）	3,000,000.00	**单价（元）**	3,000,000.00
	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：更换和增补新老区网络安全设备和安全服务

参数性质	序号	技术参数与性能指标

一、采购内容

序号	货物名称（标的名称）	数量	是否核心产品
1	零信任安全接入网关	1台	否
2	互联网上网行为管理	2台	否
3	新院区上网行为管理	2台	否
4	准入安全网关	2台	否
5	下一代防火墙	8台	否
6	数据中心防火墙	6台	否
7	**态势感知平台**	**1台**	**是**
8	互联网流量探针	1台	否
9	内网流量探针	2台	否
10	终端安全软件	1套	否

11	网闸	2台	否
12	堡垒机	1台	否
13	日志审计	1台	否
14	网络安全运营保障平台	1套	否
15	API安全监测系统	1套	否
16	数据库审计暨防统方系统	2台	否
17	数据库综合安全防护系统	1台	否
18	网间数据交换系统	1台	否
19	主机电路防护系统	1套	否
20	数据分类分级服务（HIS系统）	1次	否

二、技术指标和配置要求

序号	货物名称(标的名称）	数量（台/套/次）	技术参数	备注
1	零信任安全接入网关	1	1.最大理论加密流量（Mbps）≥300，最大理论并发用户数≥400，接口≥6千兆电口，≥2千兆光口SFP，此次配置≥100个用户接入授权，提供不少于5年的产品质保和软件升级服务； 2.至少支持通过IE8+、CHROME 69+、edge、Firefox、Opera、Safari浏览器、国产操作系统的浏览器、企业微信/钉钉等H5应用内置浏览器、ANDROID、IOS各大手机厂商的自带浏览器接入访问WEB资源，不需采用专属或指定浏览器才能访问； 3.支持以隧道应用方式发布域名资源，日志审计可以记录到URL级别，支持为隧道域名应用添加WEB水印，支持隧道域名应用单点登录功能； 4.满足单位多样化安全便捷认证需求，控制中心在不需要额外搭建认证平台、认证组件的情况下至少支持以下认证方式：本地账号密码认证、LDAP/AD认证、OAuth2.0标准协议的票据认证、CAS标准协议的票据认证、证书认证、HTTP(S)短信认证； 5.支持开启在授信终端环境下/域控环境下/特定网络区域下（即可信的终端或网络环境下），免二次认证； 6.支持本地用户、用户组可直接关联个人应用进行授权； 7.支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复； 8.支持以私有DNS发布资源，无需额外购买DNS服务即可使用域	

					名访问内网资源，支持管理员自主配置是否允许从具体网络区域接入时使用此私有DNS解析地址。（需提供产品功能截图及第三方权威检测机构出具的带CNAS标识的检测报告证明，并加盖投标人公章）； 9.支持本地集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和； 10.可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等； 11.支持分别记录用户访问日志、管理员操作日志以及设备安全日志； 12.为了最大程度缩小网络、业务暴露面，零信任安全接入网关平台需提供单包授权能力（SPA），支持UDP+TCP组合的单包授权技术，未授权用户无法连接零信任安全接入网关，无法扫描到服务端口。（需提供产品功能截图及第三方权威检测机构出具的带CNAS标识的检测报告证明，并加盖投标人公章）	
			互联网上		1.网络层吞吐量≥5.8Gb，应用层吞吐量≥750Mb，支持用户数≥4000，每秒新建连接数≥10000，最大并发连接数≥500000。内存大小≥8G，硬盘容量≥128G SSD+960G SSD，千兆电口≥6，万兆光口≥2，开启802.1x客户端认证、portal认证功能，提供不少于5年的产品质保和软件升级服务； 2.支持网关模式、网桥模式、旁路模式等多种部署模式； 3.支持根据IP、协议、带宽、域用户、域名、应用、DSCP设置选路策略； 4.支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限； 5.管理员能在管理平台首页已接入用户人数、终端类型、流量分析、应用流量排名、泄密风险、共享接入、违规访问等信息；（提供具备CMA资质的检测机构的检测报告证明） 6.支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持设置线路流控策略； 7.管理员能在管理界面分析上网权限策略，并查看各个应用的上网权限与策略是否匹配；（提供产品界面截图并加盖投标人公章）；	

		2	网行为管理	2	8.设备内置应用识别规则库，支持超过9000条应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制； 9.产品应对主流SaaS应用有默认分类标签，支持的SaaS应用数量不少于900种，并且能在管理平台进行统一配置策略；（提供产品截图证明并加盖投标人公章） 10.支持根据IP、端口、协议等自定义应用规则；支持根据端口设定用户不允许访问的目标IP组提供的服务；支持根据不同的应用类型或具体的某种应用设置允许或拒绝； 11.支持根据访问的URL和网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为；支持根据文件类型限制HTTP、FTP方式上传、下载行为； 12.支持禁止使用代理，不允许使用外部HTTP代理，不允许使用外部Socks4/5代理，不允许在HTTP,SSL一些的标准端口上使用其他协议；（提供具备CMA资质的检测机构的检测报告证明） 13.能够与本次采购的终端安全软件实现联动，当设备检测到终端未安装终端安全软件时，对终端进行断网隔离并提示需要安装。（提供产品界面截图并加盖投标人公章）	
					1.网络层吞吐量≥5.8Gb，应用层吞吐量≥750Mb，支持用户数≥1000，每秒新建连接数≥10000，最大并发连接数≥500000。内存大小≥8G，硬盘容量≥128G SSD，千兆电口≥6，开启802.1x客户端认证、portal认证功能，提供不少于5年的产品质保和软件升级服务； 2.支持网关模式、网桥模式、旁路模式等多种部署模式 3.支持根据IP、协议、带宽、域用户、域名、应用、DSCP设置选路策略。 4.支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限； 5.管理员能在管理平台首页已接入用户人数、终端类型、流量分析、应用流量排名、泄密风险、共享接入、违规访问等信息；（提供具备CMA资质的检测机构的检测报告证明）； 6.支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持设置线路流控策略； 7.管理员能在管理界面分析上网权限策略，并查看各个应用的上网	

		3	新院区上网行为管理	2	权限与策略是否匹配；（提供产品界面截图并加盖投标人公章） 8.设备内置应用识别规则库，支持超过9000条应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制； 9.产品应对主流SaaS应用有默认分类标签，支持的SaaS应用数量不少于900种，并且能在管理平台进行统一配置策略；（提供产品界面截图并加盖投标人公章） 10.支持根据IP、端口、协议等自定义应用规则；支持根据端口设定用户不允许访问的目标IP组提供的服务；支持根据不同的应用类型或具体的某种应用设置允许或拒绝； 11.支持根据访问的URL和网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为；支持根据文件类型限制HTTP、FTP方式上传、下载行为； 12.支持禁止使用代理，不允许使用外部HTTP代理，不允许使用外部Socks4/5代理，不允许在HTTP,SSL一些的标准端口上使用其他协议；（提供具备CMA资质的检测机构的检测报告证明） 13.能够与本次采购的终端安全软件实现联动，当设备检测到终端未安装终端安全软件时，对终端进行断网隔离并提示需要安装。（提供产品界面截图并加盖投标人公章）	

			4	准入安全网关	2	1.网络层吞吐量≥5.8Gb，应用层吞吐量≥750Mb，支持用户数≥4000，每秒新建连接数≥10000，最大并发连接数≥500000。内存大小≥8G，硬盘容量≥128G SSD+960G SSD，千兆电口≥6，万兆光口≥2，提供不少于5年的产品质保和软件升级服务； 2.支持网关模式、网桥模式、旁路模式等多种部署模式； 3.支持根据IP、协议、带宽、域用户、域名、应用、DSCP设置选路策略； 4.支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限； 5.支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持设置线路流控策略； 6.支持radius、AD、POP3、Proxy、PPPOE、H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定IP段的用户必须使用单点登录； 7.支持通过钉钉、企业微信等第三方协同办公软件进行授权认证；（提供产品界面截图并加盖投标人公章） 8.不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放； 9.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，可对接外部CA认证服务器进行证书认证，支持在线证书状态查询（OCSP）； 10.对网络接入的终端进行可视化管理，展示终端详细信息、合规状态等，支持查看终端类型，以及终端详细信息（厂商，系统，登录时间等）；（提供产品界面截图并加盖投标人公章） 11.可设置密码最小长度、复杂度，可设置密码不能与用户名相同、新密码不能与旧密码相同； 12.支持发现私接路由（或者共享软件等）共享网络的行为，以IP或用户名的维度统计一段时间内的趋势图； 13.支持与同品牌下一代防火墙系统实现认证联动，可以转发用户认证信息到下一代防火墙，实现单点登录。	

			5	下一代防火墙	8	1.三层吞吐量≥10G，应用层吞吐量≥5G，并发连接数≥200W，新建连接数 (CPS) ≥6W个; 硬件参数:≥8G内存，≥8个千兆电口，≥2个万兆光口，配置≥128GB SSD，配置不少于5年的WEB应用防护识别库、IPS特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和URL&应用识别库定期更新以及防病毒模块（本地或云端）；提供不少于5年的产品质保和软件升级服务； 2.同时支持IPV4和IPV6； 3.具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议； 4.支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护； 5.支持对HTTP/SMTP/POP3/FTP等协议进行病毒防御，支持针对勒索病毒进行检测并开展防御；（提供相关功能截图及“勒索病毒”防护能力检测报告并加盖投标人公章） 6.设备安全日志支持本机存储、Syslog服务器存储、态势感知平台存储等不同形式存储方式； 7.支持针对Cookie的相关攻击进行抵抗，可以在日志体现Cookie被修改等攻击记录；（提供对应功能截图及“Cookie攻击防护“检测报告并加盖投标人公章） 8.支持自定义安全策略，安全策略组功能；可针对源、目的、协议、用户、时间等进行访问控制策略配置； 9.支持策略冗余分析、策略冲突检查、策略包含分析功能； 10.支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容； 11.产品支持对X-Forworded-For的字段进行检测，并对非法源IP进行封锁；（提供产品功能截图证明并加盖投标人公章） 12.支持与安全体系联动，如能够在防火墙产品下发安全策略至终端安全软件对终端进行一键处置，将防火墙产品产生的安全日志等数据上报至态势感知平台等。（提供产品界面截图并加盖投标人公章）	

		6	数据中心防火墙	6	1.三层吞吐量≥35G，应用层吞吐量≥20G，并发连接数≥410W，新建连接数 (CPS) ≥18W个; 硬件参数:≥16G内存，≥16个千兆电口，≥6个万兆光口，配置≥256GB SSD，配置不少于5年的WEB应用防护识别库、IPS特征库、僵尸网络与病毒防护库、漏洞分析识别库和URL&应用识别库定期更新以及防病毒模块（本地或云端）；提供不少于5年的产品质保和软件升级服务； 2.具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议； 3.支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护； 4.支持对HTTP/SMTP/POP3/FTP等协议进行病毒防御，支持针对勒索病毒进行检测并开展防御；（提供相关功能截图及“勒索病毒”防护能力检测报告并加盖投标人公章） 5.设备安全日志支持本机存储、Syslog服务器存储、态势感知平台存储等不同形式存储方式。 6.支持服务器漏洞防护，针对漏洞的扫描攻击可进行IP记录和封锁。（提供产品功能截图及“漏洞防扫描”能力检测报告并加盖投标人公章）； 7.防火墙产品能够对持续变化的未知威胁的检测与防护能力。（提供关于“未知威胁检测”相关证书并加盖投标人公章） 8.产品支持对多重压缩文件进行检测和查杀，至少支持不低于15层的压缩文件查杀； 9.支持多种自定义条件快速查询安全日志，可对IP地址、时间、日志类型、日志严重等级进行查询； 10.针对账号安全能够提供检测与防护，如弱口令、暴力破解检测等； 11.产品支持与安全体系联动，能够在防火墙产品下发安全策略至终端安全软件对终端进行一键处置，将防火墙产品产生的安全日志等数据上报至态势感知平台等； 12.产品具备对CC攻击的防护功能（提供相关功能截图及“CC攻击防护”能力检测报告并加盖投标人公章）。	
					1.配置千兆电口≥4个，内存≥128GB，系统盘≥240GB，数据盘		

		7	态势感知平台	1	≥8*4TB，提供不少于5年的产品质保和软件升级服务； 2.支持大屏展示网络安全态势，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等； 3.支持基于多种检测和分析引擎分析攻击行为，能够针对不同阶段的具体攻击行为展示能力图谱，并能对受其影响的风险资产进行分析和展示； 4.支持跨三层取mac地址，识别资产mac地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题； 5.支持安全基线配置监测，可监测到开放了禁用端口、协议、属性变更等，以IP地址、MAC地址、所属租户和检测到时间来判断是否处置； 6.支持以多种方式对告警进行分类，如人工渗透、业务相关风险、程序的自动化、其他等不同维度，设备可提升威胁定性引擎，可以对告警信息进行多维度的分析（如结合告警的上下文关联、告警的时序关系、告警的历史规律等），结合安全专家的经验以及外部威胁情报等信息，最终对告警的目的性确认，实现告警的优先级； 7.支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法； 8.支持文件、邮件、勒索、挖矿相关安全事件专项页面展示，并能够直接联动处置（自动调用内置处置策略模板），也支持自定义处置流程策略； 9.具备资产主动扫描和被动发现功能，主动扫描支持自动入库、手动入库、扫描目标、定时扫描等功能，包括逻辑拓扑和物理拓扑识别及可视化展示； 10.支持多种告警方式，包括邮件告警、短信告警、声音告警等，保障我院能够在遭受高级威胁时尽快做出处置动作； 11.支持对smtp、imap、pop3、webmail等邮件协议审计，提取邮件正文和附件中的流量，并对邮件附件、正文链接、邮件行为、发件人等多维度进行规则和机器学习检测，从而识别出钓鱼邮件、比特币欺诈、垃圾邮件等恶意邮件； 12.支持与本次采购的下一代防火墙、上网行为管理和终端安全软件进行统一管理和联动处置，至少必须支持通过态势感知平台查看上述设备版本号、设备状态，支持联动下一代防火墙新增黑名单和访问控制	

					策略，支持联动上网行为管理做资产用户名对接，精准识别终端资产责任人，支持联动终端安全软件查询终端、隔离终端、新增访问控制策略、下发扫描任务等。支持联动我单位现有DMZ区超融合平台进行中病毒后的虚拟机自动快照、挂起或关机、分布式防火墙策略自动下发等。（需提供平台能力承诺函，原生支持或通过软件定制的形式均可）	
			8	互联网流量探针	1	1.支持网络层吞吐量≥500Mbps，≥4G内存，配置≥128GB SSD，配置千兆电口≥6个，配置5年特征库服务，提供不少于5年的产品质保和软件升级服务； 2.支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响； 3.支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产IP、提供的服务及其开放的端口、设备类型、操作系统等信息； 4.支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤； 5.支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测； 6.支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况； 7.支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求； 8.支持将流量还原的文件发送至沙盒分析；支持将流量还原的文件发送至沙盒分析； 9.支持流量抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式。	

		9	内网流量探针	2	1.支持网络层吞吐量≥1Gbps，≥8G内存，配置≥128GB SSD，配置千兆电口≥6个，配置千兆光口≥2个，配置5年特征库服务，提供不少于5年的产品质保和软件升级服务； 2.支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响； 3.支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产IP、提供的服务及其开放的端口、设备类型、操作系统等信息； 4.支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤； 5.支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测； 6.支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况； 7.支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求； 8.支持将流量还原的文件发送至沙盒分析；支持将流量还原的文件发送至沙盒分析； 9.支持流量抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式。	
					1.本次需配置PC端授权≥2000个，服务器授权≥300个，提供不少于5年的软件升级服务； 2.管理中心和客户端软件支持虚拟机或硬件环境部署，管理中心具备终端安全监测、事件处置管理、软硬件信息和病毒库更新、查询等能力； 3.支持多重检测能力，包括云端威胁情报、文件沙箱以及智能算法鉴定能力，可通过管理平台查看威胁检测结果和威胁详情； 4.支持针对客户端更新升级的带宽保障，根据实际情况匹配升级策略，避免客户端同时升级对网络造成的堵塞压力和降低高并发数据吞吐对带宽的影响； 5.支持基于单个终端视角的运行状态的监控，包括但不限于进程、服务、网络连接、计划任务和开放共享信息；	

★	1	10	终端安全软件	1	6.可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率； 7.支持勒索可疑行为检测，通过行为智能算法模型能力对勒索命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截； 8.支持流行Windows高危漏洞的轻补丁免疫防御，支持Windows补丁批量一键修复；（提供产品截图证明并加盖投标人公章） 9.支持根据统计周期、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，管理员操作日志，运维日志，联动日志等的日志查询和检测； 10.支持基于IP（组）、服务和角色维度进行配置项设置，并且支持对配置项的备份以及恢复操作； 11.终端安全软件需要支持实体补丁修复、轻补丁免疫、HIPS等漏洞管理和防护技术； 12.支持以可视化形式展现攻击故事，提供可视化的进程树溯源，可直观看出攻击入口、相关操作行为、高危实体文件等信息，协助客户进行事件攻击溯源和研判分析； 13.支持针对终端高级威胁行为（系统层、应用层行为数据与安全日志）数据进行采集，采集数据可以覆盖ATT&CK攻防技战法不少于150项； 14.终端安全软件支持与采购单位现有办公网防火墙进行联动处置，支持终端安全软件进行C2通信的封锁遏制后，将结果同步到现有办公网防火墙，防火墙不再进行重复告警。采购单位现有办公网防火墙下发快速查杀任务，并查看任务状态、终端安全软件进行处置和隔离。（需提供终端安全软件联动能力承诺函，原生支持或通过软件定制的形式均可）	

			11	网闸	2	1.吞吐量≥500Mbps，最大并发连接数≥10万；配置千兆电口≥6个，≥16G内存，配置≥960GB SSD，提供不少于5年的产品质保和软件升级服务； 2.外网端不允许配置任何形式的管理接口，所有管理配置操作均通过专用的网闸内网可信端管理接口进行配置； 3.设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署；（提供产品功能截图并加盖投标人公章） 4.产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC模块、MODBUS模块、组播代理模块、用户自定义应用模块等各类应用模块，并可控制相应应用协议的动作、参数、内容； 5.支持的数据库种类包括ORACLE、SQLSERVER、MYSQL、SYBASE等主流数据库支持多种关系型数据库通信，支持SQL语句的白名单和黑名单； 6.支持平台级联及平台点播，支持GB 28181视频通信国家标准及相关厂商协议规范； 7.支持TCP应用层数据单向传输的控制，保证TCP应用数据的零反馈，以满足二次防护对数据传输的安全性需求，可编辑安全通道，指定区域方向等； 8.支持DCS/SCADA生产网络与办公网络之间的OPC应用数据的传输。支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输； 9.支持TCP/IP以上的应用层协议，支持自定义的TCP、UDP协议的数据隔离交换，以用户定制的命令、参数等协议解析方式来解析自定义应用的通信内容； 10.系统可存储和审计包含：系统日志；管理日志；网络活动日志；入侵报警及处理日志；访问控制日志。	

12	堡垒机	1	1.本次配置运维授权数≥300，图形运维最大并发数≥200；字符运维最大并发数≥350，配置千兆电口≥6个，万兆光口≥2，硬盘容量≥2T SATA，提供不少于5年的产品质保和软件升级服务； 2.系统各模块访问过程中采用https等加密方式，支持B/S架构方式管理； 3.支持通过客户端配置动作流程，实现大量应用接入支持，通过动作流程配置可以不受接入资源登录设计影响，实现审计接入和单点登录。 4.支持对用户信息进行批量导出与导入；支持用户对角色进行编辑、增添、消除等；支持对用户的有效期进行设定，并可对登录指定认证方式； 5.用户可以针对证书配置类型进行禁用与启用，支持自主CA等方式；并支持AD、LDAP、手机动态令牌、短信、双因子等认证登录方式；（提供产品功能截图并加盖投标人公章） 6.支持对用户指定限制登录IP、登录时间段（可反复，如每星期一到星期五8：00-18：00时）等规则； 7.支持对控制台的登录会话时间进行监测，可会话时间设定阈值，用户在阈值内无操作则会对会话进行自动注销； 8.支持RDP远程传输协议设置，并可在安全模式下对rdp、any等进行配置； 9.支持对应急事件运维流程进行自定义开启、关闭，当应急事件发生时，可通过应急通道访问到目标设备，系统可记录为紧急工单，方便事后主管人员进行审批与查看。	

		13	日志审计	1	1.2U标准机架式设备，配置≥6个千兆电口，≥2个万兆光口，内存≥32GB，硬盘≥2*4TB SATA，日志处理性能≥3500EPS，提供≥300个审计对象的授权，提供不少于5年的产品质保和软件升级服务； 2.支持对多种类型日志的全面采集、集中存储、关联分析，支持网络设备、安全设备、操作系统、中间件、数据库、服务器等多种审计数据源的日志采集； 3.系统支持多种日志采集的方式，如Syslog、SNMP Trap、Kafka等协议被动采集，支持文件读取、JDBC等方式主动采集； 4.支持对采集策略和规则进行自定义，支持多种自定义规则类型，如正则表达式、xml、分隔符以及json，支持对字段进行解析，对解析结果字段进行合并、新增与删除； 5.支持对数据源的日志进行分析过滤，可设立多个条件规则过滤无效日志，过滤字段可包括数据来源设备、目的IP/端口、源IP/端口、事件名称、URL、事件ID、协议等； 6.支持采用传输层安全性协议TLS进行加密，支持对日志传输状态进行监控，包括最近同步时间、今日日志传输量和传输总量等； 7.可对日志进行定级、分类；系统保留归一化后的日志的同时也保留原始日志，方便用户对原始日志快速定位和取证。 8.支持用户按角色管理，支持三权分立；支持设立系统管理员、审计管理员和安全管理员； 9.支持测试工具新建数据测试任务，通过设定日志生成时间、源IP和解析规则一键生成数据； 10.支持对IPv6/IPv4资产的发现和日志源的日志进行采集。	
					1.提供网络安全运营保障平台，提供不少于5个角色设定，对招标方≥50个核心信息化资产，≥2000个PC提供365天*24小时实时网络安全威胁监测预警、事件闭环管理、脆弱性分析闭环等保障措施；实时监测招标方信息化资产的网络安全状态，对安全事件自动化生成工单，及时进行分析、预警，闭环，提供不少于5年的服务期限，每年提供≥6次线下上门协助处置，处置内容需符合用户要求，且每次服务后需用户验收；提供≥1周的线上重要保障服务，线上重要保障服务资产范围≥50资产； 2.提供独立的SAAS化的安全检测与响应平台工具（非网络安全运		

					营保障平台），平台数据采集流量授权≥3000Mbps，服务器日志采集授权≥300个，提供不少于5年的使用期限，不少于5年的产品质保和软件升级服务且安全告警及日志聚合为安全事件的效率需满足用户需求； 3.支持对招标方的安全现状进行评估，全面梳理漏洞、弱口令、潜伏威胁、安全事件、攻击行为、失陷主机、互联网暴露面等；要求招标方具备互联网暴露面梳理模块，该模块支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP地址、开放端口、资产指纹、网站截图、移动端暴露面、暴露资产的访问截图、对应暴露资产存在的漏洞等； 4.支持对招标方信息资产进行系统脆弱性和Web漏洞全量扫描，并验证漏洞发生的风险、分析发生后可造成的危害，并提供详细的举证信息及可落地建议，针对高危可利用漏洞能够自动匹配漏洞防护规则；要求招标方可以对核心资产的每一个高危可利用漏洞自动化匹配防护规则； 5.支持对威胁进行检测和分析，收集招标方安全设备和工具的告警和日志，对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，分析判断受影响范围及是否攻击成功，将分析的结果通过微信或邮件等方式提醒招标方，同时将各类安全事件自动生成工单，并在工单中展示告警/事件的基本信息，涉及用户的业务信息、威胁举证、攻击趋势等内容； 6.支持实时抓取互联网最新漏洞威胁情报和事件情报，并与招标方信息资产信息进行匹配后向招标方进行精准推送，提供可落地安全加固建议； 7.支持对招标方的安全设备策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果； 8.支持针对主机发生的安全事件开展调查分析和影响面分析，对发生的安全事件进行二次鉴定和举证分析；对招标方信息资产爆发勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，匹配对应工具和脚本对恶意文件、代码进行根除，消除或减轻影响，闭环事件；	
		14	网络安全运营保障平台	1	9.为了降低招标方因网络安全事件造成的损失和影响，按照国家标准对安全事件的分类分级指南，投标方提供的安全运营保障平台需要具备如下能力（提供平台能力承诺函，并承诺可作为合同附件进行签署，		

					并加盖投标人公章）： (1)从安全日志产生到事件通告，重大安全事件通告时间小于30分钟，一般事件的通告时间少于1小时； (2)高级威胁的处置完成时间少于1小时，一般威胁的处置完成时间少于4小时； (3)通告给招标方的各类安全事件的准确率不低于99%； (4)所有安全事件的闭环处置比例达到100%； (5)对信息资产发现的每一个高危可利用漏洞提供防护规则，防护率达到99% 10.支持导出安全保障相关报告，每周导出一次《安全运营周报》，每月导出一次《安全运营月报》，每季度导出一次《安全运营季报》，每年导出一次《安全运营年度报告》，按需触发导出《漏洞清单》、《威胁情报通告》； 11.支持对安全运营质量监管能力，支持通过可视化的数据，清晰展示某段时间的安全运营达标率，包括脆弱性的闭环率、威胁闭环率、事件闭环率； 12.安全运营保障平台支持对接招标方本次采购的主要安全设备，下一代防火墙、数据中心防火墙、态势感知平台、终端安全软件，支持实时接收安全设备检测到的安全事件信息、安全日志数据； 13.安全运营保障平台需包含提供安全检测与响应模块能力，支持对事件等级、事件来源、事件定性、威胁标签、数据源、处置状态等进行快速筛选，支持安全事件详情查看攻击故事链，以可视化链形式展示安全事件按照攻击入口和进程树的视角进行安全分析；支持安全领域GPT的智能问询能力，支持用户通过自然语言对话框交互方式，对平台安全事件、告警的分析进行智能问答，辅助招标方提升安全运营的效率；（提供投标人承诺函） 14.安全运营保障平台需包含提供安全检测与响应模块能力，支持详细点开进程链中任意进程查看进程详情，包括基础信息、威胁告警、网络连接行为、文件行为、域名访问行为、模块加载行为，并且自带解码工具； 15.安全运营保障平台需包含提供安全检测与响应模块能力，安全事件可按照时间轴查询事件聚合相关的告警举证信息，可展示关联关系		

					，且支持时间向前向后的风险全局调查； 16.安全运营保障平台需包含提供安全检测与响应模块能力，支持对安全事件推送处置和响应建议，响应建议包括原理介绍、危害影响、处置建议。通过建议描述、业务影响标签和安全效果标签清晰明确指导下一步响应动作，可一键封禁IP、隔离主机等。	
			15	API安全监测系统	1	1.单台流量采集处理能力不低于5Gbps，双向还原能力不低于2Gbps； 2.单台设备分析处理能力不低于10000条日志/秒；支持不少于100套业务系统数据；支持不少于50000条敏感API资产数据； 3.支持访问行为发生后2分钟内有效查询到相应的访问日志记录，且查询响应时间不超过20秒。访问日志记录错漏比例不高于1%，访问时间记录误差不超过10秒； 4.支持Agent引流，运行时CPU占用率低于3%，内存占用小于100M，程序文件小于10M（提供截图并加盖投标人公章） 5.支持Office/wps办公文件；支持网络文件；支持压缩文件/分卷压缩文件；支持多层嵌套压缩；（提供截图并加盖投标人公章） 6.支持webservice、restful等API协议识别；支持登录接口、文件上传、文件下载、数据查询等业务标签识别；（提供截图并加盖投标人公章） 7.内置不少于多种安全监测场景，实现API脆弱性风险监测、API异常行为监测、API备案信息监测；	

			16	数据库审计暨防统方系统	2	1.CPU：16核32线程，内存≥64GB，硬盘：≥4TB SATA企业级硬盘*2,≥SSD 240G*1企业级，≥千兆光口*2，集成≥2个100/1000M自适应以太网口，电口*2； 2.采用SSD、HDD多级存储架构，系统和业务数据分离，实现高效、安全存储； 3.性能指标：峰值事件处理能力不低于30000条语句/秒，日志存储不低于24亿条； 4.支持后关系型数据库Cache的集成工具Terminal、Portal、Studio、Sqlmanager、MedTrak工具的审计；Portal能审计到Sql语句、查询Global有返回结果；Sqlmanager支持根据SQL ID提取高效审计； Terminal能审计到SQL语句和返回结果,并支持本地审计；基于C/S的MedTrak工具能审计到操作报表的具体返回结果；（提供截图并加盖投标人公章） 5.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；（提供截图并加盖投标人公章） 6.支持Oracle、SQLServer、MySQL、DB2、PostgreSQL 、Cache、Portal、Informix、Samba、达梦、人大金仓、南大通用等数据库的审计，且支持多种不同的数据库同时审计。 7.系统自带各种常见HIS防统方规则库，且规则数量≥500条以上；支持杭创、键讯、金蝶慧通、用友、中联、阳光用药、天健、厦门智业、科进、中天、天网、方正、东华、金仕达、东软、陕西医星、长城、广州力锦等HIS的防统方审计； 8.支持特定时间区间内抗菌药，药剂及耗材的种类，型号，规格，用量，价值的排名统计，并生成报表（提供截图并加盖投标人公章）	

17	数据库综合安全防护系统	1	1.峰值事件处理能力不低于15000条语句/秒,并发连接数≥2000； 2.支持代理模式，可代理数据库，实现系统采集到数据库流量； 3.支持数据库IRIS、Caché数据库等特殊应用场景下的数据库安全审计；（提供截图并加盖投标人公章） 4.支持基于SQL语法解析实现SQL操作的风险识别能力，非正则方式模糊匹配； 5.支持后关系型数据库Cache的集成工具Terminal、Portal、Studio、Sqlmanager、MedTrak工具的审计；Portal能审计到Sql语句、查询Global有返回结果； Sqlmanager支持根据SQL ID提取高效审计； Terminal能审计到SQL语句返回结果,并支持本地审计；基于C/S的MedTrak工具能审计到操作报表的具体返回结果；（提供截图并加盖投标人公章） 6.已阻断行为支持审批放行，针对某个数据库设置放行规则，支持操作类型、关键字、访问工具、客户端IP、正则表达式、返回行数阈值等条件设置放行规则，实现灵活管控数据库操作行为，满足特殊运维场景的需要； 7.支持针对利用已公开的数据库漏洞攻击行为进行拦截的虚拟补丁功能；（提供截图并加盖投标人公章） 8.支持操作语句系列的组合规则，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；	

18	网间数据交换系统	1	1. 产品交付形式为软件，100用户并发文件交换授权，注册用户不限； 2.产品本身支持被审计，支持对管理账号细粒度权限的配置，系统的配置和变更有日志记录。有审计账号，能对其他账号的行为进行审计； 3.产品在不依赖其他产品的情况下，能够实现在不同网络间的数据安全交换，且交换中能够断开TCP/ip协议，使用自有通信协议，不引入风险，并能提供自主知识产权证明文件副本； 4.产品能提供方便员工使用的界面，产品可提供浏览器页面（B/S）或客户端（C/S）界面，不需要进行额外的界面开发或与公司内部可视化界面系统集成的开发工作； 5.在文件传输交换时，产品能对文件进行病毒和木马检测，识别可能导致系统风险的恶意文件。一旦发现可疑文件，可自动阻止文件交换至其他网络； 6.系统自带敏感文件内容识别功能，不依赖于第三方产品，文件传输过程中，能根据敏感数据定义标准，对敏感文件的传输行为进行识别。能识别加密的文件（如WINRAR密码压缩后的文件）；能识别内嵌文件中的敏感信息（如word文件内部嵌入的敏感文件）； 7.产品支持对个人的文件交换行为进行审计，审计信息包括，上传时间、文件名称、用户名称，操作类型（上传文件、下载文件、删除文件、新建目录、共享文件、移动文件）、终端IP/MAC、终端位置（外网、内网）、源/目的文件路径、终端名称等信息；且支持内容审计； 8.管理员设置某个部门具有采集外链权限，具有采集权限的内部人员文件所有者需通过生成Web链接的方式将文件夹分享给外部人员，并设置链接的有效期，外部人员可以访问链接和密码验证来上传文件；可配置邮件平台通知接收收集外链的人员去上传； 9.产品可灵活设置审批策略，如：人工单向审批、人工多向审批或自动审批等。开启人工审批功能后，可关联至特定的岗位角色负责数据审批。且需提供接口，支持与邮箱系统集成，从而实现审批；	

19	主机电路防护系统	1	1.采用微控制器主控芯片； 2.设备结构为多功能软硬件一体机，非多个设备组合，标准19英寸机架式安装，机箱挂耳可拆卸，占用机柜高度≤1.5U；提供不少于5年的产品质保和软件升级服务； 3.设备标配通讯接口至少RJ45、WIFI、4G；标配网络防雷接口≧2路、接地通路接口≧2路、RS485接口≧4路、漏电监测接口≧4路、开关量输入接口≧2路、USB接口≧2路、HDMI接口≧1路、电源输出接口≧4路国标插座； 4.支持防雷击防浪涌功能，最大放电电流Imax(8/20μs)≧40kA，电压保护水平Up≦1.7kV；支持监测功能至少包含：电流、电压、功率、断电、接地通断监测、漏电监测、防雷器状态、防雷器温度、防雷器寿命、环境温湿度、水浸、烟雾等监测；（提供第三方权威机构CNAS和CMA标志检测报告并加盖投标人公章） 5.设备标配≧2.4寸触摸显示屏，可显示监测指标信息，屏显内容包括：电压、电流、频率、功率、雷击浪涌次数、防雷器状态、防雷器温度、防雷器寿命、接地通断、漏电监测、温湿度、烟雾、水浸、安装单位、联系人、联系电话；可通过手机扫描屏显电子二维码进行关注、查询、故障报修；（提供第三方权威机构CNAS和CMA标志检测报告并加盖投标人公章） 6.支持供电BYPASS功能，即使本机系统出现问题或者系统重启也不影响正常输出供电，以保障用电设备稳定运行；（提供第三方权威机构CNAS和CMA标志检测报告并加盖投标人公章） 7.设备内置告警扬声器≧1个，具有系统、网络、入网状态指示灯，告警方式支持本机扬声器告警、手机微信告警、管理平台告警；（提供第三方权威机构CNAS和CMA标志检测报告并加盖投标人公章） 8.管理方式支持Web管理； 9.内置时钟和存储； 10.提供云管理平台，平台支持远程监控、管理、运维； 11.云管理平台支持对监测指标实时查询、数据云存储、备份、数据分析、GIS地图展示、多级用户权限管理。	

20	数据分类分级服务（HIS系统）	1	通过“人工+工具”模式，在数据定义及分类分级基础上，为采购单位HIS系统提供数据资产分布识别、数据流转情况梳理、数据脱敏情况识别、数据安全管控措施梳理等服务，协助采购单位摸清家底，形成数据资产目录；设备安装调试完毕后为采购单位提供1次本项服务。	

三、商务要求

1.交货期及交货地点

（1）交货时间：合同签订生效后，在接收到采购人正式通知的前提下90日完成安装调试，并交付采购人验收。

（2）交货地点：内江市第一人民医院指定地点。

2.质量保证

（1）投标人提供的设备必须符合国家质量标准，并具有设备生产企业质量检验合格证明。投标人所提供的设备在有效期内出现质量问题，要按质量承诺，由投标人负责退换货，并承担各项税、费或其他支出，并根据“违约责任与解决争议的方法”承担相应违约责任。投标人应保证其设备在正确安装、正常使用和维护条件下性能良好。

（2）投标人应保证所供设备是全新的、未使用过的，标识清楚，权属清楚，原产地真实，必须符合或优于国家（行业）标准，并完全符合相关采购文件规定的质量、规格和性能的要求，不得以假充真，以次充好。投标人须提供和设备性能参数匹配的光模块和光纤等配件，不得因配件性能导致设备性能降低。

（3）在设备验收后的使用中，有证据证明该设备存在重大的设计、工艺或材料缺陷,包括潜在缺陷的，投标人应当对由于上述缺陷造成的故障负责，采购人有权据此提出退货、退款或投标人承担相应的损失赔偿。

（4）中标供应商需在收到中标通知书后7个工作日内提供生产厂家对采购设备提供完整质保的承诺函或相关协议。（投标人需单独提供承诺函）

3.售后服务

（1）所有产品质保期从验收合格之后开始计算，技术参数中未明确质保期的产品，产品质保期为验收合格后≥3年（含整机所有部件，但不包括耗材和易耗品），质保期内出现质量问题，投标人在接到通知后24小时内响应，48小时内到场，质保期内投标人提供免费维修服务，如需更换零配件，投标人应保证所更换的零配件为原厂原装全新的零配件，费用包括在合同总价中。

（2）产品软件升级特别约定：投标人承诺所供设备上安装的软件已获得软件厂商的正规授权；若设备软件有升级版本时，投标人承诺及时为甲方提供免费升级服务。

（3）维修期间，根据采购人需求，投标人应向采购人提供替用设备。

（4）提供售后服务期间，投标人有专人负责售后服务，投标人人员应当遵守采购人的规章制度，尽职尽责，提供最优质的服务，应尽安全注意义务，避免不必要的损失，维保期间因投标人人员造成采购人或者第三人损失的，由投标人承担责任。

8、供应商一般资格要求

注：标注“★”的条款为本项目的实质性条款，投标人不满足的，将按照无效投标处理。

序号	资格要求名称	资格要求详细说明
1	具有独立承担民事责任的能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
2	具有良好的商业信誉	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
3	具有健全的财务会计制度。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
4	具有履行合同所必需的设备和专业技术能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
6	参加政府采购活动前三年内，在经营活动中没有重大违法记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。

序号	资格要求名称	资格要求详细说明
7	不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。

9、供应商特殊资格要求

序号	资格要求名称	资格要求详细说明
无		

10、分包的评审条款

评审项编号	一级评审项	二级评审项	详细要求	分值	客观评审项

11、合同管理安排

1）合同类型：买卖合同

2）合同定价方式：固定总价

3）合同履行期限：自合同签订之日起90日

4）合同履约地点：采购人指定地点

5）支付方式：分期付款

6）履约保证金及缴纳形式：

中标/成交供应商是否需要缴纳履约保证金：否

7）质量保证金及缴纳形式：

中标/成交供应商是否需要缴纳质量保证金：否

8）合同支付约定：

1、 付款条件说明： 如中标供应商为中小企业的，签订合同后5日内支付预付款，支付合同总金额的50%作为预付款；如中标供应商为非中小企业的，签订合同后支付预付款 ，达到付款条件起 30 日，支付合同总金额的30.00% ，达到付款条件起 30 日内，支付合同总金额的 30.00 %；

2、 付款条件说明： 如中标供应商为中小企业的，全部货物安装调试完毕并验收入库后，且收到供应商出具合法有效完整的完税发票及凭证资料后支付，支付合同总金额的50%；如中标供应商为非中小企业，付款条件为：完成全部货物安装调试完毕并完成初步验收 ，达到付款条件起 30 日，支付合同总金额的20.00% ，达到付款条件起 30 日内，支付合同总金额的 20.00 %；

3、 付款条件说明： 若中标供应商为非中小企业的，全部货物安装调试完毕验收入库后，进入设备测试运行阶段，设备稳定运行并达到6个月后视为可正常运转，且完成最终验收。设备可正常运转且收到供应商出具合法有效完整的完税发票及凭证资料后进行支付；达到付款条件后30日内进行支付，支付合同总金额的50% ，达到付款条件起 30 日内，支付合同总金额的 50.00 %；

9）验收交付标准和方法：（1）交货时间：合同签订生效后，在接收到采购人正式通知的前提下60日完成安装调试，

并交付采购人。（2）交货地点：内江市第一人民医院指定地点。（3）投标人负责产品安装、调试，直至采购人能正常使用，所需的一切材料、备件、专业工具均由投标人负责提供。投标人应向采购人提供产品安装、维修所需的专用工具和仪器，所涉及的价格包括在报价总价格中。（4）货物到达生产现场后，投标人接到采购人通知后2日内到达现场组织安装、调试，达到正常运行要求，保证采购人正常使用。所需的费用包括在报价总价格中。（5）投标人应就产品的安装、调试、操作、维修、保养等对采购人维修技术人员进行培训。产品安装调试完毕后，投标人应对采购人操作人员进行现场培训，直至采购人的技术人员能独立操作，同时能完成一般常见故障的维修工作。（6）必须保证提供的货物(包括零部件)是全新的、未使用过的，具有稳定性、可靠性、安全性，并完全符合国家、行业规定的质量、规格和性能要求等技术标准。（7）验收标准：严格按照相关法律法规以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205 号）的要求进行验收。（8）验收流程： 1.验收由甲方组织，乙方配合进行： 1.1如中标供应商为中小企业的，货物在投标人通知安装调试完毕后 15 日内初步验收。初步验收合格后，进入【 7 】日试用期；试用期间发生重大质量问题，投标人应更换全新设备，重新提供设备后试用期开始重新计算；试用期结束后 15 日内采购人完成最终验收，并在收到投标人出具合法有效完整的完税发票及凭证资料后支付剩余款项； 1.2如中标供应商为非中小企业的，货物在投标人通知安装调试完毕后 15 日内初步验收。初步验收合格后，进入6个月试用期；试用期间发生重大质量问题，乙方应更换全新设备，重新提供设备后试用期开始重新计算；试用期结束后 15 日内采购人完成最终验收，并在收到投标人出具合法有效完整的完税发票及凭证资料后支付剩余款项；1.3验收时如发现所交付的货物有短装、次品、损坏或其它不符合标准及本合同规定之情形者，甲方应做出详尽的现场记录，或由甲乙双方签署备忘录，此现场记录或备忘录可用作补充、缺失和更换损坏部件的有效证据，由此产生的时间延误与有关费用由乙方承担，验收期限相应顺延； 1.4如质量验收合格，双方签署质量验收报告。

10）质量保修范围和保修期：（1）所有产品质保期从验收合格之后开始计算，技术参数中未明确质保期的产品，产品质保期为验收合格后≥3年（含整机所有部件，但不包括耗材和易耗品），质保期内出现质量问题，投标人在接到通知后24小时内响应，48小时内到场，质保期内投标人提供免费维修服务，如需更换零配件，投标人应保证所更换的零配件与原设备相同规格和品质且是全新的零配件，费用包括在合同总价中。（2）产品软件升级特别约定：投标人承诺所供设备上安装的软件已获得软件厂商的正规授权；若设备软件有升级版本时，投标人承诺及时为甲方提供免费升级服务。（3）维修期间，根据采购人需求，投标人应向采购人提供替用设备。（4）提供质保服务期间，投标人有专人负责售后服务，投标人人员应当遵守采购人的规章制度，尽职尽责，提供最优质的服务，应尽安全注意义务，避免不必要的损失，维保期间因投标人人员造成采购人或者第三人损失的，由投标人承担责任。

11）知识产权归属和处理方式：1、投标人应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。 2、 采购人享有本项目实施过程中产生的知识成果及知识产权。 3、投标人如欲在项目实施过程中采用自有知识成果，需在投标文件中声明，并提供相关知识产权证明文件。使用该知识成果后，投标人需提供开发接口和开发手册等技术文档，并承诺提供无限期技术支持，采购人享有永久使用权（含采购人委托第三方在该项目后续开发的使用权）。 4、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法获取该知识产权的相关费用。

12）成本补偿和风险分担约定：本项目为固定总价，不进行成本补偿,因市场变化或政策变化造成的潜在风险，由甲

乙双方协议商定。

13）违约责任与解决争议的方法：违约责任： 甲方违约责任：1.采购人无正当理由拒收货物的，采购人应偿付合同总价百分之五的违约金； 2.采购人偿付的违约金不足以弥补乙方损失的，还应按乙方损失尚未弥补的部分，支付赔偿金给乙方。 3.因采购人自身原因延期付款或导致变更、中止或者终止采购合同的，采购人应对乙方的损失予以补偿。 乙方违约责任：1、中标供应商交付的设备质量不符合合同规定的，在约定的交货时间内经 1 次调换仍不能达到合同约定的质量要求，不能通过验收的，采购人有权单方面解除合同，剩余合同金额采购人不再支付，采购人有权要求中标供应商返还已支付的货款。且中标供应商应当按照合同总价的 10%向采购人支付违约金。 2、质保期内出现质量问题，经 2 次维修仍不能达到合同约定的质量要求，采购人有权单方面解除合同，并要求退货，要求中标供应商返还已支付的货款及支付货款对应的利息（其利率按全国银行间同业拆借中心公布的1年期贷款市场报价利率（LPR） 计算），中标供应商还应当按照合同总价的 10%支付违约金。3、中标供应商逾期交付设备，每逾期一天，须向采购人支付合同总额千分之三的违约金。中标供应商逾期交货超过 60 天，采购人有权单方面解除合同，有权要求中标供应商返还已支付的相应货款。且中标供应商应当向采购人累计支付违约金。 4、中标供应商在安装调试设备过程中以及售后服务等服务过程中，因未按操作规程施工、操作不当、未采取必要的安全防范措施等原因直接或间接造成采购人及第三方人身人身损害或财产损失的，由中标供应商承担全部责任。 5、如果中标供应商在接到采购人通知后，在本合同第三条第 1 款中写明的响应时间内,没有弥补缺陷，采购人可采取必要的补救措施，但由此而产生的风险责任和费用由中标供应商负担，采购人根据合同规定对中标供应商行使的其他权利不受影响。 6、中标供应商保证本合同设备的权利无瑕疵，包括设备所有权及知识产权等权利无瑕疵。如任何第三方经法院（或仲裁机构）裁决有权对上述设备主张权利或国家机关依法对设备进行没收查处的，中标供应商除应向采购人返还已收款项外，还应另按合同总价的 10%向采购人支付违约金并赔偿因此给采购人造成的一切损失。 7、若采购人单方面解除合同，则解除通知到达中标供应商时，本合同即解除。若双方协商解除合同的，则应当签订解除协议。 8、中标供应商因上述违约行为支付的违约金不足以弥补采购人损失的，还应按采购人实际经济损失足额补足。 解决争议办法： 1、因货物的质量问题发生的争议，由法定质量鉴定机构或其认可的质量鉴定机构进行质量鉴定。货物符合标准的，鉴定费由采购人承担；货物不符合质量标准的，鉴定费由乙方承担。 2、合同履行期间,若双方发生争议，可协商或由有关部门调解解决，协商或调解不成的，可向采购人所在地人民法院依法提起诉讼。

14）合同其他条款：1、质量保证 （1）投标人提供的设备必须符合国家设备质量标准，并具有设备生产企业质量检验合格证明。投标人所提供的设备在有效期内出现质量问题，要按质量承诺，由投标人负责退换货，并承担各项税、费或其他支出，并根据第八条承担相应违约责任。投标人应保证其设备在正确安装、正常使用和维护条件下，在其使用寿命期内应具有满意的性能。 （2）投标人应保证所供设备是全新的、未使用过的，标识清楚，权属清楚，原产地真实，必须符合或优于国家（行业）标准，并完全符合相关采购文件规定的质量、规格和性能的要求，不得以假充真，以次充好。 （3）在设备验收后的使用中，有证据证明该设备存在重大的设计、工艺或材料缺陷,包括潜在缺陷的，投标人应当对由于上述缺陷造成的故障负责，采购人有权据此提出退货、退款和/或相应的损失赔偿。 2、包装和运输 （1）成交投标人须严格按照《商品包装政府采购需求标准(试行)》、《快递包装政府采购需 求标准(试行)》(财办库〔2020〕123 号)的要求进行产品及相关快递服务的包装。 （2）投标人应当按照约定的方式交付标的物。对于包装方式没有约定或者约定不明确的，应当按照通用的方式包装；没有通用方式的，应当采取足以保护标的物且有利于节约资源，保护生态环境的包装方式。 （3）本次采购的标的物需要运输，投标人在合同约定的时间内将标的物运输至合同约定地点。 （4）投标人按照约定将标的物运送至采购人指定地点并完成交付的

或采购人违反约定不予收取的，标的物损毁、灭失的风险由采购人承担。

12、履约验收方案

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：否

5）是否邀请第三方检测机构：否

6）履约验收程序：一次性验收

7）履约验收时间：

供应商提出验收申请之日起30日内组织验收

8）验收组织的其他事项：无

9）技术履约验收内容：采购人按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）以及本项目合同的要求进行验收。

10）商务履约验收内容：采购人按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）以及本项目合同的要求进行验收。

11）履约验收标准：采购人按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）以及本项目合同的要求进行验收。

12）履约验收其他事项：无

五、风险控制措施和替代方案

该采购项目按照《政府采购需求管理办法》第二十五条规定，本项目是否需要组织风险判断、提出处置措施和替代方案：否