

政府采购项目采购需求

采购单位：盐源县职业技术中学校

所属年度：2023年

编制单位：盐源县职业技术中学校

编制时间：2024年01月17日

一、项目总体情况

- (一) 项目名称：信息化建设及社会培训基地建设采购
- (二) 项目所属年度：2023年
- (三) 项目所属分类：货物
- (四) 预算金额（元）：1,800,000.00元，大写（人民币）：壹佰捌拾万元整
- (五) 项目概况：本项目共1个包，为盐源县职业技术中学校信息化建设及社会培训基地建设采购项目。
- (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：政府集中采购
- (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）：1,800,000.00，大写（人民币）：壹佰捌拾万元整

最高限价（元）：1,800,000.00，大写（人民币）：壹佰捌拾万元整

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	盐源县职业技术中学校信息化建设及社会培训基地建设采购项目
	数量	1.00	单位	批
	合计金额（元）	1,800,000.00	单价（元）	1,800,000.00
	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	信息传输业

标的名称：盐源县职业技术中学校信息化建设及社会培训基地建设采购项目

参数性质	序号	技术参数与性能指标				
		序 号	采购项目 名称	技术参数要求	单 位	数 量

★	1	<p>1.主码流支持不低于1920x1080P，子码流支持不低于704x576P，第三码流为不低于704*576P；设备靶面尺寸为不低于1/2.8英寸；</p> <p>2.最低照度彩色不大于0.005 lx，黑白不大于0.001 lx；</p> <p>3.支持水平0°~ 360°，连续旋转；垂直 -15°~ 90°；支持300个预置位，可按照所设置的预置位完成大于8条巡航路径。支持预置位视频冻结功能；</p> <p>4.具有H.264、H.265、MJPEG设置选项，可将H.264、H.265格式设置为High Profile/Main/Baseline；</p> <p>5.在网络直连的环境下，只输出主码流，分辨率设置为1920x1080、帧率设置为25fps、码率设置为2Mbps时，网络协议为UDP、最短延时、智能分析关闭时，视频图像传输至客户端的延时时间≤65ms；</p> <p>6.夜间天气晴朗无遮挡，红外补光灯开启，可识别距离设备不少于100m处的人体轮廓；</p> <p>7.设备在专用聚焦模式下具有至少3种聚焦功能：前景聚焦、背景聚焦、区域聚焦；</p> <p>8.设备支持防雨帽檐、不少于1个RJ45网络接口、不少于1路音频输入接口、不少于1路音频输出接口、不少于1路报警输入接口、不少于1个SD卡插槽。设备采用DC12V供电。</p> <p>★9.要求和原有监控系统融合，本次采购的设备接入原有监控系统品牌。（提供承诺函并加盖投标人公章）</p>	台 5 3
---	---	---	-------

			<p>1.交换容量≥300Gbps/3Tbps；包转发率≥25Mpps/100Mpps；（提供官网截图证明）</p> <p>2.千兆POE电口数≥8个，千兆SFP光口≥4个；支持IEEE 802.3af/at供电标准，整机最大输出功率≥120W；</p> <p>3.支持M-LAG技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面；（提供具有CMA或者CNAS标志的第三方机构测试报告）</p> <p>4.支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时灵活的进行切换；（提供具有CMA或CNAS标志的第三方机构测试报告）</p> <p>5.支持零配置上线，支持二层广播自动发现网管中心平台；支持配置静态IP地址三层发现网管中心平台；支持DHCP Option 43方式发现网管中心平台；支持DNS域名发现网管中心平台；（提供具有CMA或CNAS标志的第三方机构测试报告）</p> <p>▲6.支持终端类型库，基于指纹自动识别PC、路由器、摄像头设备等；（提供平台终端类型识别库截图证明，提供具有CMA或CNAS标志的第三方机构测试报告）</p>		台	1	
		3	POE交换机2	1.8口POE交换机。		台	9
		4	服务器存储	1.机架式/8U 48盘位/1536Mbps接入带宽/本次含24块8T企业级SATA硬盘/64位多核处理器/4GB缓存（可扩展至128GB）/4个千兆数据网口/1个千兆管理网口/冗余电源/网络协议：RTSP/ONVIF/PSIA/（GB/T28181）。		台	1
		5	采购项目名称	1.3.5m立杆，抱箍条（300号不锈钢圈），电源线，六类网线，PVC管，水晶头，弯头。技术参数要求		套	1
				<p>▲1.标准机架式设备,内存≥16G，硬盘≥1T，≥6个千兆电口，≥4个千兆光插槽,冗余电源,2≥个扩展槽位,防火墙吞吐≥20G，并发连接≥500万，每秒新建连接≥16万，应用层吞吐量≥16G，全威胁吞吐量≥2.5G，IPSEC VPN吞吐≥3G，IPSEC VPN隧道数≥2000，SSL VPN吞吐≥2.5G，SSL VPN并发用户数≥5000，提供3年应用特征库升级许可，病毒库3年升级服务许可，攻击规则特征库3年升级许可，3年维保服务；</p> <p>2.支持路由、透明以及混合接入模式，满足复杂应用环境的接入需求；</p> <p>3.至少支持8路ADSL拨号接入，可对各ADSL链路之间通过W</p>			

	1	<p>CMP与ECMP方式进行路由均衡；</p> <p>4.支持Ipv4/Ipv6双栈工作模式；</p> <p>5.支持所有设备DNS查询域名时过滤通过请求；支持文件删除、文件下载、目录删除、创建目录、FTP上传、重命名、列表等FTP行为过滤；（提供产品功能截图，并加盖投标人公章）</p> <p>6.支持通过关键字实现对流出防火墙的http、ftp、smtp、pop3、dns等协议数据进行过滤，如网页内容、外发邮件主题及正文等</p> <p>7.具备对域名单独进行恶意代码防护，且在访问控制策略中完成；支持对电子邮件、HTTP、FTP、等协议所携带的恶意代码进行拦截、检测；（提供产品功能截图，并加盖投标人公章）</p> <p>8.支持安全或优先应用两种方式进行模式选择以处理数据，并在丢包时发送TCP reset命令，支持阻止恶意网络攻击，可通过URL过滤、关键字等进行过滤，加密的HTTPS流量在对SSL解密后检测以达到安全引擎的防护效果；（提供产品功能截图，并加盖投标人公章）</p> <p>9.内置静态黑名单功能，可设置多个对象条件，如：源目IP地址、源目端口、源目MAC、协议等，实现对特定报文进行快速过滤；</p> <p>10.支持GRE over Ipvsec隧道类型，避免动态路由OSPF和组播穿越隧道的问题出现；</p> <p>11.支持本地多配置文件存储及配置回滚功能，并且可以有选择性的下载；</p> <p>12.可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密。</p>	台 1
--	---	--	-----

	2	<p>日志审计</p> <p>1.标准机架式设备,≥7个千兆电口,≥16G内存, ≥250G SSD系统盘, 数据盘≥4T, ≥6个USB接口, 日志采集处理速度≥5000EPS, 提供100个日志源授权, 提供3年维保服务;</p> <p>2.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集;</p> <p>3.支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集; 支持通过Agent采集日志数据;</p> <p>4.支持日志归一化处理, 将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理;</p> <p>▲5.支持主动、被动相结合的数据采集, 以及重要日志的采集保障, 对流量非常大重要程度低的syslog源日志的接受速率采用限制方式以降低对系统资源的占用; (提供产品功能截图, 并加盖投标人公章)</p> <p>6.支持日志转发给第三方系统平台, 支持设置多个日志转发IP地址, 支持转发格式化日志或仅转发原始日志;</p> <p>7.支持原始日志全文检索, 以及重要单独的日志数据进行设置, 根据1个月、3个月、6个月和永久保存等设置类型, 分别独立设置每个被采集源参数; (提供产品功能截图, 并加盖投标人公章)</p> <p>8.支持存储空间图像化、动态监控, 超过阈值进行告警, 支持从存储空间、存储时间多维度进行动态监控;</p> <p>9.支持在查询结果页面上直接二次查询, 快速定位关键日志, 还可以返回上次查询条件;</p> <p>10.支持查询结果快速统计, 可自定义统计主题规则, 支持将多个主题添加为一个统计任务, 以分、时、周、月、年定时执行自动统计;</p> <p>11.支持安全告警概况、安全告警趋势的统一展示, 实时告警可根据级别、规则类型等进行分类。</p>	台 1
--	---	--	-----

	3 运维审计 堡垒机	<p>1.标准机架式设备,≥8G内存, 硬盘≥1T, ≥6个千兆电口, ≥4个SFP插槽,≥100个主机/设备许可, 用户数不限制, 图形并发≥25, 字符并发≥50, 提供3年软件升级服务和3年维保服务;</p> <p>2.支持组织结构层级化管理, 最大支持24个层级级部门分权功能;</p> <p>3.支持资源类别和资源类型管理以及资产网域化管理, 单独设置和管理在不同局域网下的资产;</p> <p>4.支持资产组管理, 根据需求自定义资产组; 支持资产组的增删改查操作;</p> <p>5.支持批量移动资产:支持单个、批量移动资产到指定资产或部门。支持单个、多个账号复制到指定一个或多个资产;</p> <p>6. 支持IP地址范围内资产发现, 对IP网段内扫描后快速发现指定的资产, 并自动识别IP地址和端口号快速添加资产, 方便管理员快速添加资产;</p> <p>7.支持对已添加的设备账号进行密码托管, 从而实现单点登录功能;</p> <p>8.支持密码口令变更方式支持手动指定固定口令、依照密码规则生成随机口令, 包括随机相同密码, 随机不同密码;</p> <p>9.支持登录规则的新建、编辑、启用、禁用和删除;</p> <p>10.支持配置指定用户、指定部门下的用户、指定角色的用户可申用的资产范围为全部, 本部门、本部门以及下级部门;</p> <p>11.支持SecureCRT、Xshell、WinSCP、Mac Terminal、xftp等客户端直接连接堡垒机进行代理运维目标资产。</p>	台 1	
--	---------------	--	-----	--

	4	<p>漏洞扫描系统</p> <ol style="list-style-type: none"> 1.标准机架式设备, ≥6个千兆电口, ≥1个扩展槽位, ≥1个Console接口, ≥2个USB接口, ≥8G内存, 硬盘≥1T, 支持无限制IP扫描授权, 并发扫描≥40个IP地址, 并发扫描≥5个系统扫描任务; 支持≥40个域名扫描授权, 并发扫描≥3个web任务, 提供3年规则库升级许可及维保服务; 2.支持Ipv4/Ipv6双协议栈地址场景漏洞扫描; 3.支持在WEB界面网络诊断, 包含PING、TRACEROUTE、TCP、HTTP、DNS多种诊断方式; 4.产品漏洞库应涵盖目前的安全漏洞和攻击特征, 漏洞库具备至少CVE、CNCVE、CNVD、BUGTRAQ、CNNVD编号; 5.允许管理员配置扫描通知, 在扫描任务运行开始时向被扫描的资产发送扫描通知; 6.支持搜索查看历史扫描收集信息并进行磁盘设置告警管理, 在管理当中选择删除无用的数据信息; (提供产品功能截图, 并加盖投标人公章) 7.支持以8位的加密密钥进行设置并加密传输, 传输时可以将数量多条的日志并合并成一条传输至日志服务器; 也支持外发至SYSLOG服务器中; 8.产品应支持对系统配置进行备份、恢复功能, 保证产品系统数据的安全性; 9.用户多次登录失败时, 自动锁定, 允许自定义超时时间及登陆失败次数; 10.支持网络打印机、摄像头、移动终端等设备的漏洞发现; 11.支持配置扫描任务最大并发线程数, 可根据网络空闲状态调整漏洞扫描的并发进程数量; 12.扫描任务下发时, 配置扫描目标时支持域名、网段、子网、ip自由组合配置, 以提高灵活性。 	台 1
--	---	--	-----

		<p>1.标准机架式设备,内存≥32G, 机械硬盘≥2T, ≥6个千兆电口, ≥4个千兆光口,冗余电源, ≥2个扩展槽位,吞吐≥1.2Gbps 可审计流量≥300Mbps。峰值SQL处理能力≥8000条/s, 日处理能力≥1000万条, 提供3年应用规则库、攻击检测规则库、僵尸主机规则库升级许可, 3年维保服务;</p> <p>2.支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata、等数据库系统;</p> <p>3.支持通过声光、邮件、短信等方式对审计日志、系统日志进行告警;</p> <p>4.支持数据库服务器弱口令扫描, 扫描出的弱密码支持脱敏显示, 支持以源IP维度柱状图展示SQL错误数,从多个维度展示SQL错误占比及趋势; (提供产品功能截图, 并加盖投标人公章)</p> <p>5.支持对针对数据库的XSS攻击行为、SQL注入攻击行为, 利用漏洞攻击等行为进行审计, 内置审计规则不需要额外配置, 并进行实时报警;</p> <p>6.支持自定义时间查看各个协议审计的流量趋势图, 直观展示应用流量的监听情况;</p> <p>7.支持会话回放以五级播放速度调节,播放倍数支持4倍、2倍、1.5倍、1倍、0.5倍;</p> <p>8.查询方式支持标准查询、经典查询和专家查询三种模式, 并支持自定义保存当前查询条件, 为后续查询提高便捷;</p> <p>9.准确审计绑定变量的SQL语句, 分离式存储SQL语句保障数据库审计效率;</p> <p>▲10.支持引用基线进行告警配置, 支持自定义基线内外、告警级别等;</p> <p>11.支持系统本身主要运行功能服务模块的运行状态巡检, 保证系统安全稳定运行;</p> <p>12.支持用户密码复杂度(高、中、低)设置、最大登录失败次数设置。</p>	台 1
		<p>1.支持态势大屏展示, 包括全网态势、资产态势、漏洞态势、攻击态势, 支持大屏展示时间设置, 支持态势大屏中相关信息下钻跳转到对应的详细页面, 含≥50个日志源接入授权;</p>	

6	<p>态势感知</p> <p>2.支持多种地图、拓扑展示方式，包括对世界、全国、省份、拓扑等以自定义顺序大屏界面展示，方式支持直接拖拽。</p> <p>3.支持漏洞态势分析，包括漏洞总体情况、漏洞类型分布、漏洞级别分布、高危漏洞排行TOP5、漏洞排行TOP10、最新漏洞发现趋势、高危漏洞类型排行、漏洞级别对比。</p> <p>4.支持对重点漏洞、重点高危漏洞影响性分析，支持展示漏洞的名称及影响的资产数量。</p> <p>5.支持以全球地图实时展示网络攻击态势，支持以不同颜色攻击线展示攻击过程，支持攻击源和攻击目的国家名称展示，支持攻击目的进行光晕显示。</p> <p>6.支持漏洞扫描器管理，支持添加、编辑、删除等操作。</p> <p>7.支持的攻击链阶段包含8种，包括漏洞利用、安装植入、命令控制、横向移动、侦查跟踪、载荷投递、目标达成、痕迹清理，支持以不同颜色标识攻击链命中阶段，支持资产攻击信息分析，包括威胁数量、遭受威胁类型、威胁源TOP5、攻击链分析、攻击链日志列表、攻击链日志关系图、攻击链日志时序图，支持按照攻击链阶段及日志级别进行分析</p> <p>8.支持全局展示资产概况，包括但不限于全部资产数/安全域数、等保业务系统数/业务系统数、已同步主库资产数/备库资产数、安全域资产分布TOP5、业务系统定级分布、主库资产类型分布等。</p> <p>▲9.支持管控拓扑图展示，支持拓扑动态提示管理设备产生的告警，支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息。</p> <p>10.支持多种类型设备策略配置，包括防火墙、僵尸蠕、EDR，支持多种策略配置，包括但不限于访问控制策略、静态黑名单、动态黑名单、安全策略等，支持联动EDR完成一键扫描、一键隔离。</p> <p>11.支持合规审计，审计设备类型包括但不限于主机、安全设备、网络设备、业务应用、中间件、数据库。</p>
---	--

	7 内网威胁分析系统	<p>1.提供仪表盘、风险分析、威胁分析、事件调查、采集管理、身份定位、知识管理等功能，含≥50个日志源接入授权；</p> <p>2.支持多主题展示系统整体态势，展示的主题包括但不限于：风险员工、风险资产、威胁事件、风险账号、风险IP、风险业务系统、高危威胁事件、高危群组、高危IP、高危账号统计；</p> <p>3.支持系统功能服务状态监控，包括但不限于：员工定位、资产定位、风险评分、智能群组、员工风险画像、行为轮廓分析；</p> <p>4.支持基于员工、资产、观察表视角展示风险，展示内容包括但不限于：总体情况、总分排行、当日分数、近期每天分数分布、最近威胁；</p> <p>5.支持根据基础风险分值、威胁事件类型过滤威胁事件。支持展示当前统计时间段内的威胁事件满足某种风险分值的次数、威胁事件类型的次数；</p> <p>▲6.提供威胁基本信息及携带重要信息的展示，包括但不限于：员工、资产、账号、IP、基线趋势、命中关键字、附件、攻击扫描IP、攻击扫描端口。</p>		
--	------------	---	--	--

8	大数据分析系统	<p>1.基于B/S架构，通过Web方式对本系统进行管理，支持分布式数据存储及检索技术，支持10亿条数据秒级检索响应，含≥50个日志源接入授权；</p> <p>2.支持配置UDP、TCP、KAFKA、NETFLOW_V5、NETFLOW_V9、SNMP、SFTP、文件、REST和JDBC等多种类型的接收进行数据采集，并支持SSL方式加密传输；</p> <p>3.支持基于关键字特征和正则表达式进行特征匹配；支持至少10种字段提取规则，包括但不限于字符串分割、KV提取、数组拼接、Avro提取、Grok、Json提取等；至少预置5种富化规则，包括但不限于DHCP映射、杀伤链事件定位库；支持通过与或逻辑进行字段过滤；</p> <p>▲4.支持绘制数据血缘拓扑图，包含日志源、接收服务器、数据类型、数据分享对象等，支持按日志类型进行过滤展示，支持拓扑图上各节点详细信息展示；</p> <p>5.支持研判策略管理，支持开启告警自动研判，支持自定义误报以及确认攻击的阈值。</p>	
	终端威胁	<p>1.提供≥8个Linux服务器客户端防病毒功能授权，含3年升级许可，提供≥100个Windows PC客户端和≥10个服务器端防病毒功能授权,含3年升级许可；</p> <p>2.病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS病毒等进行查杀，提供主动防御系统防护等功能，客户端系统支持Windows XP/VISTA/WIN7/WIN8/WIN10；</p> <p>3.系统部署采用C/S架构，管理采用B/S架构，管理员只需通过浏览器登录管理中心，即可对系统进行管理；</p> <p>4.采用Docker部署方式，能够快速恢复，横向扩展，可移植性强；</p> <p>5.客户端安装支持本地安装、WEB安装、离线安装、命令行安装；</p> <p>6.支持IP规则一键整理，根据部门规则、部门与IP规则、LDAP规则架构的导入后一键整理；、、</p> <p>▲7.支持终端在线、离线、安装情况以IP地址池方式展示，支</p>	

9	防御	<p>持通过NMAP、PING、ARP、方式扫描，及时发现尚未纳入管控的终端；</p> <p>8.支持自定义病毒、系统、网络防御、合规管控、其他设置等安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP协议控制、恶意网站拦截、IP黑名单）；合规管控（文档检测、文档跟踪、USB存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）；</p> <p>9.支持终端策略标签化管理，按需求给终端配置标签，同一标签的终端可配置相同的动态策略；</p> <p>10.支持终端防卸载、防退出功能，管理员能够统一设置防卸载密码，防止终端用户随意脱离保护；</p> <p>11.支持对webshell后门进行扫描检测，webshell后门规则数量大于100000。</p>	套1
---	----	--	----

0	1 WAF	<p>1.标准机架式设备,内存≥8G, 硬盘≥1T, ≥8个千兆电口, ≥2个千兆光口插槽,应用层吞吐≥300M, 网络层吞吐≥3G, 并发连接≥70万, 新建连接≥2400, 提供3年特征库升级许可及维保服务;</p> <p>2.提供专用硬件架构与安全操作系统, 基于操作系统内核的完全检测技术; 产品为专业性 Web 应用安全防护系统硬件设备, 而非下一代防火墙UTM 类设备集成的 WEB 防护功能模块;</p> <p>3.支持无IP纯透明模式串联部署、负载均衡模式部署、反向代理模式部署、旁路监测模式部署;</p> <p>4.支持虚拟线接入, 无论任何网络环境可强制数据从一个接口转发到另一个接口;</p> <p>5.支持网络层访问控制, 支持基于源IP 地址、目的IP 地址、协议类型及区域等条件的访问控制;</p> <p>6.支持以cookie方式进行加密签名的安全防护, 保障信息安全可信; 支持IP扫描周期设置和防护阈值以达到恶意扫描及时防护和阻断;</p> <p>7.支持URI例外配置, 包括对指定URI地址进行协议合规性检查, 防御类型设置, 参数设置, 上传下载设置;</p> <p>8.支持防护动作自定义, 包括告警、拒绝、重定向, 错误页面等多种防护动作, 同时支持返回错误页面自定义;</p> <p>9.支持HTTP/HTTPS的DdoS攻击威胁检查, 支持对慢速攻击, CC攻击进行防护;</p> <p>▲10.支持通过内置爬虫库或者导入、后端下载等自定义爬虫库的方式进行爬虫攻击防护;</p> <p>11.支持敏感信息防泄漏功能, 可自定义对身份证、信用卡、手机号码、座机电话号码、邮箱地址等敏感信息做检查;</p> <p>12.支持以文件扩展名、最大文件大小、MIME类型对文件的上传下载进行控制, 对上传文件内容进行病毒检测的功能。</p>	台 1
1	1 服务器正版化	1.Windows Server 2022 Standard - 16 Core License Pack (含1个Windows Server 2022 - 1 Device CAL) .	套 10
2	1 辅材	1.网线, 水晶头, 弯头, 配线架, 调试安装。	批 1

★	3	<table border="1"> <thead> <tr> <th data-bbox="389 911 435 987">序号</th> <th data-bbox="435 911 604 987">采购项目名称</th> <th data-bbox="604 911 1345 987">技术参数要求</th> <th data-bbox="1345 911 1391 987">单</th> <th data-bbox="1391 911 1453 987">数 位 量</th> </tr> </thead> <tbody> <tr> <td data-bbox="389 987 435 1393">1</td> <td data-bbox="435 987 604 1393">数字图书</td> <td data-bbox="604 987 1345 1393"> <p>★1.提供不低于 100000 册数字图书，要求接入原有数字图书平台。覆盖中图分类法22个分类；提供平台内图书的搜索服务；提供高清晰的全文在线阅读，并提供下载借阅功能，无副本限制；具有强大的查询检索，提供图书管理和访问量统计等功能，并支持部分页面定制；电子图书图像遵循图书的原版原貌，文字差错率不高于万分之一。（提供承诺函并加盖投标人公章）</p> </td> <td data-bbox="1345 987 1391 1393">项</td> <td data-bbox="1391 987 1453 1393">1</td> </tr> </tbody> </table>	序号	采购项目名称	技术参数要求	单	数 位 量	1	数字图书	<p>★1.提供不低于 100000 册数字图书，要求接入原有数字图书平台。覆盖中图分类法22个分类；提供平台内图书的搜索服务；提供高清晰的全文在线阅读，并提供下载借阅功能，无副本限制；具有强大的查询检索，提供图书管理和访问量统计等功能，并支持部分页面定制；电子图书图像遵循图书的原版原貌，文字差错率不高于万分之一。（提供承诺函并加盖投标人公章）</p>	项	1
序号	采购项目名称	技术参数要求	单	数 位 量								
1	数字图书	<p>★1.提供不低于 100000 册数字图书，要求接入原有数字图书平台。覆盖中图分类法22个分类；提供平台内图书的搜索服务；提供高清晰的全文在线阅读，并提供下载借阅功能，无副本限制；具有强大的查询检索，提供图书管理和访问量统计等功能，并支持部分页面定制；电子图书图像遵循图书的原版原貌，文字差错率不高于万分之一。（提供承诺函并加盖投标人公章）</p>	项	1								

4	序 号	采购项目 名称	技术参数要求	单 位	数 量
	1	页面设计	1.页面以主流简约【扁平式】设计； 2.主体部分以图片为导向，以局部文字作为网站点睛之笔；	项	1
	2	前端	1.网站主体页面前端处理，响应式布局，包含首页，内页，列表页，详细页等全部页面网站前端处理，兼容主流系统；	项	1
	3	环境搭建	1.Nginx1.14 + Mysql8.0 + PHP8.0运行环境的搭建；	项	1
	4	网站基本 技术维护	1.提供三年7x24响应，提供对网站及时处理问题，在使用过程中，出现的所有系统无法运行等问题，包括其他非人为原因导致的故障问题，及时进行维护恢复；	项	1
	5	网站安全 性维护	1.对网站系统进行周期性安全升级服务，提高网站在运行中的安全级别的更新，严防黑客、杜绝病毒、保证系统正常运行；	项	1
	6	网站BUG 处理	1.如网站在运行过中遇到相关BUG，开发人员对运行中出现 的各类BUG修复。	项	1

	序 号	采购项目 名称	技术参数要求	单 位	数 量
--	--------	------------	--------	--------	--------

1	一体机	<p>1.整机屏幕边缘采用金属圆角包边防护，整机背板采用金属材质，UHD超高清LED液晶屏，尺寸不低于86英寸，显示比例16:9，分辨率≥3840×2160；</p> <p>2.整机内置非独立的高清摄像头，不低于1300万像素，支持远程巡课等应用，摄像头视场角≥135°，拍摄范围可以涵盖整机距离摄像头垂直法线左右水平距离各≥4米，左右最边缘深度≥2.3米范围内，并且可以AI识别人像；</p> <p>3.整机内置非独立外扩展的4阵列麦克风，可用于对教室环境音频进行采集，拾音距离≥12m。整机内置2.2声道扬声器，位于设备上边框，顶置朝前发声，前朝向≥10W高音扬声器2个，上朝向20W中低音扬声器2个，额定总功率≥60W；</p> <p>4.整机具备不少于6个前置按键，可实现老师开关机、调出中控菜单、音量+/-、护眼、录屏操作；</p> <p>5.恢复出厂状态：整机关机状态下，通过长按电源键进行故障检测以及系统还原功能，无需额外工具辅助；</p> <p>6.整机支持纸质护眼模式，可以在任意通道任意画面任意软件所有显示内容下实现画面纹理的实时调整；支持纸质纹理：牛皮纸、素描纸、宣纸、水彩纸、水纹纸；支持透明度调节；支持色温调节；</p> <p>7.系统版本在安卓11.0或以上，内存不低于2G RAM，存储不低于8G ROM；</p> <p>8.内置无线传屏接收端，无需外接接收部件，无线传屏发射器与整机匹配后即可实现传屏功能，将外部电脑的屏幕画面通过无线方式传输到整机上显示；</p> <p>9.整机支持一键打开/关闭展台软件；在任意通道下均可实时查看视频展台连接状态，当设备连接/断开连接时，提供实时反馈提示；同时支持读取视频展台设备型号，显示对应设备实物图片，方便维护报修；</p> <p>10.当整机处于黑暗环境中并无人操作，一分钟后整机将可以自动进入熄屏模式；</p> <p>11.处理器：主板采用H310芯片组；内存：≥8G DDR4笔记本内存；硬盘：≥256 SSD固态硬盘；</p>	台 1
---	-----	--	-----

		2	显示器	1.≥75 寸硬屏，含HDMI高清接口；包含金属挂件，配件，安装辅材等。	台	2
		3	电脑	1.处理器：3A5000 CPU≥4核，主频 2.3GHz-2.5GHz； 2.内存：≥8GB DDR4 内存,最大可扩展 64G； 3.显卡：集成显卡； 4.硬盘：≥256G；最大可扩展至 512GBSSD+1TB 机械 硬盘混装) 5.操作系统:国产化操作系统(如银河麒麟，红旗 Linux，深度等)	台	65
		4	桌子	1.≥1200*600*740mm (+5mm)，桌面采用≥18mm实木颗粒板，桌架铁质，带主机箱，配锁，可根据实际定制。	台	3
		5	讲桌	1. ≥1400*600*740mm (+5mm)，桌面采用≥18mm实木颗粒板，桌架铁质，带主机箱，带抽屉，配锁，可根据实际定制。	台	1
		6	椅子	1. 椅面/椅背选用优质网布面料；具有透气性强，回弹性好，不易变型,不老化，依人体工学设计.使人体各部均匀受力；底座：电镀钢铁支架；配件：采用优质螺丝五金配件。	把	6
		7	交换机	1.24 口千兆接入交换机；	台	3
		8	辅材	1.网线，插板，水晶头。	批	1

8、供应商一般资格要求

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。

序号	资格要求名称	资格要求详细说明
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。{如需提供其他材料，需代理机构手动填写具体要求并关联相应格式要求，以下是样例：供应商财务状况证明材料包括采购代理机构在采购文件中明确需要供应商提供的财务状况证明材料。如XXXX或XXXX年度经审计的财务报告（包含审计报告和审计报告中所涉及的财务报表和报表附注）；XXX X或XXXX年度供应商完整的全套财务报表（应当包括资产负债表、利润表、现金流量表、所有者权益变动表、附注）；截至采购文件（资格预审申请文件）提交截止之日前一年内银行出具的资信证明；供应商注册时间截至采购文件（资格预审申请文件）提交截止之日前不足一年的，也可提供在相关主管部门备案的公司章程等证明材料。供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。}
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。
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180日

4) 合同履行地点：盐源县

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：是

履约保证金缴纳比例：5%

缴纳方式：银行转账，支票/汇票/本票，保函/保险

缴纳说明：中标价的5%

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：预付款，达到付款条件起10日内，支付合同总金额的30.00%；

2、付款条件说明：验收合格，达到付款条件起10日内，支付合同总金额的70.00%；

9) 验收交付标准和方法：（1）供应商提出验收申请之日起10日内采购人组织验收。（2）严格按照招标文件要求和中标供应商投标文件内容进行验收。（3）严格按照政府采购相关法律法规以及《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。

10) 质量保修范围和保修期：质保及售后服务要求：质保期三年。（产品有其单独的质保期限的，以其单独要求的为准。）

11) 知识产权归属和处理方式：归采购方所有

12) 成本补偿和风险分担约定：由供应商承担

13) 违约责任与解决争议的方法：诉讼

14) 合同其他条款：无

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10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：一是按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准强制性要求，由具备资格的机构（详见《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》）安全认证合格或安全检测符合要求的；二是此前已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。

10) 商务履约验收内容：按照合同执行

11) 履约验收标准：按照合同执行

12) 履约验收其他事项：按照合同执行

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