采购需求

一、项目概述

近年来，云计算、移动互联网、大数据以及社交网络等信息化热点的兴起对于我国教育信息化的迅猛发展起到了巨大的推动作用。随着干部培训规模日趋扩大，培训质量要求越来越高，专业化培训和精准化培训成为未来重要方向。面对新形势、新任务、新要求，党校信息化建设工作正站在一个新的历史起点上。在党校分类改革的大环境下，图书馆的建设迫在眉睫，图书馆网络的建设也是党校基础设施建设的重要组成部分，未来将有效支撑各类智慧校园平台各类应用和学习任务的开展。

二、产品所属行业

序号	产品名称	产品所属行业
1	无线控制器	工业
2	高密 AP（会议室）	工业
3	吸顶 AP（走廊）（核心产品）	工业
4	POE 交换机	工业
5	24 口非 POE 交换机	工业
6	内网边界防火墙	工业
7	全流量威胁分析	工业
8	防病毒系统	工业
9	考勤机	工业
10	超五类网线	工业
11	六类网线	工业
12	光纤	工业
13	光模块	工业
14	柜机	工业

三、项目清单及技术参数要求

3.1 项目清单

序号	产品名称	数量/单位
1	无线控制器	1 台
2	高密 AP（会议室）	2 台
3	吸顶 AP（走廊）	39 台
4	POE 交换机	1 台
5	24 口非 POE 交换机	1 台
6	内网边界防火墙	1 台
7	全流量威胁分析	1 台
8	防病毒系统	1 台
9	考勤机	12 台
10	超五类网线	25 件
11	六类网线	67 件
12	光纤	500 米
13	光模块	4 个
14	柜机	2 个

3.2 技术参数要求

序号	产品名称	技术参数要求
1	无线控制器	1、配置千兆电口≥8 个，千兆光口≥1 个，万兆光口≥1 个； 2、内部实配硬盘插槽，且实配硬盘容量≥1T，内存≥4G； 3、本地转发AP可管理数≥800 个； 4、支持MAC认证、WEB认证、802.1X认证、WAPI认证，认证后能实现IP、MAC、WLAN等元素的绑定信息，保证只有合法的用户才能进入网络； 5、支持内置portal认证页面定制，有专业知识的人员可以定义任何页面，做到完全自定义包上传，支持将用户上下线信息发送给第三方系统； 6、本次配置≥96 个无线AP管理授权； 7、原厂提供 3 年技术支持、问题处理、软件更新、标准保修。
2	高密 AP(会议室)	1、支持 802.11ax标准，整机支持≥6 条流，所投AP整机最大终端接入数≥1530 个，整机最大接入速率≥3.260Gbps。 2、采用硬件独立的三射频设计，支持三张射频卡同时工作在 5G

		频段，≥2 个以太网口，其中≥1 个 10/100/1000M/2.5GE电口，≥1 个 10/100/1000M电口支持端口对外供电，扩展物联网模块。 3、防护等级IP41，5GHz单射频支持 2*2MIMO，且单射频最大接入速率≥1.2Gbps。 4、支持吸顶、壁挂等安装方式。 5、避免无线网络中私接非法AP，所投AP具有非法AP的精确反制和模糊反制功能，能够主动识别非法设备并令非法设备不能使用。 6、所投AP具有WLAN自动网优功能，不借助任何网络优化软件，仅通过AP配置进行无线网络优化，降低无线网络中的频段干扰，为避免无线网络中私接非法AP的影响，设备应支持 802.11w防御Deauth攻击功能，保证终端正常关联使用。 7、原厂提供 3 年技术支持、问题处理、软件更新、标准保修。
3	吸顶 AP（走廊）	1、支持标准的 802.11acwave2 协议,采用双路双频设计，可同时工作在 802.11ac和 802.11a/b/g/n模式。 2、支持 2 条空间流,单频最大接入速率≥867Mbps,整机最大接入速率≥1167Mbps。 3、发射功率≤20dBm，支持 802.3af/本地电源DC5V两种供电模式，整机功耗小于 13w。 4、≥1 个 10/100/1000Base-T以太网口，支持POE供电。 5、设备与无线控制器配合，支持iOS、安卓和windows等主流智能终端操作系统自动识别，提供适应屏幕比例与尺寸的认证页面，实现轻松访问。 6、支持胖/瘦AP两种工作模式的切换，在瘦AP工作模式时，AP与控制器之间采用国际标准的CAPWAP协议通信。 7、原厂提供 3 年技术支持、问题处理、软件更新、标准保修。
4	POE 交换机	1、配置 10/100/1000M以太网端口≥24 个，千兆SFP光接口≥4 个；支持POE和POE+,同时可POE供电端口≥24 个，POE最大输出功率≥370W； 2、交换容量≥335G，包转发率≥50Mpps，以官方网站最小值为准； 3、为保证设备在受到外界机械碰撞时能够正常运行，要求所投交换机IK防护测试级别至少达到IK05，投标时在响应文件中提供经CNAS或CMA认定的第三方权威测试机构出具的测试报告复印件（或扫描件）进行佐证； 4、支持生成树协议STP(IEEE802.1d)，RSTP(IEEE802.1w)和MSTP(IEEE802.1s)，完全保证快速收敛，提高容错能力，保证网络的稳定运行和链路的负载均衡，合理使用网络通道，提供冗余链路利用率； 5、支持IPv4/IPv6 静态路由，RIP、RIPng； 6、支持特有的CPU保护策略，对发往CPU的数据流，进行流区分和优先级队列分级处理，并根据需要实施带宽限速，充分保护CPU不被非法流量占用、恶意攻击和资源消耗 7、设备自带云管理功能，即插即用，可随时查看网络健康度，告警及时推送，有日记事件供回溯。 8、原厂提供 3 年技术支持、问题处理、软件更新、标准保修。

5	24口非POE交换机	1、配置10/100/1000M以太网端口≥24个，千兆SFP光接口≥4个； 2、交换容量≥335G，包转发率≥50Mpps，以官方网站最小值为准； 3、为保证设备在受到外界机械碰撞时能够正常运行，要求所投交换机IK防护测试级别至少达到IK05，投标时在响应文件中提供经CNAS或CMA认定的第三方权威测试机构出具的测试报告复印件（或扫描件）进行佐证； 4、支持生成树协议STP(IEEE802.1d)，RSTP(IEEE802.1w)和MSTP(IEEE802.1s)，完全保证快速收敛，提高容错能力，保证网络的稳定运行和链路的负载均衡，合理使用网络通道，提供冗余链路利用率； 5、支持IPv4/IPv6静态路由，RIP、RIPng； 6、支持特有的CPU保护策略，对发往CPU的数据流，进行流区分和优先级队列分级处理，并根据需要实施带宽限速，充分保护CPU不被非法流量占用、恶意攻击和资源消耗； 7、设备自带云管理功能，即插即用，可随时查看网络健康度，告警及时推送，有日记事件供回溯； 8、原厂提供3年技术支持、问题处理、软件更新、标准保修。
6	内网边界防火墙	1、三层吞吐量≥4G，应用层吞吐量≥1G，并发连结数≥100W，新建连接数(CPS)≥2W个；≥4G内存，≥6个千兆电网口，≥2个千兆光网口，为防止设备关键信息泄露，设备禁止配置显示模块，配置3年IPS特征库、僵尸网络与病毒防护库、URL&应用识别库定期更新； 2、产品采用多核并行处理架构； 3、产品支持IPSecVPN智能选路功能，根据线路质量实现自动链路切换（提供产品功能截图证明）； 4、支持SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood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、产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，投标时在响应文件中提供具备第三方机构关于“勒索软件通信防护”功能项的产品检测报告复印件（或扫描件）进行佐证。 6、具备文件过滤功能，可对视频文件、音频文件、图片文件、文本文件、可执行文件、驱动文件等类型文件进行安全过滤。 7、产品支持对不少于10000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。(需提供功能截图证明) 8、产品支持对常见Web应用攻击防御，攻击类型至少支持跨站脚本(XSS)攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过3320种； 9、产品支持多种自定义条件快速查询安全日志，自定义条件至少包括时间、日志类型、安全日志严重等级等条件。 10、产品支持CC攻击防护功能，为保障CC攻击的检测效果，投标时在响应文件中提供第三方机构关于“CC攻击防护”功能项的产品检测报告复印件（或扫描件）进行佐证。

7	全流量威胁分析	1、应用层吞吐量≥600Mbps，内存大小≥16G，硬盘容量≥128GBSSD+2TBSATA，千兆电口≥6，千兆光口SFP≥2。为防止设备关键信息泄露，设备禁止配置显示模块，3 年硬件质保和软件升级服务； 2、旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响； 3、提供安全分析大屏，能够展示资产分布，看清内网风险终端和风险资产概况，能够提示终端和服务器资产数据，能够展示风险终端和服务器数量。能够基于资产展示web明文、弱密码等脆弱性概况。能够展示风险终端和服务器top5 安全事件。 4、具备失陷(业务和服务器)主机详细分析，包含攻击阶段分布、风险等级趋势、安全事件举证、开放端口等信息。攻击阶段包含存在漏洞、遭受攻击、C&C通信、黑产牟利、内网扫描、内网扩散、盗取数据支持对每个安全事件详细举证分析，包含风险危害、处置建议、专杀工具等； 5、支持终端维度展示终端IP、所属终端组、风险等级、安全事件标签、处理状态、联动状态，风险等级包含已失陷、高危、中危、低危等。支持终端的详细分析，包含风险评估、攻击阶段分布、风险等级趋势、安全事件举证等信息。 6、针对挖矿做专项性分析，比如挖矿的币种分布，威胁趋势分析。 7、支持沙盒文件检测，能够对exe可执行文件、dll应用程序扩展、BAT批处理文件、PDF、office、VB脚本、PHP网页脚本、PY脚本等进行检测。 8、支持检测 7 类以上常见协议FTP、LADP、mysql、POP3、SMTP、TELNET、WEB等的弱密码，支持镜像流量检测业务系统中的弱密码，检测列表包含账号、密码、服务器、所属分析和业务、最近登录源IP、类型、最近发现时间等信息，密码星号显示需超级管理员才可查看，并支持储存数据包内容。 9、针对主流漏洞、攻击方式等有详细而专业的介绍，并提供了专业实用的安全建议； 10、支持与内网边界防火墙进行联动响应，支持系统下发安全策略到防火墙上，阻断攻击流量。支持与防病毒系统联动，在系统发现安全事件时系统可通过防病毒系统进行对内网主机进行联动封锁，封锁后主机将无法访问全部IP（禁止出站）或者全部IP无法访问该主机（禁止入站）(需提供厂商承诺函)。
8	防病毒系统	1、为简化终端管理，要求支持自动收集终端资产状况，本次需配置PC端授权 100 个，服务器授权 5 个，并提供不少于三年的使用、升级与更新授权； 2、支持展示终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端agent版本、病毒库版本、最近登录时间、最近登录的用户名； 3、支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量；

		4、支持彻底清除当前流行的蠕虫\挖矿病毒：驱动人生病毒、DorkBot、Morto等；支持主流感染型病毒的清除，包括：Ramnit、Neshta、Parite、Virut、Jadtre、viking、Expiro；支持对宏病毒和感染型病毒的查杀和修复，覆盖office2003 和office2007 格式的文档和模板； 5、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、威胁分析和处理建议； 6、支持基于威胁情报的病毒文件哈希值和域名全网终端搜索，可定位出全网终端该病毒的感染情况； 7、支持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； 8、支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离； 9、支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具； 10、基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。
9	考勤机	1、面部容量：500； 2、卡容量：10000； 3、记录容量：120000； 4、通讯方式TCP/IP,RS232/485； 5、显示屏：4.3 英寸； 6:、识别方式：人脸、刷卡； 7、电源规格：DC12V3A。
10	超五类网线	/
11	六类网线	/
12	光纤	/
13	光模块	千兆单模
14	柜机	22U

四、商务要求

4.1 交货日期及地点：

4.1.1 交货日期：自合同签订之日起 180 日。

4.1.2 交货地点：中共宜宾市委党校。

4.2 付款方式：履约验收合格后一次性支付合同金额的100%。

4.3 质量保修范围和保修期：

4.3.1 质保期为验收合格后 壹 年，质保期内出现质量问题，乙方提供电话、远程和上门三种服务模式，2小时响应，电话不能解决的问题技术人员在24小时内到达现场进行修复，维修时间超过48小时的不能修复的，提供不低于同档次的备用设备。

4.3.2 乙方须指派专人负责与甲方联系售后服务事宜。

4.4 验收标准和方法：

4.4.1 供应商提出验收申请之日起10日内组织验收

4.4.2 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)的要求进行验收。