采购需求

一、项目概述

本次建设主要为补充更新完善校园网络安全设施，构建完善的安全防护体系，消除故障隐患；建设内容如下：

1、针对学校现网容易造成单点故障的网络安全设备节点，进行防火墙及上网行为管理设备更新升级，提升网络性能，消除网络通信瓶颈。消除故障隐患。将原有防火墙下移至内网区域防护。

2、添置日志审计设施，采用成熟的日志审计设备丰富对学校现网资产及业务系统日志进行采集，含网络地址转换日志采集，解决安全事件溯源问题。

3、建设校园网络态势感知平台，提升网络安全防范预警和监测能力。

4、补充边界区域入侵防御设施和负载均衡设备，提升安全、高速通信性能。

5、更新替换已到期的漏洞扫描安全设备。

6、新增 APT 防护沙箱，完善校园网络整体安全架构，为当下等保越来越高的要求提供基本支撑保障。

7、根据财务系统专网等保测评的实际要求，添置专网边界防火墙及专网日志审计系统一套。

二、采购清单

序号	产品名称	规格	数量	所属行业	备注
1	态势感知平台	套	1	工业	
2	入侵防御系统	套	1	工业	
3	上网行为管理系统	套	1	工业	
4	日志审计系统	套	1	工业	
5	下一代防火墙	套	1	工业	
6	漏洞扫描系统	套	1	工业	
7	APT 防护沙箱	套	1	工业	核心产品

8	校园网边界负载均衡与管控系统	套	1	工业	核心产品
9	财务专网防火墙	套	1	工业	
10	财务专网日志审计系统	套	1	工业	

三、技术参数及要求

序号	产品名称	技术要求
1	态势感知平台	1. 服务器性能要求：高度≥2U，2 颗 CPU，单颗 CPU≥12 核 2.4GHz，内存≥256G，硬盘：1.2T SAS≥23 块，600G SAS ≥2 块，接口：实配 GE 电口≥4 个,10GE 光口≥4 个，900W 冗余电源； 2. ★应用层吞吐量≥1Gbps，支持适配国产操作系统及国产数据库； 3. 内置流探针组件，若无内置探针，则需要外部补充流量探针； 4. 支持针对不同攻击场景（DGA 检测处置场景、加密流量检测处置场景、恶意 C&C 检测处置场景等）编排自动化的调查取证和告警联动，实现安全事件的自动化处置闭环； 5. 支持多种编排动作，包括：沙箱联动、终端取证、URL 封堵和网络隔离等，同时提供了灵活的动作扩展机制，可通过 Python 脚本扩展编排动作； 6. ▲为了高效检测恶意加密流量，不影响现有网络业务、性能，需要支持恶意 C&C 通讯；（需提供具有 CNAS 或 CMA 标识的第三方实验室测试报告证明，提供报告复印件并加盖供应商公章）； 7. 支持按照用户需要对 HBase 和 Hive 中的数据进行列加密，并能够支持 AES128 和 SM4 国密算法，满足国密加密需求； 8. ▲支持不同视角展示全网态势，包括综合安全态势、内网安全态势、外网安全态势、脆弱性态势、资产安全态势、威胁事件态势等 6 个独立的大屏展示功能。支持大屏轮播功能，能手动配置轮播间隔事件。并支持大屏 Logo 定制功能（安全态势可视化呈现需提供具有 CNAS 或 CMA 标识的第三方实验室测试报告证明，提供报告复印件并加盖供应商公章）。
2	入侵防御系统	9. 产品必须为标准机架的专业 IPS 设备，不能提供防火墙或 UTM 的 IPS 功能； 10. 业务口实配：业务口配置 GE COMBO≥8 个，GE 光口≥4 个，GE 电口≥4 个，10GE SFP+≥6 个，支持 1 个 GE 独立管理口，1 个 Console 口，1 个

		USB3.0 口，实配 SSD 硬盘不低于 240G，冗余电源； 11. 为有效利于设备散热，配置 3+1 冗余风扇，风扇支持热插拔； 12. ★IPS 检测吞吐量≥12Gbit/s；每秒新建连接数≥25 万；最大并发连接数≥1000 万，三年 IPS 特征库升级许可授权； 13. ▲系统预定义入侵防御签名库数量不得少于 10000 条且具备 CVE 和 CNNVD 编号的签名条目数不得少于 8000，支持用户自定义签名规则，支持正则表达式（提供功能截图,并加盖供应商公章)； 14. 支持静态路由、策略路由，OSFP、BGP、ISIS 等路由； 15. ▲为满足国家信息化创新要求，产品采用自主研发的关键芯片(CPU) (提供具有 CNAS 或 CMA 标识的第三方实验室测试报告证明，提供报告复印件并加盖供应商公章)。
3	上网行为管理系统	16. 最大功率≤120W，支持硬件、软件 Bypass 模块，在设备断电、重启时，可自动切换到 Bypass 状态，当设备恢复时，可自动切换回工作状态； 17. ★标准机架式设备，支持 100M/1000M 自适应电接口数量≥12，支持千兆光接口数量≥12，支持万兆光接口数量≥2，冗余电源，配置 2T 硬盘，3 年特征库升级许可； 18. ★网络吞吐量≥9.5Gbps，最大并发连接数≥300 万，最大新建连接数≥7 万，最大用户数≥8000； 19. ▲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，负载算法包括但不少于优先级和权重，负载均衡接口支持 pppoe、dhcp、tunnel、物理接口等三层接口。（提供 web 配置界面截图,并加盖供应商公章)； 20. 支持负载在出接口的 DNS 请求主动完成 DNS 服务器替换； 21. ▲支持配置 IPsec VPN 隧道内网段映射,解决 VPN 地址网段重叠问题（提供 web 配置界面截图,并加盖供应商公章)； 22. 支持网络社区应用管控的精细化管理，例如可管控“所有行为”、“登录”、“网页浏览”、“发表”、“上传”等行为； 23. ▲支持上网行为记录本地留存，方便事后行为回溯；支持将日志记录发送至第三方平台进行数据分析和呈现，发送数据支持蝶式交换加密算法（提供 web 配置界面截图,并加盖供应商公章)； 24. ▲支持文件缓存，支持安卓和 IOS 形式的文件，主动缓存文件形式不限于视频、APP 等；设备智能解析用户流量，针对域名或者文件请求，设备推送文件至终端，帮助用户缓解互联网出口压力，实现文件下载加速的效果（提供 web 配置界面截图,并加盖供应商公章)。

4	日志审计系统	25. 支持旁路部署、分布式部署以及级联部署模式； 26. ★配置 GE 电接口数量≥4，10GE 光口数量≥4，扩展插槽≥1，最大管理资产数 1000，EPS≥20000 EPS，本次配置 100 台日志管理授权； 27. 支持 Syslog、SNMP Trap、HTTP、SFTP 协议日志收集； 28. ▲支持对日志进行细粒度解析，包含不仅限于采集器接收时间、日志时间（起始时间/结束时间）事件级别、事件类型、事件消息、事件名称、来源地址、来源端口、目标地址、目标端口、事件设备分类、事件行为分类、事件特征分类、事件结果分类等，字段信息可通过解析规则增加和修改，默认维度超过 200+（提供 web 配置界面截图,并加盖供应商公章)； 29. 支持网络安全设备、交换设备、路由设备、操作系统、应用系统、虚拟环境等，支持 200+厂家设备的接入； 30. 支持通过日志等级进行过滤，支持配置过滤规则，将低价值的日志过滤掉； 31. 内置 5000 种以上设备类型的解析规则； 32. ▲内置 50+关联分析规则，关联规则可通过界面上传更新（提供 web 配置界面截图,并加盖供应商公章)； 33. ★支持学校现网边界路由设备 NAT 日志采集及统计分析和查询。
5	下一代防火墙	34. ★标准机架式 1U 设备，实配：千兆 Combo 接口≥8，千兆电口≥4，千兆光口≥4，万兆光口≥6，支持 USB3.0，冗余电源。配置 IPS、AV、URL 过滤升级 license 3 年，实配 SSD 硬盘 ≥240G； 35. ★防火墙吞吐量≥25Gbps，最大并发连接数≥1000 万，每秒新建连接数≥25 万 ，IPS 吞吐量≥10Gbps，IPSec VPN 吞吐量≥15Gbps，SSL VPN 吞吐量≥1.5Gbps ； 36. 支持基于 IP（IPv6）、MAC 地址，安全组，时间等字段进行安全策略规则的配置； 37. ▲支持 IPv6 over IPv4 隧道，6RD 隧道(提供证明材料,并加盖供应商公章)； 38. 可识别应用层协议数量≥5000 种；支持识别国标 SIP 协议及主流安防厂家的私有协议； 39. 支持 HTTP、HTTPS、DNS、SIP 等应用层 Flood 攻击，支持流量自学习功能，可设置自学习时间，并自动生成 DDoS 防范策略； 40. ▲为满足国家信息化创新要求，产品采用自主研发的关键芯片(CPU)(提供具有 CNAS 或 CMA 标识的第三方实验室测试报告证明，提供报告复印件并加盖供应商公章)；

		41. ▲支持 SafeSearch,过滤掉 Google 等搜索引擎返回的不健康的内容(提供 web 配置界面截图,并加盖供应商公章)。
6	漏洞扫描系统	42. 集成系统扫描、web 扫描、数据库扫描、基线配置核查、弱口令扫描于一体，提供一体化漏洞检测； 43. 支持对 Windows 系列操作系统、苹果操作系统、Linux、SUSE、AIX、HPUX、IRIX、BSD、Solaris 系统进行扫描； 44. ▲支持 60000 条以上系统特征库,特征库涵盖标准包含 CVE、CVSS、CNVID、CNNVD、CNCVE、Bugtraq5 种（提供 web 配置界面截图,并加盖供应商公章)； 45. ▲支持扫描 Checkpoint、赛门铁克、Cisco、Juniper、Palo Alto、华为，深信服等在内的主流厂商的防火墙等安全设备；(提供 web 配置界面截图,并加盖供应商公章)； 46. 支持 web 登录扫描，支持 Cookie/Session 认证、Form 认证、Basic 认证、NTLM 认证、Digest 认证和 SSL 证书认证； 47. 报表具备导出功能，可以导出 Excel、Word、HTML、Pdf、XML5 种格式； 48. 支持三种漏洞验证方式：浏览器验证、注入验证、通用验证； 49. 支持 IPV4、IPV6 双协议栈地址扫描； 50. ★千兆电口≥6 个，板卡扩展槽≥1，实配 1T 硬盘，1000 个 IP 地址或域名扫描授权，3 年漏洞升级许可授权，实配数据库扫描、web 漏洞扫描、系统漏洞扫描、配置核查功能授权。
7	APT 防护沙箱	51. 支持 HTTP、FTP、SMTP、POP3、IMAP4、NFS、SMB 这几种协议的流量还原，通过解析主流的应用协议，对协议传输中承载的文件及关键字段信息进行分析还原； 52. ▲支持检测文件大类包括：办公类文件（doc、xls、ppt、rtf、vsd 等)、可执行文件（exe、dll、sys、scr、ocx 等)、Email 文件（eml、msg 等)，能够检测分析的文件类型不少于 50+个(提供证明材料并加盖供应商公章)； 53. 检测引擎至少包括：AV 检测引擎、Windows 启发式引擎、IPS 检测引擎； 54. 支持检测包括不限于恶意广告软件、后门程序、病毒、漏洞利用、灰色软件、蠕虫、间谍软件、木马/僵尸网络、勒索软件、黑客工具、Rookit、钓鱼等；

		55. 支持根据恶意文件危害程度给出高危、中危、低危的威胁等级； 56. ▲支持通过查看恶意文件的详细检测报告，可以查阅文件行为的细节，包括文件威胁行为和文件的传播信息等(提供证明材料,并加盖供应商公章)； 57. 支持与防火墙联动部署，防火墙提取流量中文件后送至沙箱进行检测，防火墙与沙箱联动可阻断承载恶意文件的恶意流量； 58. ★硬件服务器：CPU：2*10 核处理器，内存：256G，硬盘：4*4T SATA；2*480G SSD，RAID 卡；接口：GE 电口≥4 个，10GE 光口≥2 个，冗余电源；实配安全沙箱检测能力库升级服务年数 3 年。
8	校园网边界负载均衡与管控系统	59. ★管理接口：独立管理接口千兆电口*1；扩展插槽：扩展插槽*4；数据接口：光口 10G≥4；光口 1G≥4；RJ-45 电口≥1；Console≥1；USB2.0≥2； 60. ★七层应用全功能最大吞吐量≥30Gbps;NAT 连接数≥1100 万;PPS（包转发率）≥800 万； 功能要求： 61. ▲为保障系统稳定性，需支持双 OS 备份，主 OS 故障时，备份 OS 自动切换，切换时间小于 1 毫秒（提供截图证明并加盖供应商公章）； 62. 链路管理：支持>=12 条物理链路聚合，数目和硬件接口数有关，不受软件限制；支持对各条链路进行独立的策略管理和分析统计；支持 4 条虚拟链路，基于物理接口、IP 组定义并对其统计； 63. 工作模式：支持透明网桥模式；支持 NAT 模式；支持路由、NAT、网桥和旁路分析的混合模式；能部署在 MPLS 链路中，并至少对具备 2 级标签的 MPLS 格式报文按应用进行识别、管理和统计； 64. 网络接入：支持路由功能；支持 CGNAT 功能；虚拟 LAN 接口和 WAN 线路最大支持≥600 条；WAN 口支持 PPPOE 拨号功能，自动检测链路状态，断线后自动拨号和支持计划定时重播；支持 WAN 线路独立对外 ping 的功能；支持端口映射，可以设置映射内网 ip 的某个端口或者某段连续的端口（如映射端口 5000-6000）到某个 WAN 接口，或者某些 WAN 线路组成的线路群组上;支持 DHCPSERVER,可以基于 VLAN 等条件分配 IP 地址，可以支持多个 DHCPSERVER；支持 PPPOE SERVER，单台最大支持同时在线用户不小于 18000； 65. 隧道通信：支持组建 SD-WAN 隧道，支持分部与总部之间跨运营商组网，支持吞吐≥10Gbps,支持基于域名进行隧道通信。支持国密算法 SM3,SM4 的 IPSEC VPN； 66. 应用路由：支持对 P2P 下载、网络电视、网络游戏、Web 视频和普通 HTTP 流量做应用分流；支持利用 600 条以上 WAN 线路进行分流；支持基于域名的路由；

		67. ▲网络质量感知：对网络中网络质量进行分析，实现对“客户时延+服务时延+应用时延”的输出，及网络内数据包大小的适时监控和输出，定位网络服务质量的问题点，提高运维质量（提供截图证明并加盖供应商公章）； 68. ▲负载均衡：负载均衡模式支持源 IP、目标 IP、源 IP 加目标 IP、4 元组（源 IP、源端口、目标 IP、目标端口）四种方式；需要支持 600 条 WAN 线路之间的负载均衡（提供截图证明并加盖供应商公章）； 69. 服务器负载：需支持服务器负载，服务器负载均衡需支持根据源 IP，源+目 IP 做 HASH 均衡，也支持加权轮询均衡算法； 70. ▲终端共享检测：能够及时检测通过路由共享上网的 PC 个数，支持检测并控制网关“一拖 N”行为功能；基于 7 层协议特征检测网关后面的私有 IP 地址信息，并能以“共享 IP 数”如“共享用户超过 3 人”为触发条件，对宿主 IP 进行两大类控制动作：流量控制和 HTTP 管控（提供截图证明并加盖供应商公章）； 71. ▲支持端口镜像功能；可根据设置条件将类如迅雷、网桥设备上行方向、某 IP/IP 段、iPhone 手机上网流量、未知协议等流量等镜像至指定网络接口，与第三方审计设备联动，便于用户做精细化、个性化的数据分析（提供截图证明并加盖供应商公章）； 72. ▲智能 DNS：可根据源 IP、目标 IP、访问域名、所在线路等组合条件实现对域名访问的控制；域名控制方式支持阻断、劫持和重定向和 QPS 限制。自动对移动终端型号进行识别，不依赖特征库，对移动设备的网络访问进行控制和管理（提供截图证明并加盖供应商公章）； 73. ▲微信通知和断网：通过微信通知，可以随时掌握设备的运行状态，授权信息等内容；具有“一键断网”功能，可以随时通过微信发出指令，阻断内网有问题服务器的 IP 或者域名（提供截图证明并加盖供应商公章）； 74. PPPOE 服务：支持 PPPOE SERVER，单台最大支持 32768 用户在线；支持本地认证、radius 认证、免认证功能；PPPOE SERVER 支持与 Radius 认证计费系统对接，并能接收 Radius 服务器下发的限速，踢掉在线用户等指令；可针对用户上线发布公告，用户到期提醒和过期提示；支持地址池数目>=64 个；支持外部 BAS 认证（PPPOE 旁路功能）；支持 PPPOE 代拨，最少支持 24K 外网代拨帐号，每个代拨帐号可以支持 1 个或多个内网 IP 上网；支持 PPPOE 代理，可根据服务名称代理，也可以根据帐号名称代理，在线代理帐号数>=3000； 75. ▲IPV6：支持对 IPv6 2～7 层流量的识别能力，特别是针对第 7 层的应用识别能力，能够识别主要应用协议，支持针对 ipv6 进行路由；支持 IPv6 到 IPv4 的映射，将 IPv6 的公网 IP 与内网 IPv4 的服务器做映射； 76. ▲服务器资产管理：支持服务器资产管理，能做基于服务器的负载均衡，实现一键断网功能；

		77. 缓存牵引：支持缓存牵引，可以根据策略将视频或大流量下载用户牵引到指定的缓存，提升用户体验并节省带宽；支持对不同类型的文件牵引到不同的缓存服务器；最多可以支持多达 128 台缓存设备牵引； 78. ▲其他功能：支持 web 认证；可以旁路或串接模式下，深度分析 RADIUS 数据包，找到帐号和 IP 地址对应关系；支持云平台集中管理设备；支持“内网伪 IP”防护功能； 检测并控制内网中毒设备伪装大量假 IP 攻击网络的行为；支持“垃圾包”检测及过滤功能；支持“IP 分片”攻击检测及过滤功能；支持对异常流量 IP 的实时查询、日志反查功能；支持虚拟身份如 QQ 号码、新浪微博帐号与 IP 地址、用户帐号关联的日志功能；支持 60 万同时在线 IP 环境下，可实时显示每一个 IP 流量速率和当前各个应用的速率明细；可提供 IP 对应的身份信息，如 QQ 号码、MSN 帐号、POP3 帐号、微博帐号等； 79. ▲CGNAT 防火墙，负载均衡，流控，行为管理，SD-WAN，NPM 网络质量分析，BRAS 拨号服务功能，无线 AC 控制器等功能需一体化功能全开，无需另外支付采购费用（出具承诺函并加盖供应商公章）； 80. 需提供三年特征库免费升级服务。
9	财务专网防火墙	81. 标准机架式 1U 设备，实配：千兆 Combo 接口≥8，万兆光口≥2，千兆 WAN 口≥2，配置双双电源，支持 1*USB2.0+1*USB3.0；SSL VPN 并发数实配 100 可扩展 500，IPSec VPN 隧道≥4000，虚拟防火墙数量≥50，实配 IPS、AV、URL 过滤升级 license 不低于 3 年，实配 SSD 硬盘不低于 64G； 82. ★吞吐量≥2Gbps，最大并发连接数≥300 万，每秒新建连接数≥7 万，IPSec 吞吐量≥2Gbps， SSL_VPN 吞吐量≥300Mbps ，SSL 代理吞吐量≥300Mbps，IPS 吞吐量≥1.5Gbps； 83. ▲为满足国家信息化创新要求，产品采用自主研发的关键芯片(CPU)(需提供具有 CNAS 或 CMA 标识的第三方实验室测试报告证明，提供报告复印件并加盖供应商公章)； 84. 具有未知威胁的检测能力，支持与本地或云端沙箱或类似设备联动，实现对 APT 攻击的防御功能； 85. 能够基于 IP、IPv6、MAC 地址、时间进行访问控制策略控制；支持自定义安全策略，安全策略组功能；支持策略冗余/命中分析； 86. 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议； 87. 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等； 88. 支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险； 89. 支持对 HTTPS，POP3S，SMTPS,IMAPS 加密流量代理解密后，并进行内容

		过滤，审计，安全防护。
10	财务专网日志审计系统	90. 支持旁路部署、分布式部署以及级联部署模式； 91. 配置 GE 电接口数量≥4，10GE 光口数量≥2，扩展插槽≥1，最大管理资产数 200，EPS≥8000 EPS，本次配置 30 台日志管理授权； 92. 支持 Syslog、SNMP Trap、HTTP、SFTP 协议日志收集； 93. ▲支持对日志进行细粒度解析，包含不仅限于采集器接收时间、日志时间（起始时间/结束时间）事件级别、事件类型、事件消息、事件名称、来源地址、来源端口、目标地址、目标端口、事件设备分类、事件行为分类、事件特征分类、事件结果分类等，字段信息可通过解析规则增加和修改，默认维度超过 200+（提供 web 配置界面截图,并加盖厂商供应商公章)； 94. 支持网络安全设备、交换设备、路由设备、操作系统、应用系统、虚拟环境等，支持 200+厂家设备的接入； 95. 支持通过日志等级进行过滤，支持配置过滤规则，将低价值的日志过滤掉； 96. ▲内置 5000 种以上设备类型的解析规则（提供 web 配置界面截图,并加盖供应商公章)； 97. 内置 50+关联分析规则，关联规则可通过界面上传更新。

注：1.技术参数表中标注“▲”号的为重要技术参数，参数表中有相关证明材料要求的，投标人应按要求提供证明材料。参数表中没有证明材料要求的，证明材料应当为产品制造商发布的印刷资料或说明书或技术白皮书或产品制造商官网发布的产品信息截图或第三方检测机构出具的检测报告、所投产品实际使用界面截图等证明材料，未按要求提供证明材料或者有负偏离响应的，将作扣分处理。（如相关证明材料为英文版，请同时提供中文版）。

2.技术参数表中标注“★”号的参数属于实质性要求，投标人需要提供产品制造商发布的印刷资料或说明书或技术白皮书或产品制造商官网发布的产品信息截图或第三方检测机构出具的检测报告等证明材料予以佐证是否偏离，若有负偏离或未提供证明材料，视为无效响应。（如相关证明材料为英文版，请同时提供中文版）。

★四、商务要求

1.履约保证金

1.1 金额：合同金额的 5%

1.2 交款方式：履约保证金可以以支票、汇票、本票或者金融机构出具的保函等非现金形式提交（包括网银转账，电汇等方式）。

1.3 收款单位：乐山师范学院

1.4 开户行：建行四川省乐山分行营业部

1.5 开户行行号：105 665 008 085

1.6 银行账号：5100 1698 6080 5150 2679

1.7 履约保证金退还时间：履约验收合格 10 日内退还。

1.8 履约保证金不予退还情形：验收不合格或未按照合同约定履行相关责任。履约保证金不予退还的，将按照有关规定上缴国库。逾期退还履约保证金的，将依法承担法律责任，并赔偿供应商损失。

2.付款条件（进度和方式）

2.1 采购清单中所有系统建设验收合格之日起 30 日内支付合同金额的 95%，正常运行满半年后 30 日内支付合同金额的 5%。

2.2 中标供应商须向采购人出具合法有效完整的完税发票及凭证资料进行支付结算，逾期提交的，采购人有权拒绝支付且不承担违约责任。

3.交货要求

3.1 交货时间：合同签订生效后的 30 日内交货到交货地点，按要求完成全部安装调试、验收合格并交付使用。

3.2 交货地点：乐山师范学院校内。

4.质量要求

4.1 中标供应商须提供全新的货物（含零部件、配件等），表面无划伤、无碰撞痕迹，且权属清楚，不得侵害他人的知识产权。

4.2 货物必须符合或优于国家（行业）标准，以及本项目招标文件的质量要求和技术指标与出厂标准。

4.3 货物出现质量问题时，中标供应商应负责三包（包修、包换、包退），费用由中标供应商负担，采购人有权到中标供应商生产场地检查货物质量或生产进度。

4.4 货物到现场后由于采购人保管不当造成的质量问题，中标供应商亦应负责修理，但费用由采购人负担。

5.包装与运输

5.1 包装：商品使用的塑料、纸质、木质等包装材料或快递封装材料，包括封套、胶带、面单、包装袋/箱、填充物、集装袋、周转箱等应符合环保要求，设备包装应坚固完好，能抗御运输、储存和装卸过程中正常冲击，振动和挤压，并便于装卸和搬运。设备包装前检查包装材料的材质、规格和包装结构与所装产品的规格和重量相适应。组件包装时安全，防止撞击，包装表面应清洁。组件排放整齐，不可有高低不平。外包装箱表面不应该有突出的锁扣等装置，以避免箱体移位时发生拉挂等现象，影响箱体安全。

5.2 运输：装运设备的运输工具应清洁、干燥、无污染物。敞车运输时，必须用防雨布盖好，以保证设备不被雨(雪)浸入。设备中转时，应堆放在库房内。短暂露天堆放时，必须用防雨布盖好，产品在装卸时，应采用合适的装卸方式，严防将包装箱(件)损坏，包装箱应注意谨慎堆放，防止产品碰伤。装载时，集装箱与包装箱之间、包装箱之间应用防震减压的填充物填实，不得留有空隙。防止在运输途中造成货物之间互相碰撞、摩擦，避免发生箱体移位。避免货物在运载工具上的堆码不当，使底层货物承载过重，造成包装破损，甚至商品在运输过程中变形，损坏。在运输过程中避免接触腐蚀性物质。

6.验收标准：

6.1 验收严格按照政府采购相关法律法规、《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）、招标文件要求及投标文件内容进行验收，由采购人组织，中标供应商配合进行。货物运输到采购人指定地点卸货存放和安装，卸货及安装由中标供应商负责并承担费用，采购人协调配合。采购人及中标供应商双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在招标文件和投标文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。

6.2 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，采购人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中标供应商承担，验收期限相应顺延。

6.3 如质量验收合格，双方签署质量验收报告。项目验收结果合格的，供应商凭验收合格证明书至履约保证金收取单位办理履约保证金的退付手续；验收结果不合格且拒不整改的，履约保证金将不予退还，也将不予支付采购资金，还可能上报本项目同级财政部门按照政府采购法律法规等有关规定给予行政处罚或者以失信行为记入诚信档案。

6.4 中标供应商应将所提供货物的装箱清单、配件、随机工具、用户使用手册、原厂保修卡等资料交付给采购人；中标供应商不能完整交付货物及本款规定的单证和工具的，必须在采购人书面（包括电子邮件）通知后十日内负责补齐，否则视为未按合同约定交货。

6.5 如货物经中标供应商 2 次维修或更换仍不能达到合同约定的质量标准，采购人有权退货，并视作中标供应商不能交付货物且须支付违约赔偿金给采购人，采购人还可依法追究中标供应商的违约责任。

7.售后服务：

7.1 质保期：36 个月。

7.2 安装调试：

7.2.1 中标供应商需负责设备安装、调试且承担由此产生的一切费用；

7.2.2 中标供应商须指派专人负责与采购人联系售后服务事宜；

7.2.3 货物到达现场后，中标供应商接到采购人通知后 3 个工作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。中标供应商需提供每个设备的说明书（电子版）一份给采购人。

7.3 售后内容：

7.3.1 提供现场操作培训；

7.3.2 保修期内每年至少保养 2 次并提供保养报告；保修期后，负责设备的终身维修及零配件的及时供应；

7.3.3 提供使用说明书、技术说明书。

7.4 维修响应速度：提供 24 小时售后服务热线，设备在质保期内，中标供应商负责因设备本身缺陷导致的各种故障的技术服务和设备的维修，中标供应商接到通知 2 小时响应，24 小时内完成维修或更换，并承担所有费用，若 24 小

时内无法恢复正常使用，中标供应商须提供备用机，中标供应商未按上述约定延迟服务给采购人造成的所有损失均由供应商独立承担。

7.5　质保期后若设备故障

中标供应商无条件先负责修理好设备，并经使用人员使用正常后支付相关维修费用。质保后修复设备若涉及更换配件，配件只收取厂家成本费。

7.6 培训

中标供应商要对使用人员进行现场使用培训和使用后再培训，确保使用人员能熟练的独立、正确使用。还需要对采购人设备维修人员组织培训。

五、其他要求

1.供应商需针对本项目提供售后服务方案，方案包含售后培训方案、售后服务计划及售后服务应急方案、质量保障方案、维修响应时间及保障方案等。

注：本章标注“★”号的参数为实质性要求，投标人若未满足其投标响应文件无效。