采购需求

一、项目概况

1.本次招标项目为河南交通职业技术学院智慧校园基础设施及服务保障提升项目，共 2 个标段（分包）：

1.1 河南交通职业技术学院智慧校园基础设施及服务保障提升项目包 1：职业院校数字校园建设试点数据对接系统包；

1.2 河南交通职业技术学院智慧校园基础设施及服务保障提升项目包 2：数据中心数据存储设备扩容升级、UPS 系统更新升级、服务器整机硬件质保服务延保、网络信息安全驻场运维服务支撑包；。

2.本次采购标的（货物）对应的中小企业划分标准所属行业为：

2.1 河南交通职业技术学院智慧校园基础设施及服务保障提升项目包 1：软件和信息技术服务业。

2.2 河南交通职业技术学院智慧校园基础设施及服务保障提升项目包 2：见货物清单备注。

二、招标货物清单及技术参数/服务要求

河南交通职业技术学院智慧校园基础设施及服务保障提升项目包 2

2.1 招标货物清单

序号	设备名称	数量	单位	备注
1	存储升级扩容	1	套	工业
2	UPS1	1	套	工业
3	电池	80	节	工业
4	区域监控软件	1	套	软件和信息技术服务业
5	温湿度传感器	1	个	工业
6	漏水控制模块	1	台	工业
7	数字量输入模块	1	个	工业
8	烟感探测器	2	个	工业
9	串口服务器	1	台	工业
10	模块箱	1	个	工业
11	■UPS2	3	套	工业、核心产品
12	空调	1	台	工业
13	服务器延保服务 1	1	套	软件和信息技术服务业
14	服务器延保服务 2	1	套	软件和信息技术

				服务业
15	Web 应用安全网关延保服务	1	套	软件和信息技术服务业
16	安全运维服务	2	年	软件和信息技术服务业

2.2 技术参数/服务要求

二、技术参数要求

序号	产品名称	功能参数	数量	单位	备注
1	存储升级扩容	▲1、总体要求：与现有存储（型号为：OceanStor 5310 V5）控制器兼容，无缝对接,投标时提供投标货物厂家出具的兼容性承诺，并加盖投标货物厂家公章；若不兼容，须提供合理化解决方案，满足客户实际需求，实现与学校现有存储无缝对接； 2、系统架构：多控制器架构，最大支持≥8 控；配置双 Active-Active 控制器;采用 2U 盘控一体架构； 3、控制器在线运行时，能够对主机接口卡进行热插拔； 4、为便于管理，本次扩容不采用异构存储虚拟化或虚拟化整合设计； 5、配置≥6*3.84TB SAS SSD 硬盘单元,配置≥24*8TB 7.2K NL SAS 磁盘单元，配置 1 套磁盘扩展框，扩展框≥24 个磁盘槽位，包含线缆和上架套件； 6、磁盘系统采用高安全性 RAID 保护； ▲7、支持进行 SAN 与 NAS 的一体化免网关双活，任意一套设备宕机均不影响上层业务系统运行（业务不中断）。支持 FC 链路复制，SAN 双活支持双活流量分担，支持故障自动切换和回切，提供加盖生产厂商公章的具备 CNAS 或 CMA 资质的第三方权威评测机构签字盖章的测试报告扫描件； 8、存储扩容具备安全在线，无需停机扩容能力，以保证核心应用系统不停机； ▲9、提供 SSD 硬盘寿命监控技术，并在系统中显示每一块 SSD 硬盘的磨损度以及剩余寿命，提供加盖生产厂商公章的操作界面截图扫描件； ▲10、提供三年质保服务，提供存储扩容实施服务及安装服务，提供生产厂商针对本项目的三年售后服务承诺函扫描件。	1	套	
2	UPS1	▲1、配置容量：≥60KVA，在线式双变换 UPS 2、输入电压：380VAC（-40%～+25%），输入频率：40～70Hz 3、不同负载率下的输入功率因数应为： 100%负载率≥0.99	1	套	

		50%非线性负载：≥0.99 25%非线性负载：≥0.98 提供加盖生产厂商公章的权威第三方机构检测报告扫描件证明； 4、标配主路输入，旁路输入，输出，手动维修旁路开关，设备需要标准支持上、下走线功能； ▲5、支持电池冷启动，电池节数可调范围≥14 节，提供加盖生产厂商公章的设备彩页或其他证明资料扫描件； 6、输出功率因数：1,0-40℃长期满载运行无降额；提供加盖生产厂商公章的设备彩页或其他证明资料扫描件； ▲7、满载时系统效率：≥96%；提供加盖生产厂商公章的权威第三方机构检测报告扫描件证明； 8、逆变器过载能力： 110%额定电流≥60min 125%额定电流≥10min 150%额定电流≥60s″ ▲9、工作温度：0～+40℃，满载运行无降额，提供加盖生产厂商公章的设备彩页或其他证明资料扫描件； 10、内置并机控制功能，具有多台 N+1 直接并联工作及负载均分性能，各机负载电流不平衡度 ≤2%额定输出电流，可并联数量≥4，多机并联或扩容时无需增加并机柜等设备，只需现场增加并机线缆即可，提供加盖生产厂商公章的证明材料扫描件； 11、内置双总线同步控制功能，便于现场只需连接双总线线缆即可实现双母线系统的同步输出，无需涉及其它组件，提供加盖生产厂商公章的证明材料扫描件； 12、UPS 在市电和电池两种状态间切换的时间应为0，从逆变器停止工作时起，到电网直接供电时止或从电网直接供电起到恢复逆变器工作时止所需要的时间<4ms； 13、UPS 应具备逆变器输出并网回馈自老化测试功； ▲14、UPS 具备并机系统 ECO 工作模式(经济模式)，减小并机系统中 UPS 自身损耗，提高系统供电效率至 99%以上，提供加盖生产厂商公章的证明材料扫描件； 15、UPS 具备智能并机功能，允许并机系统在轻载时，安排 UPS 轮换休眠，提升在线 UPS 负载率，进而改善带载效率，提供加盖生产厂商公章的证明材料扫描件； 16、系统应具有三遥性能，遥测项目：三相输入电			

		压，直流输入电压，三相输出电压，三相输出电流，输出频率；遥信项目：同步/不同步状态，UPS/旁路供电，蓄电池放电电压低，市电故障，整流器故障，逆变器故障，旁路故障；对遥信项目，要求设备能够对每一类故障或状态提供继电器干接点。〞 17、设备应能提供全中文监控及操作界面和全中文远程监控管理界面，应提供全中文彩色液晶屏，能够动态实时显示运行状态、输入输出电池电压、电流以及故障告警信息等；提供加盖生产厂商公章的设备彩页或其他证明资料扫描件； ▲18、产品满足长距离运输安全性，提供加盖生产厂商公章的第三方 ISTA 运输认证证书扫描件； 19、为保证售后服务能力，要求生产厂家必须有售后服务机构和备件库； ▲20、提供生产厂商针对本项目的三年售后服务承诺函扫描件。			
3	电池	1、采用 12V 100AH 蓄电池，要求使用阀控式密封铅酸蓄电池，使用过程无需补充水，完全密封，不渗漏液体，无酸性气体溢出； 2、蓄电池采用吸附式玻璃纤维隔板技术，气体复合效率达到 99%； 3、要求蓄电池可提供阻燃槽盖，使电池更安全且具有更长的寿命； 4、蓄电池温度使用范围：（放电：-15-50℃/充电：0-40℃ /贮存：5-40° C）； ▲5、对 UPS 和电池组每半年进行一次检测维护，包括清理灰尘、测量电池性能、检查主机状态等，3 年共 6 次，提供供应商承诺函； 6、提供电池运输、市电接入电缆、搬运、安装调试服务及项目所需电池架、电池空开、电池连接线等所需的各类辅材。	80	节	
4	区域监控软件	1、实时监测 UPS 整流器、逆变器、电池、旁路、负载等各部分的运行状态与参数，UPS 电源输入、输出电压、电流、频率、功率等各项参数和状态，报警参数设置等，可通过历史曲线方式显示重要参数的变化，要求接入现有机房环境监控系统管理系统统一管理； ▲2、提供生产厂商针对本项目的三年售后服务承诺函扫描件。	1	套	
5	温湿度传感器	1、供电电压 DC12V；LCD 液晶显示； 测量范围：温度：-20℃~70℃ 湿度：0~100%rh； 测量精度：温度：±0.5℃ 湿度：±3%RH；	1	个	

		RS485 输出 多点，双工位（静态及动态变量）； 最大通讯距离 1200m，端子直接连接； 地址 1~254，可通过按键设置，也可通过软件设置，要求接入现有机房环境监控管理系统统一管理； ▲2、提供原厂商针对本项目的三年售后服务承诺函扫描件。			
6	漏水控制模块	1、 供电电源 12-60VDC ； 灵敏度范围档位 1：0—250KΩ，档位 2：0—600KΩ，档位 3：0—5MΩ，档位 4：0—50MΩ ； 短路时阻抗<50Ω； 2、配置≥3 米漏水感应绳，要求接入现有机房环境监控管理系统统一管理； ▲3、提供原厂商针对本项目的三年售后服务承诺函扫描件。	1	台	
7	数字量输入模块	1、输入通道≥8； 2、隔离≥6 路差分和≥2 路单端隔离； 3、隔离电压 5000Vrms； 4、数字电平 0 1VMax； 5、数字电平 1 4V～30V； 6、输入阻抗 3Kohms； 7、输出信号 RS485； 8、功耗 0.6W； 9、电源输入 10V～30V； 10、带 LED 显示。	1	个	
8	烟感探测器	1、光电探测方式； 2、具有手动测试功能； 3、工作电压：DC 12 V； 4、静态电流：≤8Ma； 5、报警电流：≤35mA； 6、报警输出：继电器常开 / 常闭； 7、探测灵敏度：Ⅱ、Ⅲ级； 8、监测面积：≥20 平方米，要求接入现有机房环境监控管理系统统一管理。	2	个	
9	串口服务器	1、LCD 显示屏，接口模式：TCP server、TCP client、UDP，可通过 Telnet、Web 浏览器或 Windows 管理工具进行配置，支持 SNMP MIB-II 网络管理协议，输入电压 12 - 48 VDC，1 个以太网接口 ，电磁隔离保护 1.5 kV（内置），接头 接线端子，端口数量≥4，串口标准 RS-422、RS-485，可调节终端电阻，金属外壳，导轨式安装； ▲2、提供原厂商针对本项目的三年售后服务承诺函扫描件。	1	台	
10	模块箱	1、挂墙安装或就地安装； 2、标准的 DIN 导轨 模块安装数量 单排可安装 2 个，	1	个	

		最多叠加 2 排，共 8 个，内置 12V1.5A 工业电源。			
11	■UPS2	▲1、UPS 容量≥6KVA； 2、UPS 输入参数： 输入输出方式：单单 主旁电网适应性：主旁同源 输入电压范围：100-288V，输入频率范围：40Hz-70Hz，输入电流谐波含量：<5% 输入功率因数：0.99 电池节数：16（默认）、18、20 节可调 额定功率：5.4KW 3、UPS 输出参数： 输出功率因数：0.9，输出电压稳定度：0.01，输出频率稳定度：±0.1Hz 输出电压波形畸变率：阻性负载：2%；整流性负载：5% 过载能力（%额定负载）：125%，10mins 4、提供本次新购 UPS 的运输、市电接入电缆、搬运、安装调试及电池空开、电池连接线等所需的各类辅材； ▲5、提供加盖生产厂商公章的针对本项目的三年售后服务承诺函扫描件。	3	套	核心产品
12	空调	1、制冷量：≥7200W 2、制冷功率：≥2350W	1	台	
13	服务器延保服务 1	设备 SN 码：J302D3TD；J302D3TA；J302D3TB；J302D3TE；J302D3TF；J302D3TC。 1、对学校原设备提供三年原厂延保服务，日期为 2023 年至 2026 年，内容包含：延保期内，硬件发生故障免费更换；软件免费升级更新。7*24 小时电话响应；设备故障时 4 小时上门服务。 ▲2、提供加盖学校原设备生产厂商公章的针对本项目的三年售后服务承诺函扫描件。	1	套	
14	服务器延保服务 2	设备 SN 码：BL65YM2；BL7BYM2；BLN3YM2；BLP8YM2。 1、对学校原设备提供三年原厂延保服务，日期为 2023 年至 2026 年，内容包含：延保期内，硬件发生故障免费更换；软件免费升级更新。7*24 小时电话响应；设备故障时 4 小时上门服务。 ▲2、提供加盖学校原设备生产厂商公章的针对本项目的三年售后服务承诺函扫描件。	1	套	
15	Web 应用安全网关延保服务	设备 SN 码：0123201611159991 1、对学校原设备提供三年 Web 应用防护特征库升级授权，提供三年原厂延保服务，日期为 2023 年至 2026 年，内容包含：延保期内，硬件发生故障免费更换；软件免费升级更新。7*24 小时电话响应；设备故障时 4 小时上门服务。	1	套	

		▲2、提供加盖学校原设备生产厂商公章的针对本项目的三年售后服务承诺函扫描件。			
16	安全运维服务	1、日常巡检：每工作日查看设备运行日志、分析设备运行状况，及时分析处理各类安全设备、安全系统的安全事件告警； 2、漏洞扫描：定期对服务器操作系统、数据库、应用系统等进行漏洞扫描，及时发现安全隐患； 3、安全检测：定期对服务范围内的网络设备、服务器操作系统、数据库系统、应用软件系统的安全策略和安全配置进行检查和测试，从中获得相关的信息、发现系统面临的威胁以及存在的安全性。包括口令策略、帐户权限、网络服务、访问控制、用户鉴别等； 4、安全分析：搭建运维管理平台等工具，对部署的安全产品产生的网络访问日志、管理行为记录、操作行为记录、产品运行记录和网络流量等数据，设置各种关联分析负责和过滤条件，进行安全审计工作，挖掘出有价值的网络攻击、运行故障等信息； 5、设备配置及优化：根据需求调整安全设备配置，制定调整系统策略优化、网络拓扑优化、安全域规划与配置、IP 规划、VLAN 优化等策略，并根据实际情况调整与实施； 6、安全加固：根据操作系统安全评估及漏洞扫描、安全检测、日志分析和安全检测中发现的问题，对服务器、网络设备、数据库系统等安全漏洞进行修补，加强安全配置、安全加固处理； 7、配置备份：每周对安全设备配置进行备份，每次配置调整后应进行备份； 8、设备升级：在设备系统软件或特征库新版本发布后，及时完成设备软件升级； 9、病毒库系统升级：在病毒库版本发布后，利用工具及时完成 PC 终端和 Server 终端病毒库升级及维护工作； 10、新增设备维护：配合完成新增安全设备的安装调试； 11、更新替换设备维护：配合更新替换安全设备的安装调试。 12、全面、精准地梳理出暴露在互联网上的 IT 资产，并能深入识别运行在资产上的中间件、应用、技术架构的详细情况及变化情况，反应资产的动态情况； 13、基于 IP 或域名，采用多种探测技术，对学校暴露在互联网上的 IT 资产进行常态化扫描和监控，发现目标网络中资产和应用，归纳资产的安全态势、总结信息资产变化的情况；	2	年	

		14、利用互联网资产发现工具，结合应用场景实现如下需求：对信息系统内的主机/服务器、安全设备、网络设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等进行主动发现，并生成资产及应用列表，列表中至少包括设备类型、域名、IP、端口、协议； 15、根据域名、IP、端口、中间件、应用、技术架构、变更状态、业务类型（自定义）等条件对资产进行查询、统计，并能对资产进行周期变化监控； 16、对资产 IP、域名与安全大数据进行比对分析，发现互联网资产安全风险，定位高风险资产； 17、评估互联网资产的防御措施，如：是否使用了硬件 WAF 做流量清洗，是否使用了 CDN 服务，是否使用了云端的 WEB 流量清洗服务。通过对这些防御措施的检测，结合建模，形成资产防护能力的赋值评分； 18、通过多种引擎扫描网站存在的安全漏洞； 19、基于网络流量,实现对网络中存活的服务器状态进行梳理。抓取包括但不限于：服务器类型、服务器版本、在线状态、开发语言、开放端口、新增资产、资产变更、新增端口、端口变更； 20、基于网络流量，实现对网络中存在一些非常规服务进行梳理，采用被动流量抓取。抓取信息包括但不限于：源 IP、目的 IP、代理地址、代理方式、使用次数；对网络中存在的 web 攻击进行梳理分析，流量抓取方式采用被动流量抓取方式。抓取信息包括但不限于：源 IP、目的 IP、利用模块、攻击方式、结果类型、敏感信息。 21、综合安全经验、情报，并依托于学校现有安全检测设备，对现有的应用系统的主机、流量、日志等进行安全审计，找出其中存留的攻击者痕迹，发现、复盘并合理处置正在和曾经发生的入侵事件等隐藏较深的威胁； 22、能基于主流数据分析方法对 WEB 日志进行分析； 23、应能在不依赖任何规则的情况下，安全分析人员利用结合学校实际情况制定相应的分析模型，实现在无任何攻击规则情况下发现攻击后门； 24、应能结合云端威胁情报，对日志中攻击者信息进行标记，了解攻击者状况，辅助安全分析人员对学校发现的安全事件进行判断； 25、基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案； 26、对内，能关联内部的各类设备和记录数据，包			

		括 DNS 日志、HTTP 日志、DHCP 日志等，能全面追踪与相应事件关联的内部数据，发现关联的内部主机，回溯攻击位置、攻击途径与确定损失；对外，能运用威胁情报数据对攻击者身份、团伙、资产等进行追踪溯源和发现； 27、实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件； 28、在发现相应的威胁或病毒后，提供清理工具以及清除办法，进行威胁的定位与清除； 29、提供威胁态势感知能力，需要持续跟踪攻击团伙，对攻击者最新动向，包括最新的攻击手段、攻击资产进行持续监控，在相关设备上进行安全策略调整。同时，提供威胁情报共享能力，实现对威胁的提早预警，防范于未然。 30、通过自动化安全扫描和人工渗透测试对网络进行全面检测，帮助学校了解并提高应用开发程序的安全性，有效预防可能存在的安全风险。对学校现有技术系统环境提供全面的评估服务； 31、能够模拟黑客使用的漏洞发现技术和攻击手段，找到系统最脆弱的环节，需采用可控制的、非破坏性质的渗透测试,不会对被评估的系统造成严重的影响； 32、通过被披露的操作系统及应用软件（或模块）的安全漏洞，利用这些漏洞及相关工具对网站及其应用进行测试； 33、对于采用口令进行用户认证的应用，将使用工具进行口令猜测以获取用户帐号/密码，口令猜测使用字典攻击和暴力破解攻击； 34、对网站应用程序的输入数据进行合法性检查，对客户端参数中包含的某些特殊内容进行不适当的处理，进行预判。具体方法主要为：SQL 语句注入、隐蔽命令执行、遍历目录/文件； 35、利用工具对信息系统进行彻底扫描，对包括但不限于异常进程、网络异常连接、异常流量、启动项进行深入分析，查找系统是否存在后门。 36、在发生严重安全事件后或学校需要的其他时间节点时，提供安全应急响应服务，提供有效和及时的安全运营服务； 37、在重大活动、重要会议等重要时期，除现场运维人员值守外，还可提供在线安全专家 7*24 小时值守服务，监控发现所有的安全风险由安全专家审核，精准定位安全事件，包括篡改事件、网页挂马、高危漏洞、断网事件等，保证平台通报预警报告无误			

		报； 38、在完成本项目安装调试后，供应商须提供至少1名常驻我校的专职技术人员进行日常运维工作； 39、驻场运维人员工作地点在我校指定地点，工作时间与我校办公时间一致，人员所有费用及社保关系均由供应商负责； 40、根据采购人需求情况建立一套完整的文档管理体系，响应文件中应含有具体的项目档案、运维档案，包括但不限于日常记录单、故障记录单、响应记录单运维管理文档模版，文档模版须在响应文件中提供，经用户书面确认后施行；提供重大事件应急响应预案，提供对于新发现的病毒、0day漏洞，厂商能够于2小时内作出响应。			

注:本次招标核心产品为“■UPS2”。

注 1、供应商须在投标文件中如实响应上述要求，对材料真实性负责，如果存在编制虚假材料情况，采购人将有权按照政府采购相关规定上报上级管理部门。

2、供应商应如实描述所报产品的技术参数和性能，不得完全复制粘贴上表技术参数和性能描述。因完全复制粘贴上表技术参数和性能描述将视为不响应，产生的不利于供应商的评审风险由供应商自行承担。

实质性技术要求：特指技术要求中加“★”条款,本项目无。

三、供货要求

1、投标人须提供符合国家质量标准、部颁标准、行业标准或本招标文件规定标准的、供货渠道合法的全新原装合格正品（包括零部件），如安装或配置软件的，须为正版软件。所提供的货物应当同时符合国家有关安全、卫生、环保规定。本项目中所投产品涉及工业产品生产许可证的，该产品应具有由质监部门颁发给制造商的关于该产品的《全国工业产品生产许可证》；本项目中所投产品涉及纳入国家认证认可监督管理委员会现行《强制性产品认证目录描述与界定表》管理的强制性认证产品（简称 3C 认证产品）的，该产品应具有由认证机构颁发给制造商的该产品强制性认证证书；本项目中所投产品属于《信息安全产品强制性认证目录》内的信息安全产品的，该产品应具有由中国信息安全认证中心按国家标准认证颁发的有效认证证书；本项目中所投产品涉及网络通讯产品的，该产品应具有工信部门颁发的入网许可证。

2、采购人使用中标人中标的货物、技术、资料、服务或其他任何一部分时，享有无偿使用权。免受第三方提出的侵犯其专利权、著作权、商标权或其它知识产权的起诉。如果第三方提出侵权指控，中标人应承担由此而引起的一切法律责任和费用。