采购需求（十五）

注：1、以下《采购需求一览表》所列清单为招标人（采购人）所提招标（采购）需求，投标人（供应商）应认真仔细研究，投标时应慎重选择相应的产品及技术参数、规格型号等进行投标。

2、本项目涉及到的商品包装及快递包装，按财办库[2020]123 号文标准执行。

3、投标报价包括采购、运输、人工、安装、售后、验收、税费等所有费用。

4、下列《采购需求一览表》中：标注▲的产品，投标供应商在投标文件《主要成交标的承诺函》中填写名称、规格、型号、数量、单价等信息，承诺函经评标委员会评审认可后随评审结果一并公示，如投标文件中未提供、提供不全将可能导致投标无效。采购人（采购代理机构）在编制招标文件时必须将采购的主要产品(包括核心产品)标注“▲”。按照招标文件要求，标注 “▲”号的产品，投标人必须在“主要成交标的承诺函中”填写该产品的名称规格、型号、数量、单价等具体信息。

5、采购人或采购代理机构查询中国政府采购网相关链接，并根据查询结果，在采购需求一览表填写列入品目清单情况。

采购产品如有列入品目清单内强制采购类节能产品，必须按品目清单要求采购。提供国家确定的认证机构证明网页截图，及认证机构出具的、处于有效期之内的节能产品认证证书，否则按无效投标处理。

采购产品如有列入品目清单内优先采购节能或环境标志产品，根据评标办法要求提供相关证明材料，否则在评标时相关评审项不得分。

采购需求一览表

序号	名称	技术参数和规格型号	数量	单位	列入优先采购和强制采购品目清单情况（优先采购或强制采购）	备注
1	▲高性能服务器（大数据	1、规格：2U 机架式服务器高质量服务器； 2、市场地位：国产知名厂商； ★3、处理器：Intel C624 芯片组，本次配置 2 颗 Intel Xeon 金	5	项		

	运行中心扩容）	牌 5218（16 核 2.3GHz）或此标准以上 CPU，可选最大单颗 28 核处理器，最大支持 2 颗处理器； ★4、内存：配置 256GB TruDDR4 内存，最大支持≥24 条扩展插槽，最大支持≥1.5TB 内存扩展。TPC-E 大于 6500，并提供文件证明； 5、硬盘：配置 2 块 480G M.2 固态硬盘（系统盘）+3 块 1.92T SSD 固态硬盘+21 块 2.4T 10K SAS 2.5 寸硬盘，可支持 SAS/SATA 硬盘、SSD 混插，可选支持≥24 个 2.5 寸硬盘扩展机型；支持内置两个 M.2 且可支持 RAID 0/1； 6、RAID 功能： 930-24i 12Gb 4GB 闪存独立阵列卡，支持 0/1/10/5/50 RAID 卡级别，最大支持 8G 缓存； 7、网卡和 HBA 卡：配置 2 个万兆网口，含模块，4 个千兆电口，1 个独享的远程管理端口，冗余风扇； 8、配件：免工具滑动导轨套件。最大 8 个可选的 PCIE 3.0 扩展槽。 9、电源：电源输出功率≥750W 80+铂金电源，本次配置 2 个热插拔冗余电源，支持 240V 高压直流； 10、冷却系统：配置 6 个冗余（N+1）热插拔系统风扇； 11、硬件管理功能：提供集中式管理系统，方便后期服务器管理和使用，支持 Android 和 iOS 的移动 APP 登陆和查看、管理，可以通过内网和外网用移动 APP 集中监控查看设备的状态、审计日志和报警信息，以及执行设备电源开关动作，要求提供移动 APP 运行界面功能截图证明和移动 APP 下载网址，加盖公章； 12、产品认证：产品通过中国 3C 中国强制性产品检测认证（投标文件提供相关证明材料并加盖公章）； 13、售后服务：提供三年免费整机硬件保修，终生免费技术支持；为保证服务器产品质量，完全响应客户对产品的各项要求，提供 3 年免费上门硬件保修服务承诺函和设备授权函。要求本次设备原厂整机生产，不接受私自拆封和改配。中标商负责之前老系统数据迁移和备份，并提供测试机。系统总停机时间不超过 2 小时。具体测试机使用时间根据项目进展而定。				
2	分布式存储空间扩容	1.分布式存储（Server SAN），支持多个独立的服务器本地 SSD 或磁盘组成一个可以共享的存储资源池。基于面向对象的存储架构，易于管理，并支持横向扩展； 2.嵌入虚拟服务器内核，深入了解虚拟机、应用、底层存储基础架构，缩短 I/O 数据路径降低延时，虚拟服务器的 CPU 资源占用更少，小于 10%，与虚机的迁移无缝集成； 3.在同一个图形界面里管理计算和存储资源，并监控详细的性能与容量，支持 Web 界面； 4.配置部署简单，无需命令行操作，只需在图形化管理界面上点击即可完成对存储的管理简单易行，可通过图化形界面添加磁盘，组织磁盘组，制定存储策略；	1	项		

		5.提供基于存储策略的管理机制，根据业务应用的需求，可以通过变更存储策略进行在线的动态调整业务应用正在使用的存储资源； 6.采用 SSD 作为高速读/写缓存，并且提供可以动态调整的虚拟机级别的读写缓存预留，确保重要应用的读写性能； 7.可实现以虚拟机为中心的快照和克隆，支持每个虚拟机不少于 32 个快照和克隆； 8.支持精简配置功能（Thin Provisioning）支持 Oracle RAC 和 WSFC 集群技术支持去重与压缩功能； 9.企业版分布式存储节点，按物理服务器授权（4 台），支持 SSD 加速缓存技术。本次为现私有云存储节点扩容，须提供现有私有云平台（品高）授权。 提供平台升级服务及基础支持服务 Basic SNS，提供厂商两年内免费升级服务承诺函。 10.存储容量不小于 30T；				
3	虚拟化资源购置（大数据运行中心扩容）	1.企业版云计算节点授权 6 颗物理 CPU； 物理机节点可作为计算节点。 2.包含配套控制器，包括：集群控制器、节点控制器；控制器支持容灾。 3.具备功能包括：虚拟机高可用、数据高可用、支持 SAN 存储和分布式存储并存。 4.本次为现在用私有云平台节点扩容，须提供现有私有云平台厂商授权。 5.本次项目另需提供私有云平台本地化响应服务 1 年，包括故障响应、技术培训、软件版本升级等，响应时间不超过 2 小时；	1	项		
4	数据治理及学生精准画像服务二期	1.采用 B/S 结构，可运行于 Unix、Linux、windows 等高安全性操作系统。开发技术应采用 J2EE 标准、组件技术及在数据交换上对 XML 的支持，使系统功能最优化，同时将整体系统内部在技术上的相互依赖性减至最低。具体要求如下： （1）平台及应用系统软件必须遵循 J2EE 的技术路线，采用 Java 编程语言和服务器端 Java 技术进行开发，业务应用系统和数据集成平台均必须基于 oracle 11g 或以上的大型数据库之上。 （2）采用面向对象的组件技术，着重于开发构成应用程序“业务对象”的可重复使用的组件，利用这些组件顺利地建立分布式应用程序。 （3）采用成熟的 SOA 架构及设计理念，保证学校内部各业务系统集成和交互过程中异构技术架构和异构数据结构集成中的稳定性和可管理性。 （4）应用程序开发与运行结构要基于统一的技术开发平台的三层架构，即 Web 服务器、应用支撑服务器和数据库服务器。 （5）系统必须支持负载均衡，支持动态监测负载状况，自	1	项		

		动对可用资源进行并发检测，调整和分配等功能。 2.安全要求 （1）认证授权：保证用户的合法性和用户使用应用信息资源的权力，避免内部敏感信息泄漏和服务所提供的信息资源被非法访问，造成严重的安全事件。 （2）信息保密：充分利用密码技术，对于需要保密的信息，采用密码技术进行加解密处理，防止信息的非授权泄漏，确保涉密信息在产生、存储、传递和处理过程中的保密。 （3）数据完整性：建立数据完整性检验机制，保证收发双方数据的一致性，防止信息被非授权修改。 （4）审计：记录应用日志，对事件进行分析，并能提供预警信息。 （5）数据备份：利用数据库的备份功能将建设的平台和系统数据备份到指定的服务器或存储系统上。 （6）要求投标方需从物理安全、网络安全、系统安全、应用软件安全、用户安全、数据安全等几个方面提出配套的安全体系完善方案，以便防范安全风险。 3.建设需求 3.1 数据质量管理 投标方提供的数据质量管理系统需要包含数据质量评估、数据问题在线反馈以及数据问题线上跟踪处理流程。最终可以为我校提供围绕数据质量管控的闭环功能设计。数据质量评估具体功能需求如下： （1）投标方需要能够针对数据质量评估提供数据资产质量可视化展现及数据质量检测报告； （2）需要支持按天查看历史数据质量的评分及变化趋势；也支持查看历史数据每日总得分、有效表得分，完整性得分、唯一性得分、有效性得分情况、合规性得分情况； （3）针对不同的业务领域，能够得出实时评分，并以雷达图的方式进行呈现； ★（4）需要支持查看每个业务领域的数据建设及质量情况，包括总得分、主数据得分、有效表、空表、未建表、正常数据量、异常数据量情况； （5）能够支持完整性、代码有效性、一致性、合规性四个要素来查看不同业务系统单表的数据质量； （6）能够围绕业务视角，基于监测时间及数据分类进行筛选，基于异常类型展现单表遗留问题情况； （7）生成直观的质量检测报告，所见即所得的反映问题所在及动态，能够围绕模型、字段、数据三个维度生成查看数据质量问题； （8）此次能够对学校数据中心已入库数据进行标准化梳理，协助进行数据标准化处理，包括但不限于教务数据、资产数据、人事数据、OA 数据、科研数据、教学管理数据等；形成可对外推送的各标准数据集；				

		3.2 数据问题在线反馈 ★需要提供数据问题在线反馈功能，由数据使用方发现的问题，提供一个在线的反馈页面，可以将问题反馈给信息中心，由信息中心集中管理；对数据接口发生中断、数据传输异常等情况进行预警和提醒，并集中反馈； 3.3 问题数据线上跟踪管理 需要能够针对数据问题提供线上跟踪处理流程，包括责任单位数据问题、数据问题受理和数据概览。其中，责任单位所属页面，提供给权威数据责任单位查看数据质量检测问题报告，责任单位可方便的在线进行受理，并承诺完成时间。 3.4 数据资产目录开放 面向我校数据资产开放性的提升，投标方需要能够提供数据资产目录开放系统，主要包含数据资产目录管理、数据资产申请服务功能，为我校数据消费提供便利； （1）需提供的数据资产目录管理功能，支持主数据、信息编码、数据集市中数据资产的开放管理；支持按 主数据、信息编码、数据集市分类检索；支持按关键字、发布状态检索；支持单表按字段选择发布管理；也支持多表批量发布、批量取消发布管理； （2）需要能够提供集中展现我校数据资产情况的汇聚功能，可实现通过资产名称快速检索某数据资产的 API 接口使用记录，同时可以查看当前开放的资产目录数量、可下载的 excel 数量、下载次数、API 接口数量、调用次数等； （3）需能够为我校数据管理人员提供资产使用概览、资产目录管理、申请审核、资产使用记录等功能的快捷入口按钮；需支持查看主数据模型、信息编码、数据集市下的业务领域分类，并能查看分类目录下开放与未开放资源目录数量。 （4）需支持向我校提供数据资产使用情况的信息展现，主要涉及已经开放的资产目录数量、对应字段数据、API 接口数量，以及私 API 接口调用次数等信息。能够统计一定时间内的数据资产目录中数据使用情况变化趋势； （5）针对数据资产目录的管理，需支持可以按照数据分类、发布状态三个不同维度进行查询和导出，系统管理员对资产目录表及字段是否对外发布及开放时间进行管理； （6）针对开放的数据资产目录，需支持数据使用者对资产目录的使用申请，以数据分类属性结构展现数据资产的使用情况，可支持快速检索该分类下已发布的数据资产； （7）需能在资产目录使用过程中，支持用户点击总览页面逻辑类型为 API 的调用成功次数、调用失败次数、总次数，可下钻到 API 调用记录；支持用户点击总览页面逻辑类型为数据文件的调用成功次数、调用失败次数、总次数可下钻到数据文件下载记录页面； 3.5 数据资产申请服务 （1）需为我校数据管理人员提供方便查询开放的所有数据				

		资源目录及公共 API 接口的功能； （2）可以为我校各部门提供开放数据资源在线申请的功能，可以很方便的在线勾选需要开放的数据资源字段，能够提供包括字段、关系表达式在内的过滤条件；申请类型包括待定、API（开发接口）、EXCEL(查询及下载)、数据查询四个选项。API 接口申请通过后会自动添加申请中需要使用接口的 IP 地址至白名单。 （3）提供关键字进行模糊查询的功能，可查询到待审核、已通过、已打回三种不同状态的申请列表；可进一步查看资源目录申请信息，包含基本信息、申请字段、过滤条件、申请类型、审核记录信息； 3.6 数据治理服务 （1）数据管理体系建设 投标人须为我校提供数据管理体系建设参考，辅助我校信息中心完成校级数据中心/资产建设的顶层设计和管理方针的设计，确立校级数据建设的指导性纲要，包括规定校级数据建设的意义、要求；校级数据管理的目标、原则、组织架构；数据生产、采集、储存、使用、保密、安全方面的要求。 （2）数据质量管理体系建设 投标人辅助我校信息中心完成数据质量管理体系建设，需实现监控数据标准和集成执行过程；定期分析数据资产质量情况；制定相应的数据质量改进规划。 （3）数据治理执行体系建设 投标人辅助我校信息中心完成数据治理执行体系建设，需实现通过规定流程、动作、权责，促使数据治理活动能够执行到位。包括制定详细的“当期数据治理方案&计划”；在持续的集成实施同时按计划开展持续的数据质量检测；输出“质量检测结果”并制定相应的“问题数据修订计划”；最后针对性处理问题数据。 投标人需在项目验收前配合学校完成数据治理体系的梳理与调研，并针对我校现状配合学校完成上述数据治理体系的建设。 （4）数据治理组织机构建设 投标人需结合自身高校数据治理经验，配合优化我校数据治理管理体系配套组织架构的设置，实现从校级决策、部门管理到实施改进的全过程参与体系建设，且投标人需针对建立的组织架构，由数据平台提供“数据责任单位”管理，并需提供相应数据责任单位的数据管理授权、质量管理授权，促使学校规定的数据责任的信息化管理到人、执行落地。 （5）★信息需求调研和数据资源盘点 提供人员学校各主要业务部门进行实地调研。获取各业务系统的使用现状及其中数据提供情况；盘点校内的各项数据资源情况，包含各项业务系统、数据库的情况、数据管理部门和责任人/接口人、技术属性信息、数据使用和质量概况、离				

		线电子数据的情况、历史数据保存情况等。 通过此项服务，初步了解全校数据的现状和条件。根据业务需求和数据条件，初步梳理当期数据能够进行建设及治理的范围与边界。并依据各部门的工作中与外部数据的关系进行分析，初步确立和形成校级的数据流向规划设计。 最终形成数据资源盘点清单、数据责任单位清单、各部门数据关系 IPO 调研表。 此次项目需要将已入库数据进行数据治理，完成教务、资产、学工、人事、OA、教学管理与评价、站群、一卡通系统的数据清洗和标准化工作，形成可输出、可申请的数据资产。 3.7 信息编码日常治理服务 针对各业务系统梳理、完成信息编码的对标工作并常态化。针对学校业务系统运行中出现的偏差进行纠偏。根据学校实际需要，完成信息编码标准的增加、删除、修改的日常管理。此外针对国标、行标等的变化，对信息编码标准进行升级。在信息编码标准的基础上提供集成过程中的自动映射转换，对映射转换时发生的问题进行处理。 3.8 数据资产开放服务 根据校方的业务需求和管理要求，按需提供数据资产的进一步处理和开放服务，包括面向应用开发的 API 接口开放和面向公众的数据资产目录开放服务。 3.9 项目过程管理服务 在整个“数据资产建设和治理项目”的实施过程中，进行项目管理工作。包括但不限于制定实施方案、工作计划、进度监控、定期工作总结和工作成果汇报等内容，同时配合学校在关键组织会议时，参与探讨项目实施情况及数据建设和质量治理工作。 3.10 以学校数据为支撑，通过数字化技术手段，全面呈现学生在学校期间的生活、消费、学习等数据，全面展示学生详细个人数字画像，以 h5 的形式呈现出来。				
5	数据中心边界防火墙	1.软硬件平台基本系统，配置 IPS 功能，含三年硬件保修、应用识别库升级和软件升级维护服务。硬件参数：机架型 1U，2×10GE + 8×GE(光) + 16×GE(电) + MGT + HA，1 个接口扩展槽，交流双电源；性能参数：吞吐 20G，并发 1000 万，IPS 吞吐量不小于 5G。 2.ARP 攻击防护：为了防御 ARP 攻击和 ARP 病毒，提供免费 ARP 认证客户端进行 ARP 强制认证和强制安装客户端；提供 ARP 检查与 DHCP 监控，DHCP 监控和 ARP 检查功能相结合能够实现二层 ARP 攻击防护； 3.提供策略优化与策略助手功能；策略优化可对当前策略进行多维度分析，包括策略创建时间、首次命中时间、最近一次命中时间、最近未命中天数等；策略助手支持关联策略 ID 进行获取流量，并支持策略聚合条件，可一键生成策略，满足新业务上线策略梳理要求;	1	台		

		4.基于满足等级保护 2.0 物联网安全扩展要求，支持基于安全域 IoT 策略控制，支持 IoT 终端识别、终端行为、准入名单模板配置；支持 IoT 监控： 终端类型（网络摄像机等）、厂商（大华、宇视、海康威视等）、型号、MAC 地址、IoT 监控模板、认证状态、更新时间、可信、当前上下行流量等，实现 IoT 的管控与可视化（提供上述配置截图）。 5★为便于及时响应紧急网络攻击事件，需提供移动运维平台。通过移动运维平台可实时查看威胁事件（基于威胁名称、威胁类型、攻击者、受害者、威胁级别、威胁事件进行 top 排名展示）；（需提供第三方检测机构出具的功能检测报告扫描件。） 6.★产品资质：防火墙销售许可证；需具备完整的安全建设服务能力，符合国家标准 GB/T 17626.5:2008 第三级及以上标准（需提供检测报告）；下一代防火墙 CVE 兼容证书； 7.整机质保三年。				
6	现有在用部分网络安全设备升级	1. 对在用一台启明星辰 WAF（6000-M1）提供 3 年原厂硬件维保服务，3 年 Web 应用防护特征库升级授权，增加一块 WAF-NIM-L 通用接口板模块，4 个千兆 SFP 接口及 4 个 10/100/1000M 自适应电接口（不含 SFP 光收发模块），质保期与主机一致。 2. 对在用一台深信服防火墙（AF-1000-F440）提供 3 年原厂硬件维保服务，3 年软件和特征库升级服务。 3. 需提供厂商授权。	1	项		
7	容灾备份一体机	★1、非 OEM 产品，设备配置要求：2U 机架式 12 盘位，≥10 核心，≥32GB RAM，不少于 2 个千兆网络端口，2 个万兆光口，网络端口都可用且可分配不同的备份任务，支持 IPv4、IPv6，提供 IPv6 Ready logo 认证，磁盘配置 2*480G SSD、12*4TB 企业级 7200 转 数据硬盘。1×Intel Xeon Silver 4210（2.2GHz/10 核 20 线程)，64G DDR4 RAM，2×1GE+2×10GE(含多模光模块)，2G 阵列卡（含掉电保护)【含硬件 3 年整机质保服务+12 个月标准远程技术支持服务+无数量限制备份客户端授权】 2、支持通过 web 界面向导式实现主流的数据库备份恢复，包括但不限于 Oracle、 SQL Server、MySQL、Sybase、DB2、Informix 、 PostgreSQL 、 MongoDB 、 Cache 、 Exchange 、 SharePoint、Domino、达梦（DM）、人大金仓（kingbase）、南大通用（GBase）、神州通用（ShenTong）、翰高等国产数据库，必须支持单库和集群数据库的向导式备份和恢复操作（不接受前后置脚本的实现方式）。 ★3、支持 Windows SQL Server、Oracle、MySQL 等数据库的快速合成备份功能、即时恢复功能。提供（数据库快速合成备份方法、系统、装置及存储介质）的发明专利。支持对 Oracle 的日志解析功能，在数据恢复作业中可以选择准确的 SCN 来确定数据恢复点。针对 Oracle 中已经提交的事务，根	1	套		

		据日志解析后得到的 SQL 语句，创建撤销处理，把数据回滚到事务提交前的状态。支持 Oracle、MySQL 实时备份和任意时间点恢复功能。（提供产品功能截图加盖公章，不接受 CDP 实现方式）。 4、支持 Linux（文件）、Unix（文件）、对象存储、Hadoop 分布式文件系统（HDFS）的全量、增量、合成备份。支持合成数据通过挂载方式实现即时恢复，支持 Linux、Unix、Hadoop 、对象存储的异构恢复达到在不同文件系统中转换恢复。可支持跨文件系统的备份恢复（如:从 Linux 恢复 Windows），跨平台的备份恢复（如:从 X86 恢复 ARM），支持仅恢复当日增量数据，支持文件恢复“同名文件处理（覆盖、跳过、保留最新、重命名保存）”。 5、支持 ZStack、VMware、Hyper-V、Xenserver、Xen、KVM、FusionSphere、FusionCloud、FusionComputer、H3C CAS、OpenStack、CNware 等虚拟机的备份恢复。针对 Vmware、Hyper-V、H3C CAS 平台，支持直接挂载备份集即可实现虚拟机的快速恢复。 6、支持固定块、变长块的数据重删技术。支持分布式重删池，最高可扩展至 64 节点，支持动态伸缩重删节点，用户可在界面上配置副本数量，存储服务节点支持在多种处理器架构上部署，包括英特尔、飞腾、鲲鹏、海光、龙芯等。 7、支持 AES、Blowfish 等加密算法，支持国密 SM4 算法。（提供 SM4 算法功能截图）支持使用 Access Key 的用户登录模式，有效解决用户应用系统密码定期自动变更和无密码场景下备份作业的按期执行。 8、支持将源端生产主机标注为受保护状态，不允许作为恢复主机，以防止误操作造成的数据丢失。支持邮箱二次身份登录验证。				
8	校园有线网络千兆接入交换机 48 口	技术参数要求： 1.固化千兆电接口≥48 个，独立千兆 SFP 光接口≥4 个； 2.交换容量≥3.3Tbps，包转发率≥160Mpps； 3.支持 IPv4、IPv6 静态路由、RIP、RIPng、OSPFv2、OSPFv3 等三层路由和组播功能； ★4.为保证设备稳定运行、设备防浪涌≥10kv，提供第三方权威机构检验报告复印件证明； 5.设备支持 IEEE 802.3az 标准的 EEE 节能技术，最低功耗≤40W； 6.支持 openflow 1.3 协议；支持零配置，支持 CWMP(TR069)协议； 7.支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的 CPU 负载，从而保障整个网络的稳定运行； ★8.支持设备虚拟化功能，能够将 9 台物理设备虚拟成 1 台逻辑设备，同时虚拟化故障恢复时间小于 30ms，提供第三方	15	台		

		权威机构测试报告； 整机质保三年。				
9	校园有线网络千兆接入交换机 24 口	技术参数要求： 1.固化千兆电接口≥24 个，独立千兆 SFP 光接口≥4 个； 2.交换容量≥3.3Tbps，包转发率≥125Mpps； 3.支持 IPv4、IPv6 静态路由、RIP、RIPng、OSPFv2、OSPFv3 等三层路由和组播功能； ★4.为保证设备稳定运行、设备防浪涌≥10kv，提供第三方权威机构检验报告复印件证明； 5.设备采用无风扇静音节能设计，支持 IEEE 802.3az 标准的 EEE 节能技术，最低功耗≤24W； 6.支持 openflow 1.3 协议；支持零配置，支持 CWMP(TR069)协议； 7.支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的 CPU 负载，从而保障整个网络的稳定运行； ★8.支持设备虚拟化功能，能够将 9 台物理设备虚拟成 1 台逻辑设备，同时虚拟化故障恢复时间小于 30ms，提供第三方权威机构测试报告； 9. 整机质保三年。	5	台		
10	网络安全整改及监测、防护、漏扫	提供一年期限的信息安全测评整改及漏扫，要求如下： 1、提供设备巡检、审计类安全设备及应用访问日志安全巡检、防火墙安全巡检、网络设备安全巡检、主机防护安全巡检、系统运行安全巡检、防病毒安全巡检、数据备份巡检、物理机房巡检的日报告、周报告和月报告； 2、提供基于基础运维服务建立学校操作系统、中间件、数据库等项目的安全基线。对学校现网和新建、扩容的操作系统、中间件、数据库系统进行配置核查，输出核查报告并进行安全加固，并协助做配置安全分析规划； 3、针对发现的不符合标准的信息安全脆弱点，进行策略安全整改加固，包括网络设备安全加固、系统加固、数据库加固、安全设备加固等； 4、系统的分析网络与信息系统所面临的威胁及存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，并为防范和化解信息安全风险，或者将风险控制在可接受的水平，从而最大限度的保障网络和信息安全的同时也为后续的信息化建设提供科学依据； ★5、通过两种及以上漏洞扫描工具对需要检测的网络设备、安全设备、操作系统、Web 应用系统进行检测，发现其中存在的技术安全脆弱性，梳理成漏洞扫描报告，提出整改优化建议，帮助解决存在的安全隐患，达到信息系统相对安全稳定的运行状态；扫描频率为固定季度 1 次+重点保障时期随	1	套		

		时响应； 6、制定应急响应措施，协助处理应急事件。服务期内，在学校发生需要应急响应的时候，提供安全应急响应服务，确保快速处理问题，避免影响扩散； 7、提供必须的服务技能培训，并对相关技术问题进行充分交流，以提高学校信息化部门工作人员技术水平，培训包括定期或不定期为学校进行信息安全培训服务，内容包括网络安全知识、解决安全故障的常用方法和手段等内容； 8、数据备份和数据恢复服务，协助学校建立完备的数据备份和恢复的综合规划，监控并落实备份规划的执行，并进行有效的测试和演练，确保数据备份的有效性； ★9、提供 5 个信息系统（按域名计算）的监测和学校主网站云防护：信息系统的安全事件、资产变动、脆弱性监测频率：一周一次；Web 漏洞、SSL 安全监测频率：二周一次；可用性监测频率：15 分钟一次。面向主网站提供云安全监测与防护服务，能有效防止域名被劫持、网页内容被篡改；能有效防止 SQL 注入、异常 HTTP 请求、Webshell 后门请求、XSS 跨站脚本、命令执行、代码执行、文件包含、文件注入、防篡改、防盗链、防扫描等 Web 攻击。（要求国内外云防护集群节点 IP 段≥30 个、线路类型≥60 个，且覆盖移动、电信、联通国内三大主流运营商；提供网站安全报表，能够实时展示网站的总请求数、总流量、网站浏览人数、搜索引擎次数、缓存率和遭攻击次数。并能支持统计每小时网站的总请求数、总流量和网络浏览人数等。） 10、以上服务期限为一年，需由专人负责现场日常运维工作的开展（工作时间不少于每周 40h）。包括以下工作内容：运维资源协调；运维事件管理；运维沟通管理；运维知识库的建设；运维流程管理；运维工作整理和汇报；安全制度体系的建设和管控；组织和实施培训，负责学校信息系统的监控、日常巡检和故障应急处理，学校 IT 资产的管理，学校网络和系统的建设配合，各系统数据备份和恢复工作。				
11	日志审计系统	一、整体要求：日志统一管理系统对各类 IT 设备及应用的日志进行稳定收集、实时解析、针对不同类型日志提取日志关键字段，统一存储，并实现关键字段间的关联，实现海量日志高速检索，形成日志管理体系进行集中管理，满足网络安全的备查需求并为大数据分析展示提供整合数据基础。 二、性能要求： 1.采集要求： 1.1 支持多种设备日志如交换机、路由器、防火墙、NAT 设备、VPN 设备、行为审计设备、网络安全设备、流量控制设备、计费认证系统、DNS 系统、DHCP 系统、网管监控系统等。 1.2 支持主流设备厂商包括 H3C、华为、锐捷、 Juniper、思科、网康、Panabit、山石、天融信、城市热点、深澜等的数据源对接。	1	项		

		1.3 支持多种采集方式如 syslog、 trap、数据库读取、文件导入、私有协议等。 2.解析要求： 2.1 支持对日志进行解析，提取关键字段并结构化存储。 2.2 支持对不同来源的日志数据通过规则进行关联，关联后的数据可以进行关联查询分析统计等。 2.3 内置多种日志业务模型，包括 NAT、URL、网络认证计费、SYSLOG 等，针对不同的业务模型内置可以扩展的存储结构供用户直接使用。 ★2.4 支持根据内置日志业务模型将来自多个数据源的数据按模型的关联关系合并后结构化存储，避免在后续查询时再进行关联。如在 NAT 和 URL 模型中可以将来自防火墙、DPI 的业务数据和来自于认证系统的用户数据、DHCP 系统的终端数据、网管系统的位置数据通过 IP 在业务数据产生的时候立刻关联并存储而不是将上述数据分别存储在使用时再根据 IP 和时间进行关联，以提高数据的使用效率，提供系统截图加盖公章。 3.存储要求： ★3.1 支持原始日志无损存储，提供系统截图加盖公章。 3.2 支持对文本型数据压缩存储，节省存储空间。 3.3 支持对 IP 地址、日期等专有格式字段进行格式转换存储，提高索引效率。 4.查询要求： 4.1 对收集到的日志数据可以立刻按照模型结构进行条件查询，无需进行数据准备和预处理等工作。 4.2 支持将业务模型中任意结构化字段配置为搜索条件进行查询。 4.3 支持多个搜索条件的组合查询。 4.4 支持对 IP 字段进行 CIDR 的范围查询。 5.统计报表： 5.1 提供基于每个业务自身的统计分析，如数据量、增长率等。 5.2 针对不同的业务模型可以提供默认报表和用户自定义报表。 ★5.3 对网络行为模型提供账号被盗分析统计报表功能，能够发现疑似被盗账号，提供系统截图加盖公章。 5.4 对 URL 业务模型直接 TOPN 报表，支持统计域名访问的 TOPN 数据。 ★5.5 对 URL 业务模型支持自定义统计分析报表，对特定 URL/域名访问情况进行统计，并对统计结果做图表展示。比如统计特定的电子资源访问和下载的人数人次等。 5.6 对网络认证计费模型提供用户流量、时长 TOPN 报表统计。 5.7 针对 SYSLOG 模型提供分类、分级统计报表。 6.接口与导出：				

		6.1 根据查询条件将平台数据以文件形式导出，对大量数据的导出由后台在系统空闲时进行，不影响日志的收集与分析。 6.2 提供 API 接口，对外提供稳定高性能的日志导出，能够对接大数据分析展示平台。 7.监控告警： 7.1 支持对异常情况做出告警：存储空间不足告警；日志接收异常告警（不符合设置的接收规则或者长时间接收不到数据时） 7.2 支持对系统自身运行状态指标数据进行监控和告警，例如 CPU 使用率、内存使用率、磁盘使用率、网络连接异常、网络流量异常等。 7.3 对各项告警指标内置合理的阈值和等级，并支持用户根据实际情况自定义阈值和告警等级。 7.4 支持通过短信、微信、邮件向管理员发送告警通知消息，自带微信告警服务平台，只需关注即可使用。 7.5 性能要求 在 CPU E5-2620 v4 2.10Ghz、64G 内存，情况下测试: 1) 查询速度：查询响应时间在 5s 以内。 2) 采集性能：日志采集速度不小于 3 万条/秒。 3) 分析速度：日志分析处理能力不小于 2 万条/秒。 8.安全要求 1) 支持使用 HTTPS 协议传输信息，保证信息传输安全； 2) 支持内置防火墙，维护信息安全。 3) 支持 SSH 连接，防止信息泄露。 4) 数据库存储要求采用双库分离存储机制，保证系统安全。 9.系统管理要求 1) 支持分布式部署，通过部署不同的功能节点在不同的服务器上提升系统的整体性能和处理能力 2) 支持多种浏览器，要求支持在 iOS（iPhone/iPad）、Android 等操作系统的移动设备展现；无需安装插件即可在 PC 和移动端实现所有管理功能。 3) 要求所有图形采用矢量图展示方式，要求在任意浏览器放大缩小不失真不变形。 4) 支持远程协助。 10.安装方式 1) 可以通过专用的硬件设备或软件形式部署，支持虚拟化，支持虚拟机导入。 2) 提供与操作系统、数据库以及其他平台软件深度整合的统一介质，能够实现操作系统、数据库、其他平台软件和系统的统一安装。 11.要求系统获得国家信息安全产品认证，投标文件提供安全审计产品的认证证书扫描件或复印件。 12.要求投标产品获得全球 IPv6 测试中心的 IPv6 Ready				

		Phase-2 认证证书，提供测试报告。 13.提供售后服务承诺函（三年）。				
12	用户地址管理系统	★1.提供 IPv4 和 IPv6 DHCP 服务器双机热备服务。 2.单台 DHCP 节点每秒分配 IP 数：3K/S，单台 DHCP 节点最大分配 IP 地址数 12 万，支持 16000 个地址池。 ★3.支持向客户端发布 IPv6 无状态地址前缀、RDNNS，并可根据 VLAN 信息发布不同的 IPv6 前缀。提供截图证明。对 v4、v6 地址池以及无状态地址自动配置的白名单策略。提供截图证明。支持超级作用域功能实现子网规模的动态扩展，实现将多个不连续的子网合并为一个子网，在不对现有子网进行连续扩展的情况下解决子网利用率过高的问题。提供截图证明。 4.支持内置扩展选项模板，如 Aruba、华三、锐捷等主流无线厂家的 AC 控制器地址，并支持自定义扩展选项的内容。提供截图证明。 5.支持识别 PC、移动设备等终端类型，并基于 v4v6 地址池分配做终端类型控制，例如指定地址池不允许移动终端上网等。 6.支持统计分析用户终端型号，可识别 Android、iPhone/iPod/iPad、Windows Phone、Liunx、Mac/Macbook、Windows 等终端操作系统和厂商型号，并支持根据终端型号下发不同的扩展选项和参数。 7.支持下发地址的同时下发扩展选项，例如使终端获取 NTP 服务器地址、NIS 服务器地址、引导文件名、PXE 服务器地址、NIS 域名、NIS 服务器、SNMP 管理、SNMP 团体名、Option 值等信息。 8.支持自动检测全网 IP 地址使用情况，并支持在子网中用各不相同的图标来表示空闲、动态分配、固定分配、手工设置等状态。提供截图证明。 9.支持对 IP 添加自定义标签，并支持按照自定义标签进行查找。 10.支持批量导入 IPv4、IPv6 固定地址，导入信息包括 IP、MAC、所属子网、过期时间等，支持批量生效、禁用和删除固定地址。 11.支持与身份认证系统对接，实现根据身份认证系统的策略动态控制 IP 准入。 12.支持与统一身份认证系统单点登陆接口，实现统一身份认证系统账号登陆 DHCP 系统自服务页面，页面支持手机端，提供截图证明。 13.详尽 DHCP 分配日志报表，能够根据用户 IP 地址、终端 MAC、时间、设备类型、厂家品牌、终端型号等关键信息进行搜索。 14.分配日志类型能显示出分配新 IP、续约 IP、超时释放 IP、	1	项		

		冲突释放 IP 等日志类型。 15.支持配置与数据库的手动备份和还原。 16.支持对系统用户进行角色管理和细分权限设置。 17.支持操作日志的完整记录与查询，包括登录日志、DHCP 配置变更日志等。 ★18.支持以 Failover 模式部署，可以选择主备模式或负载均衡模式进行工作。 19.提供产品授权书和售后服务承诺函（三年）。				

本项目核心产品一览表

序号	核心产品内容
1	▲高性能服务器（大数据运行中心扩容）