采购需求

一、项目建设目标

按照“统一规划、统一标准、统一平台、统一管理、分级建设”的原则，大数据智能分析、人工智能等技术，整合利用信息资源管理等一体化平台，打造国内领先并具有海南特色的“智慧校园大数据中心及基础平台建设(网络基础设施及安全设备)”应用模式。另外，本项目建设旨在提升校园的信息化水平，改善学校网络基础平台问题，健全和完善学校信息系统，实现系统的集成和谷个系统之间的数据共享，建立基于数据管理和利用的综合性技术方案的共享数据中心，用以存放大量数据的同时有效地将数据管理起来，并提供数据访问的手段，为系统集成和各个系统之间的数据共享提供平台，保证数据的及时性、完整性和一致性。为全校提供信息共享服务平台和决策支持数据平台，打造大数据时代的智慧校园，构建一个集教学、科研、管理和生活为一体的新型智慧校园生态环境。

项目工期：依照投标人须知前附表约定的时间

二、建设依据与相关技术规范

（一）政策法规和规划

1、《电子政务保密管理指南》的通知（国保发〔2007〕5号）

2、《信息安全等级保护管理办法》（公信安字〔2007〕43号）

3、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007] 861号）

4、《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）

5、《信息技术、软件包质量要求和测试》（GB/T 17544-1998）

6、《国务院办公厅关于促进电子政务协调发展的指导意见》（国办发[2014]66号）

7、《国务院关于印发促进大数据发展行动纲要的通知》（国发[2015]50号）

8、《海南省“信息智能岛”规划》（修订稿）

9、《海南省人民政府办公厅关于加强全省电子政务建设的实施意见》（琼府办[2007]28 号）

10、《海南省国民经济和社会发展信息化“十三五”规划》

（二）标准与规范

1、《信息资源规划—信息化建设基础工程》；

2、《软件工程标准分类法》（GB/T 15538-1995）；

3、《计算机软件 文档编制规范》（GB/T 8567-2006）；

4、《计算机软件 需求说明编制指南》（GB/T9385-1988）；

5、《计算机软件 质量保证计划规范》（GB/T 12504-2008 ）；

6、GB/T 1900.3(ISO9000-3) 质量管理和质量保证标准,第三部分：GB/T19001（ISO9001）在软件开发，供应和维护中的使用指南；

7、《计算机信息 系统安全保护等级划分准则》（GB17859-1999）；

8、《信息安全技术 信息系统等级保护安全设计技术要求》（GB/T 24856-2009）；

9、《电子信息系统 机房设计规范》（GB 50174-2008）；

10、《信息安全技术 信息系统等级保护安全设计技术要求》（GB/T 25070-2010）；

11、《信息安全技术 应用软件系统安全等级保护通用技术指南》（GA/T711-2007）；

12、《信息技术软件工程术语》（GB/T 11457-2006）；

13、《计算机软件可靠性和可维护性管理》（GB/T 14394-2008）；

14、《计算机软件测试规范》（GB/T 15532-2008）；

15、《软件系统验收规范》（GB/T 28035-2011）；

16、《信息安全技术 应用软件系统通用安全技术要求》（GB/T 28452-2012）；

17、GB/T 30882.1-2014 信息技术应用软件系统技术要求第 1 部分:基于 B/S 体系结构的应用软件系统基本要求；

18、《计算机软件需求规格说明规范》（GB/T 9385-2008）；

19、《计算机软件测试文挡编制规范》（GB/T 9386-2008）；

20、《信息技术软件生存周期过程》（GB/T 8566-2007）；

21、《高等学校本科、专科专业名称代码》（GB/T 16835-1997）；

22、《计算机信息系统安全等级保护操作系统技术要求》（GA/T 388-2002）；

23、《计算机信息系统安全等级保护数据库管理系统技术要求》（GA/T 389-2002）；

24、《计算机信息系统安全等级保护通用技术要求》（GA/T 390-2002）；

25、《计算机信息系统安全等级保护管理要求》（GA/T 391-2002）；

26、《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）；

27、《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240-2008）；

28、《信息安全技术 信息系统安全等级保护测评要求》（GB/T 28448-2012）；

29、《TP 网络技术要求一一技术网与 PSTN、ATM、移动网互通》 (YD/T1317-2004)；

30、《IP 网络技术要求—网络总体》(YD/T 1170-2001)；

31、《IP 网络技术要求一一网络性能测量方法》(YD/T 1381-2005)；

32、《基于网络的虚拟 IP 专用网(IP-VPN)框架》(YD/T 1190-2002)；

33、《信息安全技术 计算机网络入侵分级要求》 (GA/T 700-2007)；

34、《信息技术 开放系统互连 局域网媒体访问控制(MAC)服务定义》(GB / T 16646-1996)；

35、《电工术语 计算机网络技术》(GB/T 2900. 96-2015)；

36、《有线网络建设技术规范》 (DG/TJ 08-2009-2006)；

37、《信息安全技术 入侵检测产品安全技术要求 第 1 部分：网络型产品》(GA/T 403.1-2014)；

38、《信息处理系统 开放系统互连 网络层的内部组织结构》(GB/T 15274-1994)。

（三）其他依据

1、《海南省信息化条例》

2、《海南省政府网站建设与管理规在范》

3、《海南省工业和信息化厅关于做好海南省政务信息化工程建设项目验收工作的函》、《海南省工业和信息化厅关于进一步做好海南省政务信息化工程建设项目初步验收工作的函》

三、项目建设地点

本项目建设所在地点：海南省琼海市嘉积镇富海路 128 号

四、建设内容

1、主要建设内容如下：

项目名称：智慧校园大数据中心及基础平台建设项目(网络基础设施及安全设备)(A、B 包)(5 次)

项目编号：HNQZ2019-2-2(5 次)

标包名称：网络基础设施及安全平台

标包编码（包号）：HNQZ2019-2-1(5 次)A 包

项目参考清单、规格、参数、服务等需求（最高限价：465.6156 万元）

序号	品目名称	参考规格和配置技术参数	数量	单位
1	出口路由器	▲1.交换容量≥100Tbps；转发性能 12000Mpps；路由引擎*2；交换网板*2；交流电源*2；4 端口万兆模块*2； 2.主机箱交流组合（双路由引擎插槽，交换网板插槽≥2，4 个业务载板插槽， 业务子卡插槽≥8，带防尘网和模块化）； 3.为保证路由器设备满足未来业务演进，要求 IPv4、Ipv6 路由及转发表容量：支持 IPv4 路由表容量≥25M,IPv6 路由表容量≥10M；支持 IPv4 转发表容量≥4M,IPv6 转发表容量≥2M，提供第三方权威机构测试报告证明并加盖厂商鲜章； 4. 整机业务插槽数量≥8；支持 IPv4 和 IPv6 双协议栈，支持 IPv6 邻居发现，PMTU 发现，TCP6，ping IPv6，traceroute IPv6，socket IPv6，静态 IPv6 DNS，指定 IPv6 DNS 服务器，TFTP IPv6 client；支持 MPLS、MPLS L3 VPN、MPLS L2 VPN、MPLS QoS、MPLS Over GRE；支持分布式 Netstream 功能，本次要求实配支持 NetStream 功能板卡或 license； 5.电源模块槽位数≥2，电源系统支持 n+n 冗余； 6.路由主机支持主控板、业务板物理分离，主控板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板和业务板槽位；支持不同带宽的链路捆绑功能，支持多路径负载分担功能（UCMP），支持非等速链路的负载分担，实现不同路径按带宽比例负载分担。 ★7.提供生产厂家针对本项目的售后服务承诺函并加盖厂商鲜章。	2	台
2	校园网核心交换机及认证网关	▲1.交换容量≥512Tbps；业务槽位数≥8；转发性能≥96000Mpps；主控板槽位数量≥2；交换网板槽位数量≥4； 2.硬件配置交换网板数量≥2，主控引擎模块≥2，交流电源模块数量≥2，SFP+电缆 5m 数量≥1；提供 24 个万兆光口、40 个千兆光口、48 个千兆电口，配置高性能防火墙模块*1； 3.采用多级交换架构，能够配置独立的交换网板与独立的主控板，提供厂商官网截图证明并加盖厂商鲜章； 4.支持 ARP 表项≥256K，提供第三方权威机构测试报告证明并加盖厂商鲜章； 5.二层功能：802.11Q 4K,QinQ、SUPER VLAN；链路聚合、端口镜像；三层功能：支持 DHCP+ SERVER；支持 BGP4/4+、ISISv4/v6、OSPFv2/v3、	2	台

		VRRPv2/v3；支持 BFD 与 RIP/OSPF/BGP 联动；支持 GR for RIP/OSPF/BGP/ISIS 等；支持 MPLS VPLS；支持 OpenFlow v1.3 协议，支持协议无关转发，可实现核心网络向 SDN 平滑演进；支持 VXLAN 二层网桥、支持 VXLAN 三层网关；所投交换机为 SDN Ready 的完全可编程交换机； 6.支持无线控制器板卡，满足无线控制的需求； 7.支持两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理；提供厂商官网截图证明并加盖厂商鲜章。 ★8.提供生产厂家针对本项目的售后服务承诺函并加盖厂商鲜章。		
3	网络核心服务	1.网络核心服务设备，支持智能 DNS，DHCP+以及可视化自动化 IP 地址管理，固化千兆电口≥8 个，固化千兆光口≥8 个，固化 4 个万兆光口，两个硬盘插槽，内置风扇，1+1 冗余电源，独立管理口.提供 3 年特征库升级服务；标准 2U 机箱，多核非 X86 架构；内置硬盘容量≥500G； 2.网络吞吐量≥40Gbps； 3.内存≥8G； 4.最大并发连接数≥1000 万； 5.支持 4 级层次化 QoS、支持多级用户/用户组嵌套；支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备；支持源地址转换、目的地址转换、双向地址转换、NAT44；支持一个公网 IP 映射到内网多台服务器，服务器间支持连接和源地址 hash，支持服务器健康检查。	1	台
4	对内服务器区接入交换机	▲1.交换容量≥300Tbps、包转发速率≥180000Mpps； 2.主控引擎模块槽位数≥2，业务引擎模块槽位数≥8； 3.实配主控引擎模块数量≥2，满配独立交换网板；交流电源模块数量≥2； 4.实配千兆以太网电口数量≥24，千兆以太网光口数量≥20，万兆光口数量≥20； 5.整机 ARP 表项≥180K，需提供权威第三方测试报告； 6.为了保证核心交换机能提供持续的带宽升级能力，支持独立的交换网板；为保障产品的可靠性，支持两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理；故障收敛时间小于 50ms，提供国内知名实验室测试报告并加盖厂商鲜章； 7.为实现单位企业关键业务区域之间的安全业务隔离，支持 1：N 的虚拟化技术，要求 N≥4， 即可以将一台核心交换机逻辑上虚拟成多台逻辑设备，实现关键业务区域之间的安全业务隔离，提供国内知名实验室测试报告并加盖厂商鲜章； 8.支持多对一镜像,基于流的镜像，一对多镜像；支持 SPAN、RSPAN 远程镜像，支持 VLAN 的镜像；支持 IPv6 静态路由、RIPng、OSPFv3、BGP4+ 等路由协议。 ★9.提供生产厂家针对本项目的售后服务承诺函并加盖厂商鲜章。	1	台
5	▲万兆 SFP+接口电缆	▲万兆 SFP+接口电缆，长度 3 米，包含一根线缆+两个接口模块。	4	条
6	▲万兆单模模块	▲SFP-LR-SM1310；万兆 LC 接口模块（1310nm），10km，适用于 SFP+接口。	12	个
7	▲10KM 万兆 SFP+模块	▲SFP+ 万兆模块(1310nm,10km,LC)。	2	个

8	认证计费系统	1.与本项目中的出口路由器联动，并与运营商的 BRAS 无缝对接，保留实际现场测试； 2.配置 20000 开户数授权；最大 Portal 认证并发终端数为 40000 终端；包含自助服务平台； ▲3.提供认证计费功能，实配 20000 个 802.1X 和 40000 个 WEB 并发认证用户授权，并提供自助服务平台，供学生进行套餐查询、更改、密码修改等常规操作；为降低出口链路单点故障，此次部署的认证计费系统为旁路部署模式；支持用户初次登陆的时候获取信息并自动绑定；支持基于不同区域的无感知认证；对接 LDAP 加密模式，支持无线 802.1X 无感认证；网关设备探测认证计费系统失联开启逃生；多链路下支持指定用户路由策略，保留测试权利； 4.支持与运营商 BRAS 对接，并支持校园账号与运营商账号的绑定，可实现校园网账号与运营商账号的统一认证；保留测试权利；支持一个校园网账号可与一家或多家运营商账号进行绑定；支持用户在认证计费系统自助端/微信自助端自助完成开户和绑定；支持管理员批量导入进行校园网账号与运营商账号的绑定；支持提供开户相关接口，实现完成自动化开户； 5.配置并实现校园网账号与运营商账号绑定时可以校验用户的手机号码是否是所绑定运营商的本地号码，校验运营商账号、密码的正确性，避免乱绑误绑；保留测试权利； 6.配置并实现一个校园网账号和密码，可同时通过不同终端使用不同运营商服务；保留测试权利；支持本地免费，完全由运营商的 BOSS 系统收费；要求实现本地号段限定，或者限定手机号绑定校园网账号；要求实现分地区计费，不同地区不同计费策略； ▲7.保修期内免费上门升级，永久授权使用。	1	套
9	▲认证计费硬件平台	▲Intel XEON E5-2650V4 * 2；16G DDR4 2400 *4；480G 2.5 SATA 6Gb SSD 硬盘*2；1.2T 10k 2.5 SAS 12Gb 硬盘*6；支持 RAID 0 1 5 6 10 50 60；双口万兆电口；800W 冗余电源模块。	2	台
10	网络管理系统	1.网络管理软件，提供拓扑展示，200 个设备节点授权许可； 2.具备丰富的设备管理功能，包含对设备和设备接口及其信息的增删改查具有良好的展示和基本操作功能；可以对多台设备进行批量的设备软件升级；自动识别出设备厂商、型号等基本信息； 3.支持 IPv6 环境下的资源、性能、告警、拓扑、面板管理，包括纯 IPv6 组网和双栈组网； 4.告警智能分析，包括告警分类关联分析、告警多源关联分析、告警拓扑根源分析、告警网络影响度分析；监控接口的流量，并呈现趋势图；监控接口的 UPDOWN 状态并告警；支持数据中心拓扑，包括机房拓扑、机架拓扑等；呈现设备间链路； 5.配置文件的备份与恢复；对设备批量下发 CLI 指令；以图形化的方式管理 IP-MAC-端口绑定；以图形化向导的方式提供 ACL，QoS 快速部署管理；支持对网络中的路由器、交换机、防火墙、WLAN 等有线无线一体化管理； 6.能够监控终端是否在线，是否合法；可根据时间、地点、类型等配置组合策略； 7.支持对 IP 地址的图形化管理，统一展示某 IP 地址对应设备、终端的详细信息（在线状态，合规状态，终端及设备类型，厂商，操作系统，接入位置，责任人等）；可以图形化展示某 IP 地址上联交换机端口信息（接	1	套

		口，是否启用认证等）； ▲8.保修期内免费上门升级，永久授权使用。		
11	IT 运维管理系统	1.基于 Windows Server 2003/2008 操作系统安装的基础平台；支持全类型资源设备，支持资源监控节点 300 个和无线设备 AP500 个；自动巡检管理：可以实现自定义巡检范围、巡检指标、巡检周期、巡检报表模版及巡检报告自动发送功能；端到端管理：以端到端方式完成从用户接入端到目标应用端的全路径追踪，并提供 IP 地址、位置、同设备在线用户等信息；此功能实现需要购买 IP 地址管理模块，并支持与认证计费系统进行对接；功能包含 IT 健康指数、业务服务管理、事件告警中心、资源管理、网络拓扑、无线管理、脚本监控、KPI&报表管理组件；默认赠送 5 个告警客户端授权、资源监控节点授权数 50 个、无线设备 AP 监控节点授权数 100 个、3 张无线热图和 2 年基础售后服务； 2.提供对各种业务系统的管理，包括服务器、数据库、中间件、Web 和其他业务等，配置可管理≥300 节点；为了便于从多个维度了解业务系统的运行现状，配置业务服务管理功能，可直观展示业务的健康度、繁忙度、可用性； 3.除特殊指标外，一般不需要在被管理应用所在的服务器上安装监控代理，避免对业务系统造成影响；可直接在拓扑图上调用业务管理功能，也可点击左键直接查看被监控业务系统的详细信息和性能参数；提供对各种业务的 SLA 管理，用户可以一目了然地掌握整个业务系统的运行情况，提供最近一小时、1 天、7 天、30 天可用性； 4.直观展示业务的健康度、繁忙度、可用性，便于从多个维度了解业务系统的运行现状，提供产品截图证明并加盖原厂鲜章；为了便于管理人员运维，要求支持端到端的业务故障分析，提供从用户到业务的全景故障定位拓扑； 5.支持虚拟网络资源管理、虚拟网络拓扑展示、虚拟网络告警管理、虚拟网络性能监控、虚拟网络配置迁移管理；为了便于有线无线一体化管理，可统一管理 AC、Fat/Fit AP、无线终端、PoE 交换机等设备，实配无线业务服务管理功能授权许可≥500； 6.支持分级分权管理，支持将不同的设备绑定到不同的管理员，支持对多个下级网管的统一管理和业务监视可对 30000 台 Fit AP 进行业务监视和配置下发，并提供统一界面；支持分级报表，分级管理中网管上级可以方便地管理到下级报表； 7.无线位置视图拓扑，按照设备所在区域，能够在位置视图中查看 AP 设备的物理位置；为了便于运维管理人员排查网络故障能提供帮助，要求支持查看 AC 与 AP 之间真实物理链路连接，真实显示从 AP 到 PoE 交换机、三层交换机、路由器等物理链路； 8.支持自定义视图并且在视图上显示设备告警和实时状态，可以导入背景图，方便管理员按需进行重点设备的重点管理；在拓扑上支持查看 AP 当前在线 Station 及详细信息，可以实现设备和用户的统一管理，支持进行 Station 上线历史记录浏览； ▲9.保修期内免费上门升级，永久授权使用。	1	套
12	▲电视屏	▲LED65 寸液晶电视，分辨率:3840*2160，电源输入*1，调试端口*1，网口*1，USB2.0*1，USB3.0*1，音视频输入*1，HDMI(ARC)*1，HDMI*1，有线/天线输入*1。	4	块

13	▲拼接器	▲四合一液晶电视拼接器，输入信号：VGA*1、HDMI*1、DVI*1、USB*1，输出信号：4 路 HDMI 输出，支持 2*2、1*4、4*1 拼接模式，单台最大支持 16 路 HDMI 信号输出。	1	个
14	防火墙	1.防火墙 1 台，冗余电源（电源模块数量 ≥ 2）。 2.提供 2 个千兆管理口（可以作为业务口），1 个 console 接口；固化 2 个 SFP+口，8 个 Combo 口，千兆以太网电接口数量 ≥16；千兆以太网光接口数量≥12；万兆光接口数量 ≥4； 3.内置 120G 的 SSD 硬盘；1 个 USB 口；整机吞吐量≥80Gbps； 4.最大并发连接数≥2400 万，每秒新建连接数≥400K；包括病毒库、攻击库、应用识别库、垃圾邮件库、网页分类库特征库升级服务授权 5 年；IPS 特征库 5 年授权许可，AV 防病毒特征库 5 年授权许可；提供厂商官网截图证明并加盖原厂鲜章。 ★5.提供生产厂家针对本项目的售后服务承诺函并加盖厂商鲜章。	1	台
15	日志搜集	1.满足日志审计、流量报表、ACE 流量记录要求，适用最高 2 万在线用户审计场景； 2.支持对设备健康状态的统一监控，实时显示设备的 CPU 利用率、内存利用率、磁盘利用率等参数，提供 web 界面配置截图； 3.支持对设备发送各类日志的集中分析； 4.支持版本文件和特征库文件的在线升级，提供 web 界面配置截图； 5.支持对所有设备的统一配置备份和下发；支持网站访问、NAT、上网行为等审计日志的集中收集；支持千万条级别日志的快速查询返回，方便定位事件；支持 TopN 流量用户排名，支持用户流量大小明细分析； 6.支持单用户流量趋势统计和业务分布分析；支持自定义时间内的 top 流量统计，提供 web 界面配置截图； ▲7.保修期内免费上门升级，永久授权使用。	1	套
16	网站防护系统	1.提供的产品 2U 含交流单电源，2*USB 接口，1*RJ45 串口，6*GE 电口（2 组 Bypass），2*千兆 SFP 插槽；最大支持 64 路防护；WEB 吞吐≥ 3Gbps，HTTP 最大并发 1000000；1TB 硬盘； 2.支持透明在线、旁路、链路聚部署，支持静态路由、策略路由等路由配置；支持 802.1Q 协议，支持 ARP 协议；支持镜像分析数据并实现旁路阻断功能，产品具备专门的阻断接口设置；支持对 SQL 注入、XSS 跨站脚本、信息泄露等 Web 漏洞扫描；支持对扫描状态进行查询，并提供扫描开始时间、结束时间等信息列表查询； 3.支持 SQL 注入、跨站脚本、防爬虫、扫描器、信息泄露、溢出、协议完整性等至少 7 种知识库展示说明；支持 HTTP 访问控制细粒度规则检测，至少提供 14 种 HTTP 访问控制路测参数，其中要包含 GET、Post、Head、Delete 等策略参数； 4.具备独立的防盗链规则，应支持 Referer 和 Cookie 检测方式；对 HTTP 访问控制参数提供优先级设置、并提供 3 种严重级别分类和至少 5 种处理动作设置；具备防跨站请求伪造功能，应支持 Get、Post 检测方式；具备敏感信息检测功能，用户可以自定义检测敏感信息，并提供替换功能，替换信息可以根据用户需求自行定义； 5.具备弱密码检测功能，提供用户名、密码字典检测机制；产品需至少提供 3 个威胁情报中心联动的接口配置功能，同时收集多家数据情报供设备使用；支持 TCP DDoS 防护策略，应具备端口扫描、SYN flood、Conn Flood、ACK flood、序号攻击、慢攻击等常见 TCP DDoS 攻击防御能力，	1	台

		应用特征库授权 5 年。		
17	网站防篡改软件	1.网站防篡改软件，自带支持 windows/linux 系统安装，同时附带集中管理中心，管理中心自带 5 条策略配置授权，支持 5 个站点目录的安全防护策略配置； 2.网页防篡改系统综合支持 Windows、linux、AIX 系统网站防篡改；支持对网站服务器的 CPU、内存、收包量、发包量等信息进行实施监控；支持对日志进行手工备份、自动备份、恢复等功能；支持 syslog、SNMP 协议、邮件等多种告警方式、短信报警； 3.支持双系统，支持系统回滚，避免单一系统故障而影响正常业务；须对下列事件产生审计记录： 对保护内容进行增加、删除、修改和恢复等操作行为；对保护内容进行访问等操作行为；网页篡改防护系统须对与系统自身安全相关的下列事件产生审计记录：管理员登陆后进行的操作行为；管理员的登录和退出等行为； 对安全策略进行添加、修改、删除等操作行为； 对管理角色进行增加、删除和属性修改等操作行为； 4.系统支持对一定时期（包括年、月、周）的网页篡改攻击进行统计并查询；有篡改行为发生时即刻阻断，篡改行为无法执行；能集中实时监控防篡改系统的引擎及关键资源的运行状态；网页篡改防护系统发生故障时不影响网站系统正常运行； ▲5.保修期内免费上门升级，永久授权使用。	1	套
18	数据安全平台	1.产品为软件形态，基于大数据平台构架；自带 200 个监控节点授权；最大支持监控节点授权数和服务器的配置有关，可对日志进行收集、统计与分析，同时还可收集系统漏洞，提供全面的安全评估、安全分析与安全威胁等（软件自带三年服务授权，到期后无法更新特征库，知识库，策略库，产品可继续使用）； 2.具备海量数据收集与快速检索能力：平均处理能力（每秒日志解析能力 EPS）：30000EPS；峰值处理能力（每秒日志解析能力 EPS）：60000EPS； 3.支持对日志进行收集、统计与分析；支持可收集系统漏洞；平台自身具备可扩展性、开放性，能够平滑扩展平台功能；支持安全分析与安全威胁等； 4.网络拓扑风险展示：在网络拓扑上量化展示各资产风险度，针对存在高风险的资产，可点击资产，展现该资产的风险信息和漏洞信息；业务拓扑风险展示：量化显示业务系统的风险度，基于业务拓扑展示业务内资产风险，可点击业务名称，详细显示业务资产连接关系及各个资产的风险度；攻击阶段的风险展示：展示各攻击阶段的风险主机数，可下钻； 5.攻击态势展示：从攻击维度对攻击源 IP 排名，攻击目的资产，病毒、木马、蠕虫、勒索软件排名，内网攻击情况，攻击级别，攻击类型等攻击风险的 TOPN 展示；脆弱性态势展示：从漏洞角度展示资产漏洞分布情况，包括漏洞整体分布情况，高危漏洞资产分布情况，区域漏洞分布情况，OWASP 漏洞分布情况，新增漏洞资产及业务情况，区域漏洞类型分布情况等漏洞分布情况；业务风险态势展示：从业务角度展示业务、资产的攻击和漏洞情况，可展示总资产数量，高危资产数量，总业务数量，高危业务数量，业务脆弱性分布占比及趋势，业务攻击分布占比及趋势，业务恶意程序分布占比及趋势； 6.CNVD 漏洞预警：针对最新的漏洞情报及资产操作系统补丁，判断资产是	1	套

		否存在该漏洞从而进行预警； 7.按条件进行全量归一化日志搜索，实现分页展示，根据资产类型、时间维度、攻击类型等多维度进行统计，可分为操作类、审计类、流量类、威胁类、系统类、安全控制类等多个维度，可记录事件级别、名称、类型、发生时间、源 IP 及端口，目的 IP 及端口、网络协议、应用协议等信息，并可通过多个维度进行灵活的事件检索； 8.支持互联网行为审计：URL/IM/文件共享/搜索引擎/论坛/其他； 支持时间轴形式显示特定用户一段时间内的行为轨迹；支持用户互联网访问行为画像：用户访问互联网的各种行为，包括 URL、邮件、文件传输\IM、搜索引擎；支持用户内网资产访问关系画像：用户访问内网业务资产系统频次、时间段； 9.互联网应用流量分析：展示互联网流量类型分布占比，包括 P2P/URL/IM/文件共享/搜索引擎/论坛/其他等分类，针对每一个流量分类，可以详细显示每一个流量子类型的排名； 10.支持用户流量分析：通过用户维度，对流量趋势进行分析，对访问应用类型进行分析，包括应用名称、上下行流量统计、总流量统计等；支持被动采集方式，包括 SYSLOG、SNMP Trap、NetFlow；支持主动采集方式，包括 FTP/TFTP、WEB-service、JDBC\ODBC、Agnet；支持自定义采集解析规则以兼容未适配日志； 11.支持日志格式归一化；支持保留原始日志；支持通过情景数据丰富归一化日志；日志存储空间阈值告警；支持日志采集代理，采集代理支持 Windows、linux 操作系统、中间件如 TOMCAT 等、数据库如 Oracle 等； ▲12.保修期内免费上门升级，永久授权使用。		
19	网站监控云平台	1.网站监控预警云平台（公有云）授权，用于网站可用性检测、内容监控（篡改、敏感词、 黑链）、漏洞监控（端口探测、弱口令检测、漏洞扫描）、告警服务；授权提供 1 个网站站点 5 年的监控服务； 2.监测内容与范围：能够对网站常见的隐患和安全灾害事故进行监测：漏洞隐患包括 Web 漏洞和系统漏洞，常见的灾害事故包括挂马网页、篡改网页、含敏感内容网页；授权提供 1 个网站站点 5 年的监控服务； 3.Web 漏洞监测与扫描能力：每个月可以对所监测的网站进行至少一次 Web 漏洞的扫描与检查；系统漏洞监测与扫描能力：每个月可以对所监测的网站进行至少一次系统漏洞的扫描与检查；漏洞验证能力：能够提供所有中高危漏洞的验证能力； 4.挂马监测能力：能够对网站主要页面提供挂马监测能力，根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报；篡改监测能力：能够对网站主要页面提供篡改监测能力，根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报；敏感内容监测能力：能够对网站主要页面提供敏感内容监测能力，根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报； 5.运营支撑要求：能够对监测的站点、监测项、进行配置与管理；数据要求：要求至少存储备份 6 个月以上监测数据；提供安全态势展示：能够按照单位组织架构维度、中国地图维度展示各省、各地级市漏洞曝出多寡的态势，事故曝出多寡的态势； 6.提供事件管理：支持展示挂马、黑链、篡改、敏感内容、DNS 解析异常、监测异常等事件的列表及场景详情；提供漏洞生命周期管理：能够针对资产漏洞列表的每一个漏洞展示漏洞名称、漏洞当前所处状态，漏洞类	1	套

		型、漏洞本身、漏洞验证、漏洞详情、以及漏洞处置建议；提供资产管理：能够自助管理各省、市甚至各单位组织的网站状况； 7.提供即时报表：用户可以在任意时刻下载半年内报表，同时支持随时生成某个资产或者某个地域、单位的在线 Html 格式报表，用户可以在任意时刻下载半年内报表，同时支持随时生成某个资产或者某个地域、单位的在线 Html 格式报表。		
20	▲安装调试费	▲本项目所有软硬件系统平台安装、调试、培训等安装调试服务。	1	项

项目名称：智慧校园大数据中心及基础平台建设项目(网络基础设施及安全设备)(A、B 包)(5 次)

项目编号：HNQZ2019-2-2(5 次)

标包名称：安全等保测评

标包编码（包号）：HNQZ2019-2-2(5 次)B 包

项目参考清单、规格、参数、服务等需求（最高限价：5 万元）

序号	品目名称	参考规格和配置技术参数	数量	单位
1	安全等保测评	▲1.安全风险评估费/等保测评费：竣工验收后提供本项目所有软件系统的等保测评证书和安全证书。 2.包括智慧校园大数据中心信息门户平台; 3、身份认证平台; 4、数据管理平台; 5、校园信息标准规范; 6、数据交换平台; 7、信息服务决策平台; 8、个人数据中心; 9、学生关爱数据预警分析应用等功能模块，与现有的一卡通、图书馆等系统进行融合，形成覆盖教职工，学生从入学前、在校中、离校后的整个生命周期管理。	1	项

2、其它要求

（1）供货完成时间：依照投标人须知前附表约定的时间。

（2）保修期为：依照投标人须知前附表约定的时间。

（3）交货地点：由采购人指定地点。

（4）在质保期间提供 7×24 小时免费技术支持和服务，出现质量问题时，中标人得到通知后 1 小时内响应，3 小时内派人员到达用户现场，6 小时内解决问题。

（5）所投质量出现问题，保质期间供应商应负责三包（包修、包换、包退）。

（6）所投工程成品性能指标必须与中标验收所提供的成品性能指标一致。

（7）投标人及产品厂家必须根据所投产品及服务的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人或招标代理机构有权对中标候选人所投货物的技术指标、资质证书资料、签字、印章、地址、联系人、电话、身份证等进行核查，如发现虚假应标与其投标文件中的描述不一，采购人有权取消其中标资格，没收投标保证金，并报政府采购主管部门严肃处理。