第五章 项目概述、技术参数要求、服务及商务要求

前提：本章中标注“★”号的条款为本次采购项目实质性要求必须满足的内容，供应商应全部满足，否则作无效响应处理。

一、项目概况

本项目为四川省食品药品学校网络信息安全系统项目，预算金额为 70 万元，共一个包。

二、采购内容

序号	标的名称	数量	单位	所属行业	备注
1	web 应用防护系统	1	台	工业	**核心产品**
2	日志审计	1	台		
3	堡垒机	1	台		
4	入侵防护系统	1	台		
5	网闸	1	台		
6	下一代防火墙	2	台		
7	终端安全管理系统	1	套		
8	上网行为管理	1	台		
9	安全检测与响应平台	3	年		

★三、执行标准、规范

1.《中华人民共和国网络安全法》；

2.《中华人民共和国密码法》；

3.《中华人民共和国计算机信息系统安全保护条例》（国务院令 147 号）；

4.《网络安全等级保护条例（征求意见稿）》；

5.《关键信息基础设施安全保护条例（征求意见稿）》；

6.《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）；

7.《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）；

8.《公安机关信息安全等级保护检查工作规范》（公信安[2008]736 号）；

9.《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）；

10.《教育部办公厅关于开展信息系统安全等级保护工作的通知》（教办厅函[2009]80 号）；

11.《教育部办公厅关于开展信息系统安全等级保护工作的通知》（教办厅函[2009]80 号）；

12.《教育部公安部关于全面推进教育行业信息安全等级保护工作的通知》（教技[2015]2 号）。

★四、技术参数要求

序号	设备名称	技术参数	数量	单位	备注
1	web 应用防护系统	1.设备须满足 1U 机型,含交流双电源模块,≥2 个 USB 接口,≥1 个 RJ45 串口,≥1 个 GE 管理口。≥4 个 GE 电口，≥1 个接口扩展插槽位，硬盘≥1T。 2.设备性能须满足网络层吞吐量≥2G，应用层吞吐量≥200M。产品须带三年维保及更新服务。 3.为了避免大量的突然流量而造成 WAF 成为网络出口的瓶颈，要求产品支持可配置并发连接数阈值的紧急模式，当并发连接数超过设置阈值时，WAF 自动进入紧急模式，已经代理的连接正常代理，对新增的请求不进行代理，直接转发，防止 WAF 成为访问瓶颈。当连接数恢复正常时，自动退出紧急模式。	1	台	

		4.为了避免非法文件上传到服务器上，要求支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell 及 Ruby shell。 5.支持注入 XSS、SSI 指令、Webshell 防护、路径穿越及远程文件包含的攻击防护。 6.支持爬虫防护，实现对 100 种以上的爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题。 7.要求系统在 HTTP 过滤功能中具备 HTTP 协议头各个字段的长度限制、后缀名过滤、支持多种 HTTP 请求参数编码、识别和限制 HTTP 响应码方式、URL 内容关键字过滤、WEB 服务器返回内容过滤等功能**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）**。 8.要求系统安全审计时，支持将告警日志转译成可理解的格式，同时具备防止审计数据丢失功能**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）**。 9.为保证产品能对主流高危漏洞、零 day 漏洞进行防护，要求产品具备国家信息安全漏洞库兼容性资质证书**（投标时须提供相关证书复印件）**。			
2	日志审计	1.设备须满足 1U 机架式，含交流冗余电源模块，≥2 个 USB 接口，≥1 个 RJ45 串口，≥1 个 GE 管理口，≥4 个千兆 SFP 插槽，≥6 个 GE 电口，≥1 个接口扩展槽位，≥2TB SATA	1	台	

		硬盘。 2.设备性能须满足授权接入≥40个日志源，日志平均处理性能≥1000EPS，具备1个内置采集器，含日志收集、日志查询、日志存储、报表管理、事件管理、资产管理、用户管理、系统配置等功能，产品需带三年维保及更新服务。 3.系统须支持内置采集器，不依赖其他设备即可进行日志采集。 4.系统支持的数据采集范围包括网络安全设备、交换设备、路由设备、操作系统、应用系统等。 5.系统须支持自身日志记录并可查询、自身CPU、内存和磁盘使用率可监控并以图形化方式动态显示，且支持状态监控和主动告警。 6.系统支持在事件规则中内置多种规则模式的事件规则，包括单源过滤模式、多源过滤模式、多源时序过滤模式，同时支持导入或创建事件规则（**投标时须提供带CNAS或CMA标志的第三方检测机构出具的检测报告复印件**）。 7.系统须支持在数据采集中选择日志接入对象，包括安全设备日志、网络设备日志、数据库数据、Windows主机事件日志、Linux主机系统日志、Web服务器日志、虚拟化平台日志、网络设备流量、其他日志、文件日志等日志对象（**投标时须提供带CNAS或CMA标志的第三方检测机构出具的检测报告复印件**）。 8.系统须支持内置日志解析规则，同时支持自定义解析规则，并为不同日志源匹配不同的日志解析规则（**投标时须提供带CNAS或CMA标志的第三方检测机构出具的检测报告复印件**）。 9.产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》EAL3+级或以上的证书（**投标时须提供相关证书复印件**）。			

3	堡垒机	1.设备须满足1U机架式，含单交流电源，≥2个USB接口，≥1个RJ45串口，≥1个GE管理口，≥4个GE电口，≥4T SATA硬盘，≥1个网络接口扩展槽。 2. 设备性能须满足字符并发数≥150个，图形并发数≥200个，被管资源数授权≥50个。产品须带三年维保及更新服务。 3.支持Telnet、SSH、RDP、VNC、HTTP、HTTPS等协议审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议/应用类型、事件等级、操作内容等并支持操作内容录像回放。 4. 支持设备发现，通过IP地址扫描，快速发现指定IP地址范围内的主机、服务器和网络设备，并自动识别启用服务和端口，方便管理员快速添加设备。 5. 支持异常账号功能，能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知等操作；支持自动发现网络中存活设备和已托管设备中存在的设备账号，支持对异常设备账号（幽灵账号和孤儿账号）的发现管理。 6. 密钥登录方式：在登录目标服务器时，使用的是秘钥登录，而非密码。在既可以使用密码，又可以使用秘钥的环境，可以自由选择登录认证方式。 7.系统须支持违规操作阻断能力，高可用性能力、鉴别数据保护能力、开发安全能力**（投标时须提供带CNAS或CMA标志的第三方检测机构出具的检测报告复印件）**。 8.系统须支持会话监视、会话回放、访问控制、操作审计的能力**（投标时须提供带CNAS或CMA标志的第三方检测机构出具的检测报告复印件）**。 9. 产品为自主研发多核分布式安全操作系统，提供国家版权局颁发的证明文件复印件，证明文件须明确注明‘安全	1	台	

		操作系统’和‘多核分布式’字样。			
4	入侵防护系统	1. 设备须满足 2U 机型，含交流冗余电源，≥1 个 RJ45 串口，千兆管理电口≥2 个（管理*1,热备*1），≥2 个 USB 接口，≥6 个 GE 电口(3 路 Bypass)，≥4 个 GE 光口，≥2 个接口扩展槽位。 2.设备性能须满足网络层吞吐量≥10G，应用层吞吐量≥1G，最大并发会话数≥200 万，每秒新增会话数≥5 万。具备入侵防护、应用管理、流量管理和抗拒绝服务等功能；产品须带三年维保及更新服务。 3.支持基于 SCADA 等工控协议的相关漏洞攻击检测； 4.系统提供自动在线升级、离线升级两种方式，至少每周定期升级攻击特征库，遇到重大安全事件，提供即时升级； 5.提供对 IPv6 协议族的转发和解析能力，保证设备在下一代网络的可用性，适应多种不同的网络环境； 6.为保障服务器安全，防止服务器设备非法外联行为，产品提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为**（投标时须提供产品功能截图）。** 7.系统须支持入侵事件分析功能，具备数据收集、协议分析、入侵逃避发现等功能**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）**。 8.系统须支持标识与鉴别功能，具备鉴别失败的处理、鉴别数据保护、超时锁定、多鉴别机制等功能**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）**。 9.产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》EAL4+级及以上的证书**（投标时须提供相关证书复印件）**。	1	台	

5	网闸	1. 设备须满足 1U 标准机架式网闸，采用双主机架构，内外网各≥4 个千兆电口，共≥2 个 RJ45 串口，≥4 个 USB2.0 口，单电源。 2. 设备性能须网络层吞吐 300Mbps，须具备内置模块（文件同步、数据库、邮件、组播、modbus、用户自定义等）、文件交换、视频应用等功能。产品须带三年维保及更新服务。 3. 系统内置安全浏览、文件同步、实时数据库、关系数据库、邮件模块、MODBUS、组播代理、用户自定义等应用模块,并可控制协议的的动作、参数、内容。 4. 支持 SMB、NFS、FTP、HTTP、FTPS、SFTP 等多种文件协议，可以实现内网到外网、外网到内网、双向的文件传送。 5. 支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名。 6. 支持文件交换容错和告警功能，交换出错能够自动重传，出现异常能够告警提示并记录日志。 7.系统须支持安全属性定义与属性初始化功能**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）**。 8.系统须支持信息流控制策略、强制访问控制、残余信息保护功能**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）**。	1	台	
6	下一代防火墙	1.设备性能须满足网络层吞吐量≥8Gbps，应用层吞吐量≥3Gbps，并发连接数≥200 万。 2.设备须满足千兆电口≥8 个，万兆光口 SFP 口≥2 个，1U 机箱，内存≥8G，硬盘容量≥64G，产品须带三年维保及更新服务。 3.设备须支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。	2	台	

		4.设备须支持静态路由、策略路由和多播路由协议，并支持 BGP、RIP、OSPF 等动态路由协议。 5.设备需支持支持源地址转换 SNAT，目的地址转换 DNAT 和双向 NAT 等功能， 支持一对一、一对多、多对一等形式的 NAT。 6.产品支持勒索软件通信防护功能**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）** 7.产品支持对不少于 9880 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。 8.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。 9.产品支持与终端安全管理系统进行联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理。 10.产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）**			
7	终端安全管理系统	1.最大支持管控客户端数量不少于 2000 点，本次 PC 授权不少于 200 个，服务器授权不少于 20 个。产品须带三年维保及更新服务。 2.可以对全网终端统一下发基本策略、病毒查杀策略、实时防护策略、安全加固策略、信任名单策略、漏洞修复策略、违规外联策略。**（投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）** 3.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。**（投**	1	套	

		标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件） 4.支持对 70+款软件进行广告弹窗拦截，让办公环境更纯净，支持在客户端查看拦截效果，包括拦截内容、拦截次数等。 5.支持轻补丁漏洞免疫功能（**投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）** 6.支持对已停止更新的 Windows 系统进行全网一键清点，支持对 Windows 停更的系统提供专项防护，包括 0day 漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等。 7.支持微隔离功能，在主界面以图形化显示业务系统、服务器及流量详情。 8.提供挖矿病毒巡检工具，支持通过内存、进程和启动项检索病毒相关信息。 9.支持展示全球热点风险事件在网内终端的爆发情况，方便及时了解和处置网内终端的热点风险事件，并显示影响的终端数量（**投标时须提供带 CNAS 或 CMA 标志的第三方检测机构出具的检测报告复印件）** 10.支持基于威胁情报的病毒特征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。 11.支持与安全检测与响应平台进行联动处置。			
8	上网行为管理	1.支持网络层吞吐量≥3.6G，应用层吞吐量≥450Mb，带宽≥300Mb，最大并发连接数≥15W，支持最大用户数≥800。内存≥4G，硬盘容量≥128G SSD，配置千兆电口≥6 个，产品需带三年维保及更新服务。 2.为了保证带宽的使用率，支持在不同线路上，按照不同的应用、目标 IP、时间段、日期、用户、位置、终端类型来进行流量控制。	1	台	

		3.支持根据访问的URL、网页关键字进行网页过滤，拒绝以IP访问网页行为。 4.支持对移动应用的细分权限控制，微信管控：微信网页版、微信传文件、微信朋友圈、微信游戏。移动QQ管控：QQ传文件、QQ视频语音等。 5.支持二维码认证，担保人扫描访客的二维码后对其网络访问授权。支持访客填写信息、担保人填写信息、免填写信息三种模式。 6.支持阻断终端用户使用外设，防止终端用户从内网拷贝信息，支持管理外设类型：存储设备、网络设备、蓝牙设备、摄像头、打印机。 7.支持不少于市面上10款以上主流杀毒软件的运行情况、软件版本、病毒库更新时间检查，对不满足检查要求的终端可重定向页面修复、弹窗提示、限制权限、禁止上网。 8.支持应用管控功能，能够封堵部分应用使用，同时支持记录全部或者指定类别的URL、网页标题、关键字等信息进行内容审计。 9.支持对管理员账号支持登陆尝试次数配置、双因素认证和TACACS+/RADIUS/LDAP协议外部认证**（投标时须提供带CNAS或CMA标志的第三方检测机构出具的检测报告复印件）** 10.支持账号注册审批功能**（投标时须提供带CNAS或CMA标志的第三方检测机构出具的检测报告复印件）**			
9	安全检测与响应平台	1. 支持内置报告模板，包括综合安全风险报告、网络安全保障工作总结等，平台需带三年维保及更新服务。 2. 支持云端专家提供轻量安全服务，进行持续的威胁狩猎，发现潜在威胁。在有攻击事件生成后，进行二次确认，通过Threat Hunting标签进行辨别，对热门威胁进行响应。	3	年	

		3. 支持首页展示风险总览、包括安全事件总览、资产统计、接入设备展示包括防火墙、探针、EDR、CWPP，待处置安全事件 TOP5、XTH 云端威胁狩猎分析、攻击面 TOP5、脆弱性资产 TOP5、风险资产分布及风险资产发生趋势、待处置安全事件分布及安全事件发生趋势。可清楚明晰下一步处置方向。 4.支持自定义可视化组件，包括资产范围、图表类型、聚合维度、度量模式、字段定义等。 5.支持采集网络侧遥测数据，包括脆弱性、服务探测、主机探测、网站攻击、后门通信、账号爆破、攻击利用、邮件攻击、DOS 攻击、漏洞利用、黑客工具、异常流量等。 6.以检测异常行为为目标，学习终端行为白基线。可用于检测高级威胁以及攻击举证，动态评估采集遥测数据范围，大幅降低遥测数据量的同时，保证安全效果。 7.支持攻击指标检测，对攻击者的攻击手法进行检测，指标覆盖 ATT&CK 所有阶段攻击手法，以检测攻击准确性为目标，通过采集的网端数据进行研判、挖掘。可以发现高级威胁。 8.支持对事件等级、威胁标签、数据源、处置状态等进行快速筛选，并提供简易模式和专家模式两种调查方式，简易模式可基于字段名称进行检索、专家模式采用 SPL 语句检索。 9.支持未知威胁检测功能。**（投标时须提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具相关证明文件）**			

★五、服务要求

（一）质量要求

1.供应商须提供全新的货物(含零部件、配件、使用说明书等)，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，不得以次充好，产品来源渠道必须合法。

2.货物必须符合或优于国家标准、行业标准、地方标准等标准、规范。

3.质保期内货物制造质量出现问题，供应商应负责三包(包修、包换、包退)，费用由供应商负担。质保期内，供应商无条件负责维修。

（二）服务要求

1. 货物安装、运输等过程中的一切货物和安装人员的人身安全均由供应商自行负责。**（投标时提供承诺函并加盖供应商公章，格式自拟）**

2. 项目中涉及的辅材、人工、系统集成费由供应商自行估算，辅材、人工、系统集成费包含运输费、安装费、税金、钻孔、布线、调试、所有辅材及可能漏项的一切费用，供应商可自行踏勘项目现场。

3. 供应商须承诺在成交后，若采购人要求，成交供应商须在成交后 3 个工作日内提供核心产品的样机，对响应参数进行逐一演示。**（投标时提供承诺函并加盖供应商公章，格式自拟）**

4. 供应商须承诺在成交后，若采购人要求，成交供应商须在成交后 3 个工作日内提供成交产品制造厂商加盖公章的采购技术参数内要求的检测报告原件或证书原件备查。**（投标时提供承诺函并加盖供应商公章，格式自拟）**

（三）售后服务要求

1. 质保期：自所有货物验收合格之日起 3 年。

2. 质保期内所有服务及配件由成交供应商提供，并提供上门服务，出现故障的货物成交供应商须迅速修复或更换并承担由此所发生的全部费用，质保期后维修，只收取维修成本费，成本费不得高于市场平均价。（质保期内的所有费用包含在本次报价内）

3. 对于正常使用情况下出现的故障，成交供应商须在半小时内作出响应，采购人要求到达现场的应在 4 小时内到达现场并解决问题或提出解决方案。**（投标时提供承诺函并加盖供应商公章，格式自拟）**

★六、成果要求

构建起学校的防御-检测-响应的安全建设体系，对外内网威胁进行发现和可视化展示，并能通过大数据分析，找出威胁源及未来的攻击趋势，将安全防御措施实施动态调整，发现安全威胁。实现网络威胁的监测预警，满足网络安全法和等级保护二级建设要求，且未来如需建设等级保护三级可以直接在现有建设的基础上增添三级要求的控制项,即满足合规性，又避免重复建设，而且通过安全威胁的闭环处理，能够对采购人安全运维管理能力得到提升和优化，可以整体提高网络安全防御、检测、与响应的能力，提高采购人应对勒索病毒、挖矿木马等高级攻击的应对能力。

★七、商务要求

1.交货时间：合同签订后 30 个工作日内完成安装调试并通过验收交付使用。因采购人教学、其他工程施工等特殊原因要求成交供应商暂缓施工，造成交货日期延误，交货计算时间顺延。

2.交货地点：采购人指定地点。

3.资金支付期限及付款比例：全部货物安装、调试完毕，经采购人验收合格后 30 日内支付合同总金额的 100%。所有设备验收合格后一次性无息退还本项目履约保证金。

4.履约方式：成交供应商与采购人签订合同后，合同双方应严格执行合同条款，履行合同规定的义务，保证合同的顺利完成。在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》的有关规定进行处理。

5.合同签订时效:成交供应商在成交通知书发出之日起三十日内与采购人签订采购合同。

6. 供应商须承诺本项目验收时，向采购人提供成交产品厂家出具的盖厂家公章的正品承诺函，格式自拟。**（投标时提供承诺函并加盖供应商公章，格式自拟）**

7.验收方案：

（1）履约验收的主体：四川省食品药品学校。

（2）邀请验收对象： 无。

（3）验收时间：应商提出验收申请之日起 5 个工作日内组织验收。

（4）验收方式：自行验收。

（5）验收程序：一次性验收。

（6）验收内容：采购文件的技术和商务要求、响应文件的响应和承诺、合同约定内容。

（7）验收标准：参照《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）进行验收。

8.包装方式及运输：涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》（财办库〔2020〕123 号）的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

9.其他未尽事宜以双方合同约定为准。