政 府 采 购 合 同

合同编号：_

项目名称：教育、教学设施设备软硬件建设网络设备采购项目-网络与信息安全实训室建设项目

货物名称：信息安全教学平台、信息安全虚拟环境靶标、信息安全运维靶场课程、WEB 应用防火墙、信息安全日志审计平台、信息安全网关、信息安全运维管理平台、安全感知管理平台、下一代防火墙 1、上网行为管理、下一代防火墙 2、日志审计

买　方：北京市城市管理高级技术学校

卖　方：颐信泰通（北京）信息科技股份有限公司

签署日期：2023 年 5 月 4 日

合　同

北京市城市管理高级技术学校(买方)教育、教学设施设备软硬件建设网络设备采购项目-网络与信息安全实训室建设项目(项目名称)中所需信息安全教学平台、信息安全虚拟环境靶标、信息安全运维靶场课程、WEB 应用防火墙、信息安全日志审计平台、信息安全网关、信息安全运维管理平台、安全感知管理平台、下一代防火墙 1、上网行为管理、下一代防火墙 2、日志审计(货物名称)经(采购人)北京市城市管理高级技术学校以 BJYM23HW006 号公开招标文件在国内公开（公开/邀请）采购。经评标委员会评定颐信泰通（北京）信息科技股份有限公司(卖方)为中标人。买、卖双方依据《中华人民共和国政府采购法》、《中华人民共和国民法典》，在平等自愿的基础上，同意按照下面的条款和条件，签署本合同。

1、　合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书

b. 中标通知书

c. 协议

d. 投标文件　　（含澄清文件）

e. 公开招标文件　　（含公开招标文件补充通知）

2、货物和数量

序号	货物名称	数量	单位	是否进口
1	信息安全教学平台	1	台	否
2	信息安全虚拟环境靶标	1	台	否
3	信息安全运维靶场课程	1	套	否
4	WEB 应用防火墙	1	套	否
5	信息安全日志审计平台	1	台	否
6	信息安全网关	1	台	否
7	信息安全运维管理平台	1	套	否
8	安全感知管理平台	1	台	否

9	下一代防火墙 1	1	台	否
10	上网行为管理	1	台	否
11	下一代防火墙 2	1	台	否
12	日志审计	1	台	否

3、合同总价

本合同总价为￥1,185,500；大写：壹佰壹拾捌万伍仟伍佰元人民币。

分项价格：

序号	分项名称	品牌、规格、型号	单价（元）	数量	合价（元）
1	信息安全教学平台	1.品牌：安恒 2.型号：DAS-CR-SLAB-EDU 3.规格： 平台功能： 综合管理：培训系统、实操系统、仿真功能、安全实训、资源库的统一化、集中化 3A 认证管理平台，具有云计算、云资源统一调度管理能力。 资源库：为业务实现提供便利的资源和工具，平台包含漏洞库、知识库、工具库、镜像库和场景库，在业务场景下可以随时调用所需资源，并且资源支持横向扩展。 教学培训：能够实现按照岗位技能和知识点的分类，有针对性对安全基础理论知识进行学习，并	458000.00	1 台	458000.00

		通过作业、实验与考试来验证知识掌握的熟练程度，成长路径支持按照学习方向，分红队蓝队进行学习。 考核检验：对试题、试卷和考试进行管理，平台支持人工组卷、动态组卷、智能组卷三种方式。 单台设备满足≥30 人并发，平台提供全中文 Web 管理界面，无需安装任意客户端软件或插件。 平台支持仿真节点资源类型包含虚拟终端、虚拟网络设备、虚拟安全设备、物理接入设备等；节点支持 KVM 虚拟机和 docker 容器类型； ▲虚拟安全设备类型包含数据库审计、日志审计、APT 攻击预警、主机安全、Web 应用防火墙、堡垒机等； 支持将实体设备接入平台，实体设备类型包含计算终端、路由器、交换机、安全防护设备等类型； ▲支持实体设备的注册与删除，支持设定实体设备的接入方式，支持通过单一设备接入与网络接入等方式实现实体设备的接入；能够根据接入方式提供网络选项配置，支持 L2 接入与 L3 接入，L2 模式接入不限制实体设备本身			

		使用的 VLAN，L3 模式支持 NAT 接入和路由器接入等形式； 平台支持以图形化拖拽的方式绘制场景拓扑，拓扑编辑支持根据网元类型筛选拓扑元素，网元类型包括路由器、交换机、虚拟机、docker、安全设备、物理设备等，并支持通过名称检索的方式搜索具体拓扑元素拖拽使用，同时支持对拓扑中元素的属性以及链路的属性进行配置； 虚拟交换机支持子网划分、DHCP、VLAN 划分、VLAN trunk、ACL 配置等相关设置，并支持三层交换功能，能够实现跨 VLAN 与子网的互通，同时支持端口镜像，能够将整个交换机的流量镜像输送到特定的交换机端口； 平台用户管理支持部门管理功能，可以构建至少三级以上部门组织架构，并可以设置部门所在省、市区信息，通过部门实现人员的分级管理； 平台支实例资源创建时的相关配置，支持自定义配置实例回收时间和个数以实现实例资源合理调度分配；提供实例端口映射导出能力，可批量导出正在运行的实例环境端口映射信息；			

		资源库包含镜像库、工具库、漏洞库、知识库、场景库，具有统一管理界面；支持资源的上下线、批量管理、横向扩展，所有资源支持标签化管理； ▲镜像库支持以上传或平台内直接制作镜像的方式进行镜像的创建，镜像类型支持虚拟机和容器两种：虚拟机支持 qcow2 格式，容器支持可以上传 Docker 镜像及 Docker File+源码两种方式；平台提供路径学习统计功能，能针对人员的参与、完成、学习时长等情况进行数据的统计展示； 课程可以设置多个知识点并关联相关课程，单个课程可以包含理论知识、实验、考试、作业等内容，课件资源支持 PDF、Word、MarkDown、视频、实验靶机、场景等类型； 平台支持通过关联内置课程，制定培训计划；单场培训支持添加多个班级，针对人员的学习情况，可以以个人、单个班级、整场培训的维度进行人员及相关学习成果的管理；平台支持用户自定义安全研究课题，并能够对个人安全研究进行管理，同时可以公开安全研究与成果，与所有人进行			

		共享； 平台支持对所有人员、单个部门以及个人的学习情况进行统计分析，展示数据可依据时间进行筛选，包括全部时间、近 1 个月、近 3 月、近 12 个月和自定义时间，默认按全部时间展示； 平台可对所有人员、单个部门以及个人参与的热门课程进行统计，支持通过标签云和排行榜的方式对最热门的课程标签进行展示，标签维度支持一级、二级、三级切换； ▲网络安全教学课程≥40 门，课程体系应覆盖信息安全基础、应用安全、数据安全、安全编程、安全运维、安全工具及攻防竞赛等知识领域，涵盖网络安全、系统安全、安全意识、等级保护、安全术语、保密培训、网络安全法律法规、安全协议、密码学、Web 安全、渗透测试、代码审计、移动安全、二进制安全、物联网安全、云计算安全、电子取证、数据存储安全、工控安全、编程技术、数据库技术、安全加固、安全防护技术、应急响应、渗透工具、CTF 夺旗赛等知识点； ▲恶意代码分析课程须包括：恶			

		意软件基础知识、病毒木马检测（手动）、恶意代码分析实战； 实验包括：Word 宏病毒实验、手工木马检测、脚本病毒编写实验、MPEG2 网马实验、木马攻击实验、脚本及恶意网页病毒、病毒防范-文件的扩展名、PE 型病毒实验、VBS 病毒实验、COM 病毒实验、实验工具文件格式猜测、病毒免杀实验：UPX 加壳分析、UPX 壳恶意程序分析、FSG 壳恶意程序分析、ProcessMonitor 恶意行为监测、恶意行为动态分析、使用 IDA 分析键盘记录行为与反向 shell、恶意软件后门与广告分析、恶意软件网络行为分析、使用 OD 分析恶意软件反向 shell 等内容； 安卓攻防实训课程须包括：移动 APP 安全概述、基础篇、工具篇、调试篇、加固篇、实战篇、通信篇、安全测试篇； 渗透测试实战演练实验须包括：74cms 程序、BEESCMS 程序、Linux、Tomcat、GhostScript 、metinfo、iCMS 、 seacms 、 Zzcms 、phpmyadmin、thinkphp、Struts、Spring 、Drupal 、WordPress、Weblogic、DedeCMS 程序、Discuz、ECShop、FCKeditor、FengCms、			

		Getboo、HDWiki、IIS6、Mono、Mutillidae、PHPMyWind、PHPok、SDCMS、Webgoat.Net、YunGouCMS、appcms、cacti、dvwa、espcms、flask、iwebSNS、jdcms、php168、phpwind、speedcms、tipask、酷维（Kuwei）、Apache、Bluecms、DirCMS、Easytalk、ElasticSearch、PhpMoAdmin、Simple-Log、ThinkSNS、ecmall、jishigou、qibocms、CwCMS、KirbyCMS、Mao10CMS、PHPSHE、SEMCMS、XDcms、XerCMS、bobokay、littlephpcms、国微校园 CMS、天生创想 CRM 系统、学生成绩查询分析系统、方维 O2O 系统、睿思网络学习系统等经典 CMS 渗透测试实战实验等内容； 应用密码学课程内容须包括：密码学概述、古典密码体制、对称密码体制、密码学数学基础、公钥密码体制、Hash 函数和消息认证、数字签名技术、密钥管理； 实验包括：恺撒密码、乘法密码、仿射密码、维吉尼亚密码、playfair 密码、希尔密码破解、认识 LSFR 及序列密码、RC4 实验、DES 实验、AES 实验、3DES 实验、IDEA 实验、SMS4 实验、大数运算、			

		素性测试、模幂、原根、求逆、RSA 密码实验、ECC 密码实验、SM4 密码实验、基于 PGP 的加密实验、Hash 基础、MD5 实验、MD5 破解、SHA 算法、SHA256 算法、SHA224 算法、HMAC 算法、RSA 签名算法、ELGamal 签名算法、ECC 签名算法等内容； ▲镜像数量 600 个，镜像类型应包含 Windows、Linux 两种类别，其中涵盖 Windows7、Windows10、Windows XP 、Windows Server 2003 、Windows Server 2008 、Windows Server 2012、Windows Server 2016、CentOS6、CentOS7、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Debain8、Kali2.0、Kali2017 等操作系统类型，可以根据镜像类型进行筛选； ▲漏洞数量应 40000 个，带复现环境 CVE 漏洞不少于 100 个。			
2	信息安全虚拟环境	1.品牌：安恒 2.型号：DAS-CR-LABOX-02 3.规格： 场景服务：用于部署操作机、应用服务器、管理软件，EDR 管理中心等虚拟环境靶标。 包含实验操作机、应用服务器、管理软件等功能。软硬一体化 2U	96000.00	1 台	96000.00

	靶标	标准机架式设备，双冗余电源，CPU：10 核 20 线程*2 颗，内存：128GB，硬盘容量：4TB*4，可用空间不小于 7TB，固态盘：960GB SSD*2，RAID 卡：2GB SAS 12Gb 8 口 RAID 卡，电口：千兆网口*4，万兆光口*2（带多模光模块），带滑轨，交换模组 10/100/1000Base-T 以太网端口*24，传输速率≥ 51Mbps/126Mbps；			
3	信息安全运维靶场课程	1.品牌：安恒 2.型号：DAS-CR-LABOX-03 3.规格： 学习培养网络安全技术工程师应掌握的理论知识、实战技能与项目交付能力，分为四个阶段：网络安全基础阶段：主要介绍网络安全基本概念，同时涵盖多个计算机领域安全性问题的剖析，例如操作系统漏洞分析、WEB 中间件漏洞分析等；安全设备部署阶段：主要介绍主流网络安全设备工作原理以及策略配置；威胁检测阶段：主要培养技术工程师对操作系统、中间件、数据库、安全设备日志和告警的分析研判及线索提取能力。 ▲课程内容分为至少网络技术基	85000.00	1 套	85000.00

		础、网络安全基础、安全设备部署、威胁检测、 综合演练场景实战五个阶段； 网络技术基础阶段主要包含数据通信的基本原理、Linux 基本的安装和命令使用等相关课程； 网络安全基础阶段主要介绍网络安全基本概念，同时涵盖多个计算机领域安全性问题的剖析，包含操作系统漏洞分析及加固、WEB 中间件漏洞分析及加固等相关课程； 安全设备部署阶段主要介绍主流网络安全设备工作原理以及策略配置，包含边界防护、WEB 应用安全、安全运维、数据安全、终端安全等课程； 综合演练场景实战阶段包括对技术工程师主要的设备配置能力进行全面验证和提升，包含企业基础网络安全防护能力建设实训、企业网络安全防护体系优化实训、企业威胁监测实训等场景。			
4	WEB 应用防火墙	1. 品牌：安恒 2. 型号：WAF-EDU-100AG 3. 规格： 软硬一体模块；网络吞吐量：1GbpsHTTP 应用吞吐量：500MbpsHTTP 最大并发数：3 万	26,000	1 套	26,000

	★	HTTP 新建连接(CPS)：4000HTTPS 应用吞吐量：100MbpsHTTPS 最大并发数：6000HTTPS 最大新建数：800；硬件规格：1U 工控机设备；CPU：4 核 4 线程；内存：8G；机械盘容量：2T；电口：千兆网口*6；：单电源； 支持客户端安全防护，插入特殊的 HTTP 报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options、X-Content-Type-Options、X-XSS-Protect、Content-Security-Policy； 具有机器学习安全引擎，可以对用户 web 业务系统建立安全的访问模型，学习的内容包括 URL 地址、URL 请求参数等信息；支持设定学习的周期，域名信息，可信任的客户端 IP，不可信的客户端 IP 以及不学习的 URL 信息； 支持根据细粒度条件对 CC 攻击进行检测和防护；匹配条件由 URL 参数、请求头部字段、目的 IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成；客户端检测对象由 IP、IP+URL、IP+User_Agent 等参数组成；支持从请求头字段			

		获取真实源 IP 地址； 支持按地理区域对攻击次数等进行统计，并通过地图展示；支持在地图上对某一地理区域设置阻断此区域 IP 的访问。			
5	信息安全日志审计平台	1.品牌：安恒 2.型号：DAS-EDU-LOG-50 3.规格： 软硬一体模块；日志处理能力 EPS：200/秒，全功能开放，资产授权许可数量：20 个，硬件规格：1U 工控机设备；CPU：4 核 4 线程；内存：8G；机械盘容量：2T；电口：千兆网口*6；单电源； 支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP、kafka 等协议方式进行日志收集，支持使用代理(Agent)方式提取日志并收集； 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件； ▲通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。	55000.00	1 台	55000.00
6	信息	1.品牌：安恒 2.型号：DAS-EDU-NGFW100	42500.00	1 台	42500.00

	安全网关	3.规格： 软硬一体模块；最大并发连接数：100万每秒，新建连接数：3.5万，SSLVPN并发用户数：400；硬件规格：1U工控机设备；CPU：2核；内存：2G；机械盘容量：500G；电口：千兆网口*10+Combo*2；单电源；支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能； 支持入侵防御能力，规则库≥8600条，可显示对应规则的攻击类型、严重程度、CVE编号、CNNVD编号、协议、操作系统、发布年份、漏洞厂商等详细信息； 支持对压缩文件进行病毒查杀，涵盖常见的压缩文件类型，可设置对不低于20层压缩文件进行查杀； ▲支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等。			
7	信	1.品牌：安恒	43000.00	1	43000.00

	息安全运维管理平台	2.型号：DAS-EDU-USM100 3.规格： 软硬一体模块；授权资产≥100个；硬件规格：1U 工控机设备；CPU≥4 核 4 线程；内存≥8G；机械盘容量≥1T；电口≥千兆网口*6；单电源； IE/Chrome 代填应用发布： HTTP/HTTPS 协议的 web 设备，且可以直接代填账号和密码； 支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权； 支持Windows/Mac操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作； ▲支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。		套	
8	安全感知	1. 品牌：深信服 2. 型号：SIP-Y-1600 3. 规格： （1） 硬件要求	160000.00	1台	160000.00

	管理平台	网络层吞吐量≥500Mbps；1U标准机箱，内存≥16G，硬盘容量≥128GMSATA，≥4TSATA，接口≥6千兆电口，≥2 万兆光口 SFP+； （2） 总览 支持对全网资产总览分析，包括资产概览、服务器运行状态、资产统计，其中资产概览包括 7 天即将退库资产、全部资产数、核心资产数、资产组数、服务器数、终端数； （3） 综合安全态势大屏 支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连 态势、横向威胁态势、设备运行态势；支持页面跳转到对应态势大屏，并具备大屏告警能力； （4） 横向威胁态势 支持大屏展示横向威胁态势，包括业务与终端访问、发起威胁终端 TOP5、遭受威胁业务 TOP5、访问趋势图；支持不同颜色标注横向攻击、违规访问、可疑行为、风险访问等行为； （5） 弱密码 支持检测包括 HTTP、FTP、LDAP、VMWARE、ORACLE、VNC 等不少于 15 类的常见协议的弱密			

		码，检测信息包含账号、密码、服务器、所属分支和业务、类型、最近发现时间等；支持筛选管理员账号与是否登录成功，并支持导出弱密码报告； （6） 违规访问 ▲检测内网主机的访问情况是否符合规定，需要人工事先进行梳理好访问关系再进行配置。策略从上到下进行匹配，可以通过右侧置顶功能对策略优先级进行调节。支持 IP，IP 组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式； （7） 漏洞报告 支持流量实时分析漏洞功能，漏洞类型包括配置错误漏洞、OpenSSH 漏洞、OpenLDAP、数据库、Web 应用等；支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告； （8） 风险业务视角 支持业务视角维度展示安全风险，包括攻击阶段分布、风险等级趋势、事件描述、遭受的外部攻击、脆弱性风险、行为画像、			

		开放端口等； （9） 可疑 DNS 分析 支持 DNS 异常分析，包括 DNS 通道、DGA 域名、灰域名与高风险注册地域名，其中高风险注册地域名可自定义国家和地区；并支持导出可疑 DNS 列表； （10） 访问核查 支持源 IP、目的 IP、源端口、目的端口、起始时间等维度定义核查任务；支持统计每天访问频次及访问成功和失败次数； （11） 分析中心 ▲平台内置挖矿安全知识库，对常见的挖矿如：Bluehero 挖矿蠕虫变种、虚拟货币挖矿、EnMiner 挖矿病毒、PowerGhost 挖矿病毒、DDG 挖矿病毒、Docker 挖矿、DDG 挖矿变种、GroksterMiner 挖矿病毒、Linux 挖矿木马、ZombieBoy 挖矿木马等提供详细的背景介绍、感染现象、详细分析、相关 IOC（MD5、C2、URL）、解决方案； （12） 文件威胁分析 支持文件威胁分析，可展示文件分析过程、文件检测趋势、恶意文件 TOP5；支持恶意文件的详情分析，包括支持记录恶意文			

		件感染的主机、文件名、病毒名称、传输协议等。支持挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计； （13） 异常行为分析 支持服务器行为分析，具备独立页面展示行为引擎学习的天数、异常行为与异常服务器数量，并对异常行为进行举证描述； 支持利用 EBA 技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。并支持用户对 EBA 基线进行自定义调整，优化模型； （14） 横向访问分析 支持横向访问服务器流量分析， 包括 TOP5 应用流量趋势、TOP5 协议趋势；支持服务器视角和来访分支视角，其中服务器视角可展示服务器 IP、总流量、源 IP 数量、应用 TOP10、协议端口			

		TOP10、连接失败数、最大并发，并支持以表格形式导出数据； （15） 主机安全风险报告 支持分别导出主机安全风险、脆弱性风险、总体摘要（含总体摘要、安全感知详情、行为画像、安全规划建设建议等）、综合风险四个不同维度的报告； （16） 深度检测引擎升级 ▲具备元数据行为分析引擎：httpflow、dnsflow、adflow、icmpflow、maillflow 等，通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹 shell 等事后检测场景。			
9	下一代防火墙 1	1.品牌：深信服 2.型号：AF-2000-FH2130B-LV 3.规格： （1） 硬件要求 1U 标准机箱，内存：8G，8 千兆电口，2 万兆光口 SFP+；网络层吞吐量：20Gb，应用层吞吐量：9Gb；并发连接数：200 万； （2） CC 攻击防护 产品支持 CC 攻击防护功能，为保障勒 CC 攻击的检测效果； （3） 病毒检测 ▲产品支持对多重压缩文件的病	84000.00	1 台	84000.00

		毒检测能力，支持不小于15层压缩文件病毒检测与处置； （4） 安全防护 ▲产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改； （5） 安全策略 产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制； （6） 文件目录防护 产品支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制； （7） 策略管理 ▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； （8） 深度检测 产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MS SQL 等应用协议进行深度检测			

		与防护； （9） 协议管理 产品支持 Web 管理、串口管理、SSH 管理等多种不同方式； （10） 会话管理 支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录； （11） 攻击防护 支持 SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护。			
10	上网行为管理	1.品牌：深信服 2.型号：AC-1000-B1200-OS 3.规格： （1） 硬件要求 1U 标准机箱，内存：4G，6 千兆电口，2 千兆光口 SFP；网络层吞吐量：3Gb，应用层吞吐量：300Mb；最大并发连接数：120000，每秒新建连接数：2400； （2） 部署方式 支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能；支持网桥模式，以透明方式串接在网络中；支持电口 bypass；必须支持多路桥接功能；支持旁路	26000.00	1 台	26000.00

		模式，无需更改网络配置，实现上网行为审计；旁路支持主主、主备模式部署； ▲支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6； （3） 系统管理 多台设备支持通过统一平台集中管理、集中配置等；加入集中管理时，支持身份认证，比如密码正确才能加入；解除集中管理时，要输入中心端的解控秘钥才允许解控； （4） 实时监控 提供设备实时 CPU、内存、磁盘占有率、在线用户数、系统时间、网络接口等信息； ▲针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级;支持以列表形式展示访问质量差的用户名单;支持对单用户进行定向 web 访问质量检测； （5） 第三方用户源 支持 LDAP、Radius、POP3、Proxy 等第三方认证；支持 ISA\lotus ldap\novel			

		ldap\oracle、sql server、db2、mysql 等数据库等第三方认证； （6） 认证方式 支持 radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定 IP 段的用户必须使用单点登录； 密码登录支持用户自注册，通过 Web 页面申请注册新账号，管理员审批后新账号可用，自注册同时支持 portal 认证和 802.1x 认证； 支持管理员关联了手机号码，可以通过手机号接受自注册、终端注册、终端绑定的审批通知； ▲支持通过 OAuth 认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证； 支持企业微信、MOA、钉钉 这三个平台支持同步组织结构，用户通过企业微信、MOA、钉钉认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组； （7） 网页审计 支持用户可以自定义产生根证书，导入包含秘钥的根证书； 提供产品界面截图；			

		日志中心所有导出都有对应管理员操作日志、系统日志的日志清理中记录数据删除日志、规则库升级有对应升级日志； （8） 终端日志 支持查询和导出基于指定时间段/用户/用户组的防共享接入日志、移动终端发现日志、准入日志、登录注销日志等行为日志。			
11	下一代防火墙2	1.品牌：深信服 2.型号：AF-1000-FH1300A-GH 3.规格 （1） 硬件要求 1U，内存≥4G，接口≥8千兆电口、≥2千兆光口 SFP。网络层吞吐量≥4G，应用层吞吐量≥1G；并发连接数≥100万； （2） 授权 需配备IPS、AV、WAF等模块，模块授权需提供3年，售后服务为3年； （3） Web 攻击防御 ▲产品支持对常见 Web 应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义 Web 应用漏洞特征库不低于 4580 种；	44000.00	1台	44000.00

		（4） CC 攻击防护 产品支持 CC 攻击防护功能，为保障勒 CC 攻击的检测效果； （5） 病毒检测 ▲产品支持对多重压缩文件的病毒检测能力，支持不小于 15 层压缩文件病毒检测与处置； （6） 安全策略 产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制； （7） 文件目录防护 产品支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制； （8） 策略管理 ▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； （9） 深度检测 产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MS SQL 等应用协议进行			

		深度检测与防护； （10） 协议管理 产品支持 Web 管理、串口管理、SSH 管理等多种不同方式； （11） 会话管理 支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录； （12） 攻击防护 支持 SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护； （13） 产品架构 ▲产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能。			
12	日志审计	1. 品牌：深信服 2. 型号：SIP-Logger-A600 3. 规格： （1） 硬件要求 2U 标准机箱，硬盘：4TB，内存：6G，6 千兆电口，2 万兆光口 SFP+，双电源； （2） 性能要求 最大可扩展审计主机许可数 150，平均每秒处理日志数（eps）	66000.00	1 台	66000.00

		最大性能 1200； （3） 日志采集 支持主动、被动相结合的数据采集方式，支持通过 Agent 采集日志数据，支持通过 syslog、SNMP Trap 、 JDBC 、 WMI 、webservice、FTP、文件\文件夹读取、Kafka 等多种方式完成日志收集； （4） ▲日志标准化 支通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射； （5） 日志过滤 支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用； （6） ▲日志转发 支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志； （7） 全文检索 支持通配符、范围搜索、字			

		段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件； 支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析； （8） 日志分析 支持自定义审计规则与关联规则，支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到 350 条以上； （9） 日志告警 日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量，提供截图证明； （10） 系统管理 提供管理员账号创建、修改、			

		删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持 usb-key 认证；支持个性化定制，支持全系统更换 logo 与系统名称，支持一键恢复默认。			

4、付款方式

本合同的付款方式为：签订合同后 10 个工作日内支付 60%（即人民币柒拾壹万壹仟叁佰元整（￥711,300）货款。项目整体验收合格后 10 个工作日内付 40%（即人民币肆拾柒万肆仟贰佰元整（￥474,200）尾款。乙方需缴纳合同金额 5%（即人民币伍万玖仟贰佰柒拾伍元整（￥59,275）的质量保证金，为期 1 年，如无质量问题 1 年后无息退还。

5、本合同货物的交货时间及交货地点

交货时间：自合同签订生效之日起 30 日内

交货地点：北京市大兴区康庄路 38 号

6、合同的生效。

本合同经双方全权代表签署、加盖单位印章并由卖方递交质量保证金后生效。

买 方：北京市城市管理高级技术学校　　卖 方：颐信泰通（北京）信息科技股份有限公司

名 称：（印章）　　名 称：（印章）

2023 年 5 月 19 日　　2023 年 5 月 19 日

授权代表(签字)：　　授权代表(签字)：

地　址：北京市大兴区康庄路 38 号　　地　址：北京市海淀区花园路 2 号 2 号

楼 511A 室

邮政编码：102600

电　话：

开户银行：工行北京体育场支行

开户行号：

账　号：0200053009008801339

邮政编码：100095

电　话：010-82237666

组织机构代码：911101087975998736

开户行号：301100000179

账　号：11006084101817008 4084

合同一般条款

1定义

本合同中的下列术语应解释为：

1.1 “合同”系指买卖双方签署的、合同格式中载明的买卖双方 所达成的协议， 包括所有的附件、附录和构成合同的其它文件。

1.2 “合同价”系指根据合同约定，卖方在完全履行合同义务后买方应付给卖方的价格。

1.3 “货物”系指卖方根据合同约定须向买方提供的一切设备、机械、仪表、备件，包括工具、手册等其它相关资料。“服务”系指根据合同约定卖方承担与供货有关的辅助服务，如运输、保险及安装、调试、提供技术援助、培训和其他类似的服务。

1.5 “买方”系指与中标人签属供货合同的单位（含最终用户）。

1.6 “卖方”系指根据合同约定提供货物及相关服务的中标人。

1.7 “现场”系指合同约定货物将要运至和安装的地点。

1.8 “验收”系指合同双方依据强制性的国家技术质量规范和合同约定，确认合同项下的货物符合合同规定的活动。

2技术规范

2.1 提交货物的技术规范应与招标文件规定的技术规范和技术规范附件(如果有的话)及其投标文件的技术规范偏差表(如果被买方接受的话)相一致。若技术规范中无相应说明，则以国家有关部门最新颁布的相应标准及规范为准。

3知识产权

3.1 卖方应保证买方在使用该货物或其任何一部分时不受第三方提出的侵犯专利权、 著作权、商标权和工业设计权等的起诉。如果任何第三方提出侵权指控，卖方须与第三方交 涉并承担由此发生的一切责任、费用和经济赔偿。

4包装要求

4.1 除合同另有约定外，卖方提供的全部货物，均应采用本行业通用的方式进行包装，且该包装应符合国家有关包装的法律、法规的规定。包装应适应于远距离运输、防潮、防震、防锈和防粗暴装卸，确保货物安全无损，

运抵现场。由于包装不善所引起的货物锈蚀、损坏和损失均由卖方承担。

4.2　每件包装箱内应附一份详细装箱单和质量合格证。

5装运标志

5.1.　卖方应在每一包装箱的四侧用不褪色的油漆以醒目的中文字样做出标记。

5.2　如果货物单件重量在 2 吨或 2 吨以上，卖方应在每件包装箱的两侧用中文和适当的运输标记，标明“重心”和“吊装点”，以便装卸和搬运。根据货物的特点和运输的不同要求，卖方应在包装箱上清楚地标有“小心轻放”、“防潮”“勿倒置”等字样和其他适当的标志。

6交货方式

6.1　交货方式一般为下列其中一种，具体在合同特殊条款中规定。

6.1.1　现场交货：卖方负责办理运输和保险，将货物运抵现场。有关运输和保险的一切费用由卖方承担。所有货物运抵现场的日期为交货日期。

6.1.2　工厂交货：由卖方负责代办运输和保险事宜。运输费和保险费由买方承担。运输部门出具收据的日期为交货日期。

6.1.3　买方自提货物：由买方在合同规定地点自行办理提货。提单日期为交货日期。

6.2　卖方应在合同规定的交货期 30 天以前以电报或传真形式将合同号、货物名称、数量、包装箱件数、总毛重、总体积(立方米)和备妥交货日期通知买方。同时卖方应用挂号信将详细交货清单一式 6 份包括合同号、货物名称、规格、数量、总毛重、总体积(立方米)、包装箱件数和每个包装箱的尺寸(长×宽×高)、货物总价和备妥待交日期以及对货物在运输和仓储的特殊要求和注意事项通知买方。

6.3　在现场交货和工厂交货条件下，卖方装运的货物不应超过合同规定的数量或重量。否则，卖方应对超运部分引起的一切后果负责。

7装运通知

7.1　在现场交货和工厂交货条件下的货物，卖方通知买方货物已备妥待运输后 24 小时之内，应将合同号、货名、数量、毛重、总体积(立方米)、发票金额、运输工具名称及装运日期，以电报或传真通知买方。

7.2　如因卖方延误将上述内容用电报或传真通知买方，由此引起的一切后果

损失应由卖方负责。

8保险

8.1 如果货物是按现场交货方式或工厂交货方式报价的，由卖方按照发票金额的 110%办理“一切险”；如果货物是按买方自提货物方式报价的，其保险由买方办理。

9付款条件

9.1 付款条件见第二册第七章“合同特殊条款”。

10技术资料

10.1 合同项下技术资料(除合同特殊条款规定外)将以下列方式交付：

合同生效后 30 天之内，卖方应将每台设备和仪器的中文技术资料一套，如目录索引、图纸、操作手册、使用指南、维修指南和 / 或服务手册和示意图寄给买方。

10.2 另外一套完整的上述资料应包装好随同每批货物一起发运。

10.3 如果买方确认卖方提供的技术资料不完整或在运输过程中丢失，卖方将在收到买方通知后 30 天内将这些资料免费寄给买方。

11质量保证

11.1 卖方须保证货物是全新、未使用过的，并完全符合强制性的国家技术质量规范和合同规定的质量、规格、性能和技术规范等的要求。

11.2 卖方须保证所提供的货物经正确安装、正常运转和保养，在其使用寿命期内须具有符合质量要求和产品说明书的性能。在货物质量保证期之内，卖方须对由于设计、工艺或材料的缺陷而发生的任何不足或故障负责。

11.3 根据买方按检验标准自己检验结果或委托有资质的相关质检机构的检验结果，发现货物的数量、质量、规格与合同不符；或者在质量保证期内，证实货物存在缺陷，包括潜在的缺陷或使用不符合要求的材料等，买方应尽快以书面形式通知卖方。卖方在收到通知后 30 天内应免费维修或更换有缺陷的货物或部件。

11.4 如果卖方在收到通知后 30 天内没有弥补缺陷，买方可采取必要的补救措施，但由此引发的风险和费用将由卖方承担。

11.5 除“合同特殊条款”规定外，合同项下货物的质量保证期为自货物通过最终验收起 36 个月。

12检验和验收

12.1 在交货前，中标人应对货物的质量、规格、性能、数量和重量等进行详细而全面的检验，并出具证明货物符合合同规定的文件。该文件将作为申请付款单据的一部分，但有关质量、规格、性能、数量或重量的检验不应视为最终检验。

12.2 货物运抵现场后，买方应在10日内组织验收，并制作验收备忘录，签署验收意见并报同级政府采购监督管理部门备案。

12.3 买方有在货物制造过程中派员监造的权利，卖方有义务为买方监造人员行使该权利提供方便。

12.4 制造厂对所供货物进行机械运转试验和性能试验时，中标人必须提前通知买方。

13索赔

13.1 如果货物的质量、规格、数量、重量等与合同不符，或在第11.5规定的质量保证期内证实货物存 有缺陷，包括潜在的缺陷或使用不符合要求的材料等，买方有权根据有资质的权威质检机构的检验结果向卖方提出索赔（但责任应由保险公司或运输部门承担的除外）。

13.2 在根据合同第11条和第12条规定的检验期和质量保证期内，如果卖方对买方提出的索赔负有责任，卖方应按照买方同意的下列一种或多种方式解决索赔事宜：

13.2.1 在法定的退货期内，卖方应按合同规定将货款退还给买方，并承担由此发生的一切损失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为保护退回货物所需的其它必要费用。如已超过退货期，但卖方同意退货，可比照上述办法办理，或由双方协商处理。

13.2.2 根据货物低劣程度、损坏程度以及买方所遭受损失的数额，经买卖双方商定降低货物的价格，或由有权的部门评估，以降低后的价格或评估价格为准。

13.2.3 用符合规格、质量和性能要求的新零件、部件或货物来更换有缺陷的部分或／和修补缺陷部分，卖方应承担一切费用和风险并负担买方所发生的一切直接费用。同时，卖方 应按合同第11条规定，相应延长修补或更换件的质量保证期。

13.3 如果在买方发出索赔通知后 30 天内，卖方未作答复，上述索赔应视为已被卖方接受。如卖方未能在买方提出索赔通知后 30 天内或买方同意的更长时间内，按照本合同第 13.2 条规定的任何一种方法解决索赔事宜，买方将从合同款或从卖方开具的质量保证金保函中扣回索赔金额。如果这些金额不足以补偿索赔金额，买方有权向卖方提出不足部分的补偿。

14迟延交货

14.1 卖方应按照“货物需求一览表及技术规格”中买方规定的时间表交货和提供服务。

14.2 如果卖方无正当理由迟延交货，买方有权提出违约损失赔偿或解除合同。

14.3 在履行合同过程中，如果卖方遇到不能按时交货和提供服务的情况，应及时以书面形式将不能按时交货的理由、预期延误时间通知买方。买方收到卖方 通知后，认为其理由正当的，可酌情延长交货时间。

15违约赔偿

15.1 除合同第 16 条规定外，如果卖方没有按照合同规定的时间交货和提供服务，买方可要求卖方支付违约金。违约金按每周迟交货物或未提供服务交货价的 0.5%计收。但违约金的最高限额为迟交货物或没有提供服务的合同价的 5%。一周按 7 天计算，不足 7 天按一周计算。如果达到最高限额，买方有权解除合同。

16不可抗力

16.1 如果双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。

16.2 受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知另一方，并在事故发生后 20 天内，将有关部门出具的证明文件送达另一方。

16.3 不可抗力使合同的某些内容有变更必要的，双方应通过协商在 20 日内达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

17税费

17.1 与本合同有关的一切税费均适用中华人民共和国法律的相关规定。

18合同争议的解决

18.1 因合同履行中发生的争议，可通过合同当事人双方友好协商解决。如自

协商开始之起 15 日内得不到解决，双方可将争议提交同级政府采购办公室调解。调解不成的，可向北京市通州区人民法院提起诉讼。

18.2 诉讼费用除法院另有裁决外，应由败诉方负担。

19违约解除合同

19.1 在卖方违约的情况下，买方经同级政府采购监督管理机关审批后，可向卖方发出书面通知，部分或全部终止合同。同时保留向卖方追诉的权利。

19.1.1 卖方未能在合同规定的限期或买方同意延长的限期内，提供全部或部分货物的；

19.1.2 卖方未能履行合同规定的其它主要义务的；

19.1.3 买方认为卖方在本合同履行过程中有腐败和欺诈行为的。

19.1.3.1 “腐败行为”和“欺诈行为”定义如下:

19.1.3.1.1 “腐败行为”是指提供/给予/接受或索取任何有价值的东西来影响买方在合同签定、履行过程中的行为。

19.1.3.1.2 “欺诈行为”是指为了影响合同签定、履行过程，以谎报事实的方法， 损害买方的利益的行为。

19.2 在买方根据上述第 19.1 条规定，全部或部分解除合同之后，应当遵循诚实信用原则，以政府采购监督管理部门同意的方式，购买与未交付的货物类似的货物或服务，卖方应承担买方购买类似货物或服务而产生的额外支出。部分解除合同的，卖方应继续履行合同中未解除的部分。

20破产终止合同

20.1 如果卖方破产或无清偿能力时，买方经报同级政府采购监督管理部门审批后，可在任何时候以书面通知卖方，提出终止合同而不给卖方补偿。该合同的终止将不损害或不影响买方已经采取或将要采取任何行动或补救措施的权利。

21转让和分包

21.1 政府采购合同不能转让。

21.2 经买方和同级政府采购监督管理部门事先书面同意卖方可以将合同项下非主体、非关键性工作分包给他人完成。接受分包的人应当具备相应的资格条件，并不得再次分包。分包后不能解除卖方履行本合同的责任和义务，接受分包的人与卖方共同对买方连带承担合同的责任和义务。

如未经买方同意，卖方擅自分包的，则在支付最后 40%的款项中，买方扣除合同总价款 10%作为违约金。扣除违约金后，卖方与分包人仍需对买方承担连带责任。

22合同修改

22.1 买方和卖方都不得擅自变更本合同，但合同继续履行将损害国家和社会公共利益的除外。如必须对合同条款进行改动时，当事人双方须共同签署书面文件，做为合同的补充，并报同级政府采购监督管理部门备案。

23通知

23.1 本合同任何一方给另一方的通知，都应以书面形式发送，而另一方也应以书面形式确认并发送到对方明确的地址。

24计量单位

24.1 除技术规范中另有规定外，计量单位均使用国家法定计量单位。

25适用法律

25.1 本合同应按照中华人民共和国的法律进行解释。

26质量保证金

26.1 卖方应在合同签订后 10 天内，按约定的方式向买方提交合同总价（不超过 5%）的质量保证金。

26.2 质量保证金用于补偿买方因卖方不能履行其合同义务而蒙受的损失。

26.3 质量保证金应使用本合同货币，按下述方式之一提交：

A. 买方可接受的在中华人民共和国注册和营业的银行，
按招标文件提供的格式（附件 8），或其他买方可接受的格式。

B. 支票、汇票或现金。

26.4 如果卖方未能按合同规定履行其义务，买方有权从质量保证金中取得补偿。质量保证期结束后十天内，买方将把质量保证金无息退还卖方。

27合同生效和其它

27.1 政府采购项目的采购合同内容的确定应以招标文件和投标文件为基础，不得违背其实质性内容。政府采购项目的采购合同自签订之日起七个工作日内，买方应当将合同副本报同级政府采购监督管理部门和有关部门备案。合同将在双方签字盖章并由卖方递交质量保证金后开始生效。

27.2 本合同一式 5 份，具同等法律效力。北京市城市管理高级技术学校和颐

信泰通（北京）信息科技股份有限公司各执贰份，采购代理机构执一份。

附件 1：中标通知书

永明项目管理有限公司

教育、教学设施设备软硬件建设网络设备采购项目-网络与信息安全实训室建设项目

中标通知书

颐信泰通（北京）信息科技股份有限公司：

我公司组织的教育、教学设施设备软硬件建设网络设备采购项目-网络与信息安全实训室建设项目（项目编号：BJYM23HW006）的公开招标工作已经结束。经评标委员会推荐和采购人批准，贵公司为本项目中标人。

中标金额：人民币 1,185,500.00 元。

大写：壹佰壹拾捌万伍仟伍佰元整。

请贵公司于本通知书发出之日起 30 日内，根据公开招标文件和投标文件中的合同构成文件与采购人签订合同。

特此通知！

永明项目管理有限公司

2023 年 05 月 08 日

地址：北京市丰台区广安路 9 号院国投财富广场 5 号楼 12A15 室

传真：010-63268382

电话：010-63268382 转 8007　　邮箱：bjymxmgl@163.com