**附件清单**

| 序号 | 名 称 | | 型号和规格 | 品牌 | 数量 | 单价 （元人民币） |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 内网万兆防火墙 | | 型号：网神SecGate3600防火墙 NSG4900-TG45  规格：2U机架式专用设备，冗余电源；板载8个千兆电口，8个千兆光口，6个万兆光口，2个扩展插槽，1个Console口，2个USB接口，支持液晶屏；4T存储容量的企业级硬盘，三年硬件维保服务。网络层吞吐量20G，应用层吞吐量15G，并发连接700万，每秒新建连接数25万；默认含32个IPsecVPN标配并发隧道数，最大并发隧道数10000个；默认含32个SSLVPN标配并发用户数，最大并发用户数2000个。配置防火墙、IPS模块、URL过滤、防病毒模块、流量管理、IPSec VPN等功能模块；3年质保及3年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报升级服务。 | 奇安信 | 2台 | 146000 |
| 2 | 无线万兆防火墙 | | 型号：网神SecGate3600防火墙NSG4900-TG45  规格：2U机架式专用设备，冗余电源；板载8个千兆电口，8个千兆光口，6个万兆光口，2个扩展插槽，1个Console口，2个USB接口，支持液晶屏；4T存储容量的企业级硬盘，三年硬件维保服务。网络层吞吐量20G，应用层吞吐量15G，并发连接700万，每秒新建连接数25万；默认含32个IPsecVPN标配并发隧道数，最大并发隧道数10000个；默认含32个SSLVPN标配并发用户数，最大并发用户数2000个。配置防火墙、IPS模块、URL过滤、防病毒模块、流量管理、IPSec VPN等功能模块；3年质保及3年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报升级服务。 | 奇安信 | 1台 | 146000 |
| 3 | 堡垒主机 | | 型号：绿盟运维安全管理系统OSMSNX3-HD600C  规格：1U机架式专用设备，单电源，4T数据存储空间，4\*GE电口，2\*USB，1\*串口，1\*GE管理口，1个接口扩展槽（可扩展8个千兆网络接口或2个万兆光口）。最大字符并发数1000，最大图形并发数500，最大可管理设备数500台，最大SDP远程接入并发数50个；配置200台设备管理授权及3个SDP远程接入授权；三年质保及规则库升级服务。 | 绿盟 | 1台 | 127000 |
| 4 | 日志审计系统 | | 型号：绿盟日志审计系统LASNX3-HD3000  规格：1U机架式专用设备，冗余电源，2\*USB接口，1\*RJ45串口，1\*GE管理口，4个千兆电口，3个接口扩展槽位（可扩展12个千兆接口或者6个万兆光口），8TB数据存储空间，最大日志处理性能7000EPS。配置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。授权接入200个日志源，可通过授权扩展到500日志源；三年质保及规则库升级服务。 | 绿盟 | 1台 | 160000 |
| 5 | 专线防火墙 | | 型号：网神SecGate3600防火墙 NSG2000-TE30  规格：1U机架式专用设备，单电源；6个千兆电口，6个千兆光口，1个扩展插槽，1个Console口，2个USB接口，无液晶屏；网络层吞吐量5G，应用层吞吐量3.5G，并发连接300万，每秒新建连接数6万；含16个IPsecVPN标配并发隧道数，最大并发隧道数3000个；默认含16个SSLVPN标配并发用户数，最大并发用户数300个；3年质保及3年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报升级服务。 | 奇安信 | 1台 | 79600 |
| 6 | IT运维监控系统 | | 型号：IT运维管理系统 ITCenter v6.0  规格：软件版；200资产管理授权，支持对网络设备、服务器、数据库、中间件、服务资源、网页资源、安全设备等进行监控；配置网络告警模块，采用Mail、系统告警、运维告警等多种方式，对CPU、内存、端口和链路的负载及自定义的指标进行告警；对设备的状态、应用服务的端口状态、数据包传输情况进行告警，同时具备告警的压缩，合并、过滤等功能；配置服务器管理模块、应用管理模块、网络设备管理模块、服务管理模块、安全设备管理模块、拓扑管理模块、动态背板管理模块、大屏展示模块等；3年质保服务。 | 有望科技 | 1套 | 220000 |
| 7 | 资源访问控制系统 | | 型号：资源访问控制网关VPN ITMS-SDP-5600-1000  规格：2U机架式专用设备，冗余电源，内存16G，存储容量1T，8个电口、4个万兆光口、1扩展卡。最大并发请求数2000，授权并发用户数1000，支持资源访问控制，支持校外用户访问内网 Web 业务系统，支持多种协议访问内网主机、网络设备等资源，支持对接各类认证系统，实现多维认证；结合门户自定义、精细化授权、日志全量记录、设备统一认证等丰富功能以及强大的安全防控机制；三年质保及规则库升级服务。 | 网瑞达 | 1台 | 180000 |
| 8 | 门禁一体机 | | 型号：海康威视DS-K1T804BMF  规格：指纹+密码+IC卡  操作系统 Linux  QT 版 4200 支持  存储容量 3000 合法卡、10 万刷卡记录、15 万条考勤记录  指纹容量 3000 枚，每个用户最多支持 10 枚指纹  指纹比对方式 1:1 和 1：N，N=3000 枚  读卡响应时间 < 1s  指纹验证时间 < 1s  误认率（FAR） <= 0.001 %  拒认率（FRR） <= 0.6 %  指纹采集器 光学式指纹识别模块  外接读卡器 可外接标准 wiegand26/34、hik 私有 wiegand 读卡器  读卡类型 DS-K1T804BF：不支持刷卡  DS-K1T804BMF：Mifare 卡序号，包括各种异形卡，支持金属环境使用，不支持扇区加密。  DS-K1T804BEF：EM 卡，包括异形卡，支持金属环境使用操作系统 Linux  QT 版 4200 支持  存储容量 3000 合法卡、10 万刷卡记录、15 万条考勤记录  指纹容量 3000 枚，每个用户最多支持 10 枚指纹  指纹比对方式 1:1 和 1：N，N=3000 枚  读卡响应时间 < 1s  指纹验证时间 < 1s  误认率（FAR） <= 0.001 %  拒认率（FRR） <= 0.6 %  指纹采集器 光学式指纹识别模块  外接读卡器 可外接标准 wiegand26/34、hik 私有 wiegand 读卡器  读卡类型 DS-K1T804BF：不支持刷卡  DS-K1T804BMF：Mifare 卡序号，包括各种异形卡，支持金属环境使用，不支持扇区加密。  DS-K1T804BEF：EM 卡，包括异形卡，支持金属环境使用 | 海康威视 | 2套 | 4000 |
| 9 | 磁力锁 | | 型号：海康威视DS-H4H230BSC  规格：电压  电流  DC12/24V  安全类型  通电关门，断电开门  500mA  承受拉力  190KG~280KG直线拉力  材质  铝合金外壳  表面温度  低于环境温度20°C以内  适用温度  -10°C ~ +50°C (14-131F)  适用湿度  0-95%（相对湿度）  外壳处理  阳极硬化电镀处理  锁体处理  环保锌电镀处理  吸板处理  环保新电镀处理  防护性能  内置反向突破保护功能  适用门型  木门/铁门/有框玻璃门等（无框玻璃门可配支架）  功能  可与楼宇对讲，门禁系统等配套 | 海康威视 | 2套 | 1000 |
| 10 | 出门按钮 | | 型号：海康威视EB289EB289  型号：门禁专用开关按钮 | 海康威视 | 2套 | 100 |
| 11 | 电源 | | 型号：海康威视DS-K78-12V/5A  规格：DS-K78-12V/5A门禁专用电源 | 海康威视 | 2套 | 900 |
| 12 | 机房整修 | | 定制服务，机房整修服务内容包括：针对学院24号楼107室的网络核心机房、105室的数据中心机房窗户进行封堵，封堵面积为18平米；进行防雨防漏及保温处理；采用防火材料。 | 首自信 | 1套 | 5400 |
| 13 | 系统集成服务 | | 定制服务，集成服务内容包括：  1.实施方案:项目实施前，提供详细的项目实施方案，包括实施目标、实施范围、网络架构设计、系统部署方案、测试方案、实施团队及实施人员安排、实施计划、项目管理、项目验收等，严格按照实施方案进行项目实施。  2.网络架构优化:依据等级保护三级要求，对学院网络进行分区分域设计，并完成网络架构的调整及优化。  3.网关及IP规划:根据学院实际业务需求，进行网关、路由及IP规划设计。  4.设备安装部署:根据等级保护三级要求，结合学院网络实际情况，完成本次项目新采购设备的安装部署，完成学院老旧设备的部署调整。  5.设备策略优化:根据等级保护三级要求，结合学院业务需求，对设备策略进行配置及优化，确保策略最优。  6.标签标识:设计设备标签标识规范，对设备及线缆进行标签标识。  7.配件:提供设备安装部署所需要的配件，包括但不限于光纤跳线、网络跳线、扎带、标签纸等。 | 首自信 | 1套 | 86000 |
| 14 | 等保测评服务 | | 定制服务，等保测评服务内容包括：  1.定级备案:对学院业务系统及资产、安全管理制度等进行调研梳理，确定定级对象，分析业务信息安全等级和系统服务安全等级，编制系统定级所需要的所有材料，并组织专家进行系统定级评审，协助学院提交材料到公安网安部门进行备案，获取系统备案证明文件。  2.差距分析:依据等级保护三级要求，通过等保差距分析系统等工具，对学院拟定级系统即“一站式服务大厅”信息系统（三级）进行差距分析，分析系统安全技术层面、安全管理层面存在的问题，出具《等级保护差距分析报告》。  3.安全整改建议及加固:分析《等级保护差距分析报告》中安全问题，结合学院业务系统的实际特点，编制安全整改建议方案，并经学院确认后，完成安全问题或系统漏洞的安全修复；并按照等级保护三级要求，完成安全管理制度的编制及完善，确保满足等级保护三级要求的安全管理要求。  4.等级测评:编制测评方案，通过“安全测评系统”对“一站式服务大厅”信息系统（三级）开展安全技术测评、安全管理测评，出具《系统等级保护测评报告》。 | 首自信 | 1套 | 90000 |
| 15 | 安全运维服务--漏洞扫描服务 | | 定制服务，漏洞扫描服务内容包括：在学院非业务高峰期，采用漏洞扫描系统定期对学院网络设备、操作系统、数据库、应用服务器、WEB中间件、应用系统等进行漏洞扫描，并基于漏洞情报平台提供自动化漏洞情报碰撞分析，确保能够从成千上万的漏洞扫描结果中快速精准的分析出可被利用的漏洞和漏洞利用细节分析，精确提炼安全漏洞，并给出解决办法，以便及时进行安全加固，降低漏洞暴露面和暴露时间，从而降低学院安全风险，交付《漏洞扫描报告》；服务期限一年，每季度1次，每年4次。 | 首自信 | 1套 | 16000 |
| 16 | 安全运维服务--配置核查服务 | | 定制服务，配置核查服务内容包括：采用工具或人工方式，对核心网络设备、操作系统、数据库、应用服务器、WEB中间件等系统进行安全配置检查，编制安全配置检查报告，提出改进建议。交付《安全配置检查报告》。服务期限一年，每季度1次，每年4次。 | 首自信 | 1套 | 16000 |
| 17 | 安全运维服务--渗透测试服务 | | 定制服务，渗透测试服务内容包括：针对学院核心业务系统，提供经过学院授权的渗透测试服务，通过模拟黑客攻击针对测试目标进行SQL注入、XSS、远程代码执行、上传漏洞、溢出漏洞、弱口令等漏洞的发现及利用，并输出渗透测试报告含安全加固建议，同时指导开发商进行安全加固，并对加固后的系统进行复测验证。交付《渗透测试报告》（含复测）。服务期限一年，每半年1次，每年2次。 | 首自信 | 1套 | 18000 |
| 18 | 安全运维服务--安全加固服务 | | 定制服务，安全加固服务内容包括：安全加固服务，对漏洞扫描、配置核查、渗透测试等过程中发现的安全问题提出安全加固建议或方案，并协助学院完成安全整改工作，交付《安全加固建议方案》，服务期限一年，每季度1次，每年4次。 | 首自信 | 1套 | 16000 |
| 19 | 安全运维服务--等保技术支持服务 | | 定制服务，等保技术支持服务内容包括：等保技术支持服务， 当学院开展等级保护测评时，安排安全工程师对学院的等保三级系统的安全计算环境等进行检测分析，提前找出问题，并协助整改，确保能够快速通过等保测评，服务期限1年，按需，次数不限。 | 首自信 | 1套 | 16000 |
| 20 | 安全运维服务--安全态势分析服务 | | 定制服务，安全态势分析服务内容包括：安全态势分析服务，对学院现有态势感知平台的攻击日志、安全设备日志及告警进行分析，提出安全解决方案，并根据安全解决方案对安全问题进行加固修复，交付《安全趋势分析报告》。服务期限1年，每2个月一次，每年6次。 | 首自信 | 1套 | 16000 |
| 21 | 安全运维服务--应急响应服务 | | 定制服务，应急响应服务内容包括：当学院网络中发生如网络中断、网络拥塞、黑客攻击及数据篡改等安全事件、网安大队信息安全检查时，提供上门应急响应服务，并进行事件溯源，找到真正的问题原因，同时协助学院解决问题，交付《应急响应报告》。服务期限1年，按需，次数不限。 | 首自信 | 1套 | 30000 |
| 1768000 | |