合同编号：_____

西安工程大学传统纺织产业智能化生产设备研发平台建设子项目智能化技术应用研究系统大数据网络空间安全应用模块供货合同

需方：西安工程大学

供方：西安网安网络信息技术有限公司

需方（以下简称“甲方”）：西安工程大学

供方（以下简称“乙方”）：西安网安网络信息技术有限公司

签约日期/地点：2025年___月___日　西安工程大学（临潼校区）

依据《中华人民共和国民法典》等法律法规，以及采购项目传统纺织产业智能化生产设备研发平台建设子项目智能化技术应用研究系统大数据网络空间安全应用模块及航天航空柔性材料研发设备购置与配套设施建设子项目基础测试系统平台电工电路更新模块采购项目（项目编号：ZMZB2024GCDX-425）的《招标文件》《投标文件》《成交通知书》规定，经双方协商同意，签订本合同并信守下列条款，共同严格履行。

一、产品名称、数量、价格

序号	产品名称	规格型号	品牌商标	生产厂商	单位	数量	单价（万元）	总金额（万元）	备注
1	网络空间安全实训综合应用平台（核心产品） **（教学实验攻防平台管理系统）**	ASO-CR-SLAB-PLUS	安甲	西安网安网络信息技术有限公司	套	1	57.918	57.918	
2	防火墙 **（防火墙）**	ASO-TG FW-160	安甲	西安网安网络信息技术有限公司	套	5	0.956	4.780	
3	安全防御设备 **（数据库审计与风险控制系统）**	ASO-DB 200	安甲	西安网安网络信息技术有限公司	套	1	3.244	3.244	
4	入侵检测系统 **（网络攻击感知预警平台）**	ASO-AP T-300	安甲	西安网安网络信息技术有限公司	套	1	4.151	4.151	
5	WEB 应用安全网关 **（Web 应用防护系统）**	ASO-WA F-180A G	安甲	西安网安网络信息技术有限公司	套	1	2.595	2.595	
6	其他要求	/	安甲	西安网安网络信息技术有限公司	项	1	0.00	0.00	

合计金额（大写）：人民币柒拾贰万陆仟捌佰捌拾元整（含税）	合计金额（小写）：￥72.688 万元（含税）

二、质量标准

1.乙方提供的物资（设备）必须符合中华人民共和国国家安全环保标准、国家有关产品质量认证标准。没有国家标准的，采用该产品有关行业标准（以较高标准为准）。

2.甲方对乙方所供物资（设备）有具体技术指标及系统功能要求的，该技术指标及系统功能经甲乙双方书面确认，作为质量验收标准。

3.以招投标方式采购的物资（设备），招标文件对质量有特殊要求的以双方签字确认的技术协议及招投标文件为准。

三、交货日期、方式及地点

合同签订之日起 30 日内完成交付、安装及调试，交货地点为：西安工程大学临潼校区计算机科学学院 7-519、521 房间。

四、质保及售后承诺

1.物资（设备）自甲方出具书面验收合格文件之日起质保期 3 年，（国家或行业规定有强制质保期的电子产品可按照国家或行业标准执行，比 3 年低的以 3 年为准，比 3 年高的以国家或行业标准为准）。

2.质保期内乙方免费上门维修，费用全免；质保期后，乙方仍上门维修，免人工费，可收取相关零配件和材料费。如质保期内发生质量瑕疵，乙方未能按照甲方要求及时提供维修、更换服务，甲方有权要求乙方支付合同金额 10%的违约金。

3.质保期内乙方对甲方提出的服务响应不得超出 4 小时，并在 24 小时内完成解决方案制定，1 个工作日内派人到现场维修。乙方需提供 7*24 的服务，及时响应售后服务需要及各种技术咨询，并根据本专业人才培养需要，派出经验丰富的技术人员为本专业学生提供实习实训和学科竞赛指导，同时为实验室管理员及本专业教师提供设备维护及使用的技术培训 10 次，期间因此产生的全部费用均由乙方自行承担。

4.乙方对物资（设备）出现的有关技术性问题或安全问题负责处理、解决，承担因质量引起的事故损失。

5.乙方免费培训甲方用户不限人熟练掌握所供物资（设备）为止，并就在物资（设备）使用过程中遇到的技术性等问题进行免费解答。

五、包装及运输

乙方负责运输、装卸、搬运上下楼等一切费用并承担运保费，保证所供产品为原厂包装，开箱合格率达到100%，使用说明书、质量检验证明书、随配附件和工具以及清单与物资（设备）一起发送。

六、安装、调试及验收

1.乙方负责安装调试，甲方提供必要的工作条件。

2.甲方对乙方所供物资（设备）依照合同进行现场验收。验收时甲乙双方均派人到场，由甲方先对物资（设备）外观质量进行验收（包括对包装、产品名称、规格型号、品牌商标、生产厂商、单位、数量等的验收）。乙方安装、调试完成之后，通知甲方对物资（设备）相关技术指标、系统功能进行验收，甲方应在乙方通知后3日内进行终验，终验合格后甲方向乙方出具终验合格验收报告，作为验收依据。验收不合格的，限期整改；整改仍达不到要求的，作退货处理。

3.甲方在质保期内使用过程中如因物资（设备）内在质量出现问题，甲方将乙方所交物资（设备）交至甲方属地技术质量监督部门按双方确认的技术标准进行检测；如果检测与双方确认的质量标准不符，由乙方承担检测费用及负违约责任，违约责任按本合同第八条第4款处理。

4.如果所供物资（设备）以投标时双方封存样品为准的，可做破坏性检验，以确定乙方货物是否合格。

七、付款方式及期限

1.合同签订后，乙方向甲方提供预付款等额的银行/保险公司等金融机构出具的与预付款等额的预付款保函或其他担保措施，甲方向乙方支付合同总价的40%作为预付款；待所有物资（设备）到达甲方指定地点，安装、调试完毕并验收合格后，30天内支付合同总价的60%。甲方向乙方付款前，乙方应向甲方开具符合甲方要求的发票，若因乙方未开具或逾期开具合法有效的发票，甲方有权顺延付款期限且不承担逾期付款责任。

2.支付方式：银行转帐。

乙方指定收款账户：

公司名称：西安网安网络信息技术有限公司

统一社会信用代码：91610131MA6U0OMJ0R

开户银行：招商银行西安锦业路支行

账号：129907761410902

地址：陕西省西安市高新区鱼化街办天谷七路996号西安国家数字出版基地A座12002室

乙方对上述账户的真实性、有效性、准确性负责，若变更账户需提前5日书面告知甲方，因乙方原因导致未受到款项，甲方不承担任何责任。

八、违约责任

1.合同生效后，甲乙双方应按合同规定认真履约。合同履约责任只涉及合同甲乙双方，不考虑第三方因素。违反本合同任何一条约定均视为违约。

2.乙方逾期交货，每天应按合同总价的1‰向甲方支付违约金。如乙方逾期含三十天仍未履行或未完全履行交货义务的，甲方有权终止合同，乙方须按合同总价的30%计算向甲方支付违约赔偿金。违约金不足以弥补乙方给甲方造成损失的，乙方应当承担全部赔偿责任，全部赔偿责任的范围包括但不限于预期可得利益、直接损失、赔偿金、违约金、诉讼费用、仲裁费、鉴定费、保全费、保全担保费用、律师费等。

3.甲方无正当理由拒收物资（设备），应向乙方支付合同总价款30%的违约金。

4.乙方所交的物资（设备）品种、规格型号、品牌、生产厂商、数量和质量不符合合同约定，所供物资（设备）达不到双方确认的技术标准的，乙方必须无条件退回全部货款，并向甲方支付合同总价款30%的赔偿金。

5.因乙方提供的产品存在缺陷或由于乙方的过错使产品存在缺陷造成人身、缺陷产品以外的其他财产损害，乙方应当承担全部赔偿责任。若由此造成甲方先行承担责任的，甲方在承担责任后有权全额向乙方追偿。

6.在合同余款付清后、质保期内，乙方未履行质量保证条款约定的义务，乙方对甲方承担本合同总价10%的违约金。

7.乙方应保证所提供产品均不会侵犯任何第三方的知识产权及其他任何权

利，同时就合作期间接触到的甲方知识产权、保密信息等不得向任何第三方透露，否则乙方应承担由此引发的一切法律责任。

8.乙方未按照本合同约定履行义务的，均视为乙方违约，甲方可按照本条第2款追究乙方违约责任。

九、争议解决方式

本合同在履行过程中，如发生争议，双方友好协商解决，如协商不成，双方同意在甲方注册地法院起诉解决。

十、其他

1.本合同一式六份，甲方执四份，乙方执两份，双方签字并盖章后生效，具有同等法律效力。合同未尽事宜双方可协商解决或另立补充协议。

2.在合同实施过程如双方出现争议，物资（设备）清单、技术参数、系统功能要求、甲方招标文件、乙方投标文件等均为解决争议的文件，与本合同具有同等法律效力。

3.本合同项下任何一方向对方发出的通知、信件、数据电文等，应当发送至本合同下列约定的地址、联系人和通信终端。

甲方联系人：王伟

联系电话：13609268818

联系地址：陕西省西安市碑林区金花南路19号　　邮编：710048

电子邮箱：174456430@qq.com

乙方联系人：陈清

联系电话：029-81111728

联系地址：西安市高新区丈八五路10号陕西省科技资源统筹中心A410室　邮编：710000

电子邮箱：chenqing@ansecone.com

送达时间以下列规定为准：

(1)专人递送之日视为送达之日；

(2)以邮寄方式进行的通知均应采用邮政挂号快件或特快专递的方式进行，自信件交邮后的第2日视为送达；

(3)短信、传真、微信、电子邮件以顺利发出当天后的第一个工作日视为送

达之日；

(4)一方当事人变更名称、地址、联系人或通信终端的，应当在变更后 3 日内及时书面通知对方当事人，对方当事人实际收到变更通知前的送达仍为有效送达，电子送达与书面送达具有同等法律效力。

4.合同签订地点：西安·西安工程大学（临潼校区）

5.合同签订时间：2025 年 1 月 21 日

6.附件：产品技术参数表

需方（甲方）：西安工程大学

法定代表人：

授权代表：

电话：

传真：

开户银行：中国建设银行股份有限公司西安友谊东路支行

账号：61050190540000001286

税务登记证号：12610000435204205L

地址：陕西省西安市碑林区金花南路 19 号

供方（乙方）：西安网安网络信息技术有限公司

法定代表人：孙佐强

授权代表：

电话：029-81111728

传真：029-81111728

开户银行：招商银行西安锦业路支行

账号：129907761410902

税务登记证号：91610131MA6U0OMJ0R

地址：陕西省西安市高新区鱼化街办天谷七路 996 号西安国家数字出版基地 A 座 12002 室

附件：（一）产品技术参数表

序号	名称	品牌	型号及规格
1	网络空间安全实训综合应用平台（核心产品）**（教学实验攻防平台管理系统）**	安甲	型号：ASO-CR-SLAB-PLUS 软硬一体化标准机架式设备，1+1 冗余电源，CPU 配置：2 颗 24 核 48 线程，内存配置：32G*32；硬盘容量：8T*2，固态盘：6 个 2T 混合型 SSD；Raid 卡配置：4GB SAS 12Gb 8 口，4 个千兆网口个。含 70 人的在线并发授权，提供一台 vxlan 交换机，节点包转发率 426Mpps，交换容量 7.58Tbps，接口配置 24 个千兆电口，4 个 SFP+万兆光口。
2	防火墙**（防火墙）**	安甲	型号：ASO-TGFW-160 标准机架软硬一体设备，网络接口 8 个千兆电口（含不少于 1 组电口 Bypass），4 个千兆光口，2 个 USB 接口，吞吐量 6Gbps，IPS 吞吐量 1Gbps，AV 吞吐量 1Gbps，最大并发连接数 300 万，每秒新建连接数 5 万，实配 IPS、AV、URL、威胁情报等业务功能模块。
3	安全防御设备**（数据库审计与风险控制系统）**	安甲	型号：ASO-DB200 标准机架软硬一体设备，内存 8GB，硬盘 2TB，整机吞吐量 3Gbps，SQL 处理能力 40000 条/秒，支持数据库实例数不受限制，日志存储数 10 亿条，配置 6 个千兆电口。
4	入侵检测系统**（网络攻击感知预警平台）**	安甲	型号：ASO-APT-300 标准机架软硬一体设备，配置 6 个千兆电口，1 个扩展插槽，整机吞吐率 4Gbps，HTTP 并发数 10 万/秒。
5	WEB 应用安全网关**（Web 应用防护系统）**	安甲	型号：ASO-WAF-180AG 标准机架软硬一体设备，网络接口 5 个千兆电口（提供两对 BYPASS），吞吐量 4Gbps，HTTP 并发连接数 800000 个，每秒事务处理数 30000 个。
6	其他要求	安甲	1.提供配套人才培养迭代服务：项目建设验收后的三年时间内，每年委派一位行业专家参与网络信息安全技术应用专业人才培养方案论证，协助开展制定特色化人才培养方案以及教材课程体系改革工作，提供柔性人才引进方式，聘请安全专家以“企业导师”或“客座讲授”的方式参与专业授课、专业报告、毕业设

			计课题的技术指导等。 2. 提供配套实习与就业服务：提供实习岗位服务，通过实习进一步熟悉企业环境，将学校所学与企业所需进行深入融合，为学生就业打基础；每年为学校学生提供顶岗实习等机会，并提供实习实训导师，指导学生完成实习实训工作；提供就业服务，包括就业咨询、就业推荐、模拟面试及辅导等方面的就业服务，承诺对成绩优异的在校学生，可以根据学生自己意愿进入安全企业人才库，优先提供就业机会，根据学校、学生的意愿选择各个分支机构或总部实习、就业；提供就业双选服务，每年针对人才双选会，提供多条就业通道，为院校专业学生提供实践与就业服务。 3. 承诺协助学院共同开展科学技术研究，优先支持学院研究人员和团队参与的科技技术研究；在科研合作的基础上，双方积极联合申报重点实验室，并作为校企共建的产学研平台，以更高的目标共同申报网络安全方向重大科技项目、承接国家重大科研任务，协助学院融入国家级网络安全教育技术产业融合试验区建设。

项目技术负责人签字：

日　期：

乙方公司名称（盖章）西安网安网络信息技术有限公司

授权代表签字：

日　期：

附件：（二）产品详细参数表

序号	名称	品牌	详细参数
1	网络空间安全实训综合应用平台（核心产品）**（教学实验攻防平台管理系统）**	安甲	型号：ASO-CR-SLAB-PLUS 1.★平台具有完善的动态考核机制对学员学习效果、知识与技能掌握实际情况进行全方位考核；具备节点仿真系统、实体设备管理系统、虚实结合仿真系统、场景编排系统、资源监控系统、综合管理系统、资源管理系统、教学管理系统、培训管理系统、考试管理系统、安全研究系统、教学统计分析系统等，提供70人的在线并发授权。 2.提供软硬一体化标准机架式设备，1+1冗余电源，CPU配置：2颗24核48线程，内存配置：32G*32；硬盘容量：8T*2，固态盘：6个2T混合型SSD；Raid卡配置：4GB SAS 12Gb 8口，4个千兆网口个。 3.节点仿真系统资源类型包含虚拟终端、虚拟网络设备、虚拟安全设备等；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（提供相关功能截图并加盖原厂公章）。 4.实体设备管理系统，可以与本项目防火墙、WEB应用安全网关、入侵检测系统、安全防御等实体设备接入平台，支持实体设备的注册与删除。 5.虚实结合仿真系统，可以对接入平台的实体设备（防火墙、WEB应用安全网关、入侵检测系统、安全防御设备等）能够通过拖拽的形式与虚拟设备实现实体与虚拟仿真节点网络互联的能力，并能够实现虚实节点间协议数据的透明交互，供应商提供虚实结合节点，提供一台vxlan交换机，节点包转发率426Mpps，交换容量7.58Tbps，接口配置24个千兆电口，4个SFP+万兆光口。 6.投标产品可以展示实体设备（防火墙、WEB应用安全网关、入侵检测系统、安全防御设备等）被引用场景拓扑，实体设备接入场景采用独占的形式，即限制单台实体设备同一时刻只能被同一套场景所引用。 7.场景编排系统平台可以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（提供相关功能截图并加盖原厂公章）。

			8.资源管理系统场景创建时可以以图形化拖拽的方式绘制场景拓扑，虚拟网络设备至少包含虚拟交换机、虚拟路由器，虚拟安全设备至少包含数据库审计、日志审计、高级威胁监测、主机安全、Web 应用防火墙、堡垒机等，同时支持对拓扑中元素的属性进行配置（供应商提供相关功能截图并对平台进行相关功能演示）。 9.教学课程提供随堂笔记和作业功能，学员可以提交和查看自己的学习笔记和作业，教员可以查看课程中所有学员的课堂笔记。支持学员统一查看参与的课程、路径以及相关学习进度。 10.培训管理系统提供培训管理功能，提供教员以班级的维度进行学习计划的制定和下发，并可以对学习成果进行管理。 11.培训管理系统可以通过关联内置课程，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，包括学习进度、作业提交情况及分数、考试情况及分数；同时支持教员对学员作业和考试进行批改和打分（供应商提供相关功能截图并对平台进行相关功能演示）。 12.考试管理系统可以管理题库，提供自定义创建题库，试题题目类型包含判断题、单选题、多选题、填空题、简答题，理论题库数量 3000 道（提供相关功能截图并加盖原厂公章）。 13.考试管理系统支持防作弊模式（供应商提供相关功能截图并对平台进行相关功能演示）。 14.考试管理系统提供考试统计功能，可以对考试总人数、完成人数、缺席人数、作弊人数等数据进行统计，并支持以图表的形式展示成绩分布情况以及试题正确率排行榜（提供相关功能截图并加盖原厂公章）。 15.安全研究系统提供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（供应商提供相关功能截图并对平台进行相关功能演示）。 16.安全研究系统支持用户针对自定义安全场景开展安全研究工作，提交研究成果；研究成果支持上传附件或关联平台漏洞作为相应成果，附件类型支持 word、pdf、mp4 等格式，可设置针对指定用户开放（供应商提供相关功能截图并对平台进行相关功能演示）。 17.安全研究系统可以对安全研究的参与总人数、成果提交人数、成果总数以及成果浏览量统计，并支持对安全研究成果进行管理。 ▲18.威胁捕捉与诱骗系统，具备威胁感知能力，支持根据相同攻击来源、受攻击蜜罐将告警进行智能聚合，支持但不限于 Webshell 伪装蜜罐、无线 AP、交换机、路由器、网关设备等 IT 设备伪装蜜罐；支持但不限于 LDAP、性能监控、流量监控、虚拟机平台等运维系统蜜罐；支持但不限于 phpMyadmin、Jenkins、Gitlab

			等研究环境蜜罐；支持将攻击流量加密牵引到云端蜜网、支持拉取云端蜜罐攻击时间、攻击来源、账号密码、执行命令、下载文件等信息并展示；支持拉取云端 SSH、Telnet 具体命令、生成文件、支持可视化展示攻击者和云端蜜网节点联系；支持老师和学员自定义多个 TCP 端口监听蜜罐，支持抓取指定 Web，自动克隆页面；支持老师和学员上传自定义蜜罐，支持根据当前蜜罐部署环境，自动生成蜜饵；支持为不同主机生成不同蜜饵，支持精准蜜饵互联网投放人工服务，包括但不限于网盘类、搜索引擎类、资料类、研发常用类。（提供相关功能截图并加盖原厂公章） 19.教学统计分析系统提供从教学、安全研究、考试等多个维度对所有人员、单个部门以及个人的学习情况进行分析。 20.教学统计分析系统统计数据应包含课程参与人次、课程完成人次、路径参与人次、路径完成人次、培训参与人次、培训完成人次、自学学习时长、自学学习课时、培训学习时长和培训学习课时。 21.供应商提供本科课程资源包，课程可支撑院校网络空间安全、网络安全等专业中的相关课程教学使用。从网络安全基础、应用安全、系统安全、软件安全、数据安全、二进制安全以及产业实践等多个维度涵盖网络空间安全专业培养方案中的技术核心课程建设要求。 22.供应商提供精品课程服务，网络安全教学课程 40 门，课时数 1400 课时，课程体系覆盖信息安全基础、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。 23.供应商提供教学信息资源服务，提供镜像数量 500 多个，工具数量 1000 多款，漏洞数量 80000 多个，带复现环境 CVE 漏洞 200 多个，理论题库数量 3000 多道。 24.网络空间安全实训综合应用平台提供计算机软件著作权登记证书。
2	防火墙 **（防火墙）**	安甲	型号：ASO-TGFW-160 1.标准机架软硬一体设备，网络接口 8 个千兆电口（含不少于 1 组电口 Bypass），4 个千兆光口，2 个 USB 接口，吞吐量 6Gbps，IPS 吞吐量 1Gbps，AV 吞吐量 1Gbps，最大并发连接数 300 万，每秒新建连接数 5 万，实配 IPS、AV、URL、威胁情报等业务功能模块，确保实训实验系统统一功能性，投标产品与网络空间安全实训综合应用平台同品牌。

			2.提供 IPv6/IPv4 双栈功能，支持 IPv6 安全策略，包括访问控制策略、NAT 策略、流量控制策略、黑名单、白名单、认证策略等，支持 IPv6 静态路由、IPv6 隧道，包括 4over6、6over4 等隧道模式，支持 IPv6 入侵防御、病毒防护、Web 防护、弱密码防护等安全功能。 3.提供一体化安全策略，可基于安全域、MAC 地址、IP 地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL 过滤、文件过滤、Web 防护、SSL 解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果（提供相关功能截图并加盖原厂公章） 4.提供 Telnet、FTP、IMAP、POP3、SMTP、HTTP 协议的弱密码防护，支持预定义弱密码规则和自定义弱密码防护、支持 SMTP、IMAP、POP3、FTP、Telnet、HTTP、MYSQL、SMB、MSSQL、RLOGIN、POSTGRESQL、ORACLE 协议的暴力破解侦查和访问控制，并支持用户根据实际场景修改频率阈值、支持指定接口和网段地址进行 SYN、UDP、ICMP 等协议的泛洪攻击的侦查和防护。 5.投标产品内置应用识别库，主流应用 6000 多种，支持识别多种主流应用，支持应用自定义并对自定义的应用进行分组，支持根据标签选择应用，支持自定义应用的导入和导出；支持多种升级方式升级应用特征库，支持显示升级历史和升级结果。 6.提供 SSL 加密流量解密功能，支持 HTTPS、SMTPS、POPS、IMAPS 协议加密的流量解密，支持 HTTPS 流量按域名分类做流量解密。并支持上层内容安全功能查杀和访问控制，如入侵防御，内容过滤等（提供相关功能截图并加盖原厂公章） 7.管理员认证登录支持双因子认证。以上参数提供相关报告证明并加盖原厂公章。 8.提供 HTTP、FTP、POP3、SMTP、IMAP 协议的多种预定义文件类型过滤，支持上传下载的方向选择；并支持自定义文件类型过滤（提供相关功能截图并加盖原厂公章） 9.投标产品可以与入侵检测系统协同工作，实现将安全防御分析到的 Web 攻击、Web 后门访问、SMB 远程溢出攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为等外部攻击源 IP 同步到本设备，通过本设备的黑名单实现自动阻断（提供相关功能截图并加盖原厂公章）。
3	安全防御设备 **（数据库审计与风险控制系统）**	安甲	型号：ASO-DB200 1.标准机架软硬一体设备，内存 8GB，硬盘 2TB，整机吞吐量 3Gbps，SQL 处理能力 40000 条/秒，支持数据库实例数不受限制，日志存储数 10 亿条，配置 6 个千兆电口，投标产品与网络空间安全实训综合应用平台同品牌。

			2.提供安全防御规则800多条，如SQL注入、缓冲区溢出等。 3.提供安全防御规则，包括不仅限于缓冲区溢出、SQL注入、提权、数据库内核入侵探测等常见攻击特征，内置多种数据库安全规则。 4.提供一键添加过滤规则功能，可以在告警规则中一键添加信任规则或规则白名单（提供相关功能截图并加盖原厂公章）。 5.提供告警分析功能，告警分析支持按照“客户端IP+数据库账号”的组合对SQL模板维度进行排行。 6.可以在日志页面一键取证（提供相关功能截图并加盖原厂公章）。 7.▲提供客户端访问Web服务器的URL和应用服务器访问数据库的SQL语句关联功能（提供相关功能截图并加盖原厂公章）。 8.支持敏感数据脱敏处理，内置常见敏感数据脱敏规则，并支持脱敏规则自定义（提供相关功能截图并加盖原厂公章）。 9.防御规则动作支持允许访问、命令阻断、会话阻断和动态脱敏等。
4	入侵检测系统 **（网络攻击感知预警平台）**	安甲	型号：ASO-APT-300 1.标准机架软硬一体设备，配置6个千兆电口，1个扩展插槽，整机吞吐率4Gbps，HTTP并发数10万/秒，投标产品与网络空间安全实训综合应用平台同品牌。 2.提供通过攻击者视角、受害者视角、安全事件等场景化分析对告警日志进行基于同一攻击源、同一目标、时间步长等算法自动聚合分析，降低警报数量，（提供相关功能截图并加盖原厂公章）。 3.提供手动上传文件样本进行威胁分析功能，（提供相关功能截图并加盖原厂公章）。 4.提供攻击链路可视化功能，支持溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式展示出来（提供相关功能截图并加盖原厂公章）。 5.可以将分析到的SMB远程溢出攻击、扫描行为、Web后门访问、隧道通信、暴力破解、挖矿、远控工具利用等攻击成功事件同步到防火墙和WEB应用安全网关，实现APT深度威胁分析与防火墙、WEB应用安全网关联动阻断（提供相关功能截图并加盖原厂公章）。 6.可以将分析到的WEBSHELL攻击、木马回连和恶意攻击行为同步到WEB应用安全网关，实现安全防御深度威胁分析与WEB应用安全网关联动阻断（提供相关功能截图并加盖原厂公章）。 7.提供基于入侵规则检测基础上通过加载插件、深度检测通用规则等进行二次深度检测，可支持shiro反

			序列化、蚁剑、哥斯拉、冰蝎 3.0、冰蝎 4.0 等检测能力，且能识别如 shootback、TunnaProxy、dnscat2、reGeorg、reDuh、CobaltStrike 等隧道通信工具（提供相关功能截图并加盖原厂公章）。 8.投标产品内置静态沙箱和动态沙箱，支持压缩文件密码自动猜测功能，支持通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到 APT 攻击中的恶意攻击，支持动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险并展示（提供相关功能截图并加盖原厂公章）。 9.提供资产风险及健康度评估功能，支持对资产活跃程度分类，支持对资产分组，可配置资产 IP 所属的组织和网段，以展示资产层级关系。可自定义配置资产分组属性，（提供相关功能截图并加盖原厂公章）。 10.提供大屏展示网络攻击态势功能，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP 流量、DNS 流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，（提供相关功能截图并加盖原厂公章）。 11.投标产品内置 YARA 规则，并可导入自定义 YARA 规则，可从静态文件和运行内存中检测文件威胁，支持从规则状态、类型、等级、描述等方面进行自定义配置。 12.提供沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现。 13.提供多并发沙箱检测技术，集成主流的操作系统 winXP、win7、win10、linux 等多种检测环境，结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析（提供相关功能截图并加盖原厂公章）。 14.提供场景化分析、攻击者视角分析、受害者视角分析、脆弱性分析、挖矿场景分析、勒索场景分析、主机威胁分析、失陷主机分析、情报事件分析、域名行为分析、钓鱼邮件分析、加密流量检测、文件威胁分析、敏感信息分析、流量统计、抓包分析、PCAP 文件分析、情报在线分析等（提供相关功能截图并加盖原厂公章）。 15.▲投标产品提供网络安全产品安全检测证书。
5	WEB 应用安全网关 **（Web 应用防护系统）**	安甲	型号：ASO-WAF-180AG 标准机架软硬一体设备，网络接口 5 个千兆电口（提供两对 BYPASS），吞吐量 4Gbps，HTTP 并发连接数 800000 个，每秒事务处理数 30000 个。 1.标准机架软硬一体设备，网络接口 **5 个千兆电口（提供两对 BYPASS）**，吞吐量 4Gbps，HTTP 并发连接数 800000 个，每秒事务处理数 30000 个，投标产品与网络空间安全实训综合应用平台同品牌。

			2.投标产品内置 SSL 硬件加速卡，实现对 HTTPS 的加解密，提供设备对 HTTPS 的处理性能（提供相关功能截图并加盖原厂公章）。 3.提供自动发现网络环境中存在的 Web 业务系统功能，记录服务器的 IP、Port、域名等信息（提供相关功能截图并加盖原厂公章）。 4.提供 HTTPS 站点 SSL 算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果（提供相关功能截图并加盖原厂公章） 5.提供 HTTPS 国密算法功能，支持对 HTTPS 国密业务进行防护。 6.提供对跨站脚本(XSS)和注入式攻击（包括 SQL 注入、命令注入 、代码注入、文件注入、LDAP 注入、SSI 注入等）的检测防护。 7.投标产品内置安全规则可有效识别 Acunetix、nessus 、WebScan、Webdump、AppScan 等扫描器的扫描行为。 8.提供多种盗链识别算法功能，能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问。 9.提供设定学习的周期功能，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（提供相关功能截图并加盖原厂公章）。 10.提供威胁情报能力，可对僵尸主机 IP、垃圾信息 IP、代理 IP、扫描 IP、暴力破解 IP、漏洞利用 IP、恶意爬虫 IP 进行防护。 11.提供语义分析能力，可对 SQL 注入、XSS、代码注入等攻击行为进行防护（提供相关功能截图并加盖原厂公章）。 12.提供智能识别攻击者功能，对发起攻击的 IP 进行自动阻塞，禁止其进行访问（提供相关功能截图并加盖原厂公章）。
6	其他要求	安甲	1.提供配套人才培养迭代服务：项目建设验收后的三年时间内，每年委派一位行业专家参与网络信息安全技术应用专业人才培养方案论证，协助开展制定特色化人才培养方案以及教材课程体系改革工作，提供柔性人才引进方式，聘请安全专家以“企业导师”或“客座讲授”的方式参与专业授课、专业报告、毕业设计课题的技术指导等。 2.提供配套实习与就业服务：提供实习岗位服务，通过实习进一步熟悉企业环境，将学校所学与企业所需

			进行深入融合，为学生就业打基础；每年为学校学生提供顶岗实习等机会，并提供实习实训导师，指导学生完成实习实训工作；提供就业服务，包括就业咨询、就业推荐、模拟面试及辅导等方面的就业服务，承诺对成绩优异的在校学生，可以根据学生自己意愿进入安全企业人才库，优先提供就业机会，根据学校、学生的意愿选择各个分支机构或总部实习、就业；提供就业双选服务，每年针对人才双选会，提供多条就业通道，为院校专业学生提供实践与就业服务。 3. 承诺协助学院共同开展科学技术研究，优先支持学院研究人员和团队参与的科技技术研究；在科研合作的基础上，双方积极联合申报重点实验室，并作为校企共建的产学研平台，以更高的目标共同申报网络安全方向重大科技项目、承接国家重大科研任务，协助学院融入国家级网络安全教育技术产业融合试验区建设。

项目技术负责人签字：

日　期：

乙方公司名称（盖章）西安网安网络信息技术有限公司

授权代表签字：

日　期：