更正后内容：

服务范围	**服务范围以及服务标准：** **一、攻防演训靶场系统　1 套** 1.系统须支持提供物理机管理，为满足后期扩容使用要求，须支持手动添加多台物理机设备资源；支持多台物理机资源的集群管理，支持手动添加多台物理机设备资源同时支持集群的横向扩容； ●2.为避免在靶场使用的网络冲突，系统须支持网段管理，可以配置多 IP 地址段，用以自动分配创建的实例化资产； ●3.为满足用户真实模拟场景，系统须支持虚拟仿真能力，支持仿真资源类型包含但不限于虚拟终端、虚拟网络设备、虚拟安全设备等； ●4.为满足场景的丰富性，系统须支持将物理设备接入平台，物理设备类型包含但不限于计算终端、路由器、交换机、安全防护设备等类型，且支持物理设备的添加与删除； 5.为保障使用的健康监控，系统须支持物理机的监控，包括但不限于操作系统、运行时间、CPU、内存使用情况、网卡信息、实时流量、收发包统计、端口开放情况等数据的监控；能够对关键性指标（CPU、内存、硬盘）设置报警阈值；能够查看日志吞吐量的相关数据情况； 6.为保障教学人才的多层次管理，系统用户管理须支持部门管理功能，可以构建至少三级部门组织架构，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，系统内置包含但不限于管理员、教员和学员角色，支持自定义角色，可以为角色划分不同功能和接口权限； 7.为保障资源分配合理，系统须支持对实例进行管理， 包含但不限于虚拟机、Docker 容器等类型；可以对实例进行一键回收、关机、重启、回收、快照的创建、恢复、重置等独立操作与统一化管理。 8.为保障操作可追溯，系统须支持日志审计功能，支持记录和查看平台用户的操作日志信息，同时支持日志检索以及批量导出； 9.系统须自带能满足需求的资源库，资源库包含但不限于镜像库、工具库、漏洞库、知识库、场景库，且具有统一管理界面； 10.为保障漏洞挖掘学习的有效性，漏洞库须支持漏洞的管理与创建，创建时支持关联漏洞利用方法、修复方案、复现环境、测试工具等内容，支持通过漏洞状态、漏洞来源、漏洞等级、漏洞名称、漏洞编号等信息检索漏洞； 11.系统支持用户自定义编排课程，可以将课程设置为公开课程和私有课程，满足因材施教的要求。 12.为满足教学课内容的多样性，系统课程须支持设置多个知识点并关联相关课程，通过关联课程功能可以建立多个课程之

	间的关联管理；单个课程可以包含但不限于理论知识、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； 13.为保障学习过程中的交流与分享，系统须支持课程留言交流功能，教员、学员能够针对开放的课程进行留言，支持教员、学员查看并回复留言信息； 14.实验课程支持关联相关实验工具，工具类型支持虚拟机型和下载型，虚拟机型工具可直接在界面启动后直接使用； 15.实验环境支持开机、关机、重启、重置、生成快照、恢复快照、回收资源等操作，同时具有实验环境超时自动回收、延长实验时间能力； 16.系统提供培训管理功能，支持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； 17.系统支持管理题库；支持自定义创建试题；试题类型包含判断题、单选题、多选题、填空题、简答题； 18.系统支持学员考试统计功能，支持对考试总人数、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； ●19.为满足日常竞赛要求，系统须支持混合竞赛模式， 一场竞赛可以包含多个阶段，每个阶段可以添加不同赛制类型，同时支持依据人数、分值、排名等设置阶段的准入条件。赛制须支持夺旗赛、定向渗透赛、攻防对抗赛、理论赛四种类型；竞赛支持单兵作战模式和团队作战模式，并支持设置最大参赛人数或团队数； 20.为保障竞赛的公平性，竞赛须支持设置作弊处罚方式，包括但不限于不处罚、只警告、扣除所答题分数、自动禁赛四种， ●21.夺旗赛须支持动态 Flag 的方式，以实现防作弊功能，攻防对抗赛 Flag 是通过选手拥有的随机提交申请获取，确保每个 Flag 都只有当前团队可用，防止交换 Flag； 22.平台内置漏洞数量应 80000 个。 23.安全知识分类方向包含但不限于信息安全基础、应用安全、安全运维、安全编程、安全工具、数据安全、攻防竞赛，2000 多课时的理论与实验资源； 24.理论性试题数量 3600 道； ●25.系统须内置场景库，场景可查看当前场景下包含有的镜像资源列表。 **二、实网攻防演练系统　1 套** 1.为保障一场实网攻防演练的完整，系统内置角色必须包含但不限于平台管理员、运维管理员、攻击方、防守方、裁判员 5 个角色；

	2.为保障演练的公平性，系统须对登录的账号进行唯一性识别，在同一场演练里只能拥有一种角色身份； 3.系统用户之间支持用户清单根据攻击方、防御方、裁判员几个角色进行切换展示；支持根据用户姓名/团队名称/身份证号进行检索。 4.系统可以展示累计举办演练场次、累计有效攻击成果数、累计有效防御成果数； 5.系统可以查看当前进行中的演练，包含演练名称、演练时间、演练场地、演练倒计时和演练状态，支持展开查看更多演练，点击可进入当前演练详情；查看参演人数、攻击方人数、防守方人数和裁判员人数； 6.系统支持汇报模版的设置，支持可编辑的通用模版的下载，和自定义模版的创建通用模版包含内容：成果总结、安全加固措施、改善意见和建议； 7.系统支持演练启用和未启用的状态，未启用状态只有管理员可见，选手不可见，启用状态时选手可见； 8.系统支持查看成果统计，并能够导出攻击方团队和防守单位团队的成绩表； 9.支持显示攻击成果标题、提交人、攻击方团队、目标系统名称、目标系统 IP、URL、风险等级、审核状态、评分、提交时间、查看详情； 10.支持对成果进行风险等级划分，采用不同颜色标签表示多个等级，如：紧急、高危、中危、低危； 11.在成果出现偏差时，可对成果进行重新审核； 12.在成果较多情况下可支持对攻击方和防守方提交的成果进行系统自动评分和人工评分两种评分模式； 13.针对的展示成果支持大屏 3D 地图展示，大屏包含但不限于地图台、攻击成果大屏、防御成果大屏、远程可视大屏，且支持在页面上对大屏名称和大屏展示内容的自定义修改。 **三、配套服务 1 项** 1.平台所提供的各类资源包应保持持续更新机制。每年进行一次全面更新，内容涵盖最新的网络安全技术发展、漏洞库信息、教学实验环境、课程内容及竞赛题库等，确保教学与实训内容的时效性与前沿性。资源包更新周期 3 年，3 年内应持续提供最新版本资源及更新记录，以保证教学资源的先进性与可持续使用价值。 2.在举办训练、攻防演练、网络安全竞赛、队伍选拔等活动时，乙方应提供全面的技术支持，确保活动的顺利进行，并保障活动的安全性和技术准确性。提供 3 年人员到客户现场服务保障，每年不多于 5 次，每次根据客户活动提供 7 人技术保障，根据客户实际需求配合进行出题、培训、教员、专家分析、平台运维等保障支持。技术支持包括但不限于：赛题设计与审核、赛事平台的搭建与维护、实时监控与数据分析、系统安全保障等。同时，乙方需要确保所提供的赛题为全新原创题目，未在市面上出现过，确保赛事的独特性和创新性。

	3.提供专业漏洞监测与更新服务，聚焦网络安全领域，持续追踪中高危级别漏洞，确保每年完成国内外中高危级别漏洞的实时更新，及时为系统安全加固提供依据，助力构建靶场基础设施稳定可靠的网络安全防护体系。 4.围绕网络安全科普、国防教育等主题，精准对接企事业单位、高校、教育医疗等多元领域需求，定制化开展培训组织工作。凭借丰富的课程资源与专业讲师团队，规划年度培训体系，每年精心策划并落地 5 场高质量培训活动，提升参培人员安全意识与专业知识储备，强化各领域安全防护认知。 5.参与本次项目开发、部署、运营的相关人员必须签署保密协议，不得向外提供相关信息。 **四、网络安全 AI 综合应用系统　1 套** **平台功能：** 1.系统仪表盘以极简设计理念为核心，集成三大核心功能模块：智能体交互中枢搭载多模态交互引擎，支持自然语言指令的智能解析与响应；安全智能体开发平台内置可视化编排引擎，通过零代码/低代码拖拽式界面赋能用户快速构建、测试及部署智能体服务，并提供运营管理；安全智能体商城聚合安全规划与设计、安全建设与实施、安全运行与维护、安全应急与防御等领域的专业级智能体应用，覆盖威胁检测、风险评估、合规审计等场景，构建企业级安全防护的智能化生态。 2.知识问答须包括但不限于安全法律法规、安全运营工具使用、安全基础知识、反诈识别和协助。 3.支持威胁情报、漏洞查询、沙箱扫描、内容整编、报文分析、安全月报意图、AIQL 和指令等各类意图识别。 4.支持拒绝回答涉黄、暴恐、违法、违规等敏感问题，敏感词检测。 5.支持在智能体与异构业务平台对接时，以 open API 接口的形式集成到异构业务系统中，如有双方数据定义存在不同时，支持修改智能体接口参数，调整智能体出参入参要求的方式，提升接口适配工作的开放性与兼容性。 6.支持生态共享，对外支持以扩展插件、API 接口等形式实现智能体的调用；对内支持以 API、MCP 等多种形式接入外部能力，如本地设备的数据接入与操作下发。 7.支持基于记忆的多轮对话能力，在多轮对话场景中，能够依据短期记忆快速理解用户当前的意图，灵活调整回复策略，确保对话的流畅性与连贯性。 8.支持多样化智能体调用能力，可基于工作流编排实现多个智能体根据不同工作任务互相协同完成任务，如协作完成恶意邮件检测、恶意邮件研、研判报告输出等多任务。 9.支持全审计能力，支持用户级别的智能体调用、系统操作日志记录和审计 10.支持精细化的权限控制，支持租户级别智能体调用权限、业务数据读取隔离权限、知识库访问控制权限的控制 11.支持自定义敏感词，支持拦截试图诱导模型生成敏感内容的恶意问题，支持实时过滤模型输出内容并撤回敏感回答，支

	持用户限流（并发数和 Token 数） 12.支持内置安全智能体商城，具备 100 多个优质、成熟的智能体，可用于网络安全运营、数据安全运营、IT 运维管理等场景应用。 13.支持提供大模型问答-开放服务接口，支持 websocket 聊天及 http 聊天模式 14.支持智能体服务-开放服务接口并，提供智能体服务使用指南 15.支持知识检索与创作-开放服务接口 16.支持三种智聊插件，要求包含全屏扩展插件、侧边悬浮插件、大屏订阅插件 17.支持 PEFT（Parameter-Efficient Fine-Tuning）参数微调，例如 LoRa（Low-Rank Adaption）等任务训练方式，能支持多个 LoRa 任务的在多个 GPU 卡上的并行推理。 18.支持数字字典 AIQL 指令，包括 IP、源/目标/端口、告警类型、风险等级、置信度、情报 IoC、请求响应码、数据流方向等；支持按照需求场景查询信息；支持安全产品的查询条件转移为字段组合查询条件。 19.支持处置要求，可转化为 json 格式，通过 API 调度，实现封禁、阻断、黑名单、解封 IP/域名等处置联动功能。 20.支持大模型通过正则表达式或者 Json Schema 的方式，让大模型遵循一定的格式输出，避免大模型出现幻觉，提升任务的识别率和准确性。 21.支持复杂度感知能力。当检测到结构化约束超出可承载范围时，将判断是否支持该输出，并向用户提供优化建议，以保障推理服务稳定、连续运行。 22.支持当结构化约束复杂时，平台和接口返回错误提示信息，保证系统稳定。 23.支持新建知识库、编辑知识库、删除知识库。 **五、综合靶场硬件设备 1 项** **1.综合靶场专用配备设备 1 项** 需满足≥120 人同时在线使用； CPU：两颗物理 CPU，单 CPU 核心数≥24 核，每颗 CPU 主频≥2.5GHz； 内存：容量≥8*64GB DDR4 3200； 容量要求：容量≥1.92TB SSD*6；；容量≥8TB SAS*4； 接口要求：2 千兆电口+2 万兆光口，光纤线-多模-LC-LC-3M(*2 个)，万兆多模-850-300m-双纤(*4 个)；

	高性能 raid 卡、冗余电源 1+1。 **2.核心交换机** 2 套 交换容量≥4.8Tbps,包转发率≥1620Mpps； 支持 24 个万兆 SFP+，6 个 40/100GE QSFP28； 为了提高设备可靠性，支持并实配可插拔的双电源； 为了提高设备散热性能，支持可插拔风扇框，风扇框个数≥4； 支持最大 384K 个 MAC 条目； 支持静态路由、RIPV1/2、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 支持 VxLAN 功能，支持通过 Netconf 配置 VXLAN，支持 VXLAN 分布式网关，集中式网关 ，支持 BGPEVPN，支持 SRv6 BE（L3 EVPN），支持通过 Netconf 配置 SRv6，支持基于 SDN 实现全网有线自动化部署； 支持 SNMPv1/v2c/v3； 支持 M-LAG，支持堆叠，支持 LACP、跨设备聚合，支持 Smartlink； 支持防范 DoS 攻击、TCP 的 SYN Flood 攻击、UDP Flood 攻击、广播风暴攻击、大流量攻击； 支持集群方式随板 AC 热备； **3.接入交换机** 3 套 交换容量≥1.36Tbps，包转发率≥207Mpps； 为了提高设备可靠性，支持并实配可插拔的双电源； 支持 10/100/1000BASE-T≥48 个，10GE SFP+≥4 个， 专用堆叠口≥2 个； 支持最大 32K 个 MAC 条目，支持 4K VLAN ，支持 Sub-VLAN、Super-VLAN、Mux VLAN 和 Voice VLAN 功能； 支持静态路由、RIP、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+、ECMP，最大 8192 个 FIBv4 条目； 支持 LACP，支持 BFD，支持 VRRP、VRRP6； 支持 VLAN 切片， 支持端口流量监管，CAR 双速率三色标记； 二层到四层包过滤，根据源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、TCP/UDP 端口 号、协议类型、VLAN ID 过滤非法帧； 支持防止 DOS、ARP 攻击功能、ICMP 防攻击；

	支持智能堆叠 iStack、堆叠快速升级，支持 SNMPv1/v2/v3、Telnet、RMON、SSH； 支持 WebMaster 管理，支持 SNMP v1/v2/v3、Telnet、SSH **4.管理交换机** 1 套 交换容量≥1.36Tbps，包转发率≥207Mpps； 为了提高设备可靠性，支持并实配可插拔的双电源； 支持 10/100/1000BASE-T≥48 个，10GE SFP+≥4 个， 专用堆叠口≥2 个； 支持最大 32K 个 MAC 条目，支持 4K VLAN ，支持 Sub-VLAN、Super-VLAN、Mux VLAN 和 Voice VLAN 功能 ； 支持静态路由、RIP、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+、ECMP，最大 8192 个 FIBv4 条目； 支持 LACP，支持 BFD，支持 VRRP、VRRP6； 支持 VLAN 切片， 支持端口流量监管，CAR 双速率三色标记； 二层到四层包过滤，根据源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、TCP/UDP 端口号、协议类型、VLAN ID 过滤非法帧； 支持防止 DOS、ARP 攻击功能、ICMP 防攻击； 支持智能堆叠 iStack、堆叠快速升级，支持 SNMPv1/v2/v3、Telnet、RMON、SSH； 支持 WebMaster 管理，支持 SNMP v1/v2/v3、Telnet、 SSH。 **六、数据中心物理环境建设 1 项** **1.地面环境 1 项** 600*600 静电地板，面积 36 平方，地面防静电，环保、防火性能优异、强度高，超高耐磨、防火、防潮、使用寿命长，架空结构、承载力强、便于线路铺设，满足表面电阻，集中载荷，均布载荷 **2.内部环境 1 项** 恒温恒湿，量额定电压/频率：220V/50HZ，循环风量 1500，循环风量： 1800 ㎥/h **3.电气环境 1 项** 配电系统支持双电源输入，输入空开 120A，1 输出：空开 2P 16A*8，2 输出：空开 3P 63A*2；供电系统主输入：采用 IGBT 整流，单相三线，输入电压范围 AC100-288V，输入频率 40～70Hz 输入功率因数＞ 0.99；电池输入电压 220V，额定容量 5400W

	4.设备柜 1 套 柜体 800*1000*2000mm，托盘数量 3，前后双开网门通风率建议大于 70%，配备 PDU 电源、理线装置、可调地脚与重载角轮等 **5.消防设施 1 项** 灭火剂类型 CO_2 ，灭火剂充装量≥7kg，有效喷射时间≥8 秒，有效喷射距离≥2.5 米，使用温度范围-10℃ ~+55℃，满足数据中心环境使用。 **七、培训教室建设 1 项** **1.120 处通讯点 1 项** 材质通用性、模块的传输等级以及材质的可靠性，接线 方式，免打线设计，安装更便捷，尺寸不大于 86*86*9mm **2.地面环境 1 项** 网格地板 500*500*28mm，表面 500*500*1.8mm 地板格， 面积 460 平方，上/下钢板厚度≥ 0.7mm，集中荷载 (N)，极限集中荷载 (N)，均布荷载 (N/㎡)，防火等级，表面平整度≤ 0.60mm，耐磨、防尘，满足使用要求 **3.288 处电源点 1 项** 额定电压：250V（交流），额定功率：≥ 2500W (10A) 或 3500W (16A)，面板材质：阻燃 PC 料（优于 ABS 塑料），标准面板尺寸 86mm × 86mm（方形） **4.门禁系统 8 套** ①主机支持人脸识别、刷卡、指纹开锁功能，支持 5000 张人脸数据库，支持远程管控功能，支持日志查询功能，门锁支持反馈功能 ②开门按钮 86 型 ③门磁（双门+单门门磁），最大拉低 280KG **5.监控系统 1 套** ①半球全彩摄像机*8，支持 POE 功能，像素：400 万， 防水等级：IP66，供电方式：网线 POE 供电，存储编码： H.265/H.264，支持录像回放时间≥30 天 ②硬盘录像机*1：视频接入路数：16 路；硬盘数：4 盘位，供电方式：电源供电，接口：RJ45/HDMI/VGA/USB， 解码能力：4K 高清 ③监控硬盘*1：3.5 英寸，接口：sata 接口，容量:4TB， 缓存：256MB

	④POE 交换机*1：千兆 24 口交换机,POE 供电，24 个 POE 电口+2 个光口 ⑤专用显示设备*1，支持 HDMI 输入 ⑥矩阵*1：输入：2 路输入，输出：4 路输出，接口：HDMI 接口，支持网络信号传输 **6.综合布线系统 1 套** ①线管铺设 PVC20 线管（根据图纸）， ②桥架铺设 100*100 镀锌桥架（根据图纸）； ③网络布线：数量：6680 米，规格：六类八芯双绞线， 屏蔽类型：非屏蔽，传输速率： 1000Mbps，线径：，6MM； ④电源布线数量 380 米，RVV3*2.5 平方，纯铜材质 **7.满足使用要求的其他材料和设备 1 项** 为满足本项目实际使用需求，除项目现场已有物资（详见附件平面尺寸图）外，若仍需配置其他相关材料或设备，供应商可根据平面图设计进行补充或在服务方案中予以详细说明，确保整体满足项目使用要求。 **八、性能及扩展性要求 1 项** 本项目所建设的系统须充分考虑项目全生命周期建设需求，在满足本期建设内容的基础上，具备支撑后续二期建设及后续阶段建设的扩展能力。须做到可无缝扩展以下模块： 1.WEB 漏洞训练靶场：WEB 漏洞训练靶场是专为 WEB 安全学习和渗透测试练习设计的靶场，涵盖 ASPX 漏洞靶场、PHP 漏洞靶场、Java 漏洞靶场、Python 漏洞靶场、Go 漏洞靶场等，这些靶场通常包含多种常见的 Web 安全漏洞，如 SQL 注入、XSS 攻击、CSRF 攻击等，旨在帮助安全研究人员、开发者和学习者熟悉不同 WEB 开发语言的漏洞原理和利用方法。 2.综合内网靶场：综合内网靶场是一种模拟真实网络环境的靶场，用于渗透测试训练、攻防演练、漏洞挖掘和安全技术研发等。它通过构建复杂的网络拓扑结构和多样化的系统环境，提供一个可控、可重复的实验场景，帮助安全人员提升网络攻防技能。 3.源代码审计训练靶场：源代码审计训练靶场是一个专门为安全专家设计的靶场，旨在帮助民兵小队训练和提升代码审计能力。这些靶场通常包含 aspx、PHP、JAVA、Python、Go、C/C++等多种编程语言的漏洞场景，涵盖常见的安全漏洞类型，如 SQL 注入、跨站脚本（XSS）、命令注入、远程代码执行漏洞等。 4.安全加固靶场：安全加固靶场是一个模拟真实网络环境的靶场，旨在帮助民兵小队进行网络安全加固的实践和测试。让民兵小队能够对各种业务系统、服务器、中间件、数据库、服务、网络设备和安全设备等进行安全加固操作，同时测试加固效

	果，提升整体网络安全防护能力，从而更好地应对实际的安全挑战。 5.应急响应靶场：应急响应靶场是一个模拟真实网络攻击和安全事件的靶场，旨在帮助安全人员和运维团队进行应急响应能力的训练和测试。这些靶场通过模拟各种网络攻击场景，提供实战化的环境，让参与者能够练习应对各种紧急情况，提升应急反应能力和团队协作技巧。 6.CVE 漏洞靶场：CVE 漏洞靶场是一个专门用于学习和测试已知 CVE（Common Vulnerabilities and Exposures）漏洞的靶场。它通过提供各种漏洞环境，帮助安全研究人员、渗透测试人员和学习者熟悉漏洞原理、利用方法以及防御措施。 7.自动陪练系统：① 支持实时行为识别，平台能够实时监控学员对靶机的操作，并自动识别是否符合任务要求。例如，学员是否成功开启了靶机的防火墙并完成了加固任务。系统通过行为分析判断操作是否正确。②支持自动反馈与智能提示，一旦系统检测到学员完成了正确的操作（如防火墙加固、漏洞修复等），系统会自动提供反馈，确认操作正确，并允许学员进入下一环节。 若操作错误，系统将提供针对性的提示。③平台具备智能陪练功能，能够根据学员的知识水平和学习进度，自动推荐个性化的练习题目、模拟测试或实际场景练习，提升学员的学习效率。同时，平台还支持智能评估与反馈，能够实时评估学员在练习中的表现，根据得分或正确率等指标提供针对性的学习建议，帮助学员及时调整学习策略，从而更高效地提升技能水平。 ④安全 AI 综 合应用系统应包含全面的网络安全知识库和代码支持，提供实时联网接入 DeepSeek 等国内大模型的功能，确保能够动态更新并获取最新的安全指示与技术成果。系统不仅支持学员进行实战演练，还能通过大模型的实时接入，提供前沿的网络安全技术与漏洞检测，帮助学员保持对最新威胁和防护技术的敏感性，提升实际应对能力。 8. 供应商须对上述扩展性要求提供书面承诺函并加盖单位公章，承诺函作为投标文件组成部分。未按要求提供承诺函的，视为不满足本项性能及扩展性要求。 服务时间：合同履行期限：自合同签订之日起 34 日完成。
服务要求	▲1.服务所涉及的货物，供应商保证其自 身具有销售或供货资格，不存在任何侵犯第三方销售资质的情况，包括但不限于地 区独家销售权，产品独家销售权等，且货 物是通过合法渠道进货、全新且未使用过 的，所有权没有任何瑕疵的（即不存在资 产抵押或其他可能影响货物所有权的事宜），其质量、规格及技术特征应符合采购项目技术规格、参数的要求。如标的物有对应《中华人民共和国公共安全行业标准》相关执行标准时，所投货物必须满足该标准，否则采购人不予验收。 ▲2.服务所涉及的货物，投标产品必须是具备厂家合法渠道的全新原装正品。

	▲3.服务所涉及的货物，供应商应向采购 人提供设备（软件）的使用说明或其他技术文件，包括完整的软、硬件技术资料（含 纸介质和光电介质）。 ▲4、质量保证期内： (1)质量保证期 3 年（自整体项目通过最 终验收合格之日起计），若投标产品属于国家规定“三包”范围的，其产品质量保证期不得低于“三包”规定，若供应商的质量保证期承诺优于国家“三包”规定的， 按供应商实际承诺执行。 (2) 服务响应时间：中标人开通 24 小时服务热线：热线座机：021-63812540，热线电话：13585644902，提供 7*24 小时技术服务；中标人在接到采购人通知后 0.5 小时响应、6 小时上门服务，一般问题应在 48 小时修复，重大问题应在 7 天修复， 若无法在规定的时间内修复的，中标人必须提供备用产品给采购人使用。同一产品、同一质量问题，连续两次维修仍无法正常使用，中标人予以更换同品牌、同型号（如有）全新产品，且采购人不支付任何费用。 (3)质保期内，中标人负责对其提供的全部货物进行上门维修和维护，该费用包含在报价中，不得向采购人收取任何费用。自验收合格之日起一年内提供一次上门首保服务，该费用包含在报价中，不得向采购人另行收取任何费用。质保期内非采购人的人为原因而出现货物质量及安装问题，由中标人负责包修、包换或包退并承担因此而产生的一切费用；包修、包换或包退的零部件等设备，重修、换后且验收合格之日起重新起算质保期。 (4)质保期内，若非因人为或不可抗拒因素的原因而引起损坏或质量问题，由中标人负责处理并承担一切费用。 (5)质保期内，中标人负责对其提供的系统及全部产品进行维修和软件维护、升级，不再向采购人及产品使用单位收取费用，但人为因素、自然因素（如火灾、雷击等）造成的故障除外。 (6)质保期内，中标人建立质量跟踪档案，每半年 2 次向采购人进行现场（或电话） 回访，每年 2 次全面巡检和维护保养，以保证全部设备及设施能正常高效使用，并保存售后服务情况记录及采购人的反馈意见。 (7)培训：中标人对其提供产品或服务的使用和操作应尽培训义务，使采购人的使用人员能熟练掌握各个设备、各系统等的全部功能，在质保期内每年培训 1 次。 (8)维护保养：中标人提供 3 年的维护保养服务，应建立质量跟踪档案，每半年 2 次向采购人进行现场（或电话）回访，质保期内每年 2 次巡检和培训，以保证货物的正常高效使用，并保存售后服务情况记录及采购人使用单位的反馈意见。 (9)质保期内，中标人重大活动保障，应按采购人要求提前做好设备设施的测试和安全检查。根据采购人要求委派专业人员保障活动，负责保障现场设备操作的指导、协助完成活动保障等工作。出现故障有应急预案并做应急处理。重大活动期间安排人员全程在场值班。 （10）本次招标产品定期维护提醒。

	▲5.备品备件要求：备有设备配件，能及时处理、更换损坏的零部件。质量保证期内一切因生产厂制造质量原因造成的损坏，由中标人负责维修；质量保证期满后若设备出现故障，需更换配件的，只收取配件费，免收其余费用。中标人在售后服务中，维修使用的备品备件及易损件应为原厂配件，未经采购人同意不得使用非原厂配件。 ▲6.在日常使用过程中，依据法律规定或直观观察等日常生活经验能够直接确认的事实，可以直接作为判断是否有质量问题的依据，无需鉴定；确需鉴定的，经采购人和中标人双方同意，可委托有相关资质的第三方检测机构进行质量鉴定。货物符合质量标准的，鉴定费用由采购人承担；货物不符合质量标准的，鉴定费用由中标人承担。检验报告显示货物不符合质量标准的，采购人有权追究中标人的责任。中标人拒绝送检的，采购人可判定货物不符合质量标准，不予通过验收并追究中标人责任。 ▲7.免费送货上门、免费安装调试合格，其余按厂家承诺进行。 合同履行期限：自合同签订之日起 34 日完成。
服务时间	交付时间：自合同签订之日起 34 日完成。
服务标准	同服务范围内容一致。