一、项目概况

本项目为一个包，宁南中医医院2024年网络安全加固建设项目

二、服务技术内容及要求

（一）总体要求

宁南县中医医院为落实党的二十大的要求，贯彻好中央、国家印发的各项要求，切实推动公立医院改革与高质量发展，保障好医院在“互联网+医疗健康”发展及互联网、区块链、物联网、云计算、人工智能、大数据等的应用安全，势必开展医院的网络安全加固建设，为全县人民提供高质量医疗服务。贯彻落实《网络安全法》《数据安全法》《个人信息保护法》，防范和应对来自网络的攻击、侵入、干扰、破坏、非法使用和意外事故，完善宁南县中医医院内外网安全防护体系，建立数据安全新防线，提升医院主动防御高度。

（二）服务内容

（1）服务清单

序号	服务项	技术要求	备注
1	漏洞扫描服务	1．提供一套漏洞扫描检测工具,≥6个千兆电口，≥1个扩展槽位，≥8G内存，≥1T硬盘；支持无限制IP扫描授权，并发扫描≥40个IP地址，并发扫描≥5个系统扫描任务；支持≥40个域名扫描授权，并发扫描≥3个web任务。提供≥3年规则库升级服务。 2．支持旁路接入，不改变网络架构，进行脆弱性扫描探测。 3．支持IPV4/IPV6双栈协议环境探测扫描，支持同时下发系统扫描任务、弱口令扫描任务、Web扫描任务。 4．支持扫描主流操作系统、Web服务、数据库、网络设备、安全产品、各类应用及软件的安全脆弱性信息。 **5．▲具备强大的扫描特征库，系统漏洞数≥370000种，web漏洞数量≥10000种,数据库≥3000种。（提供产品功能截图，并加盖供应商公章）** 6．支持弱口令检测，通过扫描对弱口令分析，识别网络中弱口令主机。 7．支持针对打印机、摄像头、移动终端等设备的脆弱性发现。 8．支持通过站点目录、域名等设置站点扫描范围，支持通过站点指定目录、当前目录等设置站点扫描目录进行细粒度扫描。 9．支持展示风险分布及趋势图，包括主机风险分布、站点风险分布、漏洞风险分布、漏洞top10、资产风险值趋势、资产风险分布趋势。 10．▲支持未修复、修复、已验证、确定、忽略等类型的漏洞全生命周期管理，可根据漏洞分析结果自定义安全结论并导出综述报表及主机报表。**（提供产品功能截图，并加盖供应商公章）**	

		11．支持两次扫描结果对比，分析同一资产漏洞状态变化情况，保存漏洞检测详情。 12．支持漏洞风险预警，更新后无需再次扫描即可展示更新漏洞是否影响当前资产，避免多次重复验证。 13．提供弱口令扫描、Web 扫描、系统扫描等多类型报表模板，同时支持自定义模板	
2	高级威胁检测服务	14．提供内外网各一套高级威胁检测工具,内存≥32G,硬盘≥4TB, ≥8 个千兆电口, ≥4 个千兆光口,冗余电源, ≥2 个扩展槽位,最大并发连接数≥50W，综合检测能力≥1Gbps，提供≥3 年入侵检测规则库、应用识别、ip 识别库、僵尸主机分析库、威胁情报库、URL 识别库升级服务。 **15．▲支持机器学习检测，不依赖规则库即可实现对未知恶意程序检测,实现对目标文件实时检测实时还原。（提供产品功能截图，并加盖供应商公章）** 16．支持对文件进行多维深度检测，通过虚拟沙盒技术模拟文件行为检测，增强文件检测准确性，并记录文件传输会话信息。 17．支持 HTTP-Body UTF-32（LE/BE）编码、HTTP-Body 压缩、HTTP-Post 数据编码、IP 分片、TCP 分段、RPC 分片分段、SMB 分片分段、HTTP-Header 折叠、HTTP-Body UTF-7 编码等攻击逃逸报文进行深度的智能检测。 18．支持对 11000 种以上僵尸主机行为进行监测，包括僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT 等多类型的僵尸主机行为。 19．▲支持静态、动态、压缩、加壳病毒防护，可执行恶意软件样本检测率≥90%，恶意网页脚本样本检测率≥90%，并提供病毒告警信息和报表生成、导出。**（提供第三方检测机构出具的具有 CMA 或 CNAS 标识的产品检测报告复印件，并加盖供应商公章）** 20．支持对 Windows、Linux、IOS、Android、Unix、MacOS 等多种操作系统的僵尸主机检测，并对规则可设置相应警告、联动阻断动作。 21．支持卸载 SSL，实现对 HTTPS、IMAPS、SMTPS、POP3S、FTPS、RDP、MQTT、SIP 等加密流量的分析检测。 22．支持 SQL 注入分析引擎检测、SQL 注入智慧引擎检测、命令注入智慧引擎检测、XSS 攻击检测、WEBSHELL 上传智慧引擎检测。 23．支持独立的威胁情报库，不依赖其他设备或情报平台，即可独立的实现威胁情报检测能力，可对检测到的恶意文件、恶意 IP、恶意域名、恶意 URL 等设置相应捕获、取证、联动阻断等动作。 24．提供综合性的流量审计功能，可深入内容层提取元数据信息，包括传统网络协议、物联网协议、VPN 协议、移动网协议等 60 余种流量类型。 25．支持全流量取证，将事件发生前后的流量一起留存，支持报文取证和样本文件取证。 26．支持以 PCAP 包的形式保留抓包文件，并且记录文件名、文件生成时间、文件大小、状态，支持单个或多个 PCAP 文件导出。	

		27．▲支持设备一键巡检功能，迅速展示设备当前运行状态、服务状态、接口状态、规则升级情况，帮助管理员快速定位问题。**（提供产品功能截图，并加盖供应商公章）** 28．支持针对不同类别告警信息进行配置，包括攻击检测、僵尸主机、恶意程序、威胁情报、WEB 防护、管理、系统、等，并可进行告警测试。 29．▲支持对接原有态势感知平台，可通过态势感知平台进行性能监控、日志数据采集、安全策略管理。**（提供承诺函，并加盖供应商公章）**	
3	网络数据防泄漏服务	30．提供一套网络数据防泄漏服务工具,≥6 个千兆电口、≥4 个千兆光口，Bypass 接口≥1 组，冗余电源，≥2 个扩展槽位,应用层检测吞吐率≥500Mbps ，内存≥64G，硬盘≥2T。 31．支持对 HTTPS、HTTP、SMTP、POP3、IMAP、FTP、SMB、TELNET、DNS 等协议的解析、还原、识别。 32．支持 mysql、oracle、hbase、hive、hdfs 数据库审计，支持将设备 ID、采集时间、版本号、源 IP、源端口、目的 IP、目的端口、数据库类型、数据库操作等信息进行上报。 33．支持识别文件格式，包括文字格式、图片格式、电子表格格式、演示格式、多媒体格式、封装格式类型。 34．▲支持对 bmp，jpg，tif，tif2，png、jpeg、pjx、PSD 等格式图片内容进行识别，支持对 windows 截屏、身份证或其他证件的扫描件、身份证照片、保单扫描件、保单拍照、税单扫描件进行识别。**（提供产品功能截图，并加盖供应商公章）** 35．支持权重关键字方式制定策略，利用不同关键字严重程度不同而设定不同的权重。 **36．**▲支持手动、自动抓取大量无序文档样本进行聚类分析，生成规则，也支持通过上传训练样本（ZIP 格式正向、反向源文件），建立检测模型，来判断有违规内容的文件。**（提供产品功能截图，并加盖供应商公章）** 37．支持文档指纹检测，支持对固定内容格式的文档生成文档指纹，识别外发相似文档。 38．支持识别多层压缩方式逃避文件检测的行为，包含识别压缩文件的嵌套层数，并根据设定的阈值阻断。 **39．**▲支持水印功能，可对 FTP、SMTP、HTTP 下载的 WPS 文件添加源 IP、目标 IP、数据传输类型、时间、自定义文本等水印内容，同时支持对接第三方水印服务。**（提供产品功能截图，并加盖供应商公章）** 40．支持对用户越权访问行为进行审计，通过匹配 API 调用过程中的 API 调用字段信息，对违规访问行为进行监控。 41．支持通过 Syslog 协议上报安全事件日志、系统操作日志、系统告警日志；支持通过 RESTful 接口上报安全事件日志	
4	蜜罐威胁	42．提供一套蜜罐威胁防御服务工具,≥6 个千兆电口，≥4 个	

	防御服务	SFP 插槽,冗余电源,内存≥ 32G，系统盘≥240G SSD，数据盘≥1TB，提供≥50 个进程级主机 IP。 43．支持以饼图、曲线图等可视化方式展示系统资源使用率、攻击源 ip 数量及排行信息、受攻击虚拟主机数量及排行信息、多协议攻击趋势、虚拟主机及服务数量、实时告警等信息，支持导出当前系统统计概览信息。 44．支持拓扑图方式可视化展示虚拟主机拓扑信息。 **45．▲**支持以攻击源-虚拟主机、中国地图、世界地图三种方式对主动防御态势进行展示，包括攻击源 IP TOP10、被攻击虚拟主机 IP TOP10、攻击趋势、攻击拓扑、攻击类型分布等信息。**（提供产品功能截图，并加盖供应商公章）** 46．支持展示攻击事件的网络协议、应用服务、端口、攻击类型、威胁等级、攻击源 IP、虚拟主机 IP、网络、杀伤链阶段。 47．支持事件的多维度的查询，包括时间、攻击源 IP、虚拟主机、端口、网络、网络协议、告警级别、服务类型、攻击类型、杀伤链阶段等筛选条件。 48．支持以时间线的形式回放黑客入侵全过程。 **49．▲**支持 3000 种以上操作系统和 20000 种以上设备指纹伪装，包括 Windows、Linux、macOS 等系统，包括 DELL、HP、联想等指纹，同时支持智能一键添加蜜网，自动生成虚拟主机，支持添加多个蜜网模拟真实网络区域。**（提供产品功能截图，并加盖供应商公章）** 50．支持伪装系统服务、WEB 服务、安全设备、数据库服务、大数据组件、容器级服务等服务。 **51．▲**支持文件诱饵，可虚拟主机的目标路径下发、删除诱饵文件，也支持邮件及互联网诱饵，并能爬取和自定义上传创建网站模板，生成对应的 web 仿真服务。**（提供产品功能截图，并加盖供应商公章）** 52．支持页面运维工具故障排错,提供包括Unicode编码、UTF-8编码、URL 编码/解码、Base64 编码/解码、Hex 编码/解码、二进制/十六进制等工具。 **53．**支持根据不同的业务需求添加安全报告模板并展示生成的安全报告和任务记录。 54．产品具备《计算机软件著作权登记证书》。**（提供产品证书，并加盖供应商公章）**	
5	超融合云平台服务	55．提供一套超融合云平台服务基础平台,配置 CPU≥2 颗，单 CPU 核心数≥20，主频≥2.3GHz,标配 DDR4 3200HZ 内存≥512G，后置 SSD 系统盘≥960G，缓存盘≥ 960G;配置数据盘≥24TB 7200 转 SATA 硬盘 /企业级；≥4 个千兆电口，≥2 个万兆光口（配置相同数量的万兆多模光模块），前置≥12 个 3.5″热插拔 SAS/SATA 盘位，冗余电源。 56．采用完全分布式架构构建，包括计算、存储、网络及云管，	

		单点故障不影响集群正常运行，保障集群的稳定性。 **57.** ▲支持自动化安装;在同一个管理界面下,支持同一品牌超融合、桌面云、云容器、分布式存储的管理。**（提供第三方检测机构出具的具有 CMA 或 CNAS 标识的产品检测报告复印件，并加盖供应商公章）** 58. 支持大屏展示，监控集群状态，展示内容包括集群整体拓扑展示、健康状态、资源统计、资源负载情况及告警信息，展示 CPU、内存、存储及网络使用率等信息。 59. 支持基于 Web 界面快速扩容计算和存储节点，通过扫描主机或者手动添加的方式增加主机，扩大集群功能。 **60.** ▲支持对指定网络进行包数、字节数、协议及端口的监控功能，支持规则定义、信息过滤等流量分析功能。**（提供第三方检测机构出具的具有 CMA 或 CNAS 标识的产品检测报告复印件，并加盖供应商公章）** 61. 支持蓝屏检测技术，通过界面记录重新拉起过程，包括故障、蓝屏、HA 等过程，可在日志页面查看详情。 62. 可以支持云服务器高可用性，当集群中的某台服务器节点发生故障时，该服务器上的云服务器可以自动在集群内的其它服务器上重启运行，可以查看迁移触发的时间、完成情况及迁移目标主机等日志信息。 63. 可以支持数据自动重建功能;可以支持对降级或失效的存储卷进行不同的重建策略;可自定义重建检测频率和重建时间。 64. 支持日志审计功能，可以对集群操作日志、管理操作日志及集群事件进行展示，支持将日志通过报表方式进行导出，同时可支持审计日志转发到其他日志服务器，为故障排查、日志分析功能提供依据。 65. 支持对存储卷进行统一管理，支持删除云服务器后保留存储卷，支持存储卷全生命周期管理，能够对存储卷执行精细化操作。 66. 支持存储网络隔离，可以设置独立的私有网络，保持与其他物理网络隔离，仅作为集群内存储节点间的数据交换使用，避免受到病毒攻击、ARP 攻击，保证虚拟存储集群的稳定性。 **67.** ▲支持 1-6 副本部署，支持根据业务数据的重要性灵活设置副本数量，支持在一个服务器主机节点内设置多数据副本(≥2个)，大大降低客户的成本，支持动态在线增加和删除副本，不需停机即可操作。**（提供第三方检测机构出具的具有 CMA 或 CNAS 标识的产品检测报告复印件，并加盖供应商公章）** **68.** ▲支持磁盘退役功能，被设置为退役的硬盘，数据自动迁移到集群其它服务器节点磁盘中；支持磁盘维护功能，被设置为维护的硬盘，新数据会自动使用其他磁盘，原数据不受影响。**（提供产品功能截图，并加盖供应商公章）** 69. 支持快照数据在线可见，可随时查看和读取快照数据，如当 VM 内文件发生误操作、误删、中毒、系统配置文件更改时，可以通过该功能对比查看快照时刻 VM 内的文件。 **70.** ▲支持存储分卷，在 SSD+HDD 混闪硬盘配置下，可将 SSD	

		组成一个高性能存储池，云服务器可以运行在 SSD 闪盘模式；将 SSD 与 HDD 组成一个大容量存储池，云服务器可以运行在 HDD 模式。**（提供第三方检测机构出具的具有 CMA 或 CNAS 标识的产品检测报告复印件，并加盖供应商公章）** 71．提供计算虚拟化、存储虚拟化、网络虚拟化、统一管理平台≥2 颗 CPU 授权服务。	
6	终端安全防护服务	72．提供≥300 个 PC 终端病毒防范授权及三年病毒库升级服务，提供≥25 个 Windows 服务器病毒防范授权及三年病毒库升级服务，提供≥5 个 Linux 服务器病毒防范授权及三年病毒库升级服务。 73．支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell 后门、高危漏洞及其各自影响的终端数量。 74．支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴。 75．支持下发关机、重启、升级、病毒查杀、漏洞扫描、漏洞修复、文件分发设置等操作，并对以上操作配置详情，客户端执行情况跟踪，实现管理中心对客户端的任务状况监控。 76．具备通过病毒特征匹配进行病毒查杀，通过攻击报文识别、网络攻击检测对报文进行处理，实现对网络事件处理。 77．▲支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。**（提供第三方检测机构出具的具有 CMA 或 CNAS 标识的产品检测报告复印件，并加盖供应商公章）** 78．支持导出针对全网终端的终端风险报告，从整体分析全 网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议。 79．支持展示全网补丁情况，包括补丁编号、补丁类型、操作系统、下载状态等，支持补丁忽略功能。 **80．**▲支持勒索病毒诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。**（提供产品功能截图，并加供应商公章）** 81．支持基于行为侧采集的数据，结合用户真实业务环境做 上下文强关联分析，对攻击精准研判。包括但不仅限于钓鱼、挖矿、勒索、APT 等常见攻击场景。 82．支持 agent 安装目录的文件保护，可以保护 agent 目录 和文件实时监控驱动文件，可以保护 agent 的服务/进程/ 文件不被恶意删除，以免影响正常功能，导致用户的终端受到病毒入侵。 **83．**▲支持文档检测功能，支持文档检测功能，针对 txt;doc,docx,xls,xlsx,ppt,pptx,rtf;pdf 等格式文档的名称、内容进行包含关键字检查，对含有指定关键字的文档进行禁止发送、禁止拷贝等管控，消息提醒的同时将文档违规信息上报管理平台。	

		（提供第三方检测机构出具的具有CMA或CNAS标识的产品检测报告复印件，并加盖供应商公章） 84．支持对已停止更新的 Windows 系统的全网一键清点， 管理员可快速筛选出全网已停止更新的 Windows 系统的数量和具体的终端。	
7	互联网安全监测服务	85．提供三年SaaS化互联网网站监测服务。 86．通过多线路远程探测的方式，对客户指定的Web应用系统域名或IP地址进行7×24小时互联网连通性监测，及时发现网络中断等问题，并向客户进行预警，协助客户排查、定位故障原因。 87．支持对所监测客户的所有网站的告警数进行综合显示，例如：可用性监测告警数、篡改告警数、挂马告警数等。 88．事件通报需支持通报概览、待通报事件、通报中事件、已归档事件、事件通报规则、通报报告管理等事件管理能力。	
8	安全巡检服务	89．提供三年安全巡检服务。巡检的频次要求每季度一次； 90．提供全面专业的安全巡检报告，报告包含但不限于机房环境、资产情况、业务状态分析、漏洞风险、安全日志分析、整改建议等	
9	**超融合业务存储网络服务**	91．提供两套网络交换工具，容量≥2.56Tbps/23.04Tbps；包转发率≥220Mpps； 92．提供≥14万兆光口、≥8千兆电口，固化电源。	
10	存储网络服务	93．提供一套网络交换工具，容量≥2.56Tbps/23.04Tbps；包转发率≥220Mpps；提供≥14万兆光口，≥8千兆电口，固化电源	
11	防火墙升级服务	94．提供两套IPS入侵防御特征库升级服务≥3年； 95．提供两套AV防病毒特征库升级服务≥3年	
12	上网行为管理升级服务	96．提供≥3年上网行为应用识别特征库升级授权	
13	服务配件	97．提供4套≥1张FHHL转接卡(支持≥3个X8PCIE槽位)； 98．提供4套≥1张双端口万兆光接口网卡（满配光模块)； 99．提供12套SFP+ 万兆模块(850nm,300m,LC)；网线、跳线若干。	
14	网络配件	100．提供5套工控终端工具，处理器性能不低于I5,内存≥16GB,固态硬盘SSD≥512G,显示屏≥15.6寸；分辨率：≥1366*768	

注：▲项为重点要求，若有负偏离将在评分标准做扣分处理。

2.其他服务要求

2.1.材料要求：符合国家安全、环保等方面的要求；

2.2.安全要求：所涉及的设备应满足国家有关消防、安全等方面的要求，本项目在整个活动期间,在项目实施地点范围内,所有安全责任均由成交人负责(实质性要求)；

2.3.技术标准：按照现行国家、省、市相关规范和标准执行；

2.4.质量要求：按照现行国家、省、市相关规范和标准执行；

2.5.成果要求：按照现行国家、省、市相关规范和标准及采购人相关要求执行；

2.6.安装实施要求：必须满足相关规范要求，满足国家及地方政府对安全文明安装及环境保护的相关规定；

2.7.其他要求

①本次采购项目涉及安装的供应商应附带安装；

②完成本项目所需要的其他材料均要求供应商自行提供，采购人不承担成交人除成交价外的任何费用；

③响应文件及供应商所响应产品的质量、技术和其他要求货物制造标准、安装标准及技术规范等，须符合最新国家标准。各项技术标准应当符合国家相关的质量标准和出厂标准；

④在送到采购人之前表面无划伤、碰撞等现象；供应方保证产品是全新的、未使用过的，供应商不得以次充好；产品来源渠道必须合法，同时应根据有关规定、采购人的要求做好售后服务工作；

⑤供应商所提供的产品是经试验合格的全新正品。若开箱检验中发现有诸如数量、型号和外观尺寸与合同不符，或密封包装物本身的短少和损坏，如产生更换或补货等情形并导致工期延误，买方有权据合同有关条款的规定对因此造成的直接损失向供货商索赔。

⑥供应商提供的产品属于《网络关键设备和网络安全专用产品目录》的，应该按照《关于调整网络安全专用产品安全管理有关事项的公告（2023 年第 1 号）》的规定提供相应产品《网络关键设备和网络安全专用产品安全认证和安全检测结果（2023 年 9 月 5 日更新）》截图或有效期内的《计算机信息系统安全专用产品销售许可证》，或提供承诺函承诺招标（成交）后签合同前提供按《关于调整网络安全专用产品安全管理有关事项的公告（2023 年第 1 号）》的规定提供相应产品《网络关键设备和网络安全专用产品安全认证和安全检测结果（2023 年 9 月 5 日更新）》截图或有效期内的《计算机信息系统安全专用产品销售许可证》。

（实质性要求）

三、商务要求（实质性要求）

1.服务时间：三年（签订后30日历天完成所涉及的设备供货、安装调试）。

2.服务地点：凉山州宁南县（具体采购人指定地点）。

3.付款方式和条件：签订合同后15日内支付合同金额的30%，设备安装后15日内支付合同金额的20%；完成调试经采购人核验通过正常投入使用后15日内支付合同金额的50%。

注：本项目设备材料报价包含运输、保险、税费、人工、安全、原设施设备拆除、安装调试、售后服务承载的全部费用，本项目采用总价包干。

4.售后服务要求**（供应商需针对该项提供承诺函）：**

4.1所有软件、硬件、服务和更新验收合格的售后服务期限为3年。

4.2如 4 小时远程不能解决问题需24小时内安排工程师到达现场处理。上述信息系统出现故障，做到15分钟内远程响应，若系统故障严重影响系统使用时，工程师24 小时内到达现场。提供每季度巡检一次，并出具巡检报告。如设备不能现场维修，需更换配件，能够及时更换全新配件。在此期间，需提供备机使业务系统恢复正常运行。更换配件和提供备机所需费用均由成交供应商承担。

4.3在售后服务期间，如采购人更换或变动医院信息系统，供应商按照需求提供信息系统对接所需要的相关设备技术服务支撑。

4.4如不能按上述 3条满足采购人需求违反一次,成交单位赔偿采购人5000元，大写伍仟元整。

5.验收：

（1）验收主体：采购人（宁南县中医医院）；

（2）验收时间：供应商提出验收申请之日起30日内组织验收；

（3）验收程序、方式和标准：

①验收程序：一次性验收；

②验收方式：成交人提出验收申请后，由采购人自行组织验收，验收时采购人、供应商双方皆应派员参加；需邀请一位专家参与验收，验收相关费用由成交供应商支付。

③验收标准：符合国家、行业标准、四川省地方标准规定的验收标准。严格按照《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）及《政府采购需求管理办法》（财库〔2021〕22号）的要求组

织验收。验收应以采购合同、采购文件及其补充文件、国家或行业相关标准为验收的主要依据。

6.违约责任

6.1 采购人与供应商双方必须遵守并执行本项目中约定的各项规定，保证本项目的正常实施；

6.2 如因成交人工作人员在履行职务过程中的疏忽、失职、过错等故意或过失给采购人造成损失或侵害，包括但不限于采购人本身财产损失、由此而导致的采购人对任何第三方的法律责任等，供应商对此均应承担全部的赔偿责任；

6.3 如未经采购人同意，供应商不得将本项目成果移作他用，不得向第三方泄露本项目成果，违反本条规定，给采购人造成损失的，供应商应承担相关的法律责任；

6.4 供应商未在合同规定日期内提交全部符合项目合同要求的项目成果，每延迟一天，则采购人有权要求供应商支付合同总金额 1‰的违约金，延迟累计超过 15 个日历日，采购人有权解除本合同并不向供应商支付任何费用，并要求供应商承担因合同解除而造成的相关损失。若因采购人或者客观因素造成无法在规定工期内完成任务的，双方应协商解决。

7.争议解决：当出现争议时，采购人、供应商双方应进行友好协商解决，协商不成的应将矛盾提交项目所在地法院诉讼解决。

8.其他相关事宜

8.1 本项目不组织现场勘查，但供应商应根据工作实际，自行组织现场勘察，综合考虑后进行报价；

8.2 在本采购文件中没有提及的与本项目履约切实相关的事宜，在采购人与成交供应商订立合同时按明细约定或后续补充约定（约定的内容须符合国家相关法律法规的规定）；

8.3 本项目自成交方签订合同之日起至提交全部成果验收合格之日止，成交方将负责该项目实施过程中的人身安全、财产安全、环境安全，因本项目实施过程中造成的直接或间接损失，均由供应商自行承担