第三章 谈判项目技术、服务、商务及其他要求

（带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1、采购项目概况

营山县人民医院拟采购信息等保测评安全设备一批，本项目为1个包。

3.2、采购内容

3.2.1 标的清单

采购包 1：

采购包预算金额（元）：458,700.00

采购包最高限价（元）：458,700.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	防火墙	2.00	158,000.00	台	工业	是	否	否	否
2	终端准入控制系统	1.00	83,000.00	台	工业	否	否	否	否
3	终端安全管理系统	1.00	37,700.00	套	工业	否	否	否	否
4	现有设备维保升级	1.00	45,000.00	项	工业	否	否	否	否
5	终端防病毒	1.00	135,000.00	套	工业	否	否	否	否

3.3、技术参数及要求

采购包 1：

标的名称：防火墙

参数性质	序号	技术参数与性能指标
	1	★1、标准X86架构，三层吞吐量≥20Gbps，应用层吞吐≥9Gbps，并发连接数≥200W，新建连接数≥9W；配置≥8个千兆电口，≥2个万兆光口；为防止设备关键信息泄露，设备禁止配置显示器等显示设备；提供不少于三年的硬件质保、软件升级、WEB应用识别库、IPS特征库、热门威胁库、实时漏洞分析识别库和URL&应用识别库定期更新升级服务。 2、产品支持CC攻击防护功能，**要求提供国家认可的第三方检测机构出具的关于“CC攻击防护”功能项的产品检测报告**。 3、要求设备支持多链路出站负载，能够支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能。 4、产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略。 5、产品支持用户账号全生命周期保护功能，包括用户账号多余入

		口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。 6、产品支持主动防御功能，通过与云端蜜罐智能联动，通过仿真虚拟业务混淆黑客攻击，并对攻击进行溯源取证和阻断威胁 IP，保护网络真实业务安全。 7、支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险。 8、产品支持对 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 应用漏洞特征库超过 4580 种。 9、产品支持对不少于 9160 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 10、支持针对网站的漏洞扫描进行深度防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护。 11、为了排查故障和避免配置冲突和错误，要求设备的访问控制规则能够实现数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果。 12、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等。 ★13、支持与医院现有态势感知平台联动（现有产品品牌为深信服，产品型号为 SIP-1000-E600），将防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。 14、产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为。 15、支持对单位所有的网站提供保护情况的总览，包括哪些网站当前保护措施不足，哪些网站在有效保护中，当前的漏洞、恶意扫描、WEB 攻击及篡改事件发生的总体情况，同时风险要可定位到某个网站，并可以对网站面临的威胁给出处理方式。 16、产品支持 ftp 协议命令控制功能，至少包含 delete、rmdir、mkdir、rename、mget、dir、mput、get、put 等，保护对外服务不被恶意篡改。 17、产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。 18、产品预定义漏洞特征数量超过 10800 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则。 19、产品支持用户账号安全保护功能，包括用户账号多余入口检测、

		用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。**（提供国家认可的第三方检测机构出具的关于“账号保护”的相关报告证明。）** 20、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等。 21、产品支持 X-Forworded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。 22、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。**要求提供国家认可的第三方检测机构出具的关于“漏洞防扫描”功能项的产品检测报告。**

标的名称：终端准入控制系统

参数性质	序号	技术参数与性能指标
	1	★1、配置千兆电口≥6 个，千兆光口≥2 个；吞吐量≥3.6Gb，准入终端授权数≥800；为防止设备关键信息泄露，设备禁止配置显示器等显示设备；要求提供不少于三年的硬件维保、软件升级和 URL&应用识别规则库升级服务。 2、能够与防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录。 3、对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等；支持查看终端类型，以及终端详细信息（厂商，系统，端口等），支持查看终端类型分布。 4、支持存储设备、网络设备、蓝牙设备、摄像头、打印机的使用管控；支持外设白名单，提供批量获取硬件 ID 的工具进行白名单配置；支持对终端应用联网管控，可设置禁止或允许访问互联网，禁止或允许访问指定 IP 地址，离线时继续生效。 5、支持代理控制功能，不允许使用外部 HTTP 代理，不允许使用外部 Sock4/5 代理，不允许在 HTTP，SSL 一些的标准端口上使用其他协议；（比如在 80 端口上传输非 HTTP 协议数据，在 443 端口上传输非 HTTPS 协议数据等）。 6、自动发现网络里面的终端，并获取 IP、Mac、厂商、操作系统等信息，设备支持 PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持 Windows、Linux、MAC、瘦客户机等 PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等哑终端；支持自定义终端类型。 7、支持 windows 终端安全检查，包括：杀软检查、登录域检查、操作系统检查、进程检查、文件检查、注册表检查、补丁检查、windows 账号检查、防篡改检查、客户端集成检查，对不满足检查要求的终端可弹窗提示、禁止上网、违规修复。 8、支持对终端进行安全检查，比如检查终端是否开启系统更新、开放了哪些端口、安装了哪些程序等；检测 windows 系统当前重要补丁

		是否安装，并反馈检测结果。 9、支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证。 10、具有 IPSec VPN 远程加密访问和连接的模块，并能提供 IPSec VPN 客户端授权远程接入访问；IPsec VPN 支持多线路功能，支持配置主备线路组和流量分配模式的多线路选路策略。 11、支持自定义测试地址，检查终端是否能 PING 通，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户。 12、支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网。 13、支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。 14、支持部署在 IPv6 环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持 IPv6；支持设置终端访问地址白名单和黑名单，写入终端防火墙 ACL 策略，实现强访问管控。 15、支持 windows 终端外联行为检查，包括：连接外网检查、PPPoE 拨号检查、双网卡行为检查、无线网卡检查、链接非法 WIFI 检查（可设置合法 WIFI 白名单）、4G 网卡检查、是否使用非法网关（可设置合法网关白名单），对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户。 16、支持设置终端访问地址白名单和黑名单，写入终端外设控制策略，实现强访问管控；管控规则可离线生效。 17、支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证。 18、支持 Windows 终端调用管理员上传脚本/程序以满足个性化检查要求，可设置周期性运行或者运行一次，可设置以当前用户或 SYSTEM 用户权限执行，执行结果检查是否生效。

标的名称：终端安全管理系统

参数性质	序号	技术参数与性能指标
	1	★1、本次提供 30 个服务器客户端授权，3 年的软件升级服务。支持接入到医院现有的终端安全管理平台集中管理(医院现有平台品牌为深信服，型号为终端安全管理系统软件 V3.0），和医院现有的终端安全管理平台无缝对接。 2、产品是软件形态，包含管理平台和终端 Agent 软件；Agent 软件支持 32 位和 64 位的 Windows 系统和 64 位的 Linux 系统。 3、管理平台具备终端管理、终端病毒查杀、文件实时监控防护、东西向访问微隔离、暴力破解检测响应、WebShell 检测响应、设备联动响应等功能组件，保障平台的扩展性和兼容性。 4、支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示。

		5、提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。 6、支持热点安全事件动态更新和展示及全网终端已发生的热点安全事件及其数量；支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、WebShell检测的检测和威胁处置方式、暴力破解的威胁处置方式和Windows系统下信任区文件目录配置。 7、具备基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于AI技术的引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。 8、支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具。 9、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、半夜登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户。 10、针对Windows系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范。 11、支持在安全策略中配置Windows系统下的信任文件或目录，添加至信任区的文件或目录在病毒查杀将被跳过，以提升查杀效率和降低误杀率。 12、支持与下一代防火墙设备进行联动；支持防火墙通过配置终端检测响应管理平台IP地址实现与EDR平台的联动，实现端网安全联动。 13、支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、检测引擎、最后攻击时间、攻击方法、攻击内容、攻击历史。 14、支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等。 15、支持实时扫描WebShell，并且可以配置扫描出WebShell文件后相应动作，可以设置自动隔离或者仅上报不隔离。 16、支持与上网行为管理对接，支持管理员在上网行为管理平台界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。支持管理员在上网行为管理平台界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散。 17、支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到医院现有安全态势感知平台（现有平台产品品牌为深信服，产品型号为SIP-1000-E600），安全态势感知平台进行分析和展示。 18、基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处

		置情况，对勒索病毒及变种实现专门有效防御。 19、支持对勒索入侵的 RDP 暴破做全方位保护，包括 RDP 登录校验、RDP 文件加白二次校验等功能，支持 windows 服务器 RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵。 20、支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况。 21、支持基于威胁情报的病毒 md5 值的全网终端定位搜索，适用于对变种流行病毒的快速响应，快速确认全网终端是否感染。具备基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种。 22、具备基于本地缓存信誉检测与全网信誉检测，构建单位全网信誉库的检测引擎，做到内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销。

标的名称：现有设备维保升级

参数性质	序号	技术参数与性能指标
	1	★1、深信服 SIP-1000-E600：提供 3 年的安全感知系统平台特征库更新升级服务。 ★2、深信服 STA-100-B420：提供 3 年的安全感知系统探针特征库更新升级服务。

标的名称：终端防病毒

参数性质	序号	技术参数与性能指标
	1	★1、提供 810 个服务器授权（800 个 Windows Server 版本授权，10 个 Linux Server 版本授权）。授权包含管理后台以及全模块功能（反病毒引擎、多层次主动防御系统、病毒防御、系统防御、网络防御、设备控制等），无需按照模块进行授权。 ★2、提供三年病毒库更新升级服务。 3、非 OEM 产品。 4、支持采用 B/S 架构，由控制中心、系统中心、客户端三个模块组成防病毒体系，管理员只需通过浏览器登录控制中心，即可对系统进行管理。 5、控制中心和客户端均支持 Windows XP、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019。客户端支持 CentOS、Ubuntu、SUSE、Deepin 等 Linux 发行操作系统以及中标麒麟、银河麒麟、红旗、统信、等操作系统。 6、具有多级中心，且多级中心支持无限制级数级联管理，管理员身份支持跨级登陆，上级对下级管理，最大化减少上级服务器压力。 7、支持内置控制中心配置工具，可对控制中心参数进行修改配置。 8、支持对终端进行分组及批量分组，支持分组导入、导出。要求支持对终端进行单/多标签标记，进行部分操作。

		9、客户端部署支持本地部署、网页访问部署、域推送安装方式。 10、控制中心支持展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。 11、控制中心支持实时显示客户端的状态及终端基本信息，包括客户端连接状态、服务状态；终端机器名称、IP 地址、MAC 地址、操作系统、显卡信息、内存大小、当前版本信息和物理位置等信息，支持终端信息导出。 12、控制中心支持全网/以分组、标签为单位/指定某些客户端定制操作，即时/定时实现客户端三种病毒查杀模式、显示通知、关机、重启、升级等操作，并对以上操作配置详情，客户端执行情况跟踪，实现控制中心对客户端的操作监控。支持对客户端上述操作的快速定制。 13、要求支持中心二次验证，开启该功能后，通过登录中心时进行二次验证的方式，阻止中心遭遇密码泄露、弱口令暴破、撞库等黑客破解行为带来的危害，达到保护控制中心的目的。 14、支持客户端主动升级及平台即时/定时推送升级；平台支持客户端升级包上传及配置 http(s)/ftp 远端同步方式，更新客户端升级包，可以根据不同网络环境提供在线获取和隔离网获取相应工具。 15、支持服务器带宽设置，可限制最大并发数以及单个终端最大下载速度，可避免带宽超过最大负荷。 16、要求具有终端动态口令验证功能，当终端用户登录计算机时都将弹出动态口令安全认证窗口，若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出。用户需再次输入正确的动态口令才可登入计算机。且可设置应用范围：远程登录时启用或本地登录时启用。 17、产品支持在查杀防御的同时，产生的日志记录仅存储在用户本地，不回传任何数据给厂家。 18、支持定制策略包括病毒防御（文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP 协议控制、IP 黑名单）等，可以根据部门需求定制不同的策略。 19、支持全局信任区，全局信任区有信任文件路径、信任文件校验和方法，方便添加信任文件。 20、支持统计分析客户端上报的威胁日志，包含终端/部门/责任人危险排行、防御类型分布统计、病毒类型分布统计、病毒排行统计、病毒趋势统计等，要求支持管理员操作，日志记录追踪；支持控制中心-客户端交互操作，日志记录追踪，便于问题定位。 21、支持漏洞集中修复、统一修复高危漏洞、统一修复所有漏洞，并展示以做补丁和未做补丁的信息。要求支持配置补丁从控制中心下载/从外网下载两种方式 22、具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依

		赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）。具有病毒库，有病毒查杀能力。 23、支持反病毒引擎具有虚拟沙盒技术，能对待扫描的 PE 样本应用通用脱壳和动态行为扫描技术，检出家族性样本。要求虚拟沙盒接近真实 CPU 的执行效率和操作系统环境仿真且具有抗干扰能力。 24、反病毒引擎具有代码级修复能力，对寄生类恶意代码拥有完善的解决方案。 25、要求反病毒引擎具有基于虚拟沙盒的动态行为分析，可以跟踪和记录运行在其中程序的行为，通过行为记录，可以通过启发式分析算法对程序的恶意性进行评估。 26、要求支持无需沙箱即可针对包括但不限于 Web 服务器、数据库软件、Office 软件、编辑软件、浏览器、设计软件等软件进行加固，防止前述软件漏洞被攻击者（人或程序）利用进而进行渗透攻击。 27、支持 windows 客户端防护具有系统加固功能，阻止某些流氓、广告程序对电脑系统的恶意篡改等行为，提供一套全方位的加固方案，保护电脑系统各个安全关键点。其中默认开启文件防护≥9 项,注册表保护≥23 项,危险动作拦截≥2 项,执行防护≥13 项,进程防护≥2 项,病毒免疫≥4 项. 28、要求 windows 客户端防护同时具备桌面右下角广告弹窗拦截和软件安装拦截功能，安装软件的时候帮助用户识别软件是否是推广软件，用户可以自由选择是否需要继续安装；当有发现有推广软件正在安装时，会弹窗提示，用户可以根据需要选择是否安装此软件。 29、要求具有黑客入侵拦截功能，检测通过网络传输的数据包中是否包含敏感入侵信息，从而避免电脑遭到黑客入侵。直接从网络层防御 Wanncry、MS 08-067 等漏洞攻击。 30、要求具有恶意网址拦截，访问网站时帮助用户自动分辨即将访问的网站是否存在恶意风险，如果存在风险将拦截访问行为，并告知用户，避免侵害。 31、要求具有 IP 协议控制，当需要控制网络访问的具体动作，通过在 IP 协议层控制数据包进站、出站行为，并且针对这些行为做规则化的控制。 32、要求具有设备控制功能，可管控 U 盘、便携设备、USB 无线网卡、USB 有限网卡、打印机、光驱、蓝牙设备。 33、要求具有 U 盘信任功能，当终端开启访问控制-设备控制-U 盘设备时，可以通过在中心的“信任设备”功能来添加需要信任的移动存储设备，以允许该设备在任意终端使用。 34、考虑到医院部分电脑配置很低，业务系统众多与稳定运行的重要性，要求产品的客户端安装后最多占用 50M 硬盘空间，最多 10M 的病毒库大小，日常内存占用不到 10M，有效节省电脑资源。 35、要求支持程序执行控制，自定义限制终端使用某软件；可通过文件 sha1、文件路径方式配置。

3.4、商务要求

3.4.1 交货时间

采购包 1：

自合同签订之日起 30 日

3.4.2 交货地点和方式

采购包 1：

采购人指定地点

3.4.3 支付方式

采购包 1：

分期付款

3.4.4 支付约定

采购包 1： 付款条件说明： 政府采购合同签订生效之日起支付预付款 ，达到付款条件起 7 日内，支付合同总金额的 30.00%。

采购包 1： 付款条件说明： 验收安装调试合格 ，达到付款条件起 30 日内，支付合同总金额的 65.00%。

采购包 1： 付款条件说明： 无故障运行满 1 年后 ，达到付款条件起 20 日内，支付合同总金额的 5.00%。

3.4.5 验收标准和方法

采购包 1：

（1）履约验收主体：采购人。 （2）验收时间：达到验收条件，供应商提出验收申请后 7 日内进行验收。 （3）验收方式：自行验收。 （4）验收程序：①成立验收小组；②验收合格，出具验收合格的证明材料；③验收不合格，采购人下发整改通知由供应商进行整改。（5）验收内容：包括每一项技术、服务等要求的履约情况。 （6）验收标准：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）以及《政府采购需求管理办法》（财库〔2021〕22 号）的要求进行验收。

3.4.6 包装方式及运输

采购包 1：

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

3.4.7 质量保修范围和保修期

采购包 1：

质保期：本项目质保期为验收合格之日起 3 年。 售后服务：质保期内出现质量问题，供应商在接到通知后 24 小时内响应到场，4 小时内完成维修或更换，并承担修理调换的费用；质保期内如货物经供应商 3 次维修仍不能达到合同约定的质量标准，视作供应商未能按时交货，采购人有权退货并追究供应商的违约责任。

3.4.8 违约责任及解决争议的方法

采购包 1：

①如因成交供应商工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，成交供应商对此均应承担全部的赔偿责任。②因货物的质量问题发生争议，由质量技术监督部门或其指定的质量鉴定机构进行质量鉴定。货物符合标准的，鉴定费由采购人承担；货物不符合质量标准的，鉴定费由成交供应商承担。③合同履行期间，若双方发生争议，可协商或由有关部门调解解决，协商或调解不成的，由当事人依法法向法院提起诉讼维护其合法权益。

3.5 其他要求

采购包 1：

1、以上 3.4、商务要求为实质性要求，不允许负偏离。 2、若按“5.3.9 推荐成交候选供应商”的推荐顺序仍并列的，由谈判小组在评审现场进行随机抽签决定最终推荐顺序。3、本项目涉及 CCC 认证产品参与报价的，应在响应文件中提供 CCC 认证证书。本项目无 3C 认证产品。4、政府采购供应商信用融资:根据《四川省财政厅关于推进四川省政府采购供应商信用融资工作的通知》（川财采[2018]123 号）文件要求，为助力解决政府采购中标、成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可根据四川政府采购网公示的银行及其“政采贷”产品，自行选择符合自身情况的“政采贷”银行及其产品，凭中标（成交）通知书向银行提出贷款意向申请，并按照相关规定要求和贷款流程申请信用融资贷款。中国工商银行营山支行 联系人：阳博 联系方式：0817-8310513 地址：营山县新北路 68 号 中国建设银行营山支行 联系人：刘伟 联系方式：18781741682 联系人：温东升 联系方式：18428396251 地址：营山县新北路 2 号 四川营山农商银行股份有限公司东城支行 联系人：冯荣 联系电话：13699694386 地址：营山县北塔后街文运国际商业区 四川天府银行股份有限公司营山支行 联系人：罗蓉蓉 联系电话：19982822802 地址：营山县三星北路 158 号（三星美庐）。5、质疑投诉：5.1、参与供应商：已依法在四川政府采购网（https://zfcg.scsczt.cn/）项目电子化交易系统-投标 （响应）管理-未获取采购文件中选择本项目获取采购文件的潜在供应商；5.2 供应商应当在法定质疑期内一次性提出针对同一 采购程序环节的质疑;5.3 监督管理办公室：南充市营山县财政局，联系电话：0817-8218553 ，地址：四川省南充市营山县北坝街 36 号， 邮编：637700。