

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

本项目为网络安全采购项目。

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): 672,000.00

采购包最高限价(元): 672,000.00

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	1.00	672,000.00	批	工业	是	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	技术参数及要求			
		序 号	标 的 名 称	技术参数及要求	数 量
		1	万 兆 防	1、网络层吞吐量≥ 20G,应用层吞吐量 ≥9G,并发连接数	2 套

		火 墙	<p>≥200W，新建连接数 (CPS) ≥9W 个；</p> <p>硬件参数: ≥8G 内存, ≥8 个千兆电口, ≥4 个万兆光口, 配置 ≥128GB SSD, 配置特征库升级三年；</p> <p>2、产品支持虚拟防火墙功能，支持虚拟防火墙的创建和删除，具备独立的接口、会话管理、应用控制策略、NAT 等资源；</p> <p>3、具备静态路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议；</p> <p>4、产品支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换。（需提供产品功能截图证明）。</p> <p>5、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护。</p> <p>6、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。（需提供产品功能截图证明）</p> <p>7、产品支持对不少</p>	
--	--	--------	--	--

			<p>于 10000 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。</p> <p>8、设备安全日志支持本机存储、Syslog 服务器存储、态势感知平台存储等不同形式存储方式。</p> <p>9、支持展示终端资产列表，可查看终端指纹信息和状态，如 IP、MAC、类型、系统、厂商、终端名称、在线状态、审核状态等（需提供产品功能截图证明）</p> <p>10、产品支持对常见 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 3320 种；（需提供相关功能截图证明）</p> <p>11、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。（需提供产品功能截图证明）</p>	
--	--	--	--	--

			<p>明)；</p> <p>12、安全规则库支持在线自动升级、手动升级、云端实时升级等多种方式。</p> <p>13、为了保证产品可靠性和安全性，产品支持未知威胁检测能力。（需提供相关检测报告或截图）</p> <p>14、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。（需提供产品功能截图证明）。</p> <p>15、产品支持多种自定义条件快速查询安全日志，自定义条件至少包括时间、日志类型、安全日志严重等级等条件。</p> <p>16、产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理，支持检测到某主机有僵木蠕毒的C2通信时，手动或自动化将恶意域名信息下发到终端安全软件做C2通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离。</p>	
--	--	--	--	--

			<p>（需提供产品功能截图证明）</p> <p>17、为保证设备使用实现更好的安全效果，需要保证此次设备能与原有态势感知平台实现对接（提供承诺函并加盖供应商公章）</p> <p>18、产品支持云威胁情报网关技术，通过全球超过30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品功能截图证明并提供 POP 节点在线查询链接）</p> <p>19、产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。（需提供产品功能截图证明）</p> <p>20、产品支持勒索病毒检测与防御功能（需提供产品功能截图证明）。</p>	
		2	<p>日志审计</p> <p>1、本次配置审计资产数量≥100，支持最大审计资产数量≥150，可用存储量≥2T；平均每秒处理日志数≥2500，配置千兆电口≥6个，万兆光口≥2个</p> <p>2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系</p>	1套

			<p>统等不少于 720 种日志对象的日志数据采集；</p> <p>3、支持主动、被动相结合的数据采集方式，支持通过 Agent 采集日志数据，支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka 等多种方式完成日志收集；（提供产品功能截图）</p> <p>4、内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到 200 种</p> <p>5、支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志；（提供产品功能截图）</p> <p>6、支持日志文件备份到外置存储节点，支持 NFS、NAS、ISCSI 三种存储方式，并可查看外置存储容量、状态等信息；</p> <p>7、支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段</p>	
--	--	--	--	--

			<p>的新增、合并、映射。（需提供功能截图证明）</p> <p>8、支持预置审计策略模板，包括： Windows 主机类审计策略模板、 Linux/Unix 主机类审计策略模板、数据库系统类审计策略模板等，内置审计规则数量不少于 40 条；</p> <p>9、支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到 350 条以上，支持自定义关联分析规则（提供产品功能截图）</p> <p>10、提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持 usb-key 认证</p> <p>11、支持 POC 测试工具一键生成数</p>	
--	--	--	--	--

			据。（需提供截图证明）	
		3	<p>漏洞扫描</p> <p>1、系统漏扫授权 IP 数\geq100, WEB 漏扫授权 URL 数\geq20; 主机漏扫最大并发 IP 数\geq150, WEB 漏扫最大并发 URL 数\geq5。配置千兆电口\geq6 个, 千兆光口\geq2 个, 硬盘容量\geq128GB SSD, \geq2TB SATA;</p> <p>2、支持同时开启全插件系统漏洞扫描、WEB 漏洞扫描、弱口令扫描、基线配置核查, 扫描速度不低于 1000ip/h;</p> <p>3、支持全局风险统计功能, 通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息, 并可查看详情;</p> <p>4、支持全局风险统计时段自定义, 展示近 3 个月、6 个月、1 年或自定义统计区间的风险分布和详情, 时间跨度不限制。</p> <p>5、支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型, 其中全面扫描支持系统漏洞扫描、WEB 漏洞</p>	1 套

			<p>扫描、弱口令扫描同时执行；</p> <p>6、支持检测的漏洞数大于 19000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准；支持操作系统、网络设备、数据库、中间件等漏洞扫描</p> <p>7、支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等；</p> <p>8、支持等保资产登记功能，包括但不限于物理机房、网络设备、安全设备、服务器或存储设备、终端、系统管理软件或平台、业务应用系统或平台、关键数据类型、大数据数据类别、安全相关人员、管理文档、安全文档等 12 类资产进行资产登记；</p> <p>9、支持域管理功能，系统默认内置数据域、终端接入域、运维管理域等九个域，可根据客户实际情况进行自定义管理。（提供产品功能截图）</p> <p>10、提供检测结果综述分析，按照等保 2.0 的检测项要</p>	
--	--	--	---	--

			<p>求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况（提供产品功能截图）；</p> <p>11、产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表。</p>	
<p>三、其他服务要求：</p> <p>1、日常值守服务资产数量≥40个，服务时间≥1年，提供7*24小时值守服务，每季度对映射到公网的出口进行扫描，发现漏洞，并对漏洞提出有效的处理方案，及时处理发现的漏洞；</p> <p>2、服务支持检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况</p> <p>3、服务支持提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度；（提供服务功能截图）</p> <p>4、服务支持针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的脆弱性，自动生成工单，安全专家跟进修复状态，各个处理进度透明，方便采购人清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化；</p> <p>5、服务支持针对服务平台生成的工单，采购人可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促供应商第一时间处理；（提供服务功能截图）</p> <p>6、服务支持针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户；</p> <p>7、服务支持脆弱性复测措施，及时检验脆弱性真实修复情况。供应商要支持采购人可按需针对指定脆弱性问题，指定资产等小范围进行，降低脆弱性复测时的潜在影响范围；（提供服务功能截图）</p> <p>8、服务支持对发现的脆弱性建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得采购人可做到脆弱性的可视、可管、可控；（提供服务功能截图）</p>				

- 9、服务支持通过全网大数据分析，发现有黑客或高级黑客正在攻击，立即采取行动封锁黑客行为
- 10、服务支持实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含黑客攻击事件、暴力破解攻击事件、持续攻击事件；（提供服务功能截图）
- 11、服务支持每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置
- 12、通过 SLA 对安全威胁服务水平作出承诺：
- 1) 从安全日志产生到威胁通告给采购人的时间方面，重大威胁的通告时间少于 1 小时，一般威胁的通告时间少于 2 小时。
 - 2) 在配备供应商的边界防护服务组件和终端防护服务组件的情况下，高级威胁的处置完成时间少于 1 小时，一般威胁的处置完成时间少于 4 小时；
 - 3) 在未配备供应商的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的处置完成时间少于 24 小时；
 - 4) 安全威胁经过服务人员的确认后，高级威胁和一般威胁的判断准确率不低于 99%。
 - 5) 在配备了成交供应商的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的闭环处置比例达到 100%（提供供应商承诺函，并加盖供应商公章）

四、商务要求：

（一）交货期及地点要求（实质性要求）

1、交货期：签订合同后 30 个工作日内按照合同货物交付给甲方并安装调试完毕投入使用

2、交货地点：凉山彝族自治州第一人民医院西昌市下顺城街 6 号

（二）付款方法和条件要求（实质性要求）

合同签订设备到场签收 7 日后支付项目合同总金额的 40%；安装调试完毕项目验收后 15 个工作日支付合同总金额的 30%，验收合格后平稳运行三个月后 15 日内支付合同总金额 25%，剩余 5%款项质保期满后一次性无息支付。

（三）维护期要求（实质性要求）

其中万兆防火墙、日志审计、漏洞扫描质保期从系统验收日算起 3 年，质保期内应每年派专人到现场巡检两次，对有问题的设备进行更换，并出具相关巡检报告给采购方。

（四）售后服务及其他要求（实质性要求）：

1、结合医院实际情况，拟定详细、有序、安全稳妥的实施、切换等方案，承诺保证在合同规定时间内医院信息系统的平稳过渡。

- 2、培训：培训对象包括系统管理员，系统管理人员培训内容为项目中涉及的相关技术内容，供应商需派专业技术人员到采购人指定的地点对采购单位的技术人员进行使用操作等技术的现场培训，直至采购单位的技术人员独立操作。
- 3、供应商必须合理安排进场的项目负责人和实施人员，保证其实施和协调能力。
- 4、供应商成交后，拥有专职售后服务技术人员；对于系统故障或新需求，1小时内电话响应，服务时间为7×24小时，故障严重或医院要求的情况下6小时内到达现场解决问题，并在12小时内完成故障处理工作，由此产生的费用均不再收取。
- 5、为保证产品质量，供应商如不是投标产品制造商的，应在中标后合同签订前提供制造商针对本项目的质保书。
- 6、其他实施及售后服务事项根据在合同中约定。

（五）验收要求（实质性要求）：

合同签订后，供应商应及时提供设备安装条件的技术要求与技术指导。安装完毕后，采购人按本项目验收标准进行验收，供应商需提供的技术资料（配套使用说明书、维护手册等其它相关技术资料）。验收不合格或出现争议的，采购人有权委托法定资格的检验检测机构进行检测。

成交供应商与采购人应按照政府采购相关法律法规以及《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）的要求进行验收。验收标准：按国家有关规定以及采购文件的质量要求和技术指标、供应商的响应文件及承诺与本合同约定标准进行验收。

（六）维护期收费要求（实质性要求）：

其中万兆防火墙、日志审计、漏洞扫描质保期从系统验收日算起3年，质保期满后另签维护合同，维保期满后，由甲、乙双方协商维保服务费，维保服务费不得高于合同金额的5%。

安全服务为入场验收后开始计算为期1年服务。

四、报价要求（实质性要求）：

1. 本项目预算控制价金额为67.2万元，供应商报价需符合预算控制价要求，超出预算控制价的作无效响应处理。

2. 本项目报价是履行合同的最终价格，是包含完成本项目所需的货款、培训、人员安全及各种应纳的税等完成本项目所需的一切费用，采购人不再支付任何费用；响应报价估算错误等引起的风险由供应商自行承担。

五、其他要求：

1. 知识产权归属和处理方式（实质性要求）：

1.1 . 供应商应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。

1.2 . 供应商享有本项目实施过程中产生的知识成果及知识产权。

1.3 . 供应商如欲在项目实施过程中采用自有知识成果，需在投标文件

中声明，并提供相关知识产权证明文件。使用该知识成果后，供应商需提供开发接口和开发手册等技术文档，并承诺提供无限期技术支持，采购人享有永久使用权（含采购人委托第三方在该项目后续开发的使用权）。

1.4. 如采用供应商所不拥有的知识产权，则在投标报价中必须包括合法获取该知识产权的相关费用。

2. 违约责任与解决争议的方法（实质性要求）：

2.1. 违约责任：

2.1.1 甲乙双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。

2.1.2 如因乙方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甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任。

2.2. 解决合同纠纷的方式：因本合同履行过程中产生的争议，双方应友好协商解决。经协商不能解决的，任何一方均可以向甲方所在地的有管辖权的法院提起诉讼。

3、安全责任（实质性要求）： 供应商应承诺如成交后在本项目履约或服务工作中一切的安全责任全部自行承担（提供承诺函）。

注：1、以上所有技术、服务及商务要求均为实质性要求，谈判结束后，一项不满足为无效响应。

2、国家强制节能清单产品（依据：财库〔2019〕19号文件）。

2.1 强制性节能产品仅限于采购人采购的货物，或服务中所涉及的归属权属采购人的货物，不适用于服务采购中归属权属供应商的货物，如租赁、服务外包、会议或展台搭建等。

2.2 以下为国家强制节能清单产品，响应的产品如属于以下产品的，须提供相关认证证书：

品目序号	名称			依据的标准
1	A020101 计算机设备	★A02010104 台式计算机		《微型计算机能效限定值及能效等级》（GB 28380）
		★A02010105 便携式计算机		《微型计算机能效限定值及能效等级》（GB 28380）
		★A02010107 平板式微型计算机		《微型计算机能效限定值及能效等级》（GB 28380）
2	A020106 输入输出设备	A02010601 打印设备	★ A0201060102 激光打印机	《复印机、打印机和传真机能效限定值及能效等级》（GB 21521）
			★	《复印机、打印机

				A0201060104 针式打印机	和传真机能效限定值及能效等级》 (GB 21521)
			A02010604 显示设备	★ A0201060401 液晶显示器	《计算机显示器能效限定值及能效等级》 (GB 21520)
3	A020523 制冷空调设备	★A02052301 制冷压缩机	冷水机组	《冷水机组能效限定值及能效等级》 (GB 19577), 《低环境温度空气源热泵(冷水)机组能效限定值及能效等级》 (GB 37480)	
			水源热泵机组	《水(地)源热泵机组能效限定值及能效等级》 (GB 30721)	
			溴化锂吸收式冷水机组	《溴化锂吸收式冷水机组能效限定值及能效等级》 (GB 29540)	
		★A02052305 空调机组	多联式空调(热泵)机组(制冷量>14000W)	《多联式空调(热泵)机组能效限定值及能源效率等级》(GB 21454)	
			单元式空气调节机(制冷量>14000W)	《单元式空气调节机能效限定值及能效等级》(GB 19576)《风管送风式空调机组能效限定值及能效等级》 (GB 37479)	
		★A02052309 专用制冷、空调设备	机房空调	《单元式空气调节机能效限定值及能效等级》(GB 19576)	
4	★A020609 镇流器	管型荧光灯镇流器		《管形荧光灯镇流器能效限定值及能效等级》(GB 17896)	
5	A020618 生活用电	★A0206180203 空调机	房间空气调节器	《转速可控型房间空气调节器能效限	

				器			定值及能效等级》 (GB 21455-2013), 待 2019 年修订发布后, 按《房间空气调节器能效限定值及能效等级》(GB21455-2019) 实施。
					多联式空调 (热泵) 机组(制冷量 ≤ 14000W)		《多联式空调(热泵)机组能效限定值及能源效率等级》 (GB 21454)
					单元式空气 调节机(制冷 量≤14000W)		《单元式空气调节机能效限定值及能源效率等级》 (GB 19576) 《风管送风式空调机组能效限定值及能效等级》 (GB 37479)
				A02061808 热 水器	★电热水器		《储水式电热水器能效限定值及能效等级》(GB 21519)
		6	A020619 照明设备	★普通照明用 双端 荧光灯			《普通照明用双端 荧光灯能效限定值 及能效等级》 (GB 19043)
		7	★A020910 电视设备	A02091001 普 通电视 设备(电视机)			《平板电视能效限 定值及能效等级》 (GB 24850)
		8	★A020911 视频设备	A02091107 视频监控设备	监视器		以射频信号为主要 信号输入的监视器 应符合《平板电视 能效限定值及能效 等级》 (GB 24850), 以数字信号为主要 信号输入的监视器 应符合《计算机显 示器能效限定值及 能效等级》 (GB 21520)

			9	★A060805 便器	坐便器		《坐便器水效限定值及水效等级》 (GB 25502)
					蹲便器		《蹲便器用水效率限定值及用水效率等级》 (GB 30717)
					小便器		《小便器用水效率限定值及用水效率等级》 (GB 28377)
			10	★A060806 水嘴			《水嘴用水效率限定值及用水效率等级》 (GB 25501)

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:

凉山彝族自治州第一人民医院西昌市下顺城街 6 号

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: 合同签订设备到场签收 7 日后支付项目合同总金额的 40% , 达到付款条件起 7 日内, 支付合同总金额的 40.00%。

采购包 1: 付款条件说明: 安装调试完毕项目验收后 15 个工作日支付合同总金额的 30% , 达到付款条件起 15 日内, 支付合同总金额的 30.00%。

采购包 1： 付款条件说明： 验收合格后平稳运行三个月后 15 日内支付合同总金额 25% ， 达到付款条件起 15 日内， 支付合同总金额的 25.00%。

采购包 1： 付款条件说明： 剩余 5%款项质保期满后一次性无息支付 ， 达到付款条件起 30 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:

验收内容包括每一项技术和商务要求的履约情况， 验收标准要包括所有客观、 量化指标。 按国家有关规定以及采购文件的质量要求和技术指标、 供应商的响应文件及承诺与本合同约定标准进行验收； 采购人与供应商双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项， 由采购人在采购文件及响应文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。

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:

其中万兆防火墙、 日志审计、 漏洞扫描质保期从系统验收日算起 3 年， 质保期内应每年派专人到现场巡检两次， 对有问题的设备进行更换， 并出具相关巡检报告给采购方。

3.4.8 违约责任及解决争议的方法

采购包 1:

2.1.违约责任： 2.1.1 甲乙双方必须遵守本合同并执行合同中的各项规定， 保证本合同的正常履行。 2.1.2 如因乙方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甲方造成损失或侵害， 包括但不限于甲方本身的财产损失、 由此而导致的甲方对任何第三方的法律责任等， 乙方对此均应承担全部的赔偿责任。 2.2.解决合同纠纷的方式： 因本合同履行过程中产生的争议， 双方应友好协商解决。 经协商不能解决的， 任何一方均可以向甲方所在地的有管辖权的法院提起诉讼。

3.5 其他要求

采购包 1:

无