永州市政府采购文件

采购项目名称：	东安县人民医院网络安全设备更新改造项目（第二次）
采购人：	东安县人民医院
采购方式：	询价
采购代理机构：	湖南永冲锋项目管理有限公司
委托代理编号：	HNYCF-CG-2026-026
代理费收取方式：	采购人支付代理费（按成交金额百分比收取）
代理费支付标准：	项目成交金额的1.2%
专家评审费收取方式：	专家评审费由 采购人 支付
采购计划编号：	东财购计2026[00079]号
采购项目预算：	780,000元
是否进行资格预审：	否
需求编制时间：	2026年11月09日

采购人签章：

东安县人民医院

需求编制人签章：

李霞

编制依据

《中华人民共和国政府采购法》（中华人民共和国国家主席令第14号修改）
《中华人民共和国政府采购法实施条例》（中华人民共和国国务院令第658号）
《政府采购非招标采购方式管理办法》（财政部令第74号）
《政府采购货物和服务招标投标管理办法》（财政部令第87号）
《政府采购框架协议采购方式管理暂行办法》（财政部令第110号）
财政部关于印发《政府采购需求管理办法》的通知（财库〔2021〕22号）
财政部关于印发《政府采购进口产品管理办法》的通知（财库[2007]119号）
财政部、工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知（财库[2020]46号）
关于进一步加大政府采购支持中小企业力度的通知（财库〔2022〕19号）
湖南省财政厅湖南省司法厅关于政府采购支持监狱企业发展的有关通知
财政部关于《推进和完善服务项目政府采购有关问题》的通知（财库〔2014〕37号）
国务院办公厅关于政府向社会力量购买服务的指导意见（国办发〔2013〕96号）
湖南省财政厅关于印发《湖南省政府采购非公开招标采购方式审批管理办法》的通知（湘财购[2025]7号）
关于推动解决政府采购异常低价问题的通知（财库〔2026〕2号）
其他政府采购法律法规及政策

编制基本要求

采购人在招标公告、采购需求和评审标准中不得按以下不合理的条件对供应商实行差别待遇或者歧视待遇：
(一)就同一采购项目向供应商提供有差别的项目信息；
(二)设定的资格、技术、商务条件与采购项目的具体特点和实际需要不相适应或者与合同履行无关；
(三)采购需求中的技术、服务等要求指向特定供应商、特定产品；
(四)以特定行政区域或者特定行业的业绩、奖项作为加分条件或者中标、成交条件；
(五)对供应商采取不同的资格审查或者评审标准；
(六)限定或者指定特定的专利、商标、品牌或者供应商；
(七)非法限定供应商的所有制形式、组织形式或者所在地；
(八)以其他不合理条件限制或者排斥潜在供应商。
采购人应对采购标的的市场技术或服务水平、供应、价格等情况进行市场调查，根据调查情况科学、合理确定采购需求和价格测算。
采购需求应符合国家相关法律法规和政府采购政策的规定。
采购人根据价格测算情况，可以在采购预算额度内设定最高限价，但不得设定最低限价。
采购人根据编制依据和基本要求提出采购需求，采购需求中应落实节约能源、保护环境、扶持不发达地区和少数民族地区、促进中小企业发展等政府采购政策。
采购人应就采购公告、采购需求和评分标准自行组织征询专家意见（本系统、本单位人员不得作为专家参与征询意见）。
采购需求的内容应当完整、明确，主要包括：
(一)采购需求明细包括：货物或服务名称、技术规格和技术参数、产地类型（国产或进口）、是否接受进口产品、是否为采购节能环保产品、是否为核心产品(必要时需设置同品牌淘汰策略)、技术标准或服务标准、数量、单价（元）、小计（元）、总合计（元）等。
(二)采购标的执行的国家相关标准、行业标准、地方标准或者其他标准、规范；
(三)采购标的所要实现的功能或目标，以及需落实的政府采购政策；
(四)采购标的需满足的质量、安全、节能环保、技术规格、服务标准等性能要求；
(五)采购标的的物理特性，如尺寸、颜色、标志等要求；
(六)采购标的的数量、采购项目交付或执行的时间和地点，以及售后服务要求；
(七)采购标的的验收标准；
(八)采购标的其他技术、服务等要求。

第一章 项目分包

项目简述（本项目不专门面向中小企业采购）：

本项目的供应商来源为公告邀请

编号	包名	采购金额（元）	评审方法
1	第一包	780,000	最低评标价法

询价文件获取方式、时间：

获取时间：详见采购公告　　获取方式： 下载投标工具,安装后联网获取

项目对应的采购意向

意向项目名	涉及的预算金额（元）	采购内容概况	预期采购时间
东安县人民医院网络安全设备更新改造项目	780,000	网络安全设备12台，包括下一代防火墙、IPS、WAF、日志审计、堡垒机、漏洞扫描、上网行为管理、数据库审计系统。要求国产CPU/操作系统/数据库，支持国密算法，具备等保三级认证，三年原厂质保，通过现有核心业务系统兼容性测试。	2026-06

第二章 项目采购需求

包名：第一包 采购金额：780,000元

包概述：东安县人民医院网络安全设备更新改造项目				
评标方法： 最低评标价法	采购文件费：0元	资格合格最少供应商数： 3个	是否接受联合体：否	是否完全面向中小企业： 否
是否接受进口产品：否	资格预审后的合格供应商进入下一阶段投标/响应的数量限定： 不进行资格预审	期望成交供应商数：1个	投标有效期：90个自然日	合同履约保证金：无
合同内容是否可变：是	需求是否可变：否	供应商二次报价的时长限制：供应商不需要二次报价/无时长限制		
本包所属行业：软件和信息技术服务业			本包类型：货物类	
是否设置了核心产品：是	核心产品同品牌供应商的确定中标/成交候选人规则：最低评标价法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，报价低的同品牌投标人获得中标人推荐资格；若同品牌供应商报价恰好相同，采取随机抽取方式确定推荐资格；			
特殊情况下确定成交/中标/入围供应商的约定：本包在评审过程中，若发现中标/成交/入围候选供应商存在报价相同的，约定由评委组长采取随机抽取方式来确定最终中标/成交/入围供应商。				

本包基本资格要求	本包基本资格证明材料上传要求
1.具有独立承担民事责任的能力。 2.参加政府采购前三年内，在经营活动中无重大违法记录，有依法缴纳税收和社会保障资金的良好记录，具有良好的商业信誉和健全的财务会计制度，具有履行合同所必需的设备和专业能力。 3.供应商不得为信用中国网站（www.creditchina.gov.cn）中列入失信被执行人和重大税收违法案件当事人名单的供应商，不得为中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商（处罚决定规定的时间内）。 4.法律、行政法规规定的其他条件。 5.参加开标的是法定代表人（单位负责人）本人，需上传法定代表人（单位负责人）身份证复印件，若不是法定代表人（单位负责人）本人，需提供授权委托书。	1.提供三证合一或五证合一的营业执照扫描件（加盖供应商公章）和法定代表人（单位负责人）身份证复印件（加盖供应商公章）的扫描件，若投标人是自然人的，提供身份证扫描件。具体见下述： （1）投标人为企业的，应提交营业执照或法人登记证书的复印件； （2）投标人为非法人组织的，应提交依法登记证书复印件； （3）投标人为个体工商户的，应提交个体工商户营业执照复印件； （4）投标人为自然人的，应提交自然人的身份证明复印件。 2.投标人提供湖南省政府采购供应商资格承诺函（下载投标工具后获取），须加盖供应商公章（可在模板中填写好后打印出来加盖公章，再拍照或扫描成图片上传）。 3.供应商无需上传证明材料，由评委在www.creditchina.gov.cn和www.ccgp.gov.cn现场联网查验。 4.提供承诺函，承诺：（1）投标供应商与采购人或采购代理机构不存在隶属关系或者其他利害关系；（2）投标供应商与参加本项目的其他供应商不存在控股、关联关系，或者与其他供应商法定代表人（或者负责人）为同一人；（3）投标供应商未为本项目提供过整体设计、规范编制、项目管理、监理、检测等服务（单一来源采购项目除外）；（4）投标供应商未为本项目提供过前款第（3）项所列服务之外的其他采购活动。须加盖供应商公章。 5.下载投标工具后获取，须加盖供应商公章，可在模板中填写好后打印出来加盖公章，再拍照或扫描成图片上传。

以上所有要求提供的资格证明材料，供应商均需在电子投标工具的指定位置上传，不按指定位置上传的，将被视为无效投标。

本包货物类需求

货物类需求特别约定：实质性参数用★标注，重要参数用▲标注，一般参数和不区分类型参数用文字标注。

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
1	入侵防御系统（IPS）(A02010303-入侵防御设备)	是	否	否	套	89,000	2	178,000

本货物共设置了10条参数。

其中：实质性参数：10条。

参数序号	参数类型	参数名	参数值
1	★	入侵防御系统（IPS）	国产CPU，国产操作系统，标准机架式硬件，交流双电，扩展槽位≥2个，USB接口≥2个，RJ45串口≥1个千兆电口≥2个（1*管理，1*热备），≥16G内存，≥128G SSD，硬盘≥4T，电口≥6个，千兆光口≥4个。
2	★	入侵防御系统（IPS）	网络层吞吐量≥15G,应用层吞吐量≥10G,Realworld吞吐量≥1G（适用带宽）,新建连接数≥21W,最大并发连接数≥400W。
3	★	入侵防御系统（IPS）	具有入侵检测防护功能保护弱口令配置、暴力猜测、攻击响应、抗逃逸功能。
4	★	入侵防御系统（IPS）	系统应提供DoS/DDoS攻击防护能力，支持PING、UDP、SYN、ACK、DNS Reply、DNS Req等Flood，支持TCP Port Scan、UDP Port Scan，支持 PING Sweep，支持ARP Spoof以及HTTP GET、HTTP POST FLood等常见的DoS/DDoS的攻击。
5	★	入侵防御系统（IPS）	日志告警内容应至少包括攻击源IP地址、攻击目的IP地址、源端口、目的端口、协议、事件发生时间、威胁类型、攻击手段、威胁级别等。
6	★	入侵防御系统（IPS）	规则应支持双向检测功能，根据双向流量检测攻击，输出检测结果包含正在利用、攻击成功，应支持HTTP请求/响应缓存。
7	★	入侵防御系统（IPS）	支持部署在IPV6，VLAN，QINQ，MPLS，GRE，VXLAN，PPPOE等常见协议封装的环境中，可检测和拦截攻击行为。
8	★	入侵防御系统（IPS）	设备浪涌（冲击）抗扰度性能须符合GB/T17626.5标准要求。
9	★	入侵防御系统（IPS）	所投产品制造商截止投标时间前一周其原创漏洞挖掘数量在“国家信息安全漏洞共享平台（CNVD）”官网公布的企业单位原创积分获得5500分以上，提供官网截图或相关证明材料并加盖供应商公章。
10	★	入侵防御系统（IPS）	提供三年产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
2	防火墙系统（下一代）(A02010301-防火墙)	否	否	否	套	70,000	4	280,000

本货物共设置了8条参数。

其中：实质性参数：8条。

参数序号	参数类型	参数名	参数值

		1	★	防火墙系统（下一代）	国产CPU，国产操作系统，标准机架式硬件，含交流冗余电源，RJ45串口≥1个，RJ45管理口≥1个，USB接口≥2个，电口（Bypass）≥6个,SFP光口（不含光模块）≥4个，接口扩展槽位≥2个，固态硬盘≥256G，机械硬盘≥4T ，≥16G国产内存。
		2	★	防火墙系统（下一代）	整机吞吐量≥12G,应用层吞吐量≥10G,最大并发连接数≥200万,新建连接数≥15万，虚拟防火墙数量≥20。SSL VPN并发用户数≥1000。
		3	★	防火墙系统（下一代）	包含防火墙、流量管理、IPSec VPN、应用管理、入侵防护、URL过滤、防病毒模块。
		4	★	防火墙系统（下一代）	支持虚拟线，二层透明，三层，混合，旁路监听，单臂接入方式。
		5	★	防火墙系统（下一代）	支持对SRv6协议进行过滤、检测及管控。
		6	★	防火墙系统（下一代）	支持基于域名的防火墙策略，一条策略中最多支持同时配置128个域名（支持IPV6），支持通配符格式的域名如*.test.com，最多支持10级域名且层级可配置，系统内置国内外大模型域名站点模板。
		7	★	防火墙系统（下一代）	所投产品需提供中国信息安全测评中心颁发的《国家信息安全测评信息技术产品自主原创测评证书》，提供证书复印件或相关证明材料并加盖供应商公章。
		8	★	防火墙系统（下一代）	提供三年产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
3	WEB应用防护系统（WAF）(A02010399-其他信息安全设备)	否	否	否	套	76,000	1	76,000

本货物共设置了8条参数。

其中：实质性参数：8条。

参数序号	参数类型	参数名	参数值
1	★	WEB应用防护系统（WAF）	国产CPU，国产操作系统，标准机架式硬件，交流冗余电源，USB接口≥2个，RJ45串口≥1个，GE管理口≥2个，千兆电口（带bypass）≥6个，千兆光口（非bypass）≥4个，接口扩展槽位≥2个。硬盘≥4T， SSD固态硬盘≥256G，≥32G国产内存。
2	★	WEB应用防护系统（WAF）	网络层吞吐量≥20G，应用层吞吐量≥3Gbps。最大并发连接数≥45W，每秒新建连接数≥3W。
3	★	WEB应用防护系统（WAF）	支持基于五元组（源IP地址、目的IP地址、源端口、目的端口、协议类型）及接口的网络层访问控制功能。
4	★	WEB应用防护系统（WAF）	支持对注入（包括SQL注入、LDAP注入、XPATH注入及命令行注入）、XSS、SSI指令、路径穿越、远程文件包含、WebShell防护。
5	★	WEB应用防护系统（WAF）	支持透明桥部署，串联部署，路由旁路部署，镜像模式，反向代理模式以及插件式部署模式。
6	★	WEB应用防护系统（WAF）	支持API资产梳理，可基于API流量进行API资产学习，支持API的导入导出。可识别影子API，可查看API列表和API资产详情。支持API攻击防护，包括注入类攻击、滥用事件、敏感信息泄露、协议违背、安全配置错误等，并可查看API安全事件详情。
7	★	WEB应用防护系统（WAF）	软硬一体设备，其中软件功能应具备功能完备性、高可用性、BOT防护、API防护、功能完备性等功能。
8	★	WEB应用防	提供三年产品系统升级授权、提供规则库升级授权、远程支持服务、产品保修服务、硬件故障上

				护系统（WAF）	门支持。

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
4	日志审计系统(A02010399-其他信息安全设备)	否	否	否	套	50,000	1	50,000

本货物共设置了12条参数。

其中：实质性参数：12条。

参数序号	参数类型	参数名	参数值
1	★	日志审计系统	国产CPU，国产操作系统，标准机架式硬件，交流冗余电源，USB接口(USB2.0*1,USB3.0*1)≥2个，RJ45串口≥1个，GE管理口≥1个，千兆SFP插槽≥4个，GE电口≥6个，接口扩展槽位≥2个，≥4TB SATA硬盘，≥256G SSD固态硬盘，≥16G国产内存。
2	★	日志审计系统	可接入日志源数量≥40，支持扩展日志源数量≥300，应支持不低于每秒2000EPS的日志平均处理能力。
3	★	日志审计系统	数据存储能力：支持日志压缩存储，1T存储空间至少可存储200亿条日志。
4	★	日志审计系统	支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s，千亿级日志查询时间小于10s。
5	★	日志审计系统	内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败、暴力破解等，可启用/禁用规则。
6	★	日志审计系统	支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间满足等保要求，可以自定义设置存储时间为1个月、3个月、6个月和永久保存等参数。
7	★	日志审计系统	支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析；支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析。
8	★	日志审计系统	系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。
9	★	日志审计系统	支持将常用IP地址或IP地址网段标记为自定义名称，在日志查询界面可以在IP列中对应悬浮显示自定义名称。
10	★	日志审计系统	所投产品需具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》EAL3+级或以上，提供证书复印件或相关证明材料并供应商加盖公章。
11	★	日志审计系统	数据库审计系统产品制造商应具备中国软件评测中心颁发的“数据安全服务能力评定资格证书-数据安全评估”，提供有效期内的证书复印件或相关证明材料并加盖供应商公章。
12	★	日志审计系统	提供三年产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
5	运维审计系统 （堡垒机）(A02010399-其他信息安全设备)	否	否	否	套	46,000	1	46,000

本货物共设置了8条参数。

其中：实质性参数：8条。

参数序号	参数类型	参数名	参数值
1	★	运维审计系统 （堡垒机）	国产CPU，国产操作系统，标准机架式硬件，交流冗余电源，千兆电口≥10个，combo千兆光电复用口（不含光模块）≥4个，接口扩展槽位≥2个，≥32G EMMC系统盘，机械硬盘≥4T，内存≥16G。
2	★	运维审计系统 （堡垒机）	设备授权管理设备数≥50，最大可扩展管理设备数≥500。字符推荐并发会话数≥800，图形推荐并发会话数≥300。
3	★	运维审计	堡垒机具有用户角色权限自定义功能，可对用户进行细粒度权限划分，可细分用户管理，用户角

			系统（堡垒机）	色管理，资产管理，密码管理、策略管理、审计管理，支持不同角色相互组合。
		4	★	运维审计系统（堡垒机）	支持可通过参数配置开启或关闭字符、图形、文件、数据库等协议的审计范围，但不影响对应协议的基础会话审计。
		5	★	运维审计系统（堡垒机）	支持通过堡垒机直接代理HTTP/HTTPS协议，无需前置机。
		6	★	运维审计系统（堡垒机）	支持提供静态PIN+动态OTP口令认证方式，并支持配置PIN码的有效期、到期提醒、PIN码强度及弱PIN码字典。支持通过电子邮件、短信方式找回密码。
		7	★	运维审计系统（堡垒机）	堡垒机产品为软硬件一体设备，其中软件具备账户安全、认证户端、应用隐藏、零信任SDP远程运维功能，策略、终端合规检测、静态密码认证、动态口令认证、企业微信扫码认证、钉钉扫码认证、属性授权、动态授权、专用运维客，请提供由CNAS认可的第三方检测机构出具的检测报告证明。
		8	★	运维审计系统（堡垒机）	提供三年产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
6	漏洞扫描系统(A02010304-漏洞扫描设备)	否	否	否	套	40,000	1	40,000

本货物共设置了8条参数。

其中：实质性参数：8条。

参数序号	参数类型	参数名	参数值
1	★	漏洞扫描系统	国产CPU，国产操作系统，标准机架式硬件，交流冗余电源，RJ45串口≥1个，GE管理口≥2个，10/100/1000M电口≥4个，千兆SFP插槽≥4个，网卡扩展插槽≥4个，≥32G内存，≥256G固态硬盘，≥4T机械硬盘，标准配置提供≥1路授权扫描端口。
2	★	漏洞扫描系统	最大并发主机数≥50,最大并发任务数≥10，授权可扫描总数量不多于1000个无限制范围的IP地址或域名。
3	★	漏洞扫描系统	云大物扫描模块，对云计算平台、大数据组件、物联网设备提供漏洞检测和分析。
4	★	漏洞扫描系统	支持扫描国产化数据库，包括但不限于达梦、南大通用、人大金仓、神通（ShenTong）、antdb（亚信）、seasql（H3C）、高斯、瀚高（HighGo）、优炫（uxdb）、GoldenDB（ZTE ）等。
5	★	漏洞扫描系统	支持扫描国产化中间东方通、金蝶、宝兰德、中创等。
6	★	漏洞扫描系统	所投产品需具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》EAL3+级或以上，提供证书复印件或相关证明材料并加盖供应商公章。
7	★	漏洞扫描系统	所投产品制造商截止投标时间前一周其原创漏洞挖掘数量在“国家信息安全漏洞共享平台（CNVD）”官网公布的企业单位原创积分获得5500分以上，提供官网截图或相关证明材料并加盖供应商公章。
8	★	漏洞扫描系统	提供三年产品系统升级授权、系统漏洞库升级服务、远程支持服务、产品保修服务、硬件故障上门支持。

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
7	上网行为管理系统(A02010311-网上行为管理设备)	否	否	否	套	35,000	1	35,000

本货物共设置了10条参数。

其中：实质性参数：10条。

参数序号	参数类型	参数名	参数值

1	★	上网行为管理系统	国产CPU，国产操作系统，标准机架式硬件，冗余电源，千兆电口≥10个，千兆Combo接口（光电复用）≥4个，接口扩展槽≥2个，机械硬盘≥1T。		
2	★	上网行为管理系统	网络层吞吐量≥10G，应用层吞吐≥4G，适用带宽≥500M。		
3	★	上网行为管理系统	内置软件Bypass机制，在设备流量异常、突增、异常断电、重启等情况时，可自动切换到Bypass状态，当设备恢复时，可自动切换回工作状态。		
4	★	上网行为管理系统	支持端口镜像功能，可选择入流量、出流量和双向流量等方向，支持将接口的流量镜像到另一个接口，方便网络问题定位。		
5	★	上网行为管理系统	支持资产的主动扫描发现和被动流量识别，获取资产基本信息。支持用户手动新建、导入、导出资产。支持对内网资产的IP、用户、部门、操作系统、重要程度、可用服务进行统一梳理。		
6	★	上网行为管理系统	防私接路由,针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。		
7	★	上网行为管理系统	支持上网行为记录本地留存，方便事后行为回溯，支持将日志记录发送至第三方平台进行数据分析和呈现。		
8	★	上网行为管理系统	支持旁路部署时对违规上网行为进行阻断过滤;支持配置旁路认证策略，请提供由CNAS认可的第三方检测机构出具的检测报告证明。		
9	★	上网行为管理系统	所投产品需具备领先的漏洞监测与挖掘能力，近三年内应获得CNVD颁发的原创漏洞发现突出贡献单位，提供官网截图或相关证明并加盖供应商公章。		
10	★	上网行为管理系统	提供三年产品系统升级授权、上网行为特征库升级授权、系统漏洞库升级服务、远程支持服务、产品保修服务、硬件故障上门支持。		

货物序号	货物名(货物标的)	是否为核心产品	是否强制采购节能产品	是否接受进口产品	单位	单价（元）	数量	小计（元）
8	数据库审计系统(A02010399-其他信息安全设备)	否	否	否	套	75,000	1	75,000

本货物共设置了13条参数。

其中：实质性参数：13条。

参数序号	参数类型	参数名	参数值
1	★	数据库审计系统	国产CPU，国产操作系统，标准机架式硬件，交流冗余电源，USB接口(USB2.0*1,USB3.0*1)≥2个，RJ45串口≥1个，GE管理口≥1个，千兆SFP插槽≥4个，GE电口≥6个，接口扩展槽位≥2个，SATA硬盘≥4TB ，固态硬盘≥256G，内存≥32G。
2	★	数据库审计系统	性能参数：网络层吞吐量≥5000Mbit/秒,SQL语句处理能力≥40000条/秒。
3	★	数据库审计系统	支持系统一键巡检、网络诊断等系统维护功能，支持立即显示当前设备各服务状态信息，并以加密方式导出健康记录，方便排除设备异常原因。
4	★	数据库审计系统	支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。
5	★	数据库审计系统	支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估。
6	★	数据库审计系统	支持敏感信息掩码，用户可以针对邮箱、身份证号、手机号、银行卡号以及自定义信息进行敏感信息掩码配置，防止敏感信息在审计系统中进行泄露。
7	★	数据库审计系统	支持端口重定向审计，在服务器端口变化动态协商为其他端口时同样能精确审计。
8	★	数据库审计系统	支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，降低了存储空间和无用信息的堆砌，白名单内容包括但不限于SQL语句、数据库类型、业务URL地址、数据库名、HTTP访问域等。
9	★	数据库审计系统	支持IPv6网络环境下的数据库审计，可识别IPv6的相关主体与客体资源。
10	★	数据库审计系统	支持通过声光、邮件、短信等方式对审计日志、系统日志进行告警通知。

		11	★	数据库审计系统	所投产品需具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》EAL3+级或以上，提供证书复印件或相关证明材料并加盖供应商公章。
		12	★	数据库审计系统	所投数据库审计系统产品制造商须具备中国软件评测中心颁发的“数据安全服务能力评定资格证书 – 数据安全评估”，提供有效期内的证书复印件或相关证明材料并加盖供应商公章。
		13	★	数据库审计系统	提供三年产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

本包货物类需求的实质性评审(标)规则

货物序号	货物名	参数序号	参数名	是否需要上传证明材料	证明材料类型	上传证明材料的要求
1	入侵防御系统（IPS）	1	入侵防御系统（IPS）	否	无	无
		2	入侵防御系统（IPS）	否	无	无
		3	入侵防御系统（IPS）	否	无	无
		4	入侵防御系统（IPS）	否	无	无
		5	入侵防御系统（IPS）	否	无	无
		6	入侵防御系统（IPS）	否	无	无
		7	入侵防御系统（IPS）	否	无	无
		8	入侵防御系统（IPS）	否	无	无
		9	入侵防御系统（IPS）	是	图片	提供官网截图或相关证明材料并加盖供应商公章
		10	入侵防御系统（IPS）	否	无	无
2	防火墙系统（下一代）	1	防火墙系统（下一代）	否	无	无
		2	防火墙系统（下一代）	否	无	无
		3	防火墙系统（下一	否	无	无

			代）			
		4	防火墙系统（下一代）	否	无	无
		5	防火墙系统（下一代）	否	无	无
		6	防火墙系统（下一代）	否	无	无
		7	防火墙系统（下一代）	是	图片	提供证书复印件或相关证明材料并加盖供应商公章
		8	防火墙系统（下一代）	否	无	无
3	WEB应用防护系统（WAF）	1	WEB应用防护系统（WAF）	否	无	无
		2	WEB应用防护系统（WAF）	否	无	无
		3	WEB应用防护系统（WAF）	否	无	无
		4	WEB应用防护系统（WAF）	否	无	无
		5	WEB应用防护系统（WAF）	否	无	无
		6	WEB应用防护系统（WAF）	否	无	无
		7	WEB应用防护系统（WAF）	否	无	无
		8	WEB应用防护系统（WAF）	否	无	无
4	日志审计系统	1	日志审计系统	否	无	无
		2	日志审计系统	否	无	无
		3	日志审计系统	否	无	无
		4	日志审计系统	否	无	无
		5	日志审计系统	否	无	无
		6	日志审计系统	否	无	无

		7	日志审计系统	否	无	无
		8	日志审计系统	否	无	无
		9	日志审计系统	否	无	无
		10	日志审计系统	是	图片	提供证书复印件或相关证明材料并供应商加盖公章
		11	日志审计系统	是	图片	提供有效期内的证书复印件或相关证明材料并加盖供应商公章
		12	日志审计系统	否	无	无
5	运维审计系统（堡垒机）	1	运维审计系统（堡垒机）	否	无	无
		2	运维审计系统（堡垒机）	否	无	无
		3	运维审计系统（堡垒机）	否	无	无
		4	运维审计系统（堡垒机）	否	无	无
		5	运维审计系统（堡垒机）	否	无	无
		6	运维审计系统（堡垒机）	否	无	无
		7	运维审计系统（堡垒机）	是	图片	请提供由CNAS认可的第三方检测机构出具的检测报告证明。
		8	运维审计系统（堡垒机）	否	无	无
6	漏洞扫描系统	1	漏洞扫描系统	否	无	无
		2	漏洞扫描系统	否	无	无
		3	漏洞扫描系统	否	无	无
		4	漏洞扫描系统	否	无	无

		5	漏洞扫描系统	否	无	无
		6	漏洞扫描系统	是	图片	提供证书复印件或相关证明材料并加盖供应商公章
		7	漏洞扫描系统	是	图片	提供官网截图或相关证明材料并加盖供应商公章
		8	漏洞扫描系统	否	无	无
7	上网行为管理系统	1	上网行为管理系统	否	无	无
		2	上网行为管理系统	否	无	无
		3	上网行为管理系统	否	无	无
		4	上网行为管理系统	否	无	无
		5	上网行为管理系统	否	无	无
		6	上网行为管理系统	否	无	无
		7	上网行为管理系统	否	无	无
		8	上网行为管理系统	是	图片	请提供由CNAS认可的第三方检测机构出具的检测报告证明
		9	上网行为管理系统	是	图片	提供官网截图或相关证明并加盖供应商公章
		10	上网行为管理系统	否	无	无
8	数据库审计系统	1	数据库审计系统	否	无	无
		2	数据库审计系统	否	无	无
		3	数据库审计系统	否	无	无
		4	数据库审计系统	否	无	无
		5	数据库审计系统	否	无	无
		6	数据库审计系统	否	无	无
		7	数据库审计系统	否	无	无
		8	数据库审计系统	否	无	无
		9	数据库审计系统	否	无	无
		10	数据库审计系统	否	无	无
		11	数据库审计系统	是	图片	提供证书复印件或相关证明材料并加盖供应商公章
		12	数据库审	是	图片	提供有效期内的证书复印件或相关证明材料并加盖供应商公章

			计系统			
		13	数据库审计系统	否	无	无

本包其他评审要求

序号	需求名	需求类型	需求描述
1	商务要求	商务	1．产品运输、保险及保管： 1.1中标人负责在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物完好无损安全运达采购单位指定地点，包括装卸及现场搬运等。使用说明书、合格证、随配附件和工具等产品资料一并附于货物包装内。 1.2中标人负责货物在实施地点的保管，直至交货，货物在安装完毕前发生的风险均由中标供应商负责。 1.3中标人负责其派出的项目实施人员、相关管理人员的一切人身和财产安全，采购人不承担任何责任。 2.交货与安装调试： 2.1交货时间：自合同签订生效之日起30日历天完成供货、安装调试。 交货地点：采购人指定地点。 2.2中标人须负责所有设备的安装调试（含采购人原有设备拆卸、更换和位置调整），确保设备和整个系统正常运行。在项目实施过程中须加强项目实施的组织管理,所有施工人员须遵守文明安全施工的有关规章制度，持证上岗。 2.3项目完成后，中标人应将项目有关的全部资料，包括产品资料、技术文档等移交采购人。 2.4 延期交货：中标人如未按照合同规定的时间交货和提供服务，采购人有权从货款中扣除误期赔偿费而不影响合同项下的其它补救方法，赔偿费按每周(一周按七天计算，不足七日按一周计算)赔偿迟交货物的交货价或延期服务的服务费用的百分之零点五(0.5%)计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五(5%)。一旦达到误期赔偿的最高限额，采购人可以终止合同。 3.验收：

			3.1中标供应商交货前应对产品作出全面检查并列出清单，负责安装并培训采购单位的使用操作人员，直到符合技术要求，设备正常运营一个月后，采购单位最终验收。由采购人负责组建验收小组，货物必须由验收小组鉴定是否符合招标项目的验收标准和实际需要，按相关招标文件技术要求提供的性能指标、投标文件响应条款、国家及行业相关标准进行验收，验收费用由中标人承担。 3.2货物产品经过双方检验认可后，签署验收报告，验收报告作为申请付款的凭证之一。 3.3 验收过程中产生纠纷的，由具有相关资质的检测机构检测，如为中标人原因造成的，由中标人承担检测费用；否则，由采购人承担。 3.4项目验收不合格，由中标人返工直至合格，再行验收，由此给采购人造成的损失等费用由中标人承担。连续两次项目验收不合格的，采购人可终止合同，另行按规定选择其他供应商采购，由此带来的一切损失由中标人承担。 4.质量保证： （1）成交供应商必须严格按照磋商文件要求提供符合技术标准的产品，所有的软件产品应为正版软件，并确保该产品知识产权的合法有效性，应保证货物和货物包装完整，到达采购人收货地前未拆封。 （2）成交供应商必须保证所提供的货物（包括零部件）是原装、全新、通过合法渠道取得的产品，并且符合有关检测标准和合同规定的质量、性能、技术规范等的要求以及该产品的出厂标准和原装配置。 （3）成交供应商所提供的货物及服务应符合国家标准或行业标准；这些标准必须是有关机构发布的最新标准。 （4）在质保期内提供设备维护更换，零配件的更换、软件系统升级及技术支持相关服务，相关费用均已包含在投标报价内，采购人不再另行支付。 5.售后服务： （1）严格遵守《产品质量法》，在响应文件中对产品质量保证体系做出说明，并完整地履行质保期内的免费现场维修服务承诺。 （2）提供多种服务方式，通过电话、电子邮件、远程网络协助等方式提供软件系统技术支持；提供7*24小时故障排除服务。 （3）出现紧急情况时，无论是正常工作时间或非正常工作时间，成交供应

			商必须在确认后立即派工程师进行电话支持或远程支持，同时派工程师赴现场提供现场紧急技术支持；成交供应商负责协调电话支持工程师、远程支持工程师和现场支持工程师的工作关系。 （4）成交供应商须在项目验收合格之日起三年内免费提供软件升级维护及技术支持服务，包括性能改善，功能完善，安全性改善等维护等。 （5）在质保期内，及时免费维修、更换有缺陷的货物或部件。如果收到采购人通知后，未在规定的响应时间内赶到现场弥补缺陷，采购人可采取必要的补救措施，但风险和费用全部由成交供应商承担。 6.培训 成交供应商应负责对系统使用方技术人员进行全面培训，确保技术人员能独立进行管理、运行、故障处理及日常测试维护等工作，确保软件系统能正常安全运行。在系统网络运行一段时间后，成交供应商应对系统使用方技术人员进行后续培训，以提高管理、维护人员的技术水准。 7、其他要求 （1）实施方案： 1）信息安全管理要求： （a）根据网信办信息安全要求为我院技术人员提供必要的安全培训，制定必要的培训计划表、安全培训 PPT。 （b）根据网信办信息安全要求帮助用户针对信息安全措施在管理制度分项中结合用户实际工作情况，完善建设对应制度，并辅助用户进行有效的落地实施。 2）安全事件应急响应：在项目期内，提供信息安全应急响应服务，对发生的安全事件必须在指定时间内响应或处理完毕，包括问题事件的恢复、故障原因、事件跟踪。使信息系统和网络系统在最短时间内恢复正常使用。应急响应服务提供包括远程应急响应服务和现场应急响应服务，保证 15 分 钟内响应，4 小时到达现场，8 小时内排除故障。 （2）安全防护及上网管控： 1）根据医院三级等保要求，提供新增防火墙及行为管理的部署配置，需兼容医院现有防火墙和行为管理。

			2）要求与医院现有态势感知系统联动对接，并能直接通过态势感知系统调用防火墙的安全策略实施流量拦截。提供详细的对接方案。 （3）运维安全 1）根据医院网络环境及三级等保要求，提供 VPN 及堡垒机接入配置。 2）要求所有第三方运维通过 VPN 接入，院内所有运维操作接入堡垒机审计。 （4）漏洞扫描 1）支持所有业务系统的漏洞扫描。 （5）技术保障 1）成交供应商须随货物提供随机工具包、必备的配件、完整配套的产品说明及相应的中文技术文件资料（包括货物合格证、操作手册、检测报告等资料）。 2）成交供应商负责现场安装、调试，并提供试运行技术保障服务。 3）成交供应商需在项目现场就硬件及软件的安装、启动、运营、维护对采购人操作人员进行培训，达到熟练掌握产品性能，能及时排除一般故障的程度。 8.结算方法 8.1付款人：东安县人民医院 8.2付款方式和条件：设备到货安装调试运行正常后支付合同总款的30%，设备正常运行一个月后经验收合格支付合同总款的30%，正常使用一年后付合同总款的35%，余款5%作为质量保证金，质保期满后一次性无息付清。 8.3本项目采用费用为包干方式，投标人应根据项目要求和现场情况，详细列明项目所需的设备及配套附件，以及产品运输保险保管、安装调试、试运行测试通过验收、培训、质保期免费保修维护等所有人工、管理、财务等所有费用，如一旦中标，在项目实施中出现任何遗漏，均由中标供应商免费提供，采购人不再支付任何费用。
2	合同	商务	采购人（全称）：东安县人民医院 （甲方） 供应商（全称）： （乙方）

为了保护甲、乙双方合法权益，根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及其他有关法律、法规、规章，双方签订本合同协议书。

1.项目信息

（1）采购项目名称：东安县人民医院网络安全设备更新改造项目

（2）采购计划编号：

（3）项目内容：

2.合同金额

（1）合同金额小写：

大写：

（2）具体标的见附件。

（3）合同价格形式：固定总价合同 。

3.履行合同的时间、地点及方式

起始日期： 。

地点：东安县人民医院。

方式：

4.付款：。

5.解决合同纠纷方式

首先通过双方协商解决，协商解决不成，则通过以下途径之一解决纠纷：向甲方所在地人民法院提起诉讼。

6.组成合同的文件

本协议书与下列文件一起构成合同文件，如下述文件之间有任何抵触、矛盾或歧义,应按以下顺序解释：

（1）在采购或合同履行过程中乙方作出的承诺以及双方协商达成的变更或补充协议

（2）成交通知书

（3）响应文件

			（4）政府采购合同格式条款及其附件 （5）专用合同条款 （6）通用合同条款（如果有） （7）标准、规范及有关技术文件，图纸，已标价工程量清单或预算书（如果有） （8）其他合同文件。 7.合同生效 本合同自_签字生效。 8.合同份数 本合同一式4份，采购人执2份，供应商执2份，均具有同等法律效力。 合同订立时间： 年 月 日 合同订立地点： 甲 方：（公章） 乙 方：（公章） 法定代表人： 法定代表人： 委托代理人： 委托代理人： 电话： 电话： 传 真： 传 真： 开 户 银 行： 帐 号： (注：本章提供的政府采购合同格式为一般格式范本，仅供参考。合同双方可根据项目实际 情况依法签订合同或进行补充修订或依法另行签订补充合同。)

本包其他评审要求的实质性评审(标)规则

序号	需求名	需求类型	是否需要上传证明材料	上传证明材料类型	上传证明材料要求
1	商务要求	商务	否	无	无
2	合同	商务	否	无	无

本包执行的优惠政策

优惠政策	优惠方式	供应商所需出示材料	优惠比例(或分数)	备注
小型、微型企业优惠	总报价减免优惠	提供财政部《政府采购促进中小企业发展管理办法》（财库[2020]46号）中规定格式的《中小企业声明函（货物）》	10%	供应商提供的货物均由小型、微型企业制造，即货物均由小型、微型企业生产且使用该小型、微型企业商号或者注册商标的，享受此优惠；监狱企业、残疾人福利性单位视同小型、微型企业，享受此优惠政策，货物制造商为监狱企业、残疾人福利性单位的，需提供货物制造商的监狱企业/残疾人企业声明函。
节能产品优惠	产品报价减免优惠	提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书复印件。	5%	评标方法为最低评标价法时，节能产品享受产品报价优惠，优惠比例为5%。投标产品同时取得节能产品、环境标志产品认证的，评审时只可享受其中一项优先采购优惠(由投标人自行选择，并在投标文件中填报相关信息及数据)，强制采购节能产品的货物，投标人提供的产品不享受节能产品、环境标志产品优惠。
环境标志产品优惠	产品报价减免优惠	提供国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书复印件。	5%	评标方法为最低评标价法时，环境标志产品享受产品报价优惠，优惠比例为5%。投标产品同时取得节能产品、环境标志产品认证的，评审时只可享受其中一项优先采购优惠(由投标人自行选择，并在投标文件中填报相关信息及数据)，强制采购节能产品的货物，投标人提供的产品不享受节能产品、环境标志产品优惠。

本包【异常低价】的审查规定

政府采购评审中出现下列情形之一的，评审小组应当启动异常低价投标（响应）审查程序：

1.投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值65%的，即投标（响应）报价<全部通过符合性审查供应商投标（响应）报价平均值×65%；
2.投标（响应）报价低于通过符合性审查的次低报价供应商投标（响应）报价65%的，即投标（响应）报价<通过符合性审查的次低报价供应商投标（响应）报价×65%；
3.投标（响应）报价低于采购项目最高限价65%的，即投标（响应）报价<采购项目最高限价×65%；
4.评审小组基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形；

评审小组启动异常低价投标（响应）审查后，属于前述第1项至第4项情形的，应当要求相关供应商

在评审现场合理的时间内对投标（响应）价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等，给予相关供应商的合理时间一般不少于30分钟。

评审小组依据专业经验，参考同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。投标（响应）供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评审小组应当将其作为无效投标（响应）处理