**镇海区政府采购中心**

**关于宁波市镇海区人民医院医疗集团**

**网络安全改造项目**

公开招标文件

项目编号：ZHZFCG2021004G004

项目名称：网络安全改造

采购人：宁波市镇海区人民医院医疗集团

招标人：宁波市镇海区政府采购中心

 2021年1月28日

**目录**

第一章 投标邀请

第二章 招标需求

第三章 投标人须知

第四章 评标方法及评标标准

第五章 镇海区政府采购合同

第六章 投标文件格式

**第一章 关于宁波市镇海区人民医院医疗集团网络安全改造项目的投标邀请**

项目编号：ZHZFCG2021004G004

根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》及镇海区政府采购有关规定，受采购人委托现就宁波市镇海区人民医院医疗集团网络安全改造项目进行公开招标，欢迎合格的投标人前来投标。

**一、采购项目的名称、需求**

1、项目名称：网络安全改造

2、采购需求：网络安全改造，1套，详见招标需求

**二、采购项目预算金额、最高限价**

1、预算金额：人民币40万元

2、最高限价：人民币40万元

**三、采购项目需要落实的政府采购政策**

执行政府采购相关政策。

**四、合格投标人的资格与要求**

1、符合《中华人民共和国政府采购法》第二十二条第一款规定条件；

2、未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

3、特定条件：本项目不接受联合体投标，不允许转包。

**五、招标公告期限、获取招标文件的时间、地点、方式及招标文件售价**

1、公告期限：2021年1月28日至2021年2月4日

2、获取时间：2021年1月28日至2021年2月4日

3、获取地点：政府采购云平台（http://www.zcygov.cn/）

4、获取方式：本项目实行“政府采购云平台”（http://www.zcygov.cn/）网上获取。

（1）根据《浙江省政府采购供应商注册及诚信管理暂行办法》规定，已在“政府采购云平台”（www.zcygov.cn）注册的投标人获取路径：【用户登录】—【项目采购】—【获取采购文件】

（2）未注册投标人获取路径：【商家入驻】—完成政府采购供应商入驻注册—【项目采购】—【获取采购文件】

**请注意注册所需时间。**

注册流程：https://service.zcygov.cn/#/knowledges/cm2eqWwBFdiHxlNd\_otq/w3Cd3GwBFdiHxlNd-BRD

注册咨询电话：400-881-7190

（3）未在规定期限内或未按规定方式获取招标文件的，其投标均视为无效，并不得对招标文件提起质疑投诉。

5、招标文件免费获取。

**六、投标与开标注意事项**

1、本项目实行网上投标，采用电子投标文件。若投标人参与投标，自行承担投标一切费用。

2、标前准备：各投标人应在开标前确保成为浙江政府采购网正式注册入库供应商，并完成CA数字证书办理。（具体操作详见供应商CA申领操作指南https://edu.zcygov.cn/luban/e-biding）。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由投标人自行承担。

3、投标文件制作

（1）应按照本项目招标文件和政采云平台的要求编制、加密并递交投标文件。投标人在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线咨询，咨询电话：400-881-7190。

（2）投标人通过政采云平台电子投标工具制作投标文件，电子投标工具请投标人自行前往浙江省政府采购网下载并安装，（下载网址：http://www.zjzfcg.gov.cn/bidClientTemplate/2019-05-27/12946.html），投标文件制作具体流程详见政采云平台“供应商政府采购项目电子交易操作指南”。

**4、本项目投标人按政采云平台“供应商政府采购项目电子交易操作指南”上传成功后形成的备份电子投标文件（.bfbs格式，文件名应包括本项目编号和投标人名称），在开标前上传至电子邮箱zhzfcggov@163.com，以用于异常情况处理。因备份电子投标文件格式原因未能成功上传政采云系统的均作无效投标处理，一切责任由投标人自行负责。**

**七、投标截止时间和地点**

投标人应于2021年2月26日9时前将电子投标文件上传到政采云平台，并于2021年2月26日9时前，将备份电子投标文件（.bfbs格式）上传至电子邮箱zhzfcggov@163.com。

**八、开标时间及地点**

开标会于2021年2月26日9时在宁波市镇海区骆驼街道金华南路55号三楼开标厅一进行。

开标时间后0.5小时内（2021年2月26日9：30时前）投标人应登录政采云平台，在“项目采购—开标评标”中使用CA证书解密投标文件。若投标人在规定时间内无法解密或解密失败，使用备份电子投标文件（.bfbs格式）进行开标。

**九、采购人的名称、地址和联系方法**

名称：宁波市镇海区人民医院医疗集团

地址：宁波市镇海区骆驼街道南二西路718号

联系方法：0574-86655272

**十、采购代理机构的名称、地址和联系方法**

名称：宁波市镇海区政府采购中心

地址：镇海区骆驼街道金华南路55号E座3楼

联系方法：0574-86276629

**十一、采购项目联系人姓名和电话**

采购单位联系人：张玉龙；联系电话:0574-86655272

宁波市镇海区政府采购中心联系人：唐海忠

联系电话：0574-86276629 传真：0574-86276593

**十二、其他**

1、投标人认为招标文件和采购过程使自己的权益受到损害的，可以自收到招标文件之日或者招标文件公告期限届满之日起七个工作日内，以书面形式向采购人和招标人提出质疑。投标人在法定质疑期内须一次性提出针对同一采购程序环节的质疑。

2、招标人对已发出的招标文件进行必要的澄清或者修改时，将以“公告”的形式分别在“浙江政府采购网”（http://zfcg.czt.zj.gov.cn/）和“宁波政府采购网”（http://www.nbzfcg.cn/）上发布，投标人应及时登录上述网站查看和下载，未及时查看和下载的后果自负。

3、投标人信用信息查询渠道及截止时点：

在2021年1月28日之前，中国政府采购网、浙江省政府采购网、宁波市政府采购网上有不良行为记录的，按不良行为记录的处理规定执行。

**十三、采购监管及投诉受理单位**

宁波市镇海区政府采购管理办公室；

联系人：金国军； 联系电话：0574-89389666

地址：宁波市镇海区骆驼街道民和路569号

2021年1月28日

**第二章** **招标需求**

**一、****采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 技术要求 | 数量 |
| 1 | 态势感知平台 | 详细技术要求见附件 | 1套 |
| 2 | 态势感知探针系统 | 详细技术要求见附件 | 1套 |
| 3 | 项目系统集成 | 详细技术要求见附件 | 1项 |

**二、招标技术参数要求**

**（一）态势感知平台**

|  |  |
| --- | --- |
| **指标项** | **详细技术要求** |
| 硬件架构与性能 | ▲2U标准机架硬件，2\*CPU ≥40线程，内存≥128G，SSD硬盘≥256G，SATA硬盘≥32T，支持RAID，设备具备前面板液晶屏显示设备状况 |
| 6个千兆电口，3个接口扩展槽位，含交流冗余电源模块 |
| 平均处理能力（每秒日志解析能力EPS）：1000EPS数据入库性能（每秒日志解析能力EPS）：1000EPS |
| 数据采集 | 平台应基于大数据基础构架，具备海量数据接入、存储、访问、计算能力 |
| ▲平台应支持内置300+设备日志解析规则查看以及筛选，包括但不限于网络设备（防火墙、交换机、网关）、安全设备（入侵检测设备、WEB攻击防护设备、APT检测设备、防火墙、网络审计、流量探针等）、终端主机日志、数据库等（提供功能截图） |
| 平台应支持ipv4\ipv6、多种协议的数据接入，包括但不限于FTP、SFTP、UDP、TCP、Netflow、本地文件系统、KA\*\*A、JDBC/ODBC |
| 平台应支持外置转发器、转发器内置部署，支持单向光闸场景数据接入及不同网络间的数据采集 |
| 平台应支持界面化配置规范化规则采集第三方日志实现异构日志格式归一化。解析规则支持正则表达式等前置过滤方式及json、kv、csv、正则表达式类型的解析规则，支持界面划取字段配置、多级解析提取嵌套字段、配置规范化规则对解析提取的字段进行字段类型、名称、取值规范化。 |
| 平台应支持采集数据源的界面统计和监控，包括日志源数、已接入日志种类、接收总速率、解析总速率以及数据源纬度限流阈值、数据接收速率、解析速率等，支持查看最近解析失败的原始日志 |
| 平台应支持支持针对采集日志配置数据清洗规则以过滤无业务价值数据（提供功能截图） |
| 威胁检测与分析 | 平台应支持多源异构安全设备、网络设备、全流量设备、终端设备、APT威胁检测设备、漏洞扫描设备、网站安全检测、VPN设备等数据接入与威胁分析，输出可疑威胁事件 |
| 平台应支持规则分析能力，应支持不少于300种内置分析识别规则并支持内置规则的升级，支持用户自定义规则，用户自定义规则可以支持导入导出。 |
| 平台应支持复杂模型的分析能力，应支持DGA、决策树机器学习算法，提供僵尸网络场景、隐蔽信道场景、WebShell场景的检测，并输出相关的可疑事件。 |
| 平台应支持原始日志的查询分析能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP地址、日志类型、来源设备等条件进行查询，并对查询结果提供按时间分段的统计图，查询结果支持列表形式进行展示，支持自定义列表中展示的列，查询结果支持导出为Excel文件。 |
| 平台应支持安全事件的查询分析能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP地址、事件类型、来源设备、威胁等级等条件进行查询， 并对查询结果提供按时间分段的统计图，查询结果以列表形式进行展示，支持自定义列表中展示的列，查询结果支持导出为Excel文件。支持在页面内展示事件详细信息，事件详情包括但不限于：事件摘要、事件关键属性，攻击过程，涉及的攻击者、受害者详情，还包括关联的日志信息、情报信息，并展示攻击者使用的ATT&CK中定义的战术及技术。 |
| 平台应支持按业务系统、网站、终端三种视角的威胁分析能力，支持根据受到的攻击和外发攻击两种维度展示资产相关的事件，并将事件以攻击链阶段统计和展示。 |
| ▲平台应支持对失陷资产进行判定并提供失陷资产的判定依据，包括但不限于失陷资产概要信息、攻击结果、攻击链分布阶段、失陷资产的攻击过程及过程判定依据如攻击特征、流量上下文、关联的告警日志及流量日志以及pcap包下载，并可快速扩展该失陷资产的全部攻击事件以及该失陷资产攻击者发起的攻击、该失陷资产的同类型威胁事件（提供功能截图） |
| 平台应支持简易模式的自定义规则，可支持用户在选择日志类型、设置常见日志类型字段过滤条件之后，即可新建或编辑规则，从而生成事件。（提供功能截图） |
| 平台应支持专家模式的自定义规则，可支持行为分析、多源关联分析、机器学习等多种分析模式，同时可按需自定义生成的事件模版信息如威胁等级、攻击链阶段、事件类型、攻击意图等 |
| 平台应支持主机、应用等弱口令访问行为的检测，弱密码应加密展示且需要管理员的二次独立认证授权后方可查阅明文弱口令。同时支持批量导出弱口令帐号能力以便于弱口令帐号的分发整改（提供功能截图） |
| 平台应支持网络代理软件、自由门软件、无界软件等代理翻墙风险行为的检测 |
| 平台应支持远程控制控制风险行为的检测，如向日葵、TeamViewer、远程连接windows命令行、远程控制工具等（提供功能截图） |
| ▲平台应支持资产外联风险行为的检测，可检测存在外联行为的风险资产，可查看风险资产的IP、访问次数以及外联地域端口等的行为（提供功能截图） |
| 平台应支持POP3、IMAP、SMTP、FTP、TELNET应用帐号的异地登录风险行为检测 |
| 平台应支持对重点事件的标记监控以及对重点事件的攻击结果进行判断，判断攻击成功/失败/未确定 |
| 平台应支持基于全流量数据进行流量纬度的可视化统计，包括流量趋势、应用分布、主机流量、端口访问、境外访问、主机外联、域名访问、DNS请求、高频访问页面、低频访问TOP 10 |
| 平台应支持接入还原的流量包数据，并在关联的流量日志查询页面提供下载。 |
| 资产管理 | 平台应支持多维度资产管理，进行多维度资产视图分析，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图（提供功能截图） |
| 平台应支持对客户给定的互联网IP段或网站域名进行扫描，比对已知网站资产备案情况，及时识别未备案的资产情况 |
| ▲平台应支持资产发现能力，至少具备主动扫描发现资产能力，主动扫描支持联动漏扫设备下发资产扫描策略并上报扫描结果（提供功能截图） |
| 平台应支持资产稽查比对，对于实时发现资产和已有资产库资产比对分析资产新增、变更、减少的情况，变更分析需要细致到资产属性粒度，即可查看具体端口、服务的变化情况；并支持对资产发现结果进行处理，可选择入库或者丢弃 |
| 平台应支持资产的导入/导出、全量备份及恢复能力 |
| 平台应支持“IP+探针ID”的资产识别方式，支持对不同单位监测到的相同内网IP资产进行区分和处理 |
| ▲平台应支持围绕客户的资产树展开风险分析。通过基于资产树的方式对资产进行脆弱性呈现，通过资产数能够快速了解出现高危脆弱性的资产所处位置、所属单位（部门）、负责人等，从而快速定位、快速解决（提供功能截图） |
| 漏洞管理 | ▲平台应支持对重点单位或重点网站的漏洞扫描能力，平台支持向安全采集探针下发系统漏洞扫描任务、网站安全漏洞扫描任务、口令猜测扫描任务，通过平台进行统一扫描任务监控、管理，对扫描结果可以进行可视化呈现（提供功能截图） |
| ▲平台应支持离线漏洞结果数据导入平台进行进一步分析的能力，至少支持绿盟RSAS的离线导入；（提供功能截图） |
| 平台应支持在线下发漏洞扫描任务的能力，应支持灵活的任务策略配置，包括但不限于：调度策略（立即、定时、周期）、扫描设备选择（支持自动/手动指定扫描设备进行漏洞扫描）、漏洞模板策略、登录扫描参数、扫描引擎参数等； |
| 平台应支持对扫描任务进行灵活多样管理的能力，支持扫描任务过程中的进度及状态查看，支持对任务的删除，重扫、查询等操作； |
| 平台应支持对于漏洞扫描任务进行结果展示的能力，包括但不限于：发现的资产列表、漏洞列表、漏洞统计、漏洞分布、脆弱性评分等数据展示 |
| 平台应支持漏洞库管理能力，本地漏洞数应不少于5万，支持漏洞模板自定义和配置模板管理，支持漏洞库升级；（提供功能截图） |
| 平台应支持漏洞扫描结果手动和自动验证能力，可手动选择部分漏洞处置单进行验证扫描，支持漏洞批量处置；（提供功能截图） |
| ▲平台应支持漏洞扫描结果自动生成漏洞处置单的能力，支持对漏洞处置单闭环处理，可设置漏洞处置单状态包括：新增、待修复、已修复、已验证、单次忽略、永久忽略；（提供功能截图） |
| 平台支持对漏洞处置单进行批量处理的能力，可批量设置状态，批量设置责任人，批量添加备注 |
| 平台应支持对漏洞处置单中的每个漏洞情况展示详情的能力，包括扫描验证信息，漏洞描述、漏洞修复建议，漏洞处置耗时信息等，漏洞处置时支持用户添加自定义解决方案，支持添加备注信息； |
| 平台应支持对漏洞处置单的处置过程进行记录的能力，记录应包括：时间、账号、具体操作、备注等信息 |
| 平台应支持对漏洞处置单进行多维度统计，包括资产维度，状态维度，优先级维度统计； |
| 平台应支持对漏洞处置单中的内容进行灵活搜索，支持按照漏洞名称，漏洞等级，漏洞分类，来源，资产名称，资产IP、URL，资产组等维度进行查询； |
| 平台应支持漏洞分析能力，支持通过资产视角浏览不同资产上的漏洞分布情况，描述资产风险并统计不同资产上发生不同危险等级的漏洞数量，也支持通过漏洞视角浏览漏洞在不同资产上的分布情况，监测该漏洞发生的次数和出现在资产上的情况等 |
| 平台应支持漏洞闭环分析可视化展示，包括脆弱性值、脆弱性等级分布、漏洞数趋势、脆弱性值趋势、漏洞类型分布、漏洞TOP、资产脆弱性TOP等； |
| ▲平台应支持漏洞报表功能，可选择生成资产风险报表、系统扫描报表、网站扫描报表、漏洞处置报表、配置核查报表等，为客户撰写安全分析报告提供支撑（提供功能截图） |
| 情报分析 | 平台应支持接入威胁情报，支持在线自动接入和离线手动导入（提供功能截图） |
| 平台应支持多种类型的情报接入，至少包含：ip、url、域名、样本、漏洞、热点事件情报 |
| 平台应支持接入热点事件情报，热点事件情报至少包含：事件名称、事件描述、首次发现时间、最近更新时间、关联的ip列表、关联的url列表、关联的域名列表、关联的样本列表、关联的漏洞列表、其他关联情报信息 |
| 平台应支持接入情报的本地化存储，并记录情报更新历史，情报存储支持千万级情报条目存储能力，界面可以查看本地各类型情报数量以及存储空间占用和更新历史 |
| 平台应提供情报信息的界面查询能力，展示情报的详情信息 |
| 平台应支持自动对安全事件、资产进行情报匹配，支持展示不同类型情报匹配中事件的历史趋势、各类型情报命中事件top条目、攻击链各阶段命中情报事件数目、命中情报事件攻击类型分布、命中情报事件威胁级别分布、高中低各级别漏洞情报匹配资产数目、关联资产数目漏洞情报top条目，对于匹配中情报的事件、资产，能够在相应列表或详情界面下钻到匹配中的情报详情 |
| ▲平台应支持界面查看最新漏洞情报列表以及配置漏洞情报预警，根据漏洞情报信息与平台管理资产进行匹配，匹配中后进行预警，通过邮件等方式发送预警信息。预警信息应包含漏洞情报详情以及影响的资产。漏洞情报预警支持在漏洞情报更新时自动触发，也可手动触发执行（提供功能截图） |
| 平台应支持界面查看热点事件情报以及配置热点情报预警预警，支持界面配置关心的情报关键词和预警邮箱，当收到事件情报更新时自动匹配关键词，如果匹配中，触发预警发送邮件 |
| 态势呈现 | 平台应支持所监测网络安全情况的态势呈现能力，态势呈现包括但不限于综合态势、威胁态势、脆弱性态势、环境感知态势、运维响应态势。（提供功能截图并） |
| 平台应支持从网络风险状况及健康状态纬度对网络的综合风险态势进行量化评估感知及可视化呈现，包括但不限于网络风险综合评分及评分指数、网络健康状态评分以及日志、漏洞、资产、设备接入数，攻击链威胁分布、威胁场景分类统计、攻击意图TOP、资产脆弱性统计和影响资产漏洞TOP、最近重点事件等 |
| 平台应支持对网络内外部威胁态势感知与可视化呈现，包括但不限于外部攻击与外部攻击类型TOP、内部攻击类型TOP、行为分析机器学习以及多源分析的威胁感知事件数、僵木蠕态势的详细分布、网络入侵事件分布、网站安全事件分布以及APT攻击事件TOP等 |
| 平台应支持对网络内资产脆弱性的态势感知与可视化呈现，包括但不限于资产脆弱性TOP、漏洞脆弱性TOP、漏洞情报TOP、服务系统威胁分布、风险等级及漏洞分布趋势和脆弱性趋势、WASC漏洞分布、OWASP-2013漏洞分布等 |
| 平台应支持对网络环境中各元素多方位的态势感知与可视化呈现，包括但不限于资产数量、失陷资产数、业务访问TOP、端口开放端口TOP、应用分布TOP、协议分布TOP、外联国家TOP、设备类型分布、风险帐号TOP及告警来源TOP等 |
| 平台应支持对网络环境中威胁、漏洞、资产各种事件多种运维方式的可视化呈现，包括但不限于人工处置的各类型运维事件的状态统计、数量统计、数据量统计以及任务数统计等（提供功能截图） |
| 安全治理 | ▲平台应支持安全治理能力，能够结合环境数据自动化评估安全治理等级和评分，安全治理等级应包括优、良、待改进三级，总评分应充分结合建设情况指标、运行能力指标、安全态势指标、合规指标等加权计算得到。（提供功能截图） |
| 平台应支持安全态势指标展示，安全态势指标应至少包含威胁指标、隐患指标、事件指标等，支持通过加权计算得到综合指标值。 |
| 权限管理 | 平台应支持权限管理能力，支持对界面菜单功能访问以及平台数据访问进行权限控制 |
| 为保证不同角色人员对平台的友好使用，平台应支持通过角色分离实现三权分立，且至少应包含三类内置角色：系统管理员：负责除日志审计管理外的所有功能；用户：由系统管理员生成，管理其相应业务；审计管理员：负责审计系统管理员和用户的工作 |
| 平台应支持用户管理能力，支持系统管理员在界面查看已创建用户，除顶级域系统管理员，只能查看当前所在域用户账户，可对用户账户进行启停、编辑操作，可创建新用户账户。账户属性应至少包含：用户名、密码、邮箱、电话、所属权限域、角色、所属用户组、登录ip列表、用户首页。其中除了用户名，其他属性支持创建后可编辑 |
| 平台应支持账号操作审计能力，所有账号界面操作记录审计日志，审计员角色账号可查看审计日志，可根据时间范围、登陆ip、登陆用户、操作内容搜索过滤审计日志，支持导出备份审计日志，审计日志不可删除，最长保留至少一年 |
| 多级部署 | 平台应支持多级部署，可向上级平台按需发送数据 |
| 平台应支持通过北向接口向其他平台提供数据外发和查询能力，发送通道包括UDP、FTP/SFTP、KA\*\*A、NPAI等，支持按需限制外发速率 |
| 平台应支持webservice北向接口能力，基于HTTPS的API接口向其他经过token验证的平台发送数据 |
| 事件运维与监控 | 平台应支持对威胁、失陷主机、漏洞等事件进行统一运维处理，提供统一入口 |
| 平台应支持对各类运维事件进行运维处置，包括但不限于提交研判人员进行分析、忽略、误报、处置、优先处理、加入白名单、生成报告、联动封堵设备封堵处置、邮件通报、工单通报等 |
| 平台应支持可视化展示运维事件详情，包括但不限于：事件关键属性如攻击结果、响应码、事件描述处置建议、攻击类型、原目的IP端口等，攻击长镜头、攻击时序过程及攻击载荷、流量上下文、告警日志、关联的会话日志流量日志、情报命中信息以及可快捷扩展调查同类型或者同IP或同资产的相关运维事件，攻击者使用的ATT&CK中定义的战术及技术，处置历史及处置建议等，支持攻击证据如攻击载荷、流量取证PCAP包导出，并支持运维事件详情报告的导出下载 |
| 平台应支持最近1小时、24小时、7天的全局运维事件统计与监控并可按需自定义仪表盘，监控内容包括但不限于各类统计数据如事件、失陷资产、日志、攻击源、情报等，支持重点事件、风险处置监控、攻击源、事件类型、外发事件类型TOP等统计监控，支持资产威胁类型、资产发现、高危资产、资产脆弱性TOP等统计监控；支持漏洞、网站监测事件、脆弱性资产TOP等统计监控 |
| 平台应支持关注的重点资产/资产是否失陷、针对资产的攻击行为的监控，可按照资产名称、攻击链阶段、资产状态等纬度进行筛选过滤（提供功能截图） |
| 平台应支持对关注的IP从攻击者或受害者资产两种维度进行跟踪监控，监控该目标最近的攻击行为，如发生的攻击事件、日志并支持基于相关数据进行目标分析。 |
| 平台应支持基于源目的IP、源目的端口、规则ID、URL等纬度的运维事件白名单的按需定义。 |
| ▲平台应支持将威胁、漏洞、失陷资产等事件以工单的形式通知用户进行工单处理，支持邮件通知（提供功能截图） |
| 平台应支持工单数据的权限管理，所有的运维人员都可查看平台所有工单，可通过责任人是自己来查看自己的工单；仅支持对责任人是自己账号的工单进行操作。 |
| 一键封堵 | ▲平台应支持针对IP、域名、会话进行封堵，支持主机隔离、流量牵引等方式联动设备进行封堵，设备类型包括但不限于防火墙、抗拒绝服务系统、WEB应用防火墙、网络流量探针等（提供功能截图） |
| ▲平台应支持封堵状态获取及查看，支持判断封堵成功、封堵失败、解封成功、解封失败等状态（提供功能截图） |
| 平台应支持对被封堵对象的解封能力，支持配置解封时间，到期自动解除封堵（提供功能截图） |
| 平台应支持插件方式扩展第三方设备，实现对第三方设备的创建、启动、禁止、删除等操作。在第三方设备接口能力具备的情况下支持：域名封堵、IP封堵、会话封堵、流量牵引、主机隔离 |
| 平台应针对不同客户场景，平台应至少支持2类以上旁路部署的封堵设备进行联动封堵，当封堵设备发生故障时，不会影响被监测单位的自身业务 |
| 应用场景 | 可以应用在等保合规、日志审计、攻击检测、响应处置、资产发现、漏洞管理、情报预警、态势感知、安全运营、安全报表等场景使用 |
| 产品资质 | 具备安全管理平台类《计算机信息系统安全专用产品销售许可证》 |
| 具备中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书》 |
| 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+等级证书 |
| 具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》 |
| 公司资质 | 该产品生产厂家应具有对信息安全漏洞研究能力，通过国际 CVE 漏洞库官网，用厂商英文关键字检索漏洞条目不少于 20 个（要求只能用厂商的英文关键字搜索而且搜索关键字内不能包含空格，在应答时必须提供搜索的关键字）。 |
| ▲该产品生产厂家应获得ISO20000服务管理体系认证证书：厂商应通过ISO 20000-1:2011标准认证，且认证范围至少包含向外部客户提供整体安全解决方案，安全软件的设计、开发和运行维护，硬件的运行维护，安全相关的SaaS及运营服务等 |
| ▲产品生产厂商应属于国家互联网应急中心CNCERT网络安全应急服务支撑单位（国家级） |
| 产品生产厂商应是互联网安全研究中心-应用安全联盟成员 |
| 产品生产厂商应是微软MAPP合作伙伴，提供相关证明材料并加盖原厂公章 |
| ▲中国互联网协会反网络病毒联盟 |
| ▲国家信息安全测评信息安全服务资质证书-安全工程类（3级） |
| 国家信息安全测评信息安全服务资质证书-风险评估类2级 |
| CCRC信息安全服务资质认证证书-应急处理（1级） |
| CCRC信息安全服务资质认证证书-风险评估（1级） |
| CCRC信息安全服务资质认证证书-安全集成1级 |
| CCRC信息安全服务资质认证证书-安全运维1级 |

**（二）态势感知探针系统**

|  |  |  |
| --- | --- | --- |
| **指标项** | **参数** | **详细技术要求** |
| **硬件指标** | **基础配置** | 2U,含交流冗余电源模块,8GCF卡,16G内存,6T SATA硬盘,USB\*2,管理口RJ45\*1,RJ45串口\*1,板载1000M电口\*6(3组BYPASS),4个千兆SFP插槽（不含光纤接口模块） |
| **流量采集** | **采集** | 支持IPV4/IPV6流量解析 |
| 支持导入HTTPS证书，对流量进行解密和还原。须提供HTTPS证书功能截图 |
| 支持常见应用的识别不低于3000种 |
| 支持VXLAN、GRE、VLAN流量解析 |
| 支持对DNS、HTTP、FTP、SMTP、POP3、IMAP、SMB、Telnet、LDAP、MYSQL、ORACLE、MSSQL、SSL、TLS、QQ、TCP、UDP、ICMP、SMB、WEBMail等常见协议的深度解析和还原。 |
| 支持对工控和物联网协议的深度解析和还原，常见协议包括MODBUS、GOOSE、MQTT、COAP、S7。须提供界面元数据截图 |
| 支持VPN协议的识别，识别的VPN类型主要包括：open-vpn、ciscovpn、tinyvpn、securityKiss vpn、MS-SSTP、hamachi， remobo（vpn）、Firephoenix vpn、Reduh vpn、rdp2tcp vpn、mult-ip vpn、freenet vpn、realtunnel vpn、swipe vpn、gpass vpn、PacketiX VPN、i2p vpn、tunnelbear vpn、Hotspot Shield vpn、Mobility XE vpn、vtun vpn、Panos Global Protect vpn、Hola Unblocker vpn、ngrok（花生壳）、pagekite、vipnet、psiphon（赛风）vpn、ipsec esp、ipsec esp udp、ipsec ah、ike vpn、Steganos VPN、SSH Tunnel、Cyberghost VPN、Frozenway vpn、vnn vpn、gtunnel、gbridge |
| ▲支持流量白名单，过滤掉不关注资产流量，白名单类型应包括IP、端口、邮箱、域名。须提供功能界面截图 |
| 支持流量灰名单，关注重点资产流量，对命中灰名单的流量进行流量还原和威胁检测。灰名单类型包括IP、端口、IP+端口。 |
| **文件还原** | 支持对流量中出现的文件进行发现和还原，支持还原的协议包括：http、smtp、pop3、imap、ftp、webmail、samba |
| 支持还原的可执行类型：bat、dll、sys、exe、com、src、pif。 |
| 支持还原的文档类型：doc/docx、xls/xlsx、ppt/pptx、pdf、rtf、 wpt、pot、wps、pps、mpp、et、dpt、dps、ett、dot。 |
| 支持还原的压缩包类型：zip、7z、rar、gzip、tar、bz。 |
| 支持还原的网页脚本类型：asp、js、jsp、html、phtml、xhtml、php 、htm、mhtml、 htx、 plg |
| **流量存储** | **元数据存储** | ▲支持对深度解析的协议进行存储，存储日志类型至少包括：会话日志、HTTP日志、EMAIL日志、TELNET日志、认证日志、数据库日志、登录日志、SSL&TLS日志、FTP日志、DNS日志、ICMP日志、文件还原日志、社会账号日志。须提供功能界面截图 |
| **原始pcap包存储** | 支持对实时流量采集的pcap包进行全量存储，供追溯分析和取证使用。 |
| **威胁包存储** | 支持对威胁相关的数据包进行存储，供关联分析和取证使用 |
| **恶意文件存储** | 支持对流量中检测到的恶意文件进行存储，供关联分析和取证使用。 |
| **威胁检测** |  | 在不完整会话的场景下，支持会话乱序重组，支持单向和双向流量检测。 |
| **入侵检测** | 应覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，攻击特征库数量至少为9000种以上。 |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、RDP）的口令暴力破解检测。 |
| 支持常见数据库协议（MySQL、Oracle、MSSQL）的口令暴力破解检测告警，告警信息至少包括爆破告警类型和爆破威胁事件名称。 |
| 支持多种抗逃逸攻击检测，检测类至少包含TCP标志位规避攻击、URL斜线分隔符规避攻击、TCP校验和规避攻击、URL NULL字符分割规避攻击、HTTP长URL规避攻击、HTTP请求伪造参数规避攻击。在告警信息中至少显示规避攻击的类型和规避攻击的事件名称。 |
| 支持基于SCADA等工控协议的相关漏洞攻击检测 |
| **DoS/DDoS** | 支持网络层/应用层DDOS检测和告警 |
| 支持自定义pingFlood、sysflood、udpflood、Pingsweep和arpspoof检测模型，支持配置的参数包括检测阈值、检测周期，提供默认配置。 |
| 支持自定义Dnsreqflood、Dnsreplyflood、httpgetflood和httppostflood检测模型，支持配置的参数包括检测阈值、检测周期，提供默认配置。 |
| **扫描检测** | 支持自定义TCP/UDP端口扫描检测模型，结合模型对流量进行检测和告警。 |
| 支持自定义TCP端口扫描检测模型，支持配置参数包括检测阈值、检测周期，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。 |
| 支持自定义UDP端口扫描检测模型，支持配置参数包括检测阈值、检测周期，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。 |
| **WEB应用检测** | 支持针对主流Web服务器及插件的已知漏洞攻击检测。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等。 |
| 支持爬虫检测，具备对100种以上的爬虫特征进行识别和检测的能力,检测特征至少包括 ：WebInspect、穿山甲扫描、appscan、 burpsuite扫描 、长亭xray社区版扫描、Acunetix Web Vulnerability Scanner、netsparker。 |
| 支持对sql注入、XSS、SSI指令、Webshell、目录遍历、远程文件包含等网络攻击检测。 |
| 支持对WEB服务器上的文件下载进行检测，检测的文件扩展名包括ini、sql、mdf、mdb、prm、conf、htpasswd、backup、bak、old、bash\_history 。 |
| 支持对WEB服务器的慢速攻击检测，能够检测低频的HTTP请求，避免多个请求造成拒绝服务攻击。 |
| 支持对敏感信息进行检测，敏感信息至少包括：身份证号、手机号、银行卡号、信用卡号。 |
| ▲内置WEB应用机器学习检测模型，支持对sqli，xss，exec，phprce，ptravel和jeli攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和告警信息。须提供告警界面信息截图 |
| WEB类告警详情中包含请求和响应信息，在请求和响应信息中能标记规则匹配中的字段信息，便于运维人员快速进行确认攻击事件。须提供告警界面详情截图 |
| **恶意文件检测** | 内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件家族信息和恶意文件变种信息。须提供告警界面信息截图 |
|
| **威胁情报检测** | 支持与威胁情报联动，可进行实时流量匹配检测和告警，支持对恶意IP、恶意域名、恶意URL和恶意文件进行检测。 |
| 支持自定义威胁情报，自定义情报类型包括IP、IP+端口、URI、目的端口+URI、域名、文件 |
| **WEBshell检测** | 内置基于统计学特征和操作码序列训练的检测模型，支持对asp、jsp、php文件类型进行检测和告警 |
| 内置基于webshell通信特点以及流量特征构建决策模型，支持对asp文件、php文件、jsp文件和图片马进行检测和告警 |
| 告警信息至少包括机器学习告警类型和事件名称 |
| **自定义规则检测** | ▲支持自定义规则结合用户业务进行深度检测，自定义内容包括源IP、源端口、目的IP、目的端口、威胁级别、协议、端口和匹配特征(可匹配payload信息)。须提供功能界面截图 |
| **告警白名单** | ▲支持对告警进行一键例外，快速屏蔽掉业务异常告警。须提供功能界面截图 |
| ▲支持自定义告警白名单，自定义类型包括：源IP、源端口、目的IP、目的端口、请求URL和规则ID规则。须提供功能界面截图 |
| **威胁研判** |  | 支持对检测的告警事件(包含入侵检测告警、WEB应用告警、威胁情报告警、恶意文件告警和WEBSHELL告警)结合双向检测机制、元数据、原始数据包和研判模型进行深层次研判给出告警事件的攻击结果：尝试攻击、高可疑攻击、攻击成功、失陷。须提供功能界面截图 |
| **威胁分析** | **流量统计**  | 支持对网络中的流量统计，统计类型包括应用流量的构成和占比、协议的构成和占比和VPN的构成、接口流量统计和接口流量趋势。 |
| **威胁统计** | ▲支持对网络中的威胁进行统计，统计类型包括：攻击者TOP视图、受害者TOP视图、恶意文件TOP视图、威胁事件分布、规则命中TOP视图、资产识别占比视图。须提供功能界面截图 |
| **攻击者分析** | ▲支持从攻击者角度进行分析，对攻击者进行画像，攻击者属性包括地理位置、资产属性、相关账号、攻击手段、攻击详情和行为分析须提供功能界面截图 |
| **受害者分析** | 支持从受害者角度进行分析，对受害者进行画像，受害者属性包括地理位置、资产属性、相关账号、被攻击手段、被攻击详情和行为分析须提供功能界面截图 |
| **回溯分析** | 支持对存储的元数据日志进行快速检索和呈现，检索的日志至少类型包括：TCP&UDP日志、HTTP日志、EMAIL日志、FTP日志、DNS日志、ICMP日志、文件还原日志。须提供功能界面截图和日志截图 |
| **威胁取证** | **原始数据取证** | 支持对采集的全部流量进行存储、检索和下载，检索条件包括源IP、目的IP、源端口、目的端口和起止时间。 |
| **威胁数据取证** | 支持将存储的数据包与告警关联并提供下载便于取证。 |
| **文件取证** | ▲支持将存储的恶意文件与告警关联并提供下载便于取证。须提供功能界面截图 |
| **联动取证** | 提供原始pcap包查询API接口，大数据平台可通过该接口下发查询条件、获取指定pcap包。须提供功能界面截图 |
| **异常行为审计** | **异常访问监测** | ▲支持自定义TCP/UDP行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和事件名称。须提供告警截图(包含告警类型和威胁事件名称) |
| 支持自定义TCP行为模型，配置参数至少包括检测阈值、检测周期、IP对象。须提供功能界面截图 |
| 支持自定义UDP行为模型，配置参数至少包括检测阈值、检测周期、IP对象。须提供功能界面截图 |
| **违规行为监测** | ▲支持对翻墙行为进行检测和告警，告警信息至少包括翻墙时间、使用工具。须提供功能界面截图 |
| 持对违规访问网站进行检测和告警，系统应提供默认违规网站（黄赌毒）并支持自定义违规网站。须提供功能界面截图 |
| **数据异常监测** | ▲支持对常见的数据库协议深度解析，能对相关用户、数据库类型和操作内容进行监测和告警。须提供功能界面截图 |
| **威胁展示** |  | 支持展示威胁告警信息，展示的告警分类包括入侵检测告警、WEB应用告警、恶意文件告警、威胁情报告警和WEBSHELL告警。 |
| 入侵检测告警 | 入侵检测告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、告警类型、事件名称、威胁等级、研判结果、详情。 |
| WEB应用告警 | WEB应用告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、告警类型、事件名称、URI、威胁等级、研判结果、详情。 |
| 恶意文件告警 | 恶意文件告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、传输协议、应用层协议、文件类型、文件名、文件md5、研判结果、详情。 |
| 威胁情报告警 | 威胁情报告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、告警类型、事件名称、命中的威胁情报、研判结果，详情。 |
| WEBshell告警 | WEBSHELL告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、传输协议、应用层协议、文件类型、文件名、文件md5、研判结果、详情。 |
| **响应处置** | **告警处置** | 支持对入侵检测告警、WEB应用告警、威胁情报告警和恶意文件告警中的攻击IP和受害IP发送阻断报文，进行旁路阻断。 |
| **自定义处置** | ▲支持自定义一键封堵，配置策略包括IP、IP范围、会话、域名、生效时间和失效时间。须提供功能界面截图 |
| **联动处置** | ▲支持与大数据平台联动：提供API接口，由大数据平台通过接口下发一键封堵断策略，探针执行封堵动作并将封堵日志信息发送给大数据平台。须提供功能界面截图 |
| **资产管理** | **资产定义** | 支持用户自定义内网资产网段和分组 |
| **资产识别** | ▲支持从流量中自动识别资产信息和归类，识别的信息至少包括资产IP、资产MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。须提供功能界面截图 |
| **资产梳理** | ▲支持人工录入资产维护整体资产库，并支持增删改查。须提供功能界面截图 |
| **资产风险评估** | 支持对资产进行风险评估，结合威胁事件对资产判定为是否失陷。须提供功能界面截图 |
| **联动** | **沙箱联动** | 支持与沙箱进行联动，将未检测出病毒的文件通过接口传给沙箱进行进一步动态行为分析，沙箱分析完成后将结果返回进行统一展示须提供功能界面截图 |
| **大数据平台联动** | 支持将告警日志/元数据外发给第三方平台进行汇总展示和分析，日志传输接口支持syslog、sftp |
| 支持自定义外发告警的类型 |
| 支持导入日志插件，快速满足定制外发标准须提供功能界面截图 |
| 支持与第三方设备联动，支持分布式部署。 |
| **管理功能** | **管理方式** | 系统应提供基于Web的远程GUI管理，可以在任何IP可达地点，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。 |
| **系统监控** | 系统应具备系统运行状态监控功能，能够实时查看CPU使用率、内存使用率、磁盘剩余空间、系统运行时间、接口状态、流量等信息。 |
| **策略配置** | 支持每种协议还原功能的开启/关闭 |
| 支持每种协议文件还原功能的开启/关闭 |
| 支持入侵检测功能开启/关闭 |
| 支持恶意文件检测功能开启/关闭 |
| 支持WEB应用检测功能开启/关闭 |
| 支持情报检测功能开启/关闭 |
| 支持DDOS检测功能开启/关闭 |
| 支持WEBshell检测功能开启/关闭 |
| 支持暴力破解功能开启/关闭 |
| 支持恶意流量存储功能开启/关闭 |
| 支持原始流量存储功能开启/关闭 |
| 支持对每种入侵检测规则检测功能开启/关闭 |
| 支持对每种WEB应用规则检测功能开启/关闭 |
| 支持对自定义规则进行管理配置 |
| 支持对告警白名单进行管理配置 |
| 支持对自定义威胁情报进行管理配置 |
| 支持检测场景配置，场景包括高性能规则策略模板和全面检测规则策略模板 |
| **升级功能** | 系统应提供多种升级方式，至少提供自动在线升级、离线升级两种方式 |
| 投标厂商应承诺至少每周定期升级攻击特征库，遇到重大安全事件，提供即时升级。厂商官方站点需同时提供升级包下载页面，并提供详细的升级事项说明。 |
| **备份** | 支持配置策略的备份，备份数据至少包括全部配置、引擎参数、接口参数和白名单。 |
| 支持备份策略恢复，恢复的类型包括全部配置、引擎参数配置，接口参数配置和白名单配置。 |
| **二次开发** | 具备二次开发能力，支持第三方通过探针的标准接口进行新的业务开发。 |
| **部署能力** | **部署模式** | 系统应支持监听（Monitor），能够快速部署在各种网络环境中。 |
| **网络适应能力** | 系统支持旁路部署，支持IPv4/IPv6环境部署。 |
| **典型应用场景** | **场景** | 可以应用在异常流量审计、回溯分析、未知威胁检测、威胁态势分析、安全运营、数据治理等场景 |
| **产品资质** | **销售许可证** | 销售许可类型-综合型安全审计类 |
| **软件著作权** | 具备计算机软件著作权登记证书 |
| **厂商实力证明** | **厂商资质** | 该产品生产厂家应具有对信息安全漏洞研究能力，通过国际CVE漏洞库官网，用厂商英文关键字检索漏洞条目不少于 20 个（要求只能用厂商的英文关键字搜索而且搜索关键字内不能包含空格，在应答时必须提供搜索的关键字）。 |
| ▲该产品生产厂家应获得ISO20000服务管理体系认证证书：厂商应通过ISO 20000-1:2011标准认证，且认证范围至少包含向外部客户提供整体安全解决方案，安全软件的设计、开发和运行维护，硬件的运行维护，安全相关的SaaS及运营服务等 |
| ▲产品生产厂商应属于国家互联网应急中心CNCERT网络安全应急服务支撑单位（国家级） |
| 产品生产厂商应是互联网安全研究中心-应用安全联盟成员 |
| 产品生产厂商应是微软MAPP合作伙伴，提供相关证明材料并加盖原厂公章 |
| ▲中国互联网协会反网络病毒联盟 |
| ▲国家信息安全测评信息安全服务资质证书-安全工程类（3级） |
| 国家信息安全测评信息安全服务资质证书-风险评估类2级 |
| CCRC信息安全服务资质认证证书-应急处理（1级） |
| CCRC信息安全服务资质认证证书-风险评估（1级） |
| CCRC信息安全服务资质认证证书-安全集成1级 |
| CCRC信息安全服务资质认证证书-安全运维1级 |

**（三）系统集成要求**

|  |  |
| --- | --- |
|  | 详细技术要求 |
| 1 | 完全新增安全设备的安装、调试 |
| 2 | 完成与本次采购设备相关的原有网络设备的安全策略调整，配置调整 |

**三、售后服务要求**

1、免费维护期：质保期不少于3年。

本项目投标方须提供质保承诺函，在设备保修期内，由于质量因素而造成的损坏，均由投标人负责免费维修和更换配件。

2、投标人须按照采购人要求，提供相应技术人员必要的免费现场技术培训服务。

3、投标人须对整个系统至少提供3年的升级更新以及其他的支持服务，并提供永久性7\*24小时技术支持，包括各种系统故障及对各种突发事件采取应急措施等，服务响应时间为3小时。

4、必须满足国家、行业及浙江省地方标准等相关标准规范外。投标人须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由中标人负责，采购人和采购机构不承担任何责任。

5、投标人应遵循采购人各项安全保密制度和规章，在项目改造建设过程和系统运行过程中，投标人所获得的、有关采购人或属于采购人相关的秘密信息，未经采购人同意，不得泄露给任何第三方。

**五、报价要求**

投标报价应包括货款、运输、安装、调试、服务费、维护服务费、税费及其他等一切费用。

本项目为交钥匙工程，包工包料，项目实施所需的一切配件均需投标人提供，费用计入投标报价。。

**六、付款方式及交付事项**

1、付款方式：由采购人和中标人签订合同时约定。

2、交货安装地点：采购人指定的地点。

按国家和招标文件规定标准验收，质量、环保等要求须符合国家规定标准。若有差异，应由投标人承担责任。

★所有货物必须经正规渠道供货，不得提供旧货、水货、假货，最终用户名必须为宁波市镇海区人民医院医疗集团。

3、交货安装时间

本项目要求合同签订后30日内完成系统的终验工作，请投标人细化工作计划。

**七、项目的特殊要求**

★1、根据《浙江省政府采购供应商注册及诚信管理暂行办法》规定，凡参与镇海区政府采购活动的投标人，必须在“**政府采购云平台**”（www.zcygov.cn）或“**浙江政府采购网**”（ http://zfcg.czt.zj.gov.cn/）进行供应商注册登记。

★2、政府采购政策

落实《政府采购促进中小企业发展管理办法》(财库〔2020〕46号)等政府采购政策。

符合《政府采购促进中小企业发展管理办法》(财库〔2020〕46号)规定的中小企业投标人，应提交《中小企业声明函》。

按政府采购政策本项目对小型和微型企业提供货物或服务的价格给予6%的扣除。

★3、现有系统平台提供免费标准化接口，投标人需做出无推诿承诺：承诺在项目实施中与第三方供应商配合完成整体项目及现有软硬件环境的无缝升级改造。

4、投标人必须负责对本项目所有设备及当前原有设备合理利用，配合采购人项目建设进行硬件系统集成工作，解决系统集成中的全部技术问题，对采购人项目建设中碰到的其他技术问题，有责任和义务提供咨询和帮助。

**第三章 投标人须知**

**投标人须知前附表**

|  |  |
| --- | --- |
| 序号 | 内容、要求 |
| 1 | 项目名称：网络安全改造 |
| 2 | 项目编号：ZHZFCG2021004G004 |
| 3 | 采购人式：公开招标 |
| 4 | 采购人：宁波市镇海区人民医院医疗集团联系人：张玉龙联系电话：0574-86655272招标人联系人：唐海忠联系电话：0574-86276629 传真：0574-86276593 |
| 5 | 项目预算价：40万元。最高限价：40万元。付款方式：按招标文件中相关规定。 |
| 6 | 采购内容：网络安全改造，一套。详见第二章招标需求。 |
| ★7 | 投标所提供的货物、服务国家有强制性要求的，投标人应具备相应的资格或资质。 |
| 8 | 本项目为政采云平台电子交易全流程项目。招标文件实行“政府采购云平台”（[http://www.zcygov.cn/）网上获取](http://www.zcygov.cn/%EF%BC%89%E7%BD%91%E4%B8%8A%E8%8E%B7%E5%8F%96%22%20%5Ct%20%22_blank)。 |
| 9 | 投标人成功上传电子投标文件，但无法读取时，方可调用备份电子投标文件，因投标人自身原因导致无法解密的后果自负；若出现投标人上传的电子投标文件和备份电子投标文件均无法读取的情况，则该投标人作无效投标处理。 |
| 10 | 1、本项目实行网上投标，投标人应准备以下投标文件：（1）投标人应在政采云平台上传电子投标文件。（2）符合政采云平台要求的备份电子投标文件，上传至指定电子邮箱，数量1份 。（3）投标文件组成：资信商务文件、技术文件、投标报价文件。2、投标文件的签署、盖章要求等按照招标文件规定。 |
| 11 | 投标截止时间、开标时间及地点：按招标文件中规定。 |
| 12 | 投标人认为招标文件有表述不清晰等疑问的，应在获得招标文件之日或者招标公告期限届满之日七个工作日内提出询问。 |
| 13 | 1、投标人如认为招标文件存在限制性、排他性或者其他违法等内容，使自己权益受到损害的，应在获得招标文件之日或者招标公告期限届满之日七个工作日内提出质疑。质疑书必须按《政府采购质疑和投诉办法》（财政部令第94号）规定。2、投标人在法定质疑期内须一次性提出针对同一采购程序环节的质疑，不符合一次性要求的，对其相应质疑不予答复。3、招标人对已发出的招标文件进行必要的澄清或者修改时，将以“公告”的形式分别在“浙江政府采购网”（http://zfcg.czt.zj.gov.cn/）和“宁波政府采购网”（http://www.nbzfcg.cn/）上发布，投标人应及时登录上述网站查看和下载，未及时查看和下载的后果自负。4、接收质疑书联系人：姚莹联系电话：0574-55886176 传真：0574-86276593 |
| 14 | 1、本项目投标应以人民币报价；2、不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用；3、本项目不收招标代理服务费。 |
| 15 | 现场考察：自行踏勘。 |
| 16 | 除招标文件明确的品牌外，欢迎其他能满足本项目技术需求且性能与所提供品牌相当或优于的产品参加投标。 |
| 17 | 评标方法及标准按招标文件中评标方法及评分标准。 |
| 18 | 本次招标有关信息公告媒体：“浙江政府采购网”（http://zfcg.czt.zj.gov.cn/）和“宁波政府采购网”（http://www.nbzfcg.cn/）请投标人随时关注本项目招标公告发布后，后续可能出现的修改通知、澄清说明、评标结果公告等，如有错过，后果自负。 |
| 19 | 签订合同：按中标通知书的规定。 |
| 20 | 投标文件有效期：六十天。 |
| 21 | 解释：招标文件的解释权属于采购人、招标人。 |

**一、总 则**

**（一）适用范围**

本文件适用于本项目的招标、投标、评标、定标、验收、合同履约、付款等。法律、法规另有规定的，从其规定。

**（二）定义**

1、“采购人”系指提出本次项目采购的单位。

2、“招标人”系指宁波市镇海区政府采购中心。

3、“投标人”系指响应招标、参加投标竞争的法人、其他组织或者自然人。

4、“货物、服务”系指投标人按招标文件规定，须提供的设备、设施、配件、安装、调试、售后服务或项目服务及相关全部内容。

5、“项目”系指招标文件中所采购的货物、服务及相关全部内容。

6、“书面形式”包括信函、传真、电子文档等。

7、“★”系指不允许偏离的实质性要求和条件，不得有正偏离和负偏离。

**（三）招标方式和项目预算价**

1、公开招标。

2、本次项目预算价和最高限价见投标人须知前附表。

**（四）投标委托**

如投标人代表不是法定代表人，还须有法定代表人出具的授权委托书。被授权人不得再授权。

**（五）投标费用**

本项目不收取招标代理服务费。

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用。

**（六）联合体投标要求**

本项目不接受联合体投标。

**（七）转包与分包**

不允许转包。

若允许分包的，投标人在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

★**（八）特别说明**

1、投标人在投标时使用的资格、信誉、荣誉、业绩、企业认证等应当是本法人所拥有，属于投标人母公司（总机构）或者同一母公司下属的其他子公司（同一总机构下属的其他分支机构）的人员、业绩、荣誉、知识产权、项目案例等，一律不予以确认。

2、根据《关于规范政府采购供应商资格设定及资格审查的通知》（浙财采监[2013]24号）规定，金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构以及个体工商户、个人独资企业、合伙企业，如果已经依法办理了工商、税务和社保登记手续，并且获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料，证明其具备实际承担责任的能力和法定的缔结合同能力，允许其独立参加招标投标活动。

3、投标人应仔细阅读招标文件所有内容，按照文件要求提交投标文件等，全面客观地反映自身能力和投标货物技术参数、性能指标或提供服务具体内容等，并对真实性负责。

**（九）质疑和投诉**

1、投标人认为招标过程和中标结果使自己的合法权益受到损害的，应当在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向采购人提出质疑。投标人在法定质疑期内须一次性提出针对同一采购程序环节的质疑，不符合一次性要求的，对其相应质疑不予答复。

2、投标人对采购人的质疑答复不满意或者采购人未在规定时间内作出答复的，可以在答复期满后十五个工作日内向镇海区财政局投诉。

★3、质疑应明确阐述使自己合法权益受到损害的实质性内容，提供相关确凿的事实、证据、来源或线索，及其所依据的有关法律、行政法规、部门规章名称及具体条款的内容，并符合《政府采购质疑和投诉办法》（财政部令第94号）有关规定，便于调查、答复和处理。

**二、招标文件**

**（一）招标文件的构成**

招标文件由以下部分组成：

1、投标邀请

2、招标需求

3、投标人须知

4、评标方法及评标标准

5、镇海区政府采购合同

6、投标文件格式

**（二）投标人的风险**

投标人没有按照招标文件要求提供全部资料、没有对招标文件内容作出全部实质性响应、提供材料有误或表达不清，均是投标人的风险，并可能导致其投标认定为投标无效。

**（三）招标文件的澄清与修改**

1、投标人应认真阅读本招标文件，发现其中有误或有要求不合理的，应在规定期限内以书面形式向采购人提出。

2、采购人对投标人提出的问题在原公告发布网站公告或以书面形式答复所取得招标文件的投标人，其他形式的答复均无效。

3、采购人对已发出的招标文件进行必要澄清、答复、修改或补充的，在招标投标截止时间前十五日在原公告发布网站公告并以书面形式通知所有取得招标文件的投标人。投标人以传真或书面确认答复已收悉，没有确认的，视为默认。

4、招标文件澄清、答复、修改、补充的内容为招标文件组成部分。当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容表述不一致时，以最后发出的文件为准。

**三、投标文件**

**（一）投标文件编制**

投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应。

投标文件内容不完整、内容错误、表述不清、编排混乱等导致投标文件被误读、漏读、解读不一或者查找不到等引起的一切后果由投标人负责。

1、投标文件的形式

投标文件分为电子投标文件和备份电子投标文件。

（1）电子投标文件，按政采云平台“供应商政府采购项目电子交易操作指南”及本项目招标文件要求制作、加密并上传的投标文件。

（2）备份电子投标文件，按政采云平台要求上传成功后形成的备份电子投标文件（.bfbs格式），并上传至指定电子邮箱。

（3）按“投标文件的组成”要求编制而成的投标文件。

投标文件应清晰明确，不得涂改。除投标报价外，若有修改错漏处，须投标人盖印章或者法定代表人、被授权人签字或盖印章。信誉业绩、合同等是复印件的应加盖单位印章。

2、投标文件的效力

投标文件的启用，按先后顺位分别为电子投标文件、备份电子投标文件。在下一顺位的投标文件启用时，前一顺位的投标文件自动失效。

投标文件未按时解密，投标人提供了备份电子投标文件的，以备份电子投标文件作为依据，否则视为投标无效。电子投标文件已按时解密的，备份电子投标文件自动失效。

**（二）投标文件的组成**

投标文件由资信商务文件、技术文件、投标报价文件三部分组成。

1、资信商务文件由资格文件、信誉业绩和商务条款组成。

（1）资格文件：

投标人应符合招标公告中合格投标人的资格与要求，并提供真实的以下证明材料，若提供材料不全、有误或表达不清，可能导致资格无效，责任均由投标人自负。

①法人或者其他组织的营业执照等证明文件，自然人的身份证明；

②投标人声明函、政府采购统计基础信息表；

③法定代表人身份证明书或法定代表人授权委托书；

④最近一个季度财务状况报告、依法缴纳税收完税单和缴纳社会保障资金记录；

⑤具有履行本项目合同所必需的设备和专业技术能力的承诺。

（2）信誉业绩

①具备法律、行政法规规定的信誉、荣誉证书、自主创新、节能环保、认证证书等材料；

②业绩

③参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（债务纠纷、违法违规记录等）；

（3）商务条款

①政府采购合同条款修正条款；

②售后服务措施和承诺给予采购人的各种优惠条件；

③商务响应偏离表。

2、技术文件

（1）技术参数性能指标资料；

（2）技术方案资料；

（3）产品配置资料；

（4）项目整体实施方案情况；

（5）项目人员综合实力情况资料；

（6）产品参数响应情况表；

（7）技术响应偏离表；

（8）技术培训方案资料

（9）其他需提供的技术资料

3、投标报价文件：

（1）开标一览表；

（2）投标报价明细表；

（3）中小企业声明函；

（4）落实政府采购政策的其他材料。

**（三）投标文件的语言及计量**

1、投标人及投标文件与采购人或招标人就有关招投标事宜所有来往函电，除签名、盖章、专用名称等特殊情形外，均应中文汉语书写。投标人因项目实际需提供的外文资料的，应当完整、客观、真实的翻译为中文汉语。中文汉语以外文字表述视同未提供。

2、计量单位，除招标文件有明确规定外，一律采用中华人民共和国法定计量单位，否则视同未响应。

**（四）投标报价**

1、投标以人民币报价，其他币种视同未响应。

★2、投标报价按招标文件提供的格式填写。报价应是履行合同的最终价格，包含税费一切费用。不允许有选择性投标报价。

**（五）投标文件的有效期**

投标有效期从提交投标文件的截止之日起算。投标文件中承诺的投标有效期应当不少于招标文件中载明的投标有效期。

**（六）投标文件的份数、签署、递交和撤回**

1、投标人按招标文件要求编制资信商务文件、技术文件、报价文件。电子投标文件1份，按政采云平台规定进行CA签章，上传至相关模块；备份电子投标文件1份，上传至指定电子邮箱。

★2、投标文件签署要求

（1）投标文件，投标人名称和签名在手写时应书写工整，字迹清晰。

（2）按投标文件（格式）要求位置盖章签署，印章、字迹清晰。要求法定代表人或被授权人签名的，应其本人签署。

3、投标人在投标截止时间之前，可以对已提交的投标文件进行修改或撤回，以书面通知采购人或招标人。修改后重新递交的投标文件应当按招标文件的要求签署、盖章和密封。投标截止时间后，投标人不得修改或撤回投标文件。

4、投标截止时间后一律拒收投标文件。

**四、开标**

**（一）开标准备**

1、采购人或招标人按照相关规定，在招标文件确定的时间、地点主持开标。

2、投标人不足3家的，不得开标。

**（二） 开标程序**

1、宣布开标、评标期间的纪律和有关事项。

2、投标人登录政采云平台，在“项目采购—开标评标”功能模块使用CA证书对电子投标文件进行在线解密。在线解密电子投标文件时间为自开标时间起0.5个小时内。

3、政采云平台系统内开启资信商务文件、技术文件、报价文件，线上公布投标人名称、投标价格。

4、若投标人在规定时间内（自开标时间起0.5个小时内）无法解密或解密失败，使用备份电子投标文件（.bfbs格式）进行开标。

投标人成功上传电子投标文件，但无法读取时，方可调用备份电子投标文件。

5、开标过程由采购人或者招标人负责记录。

6、投标人代表对开标过程和开标记录有疑义，以及认为采购人、招标人相关工作人员有需要回避的情形的，应在线提出询问或者回避申请。采购人、招标人对投标人代表提出的询问或者回避申请应当及时处理。

**（三）开标异常情况处理**

本项目采用政采云电子化开标及评审程序，但有下列情形之一的，按以下规定处理：

1、若投标人在规定时间内无法解密或解密失败，政府采购中心将开启投标人递交的备份电子投标文件，上传至政采云平台项目采购模块，以完成开标，CA加密的电子投标文件自动失效。

2、若出现投标人的电子投标文件和备份电子投标文件都无法读取的情况，则该投标人作无效投标处理。

3、采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，政府采购中心可中止电子交易活动：

（1）电子交易平台发生故障而无法登录访问的；

（2）电子交易平台应用或数据库出现错误，不能进行正常操作的；

（3）电子交易平台发现严重安全漏洞，有潜在泄密危险的；

（4）病毒发作导致不能进行正常操作的；

（5）其他无法保证电子交易的公平、公正和安全的情况。

 出现前款规定情形，不影响采购公平、公正性的，政府采购中心可以待上述情形消除后继续组织电子交易活动。

**五、资格审查**

1、开标后，采购人或招标人按照招标文件的要求，对投标人提供的资信商务文件中资格文件进行资格审查，确定合格投标人。

2、经审查，合格投标人大于三家的，进入评标程序环节。合格投标人不足三家的，不得评标。

**六、评标**

**（一）评标委员会组成**

评标委员会按政府采购法和政府采购有关规定组成。

**（二）评标的方式与原则**

按照政府采购的法律法规、招标文件、评标方法及评分标准对投标文件进行评审，投标文件以外的补充、纠正、佐证等一概不予认可，依法进行澄清、说明、纠正除外。

评标委员会应遵循公平、公正、客观的原则，按招标文件中规定的评标标准、方法和中标条件进行评标、定标。

评标委员会及有关工作人员不得私下与投标人接触。不向外界透露任何与评标有关的内容。

任何单位和个人不得干扰、影响评标工作的正常进行。

**（三）评标程序**

1、评标委员会对资格审查合格的投标人进行符合性审查。依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查,以确定是否对招标文件的实质性要求作出响应。

2、通过符合性审查合格投标人不少于3家的，评标委员会按照招标文件中规定进行评审。投标文件中的存在含义不明确、同类事件表述不一致或者有明显笔误、小数点移位、计算错误等问题，评标委员会可以要求投标人作出必要的澄清、说明或者纠正。投标人的澄清、说明或者补正应当采用书面形式，其内容不得超出投标文件的范围或者改变投标文件的实质性内容，并由法定代表人或被授权人签字。投标人代表未能作出澄清、说明、纠正的，投标人拒绝澄清、说明、者纠正的，投标人澄清、说明、纠正的内容改变了投标文件实质性内容的，评标委员会有权对该投标文件作出不利于投标人的评判。

3、评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，将要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，投标将作为无效投标处理。

4、评标委员会按照招标文件中规定对符合性审查合格的投标文件评审后，依据评标方法和标准对资信商务、技术和价格综合评估比较与评价。

5、评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告，按得分由高到低顺序推荐（确定）中标候选人。

**（四）错误修正原则**

开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准。

大写金额和小写金额不一致的，以大写金额为准。

单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价。

总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

不同文字投标文件的解释发生异议时，以中文文本和法定计量标准为准。

按上述要求修正错误后投标人不同意的可书面提出意见，但其投标文件作为无效投标处理。

投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

**（五）****投标无效的情形**

实质上没有响应招标文件要求的投标被视为无效投标。投标人不得通过对投标文件修正、撤消不符合要求的条款或通过投标文件以外的补充、纠正、佐证等，使其投标成为实质上响应的投标，依法进行澄清、说明、纠正除外。

1、有下列情形之一的，投标文件将被视为无效投标：

（1）投标文件未按照招标文件规定要求签署、盖章的；

（2）不具备招标文件中规定资格要求的或未通过资格审查的；

（3）投标超出经营范围且不能证明履约能力的；

（4）投标文件格式项目不齐全、意思表述不明确、前后矛盾、使用文字、计量单位不符合招标文件要求的（评标委员会认定为笔误、小数点移位等，允许其当场更正的除外）；

（5）投标文件的关键内容字迹模糊、无法辨认的或者投标文件中经修正的内容字迹模糊难以辨认或者修改处未按规定签名盖章的；

（6）对招标文件中标有“★”条款发生正或负偏离的。

（7）未在规定期限内或未按规定方式获取招标文件的。

（8）投标人未在规定期限内在政采云平台成功上传电子投标文件的。

（9）投标人上传的电子投标文件和备份电子投标文件均无法读取的。

2、在资信商务、技术评审时，有下列情形之一的，投标文件将被视为无效投标：

（1）未提供或未如实提供投标货物或服务的技术参数，或者投标文件标明的响应或偏离与事实不符或虚假的；

（2）明显不符合招标文件标明的技术指标、质量标准的;

（3）允许偏离的技术、性能指标，偏离项或值超过招标文件规定的；

（4）投标技术方案不明确，存在二个或二个以上备选（替代）投标方案且未注明哪个有效的；

（5）擅自改变招标文件要求或者投标文件有招标人不能接受的附加条件的；

（6）对招标文件中标有“★”的条款发生正或负偏离的。

3、在价格评审时，有下列情形之一的，投标文件将被视为无效投标：

（1）未采用人民币或未按照招标文件标明币种报价的；

（2）报价超出采购最高限价，采购人不能支付的；

（3）具有选择性投标报价的。

★4、法律法规或招标文件明确规定应作为无效投标的。

**（六）评标过程的保密**

采用不公开方式评标。凡是属于审查、澄清、评审和比较的有关资料以及授标建议，任何人均不得向投标人或其他无关的人员透露。投标人在评标过程中，所进行的力图影响评标结果的不公正活动，可能导致其投标被拒绝。

**七、定标**

评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告。采购人按照评标报告中推荐的中标候选人顺序确定中标人或授权评标委员会确定中标人。中标人确定后，中标公告发布在“浙江政府采购网”（http://zfcg.czt.zj.gov.cn/）和“宁波政府采购网”（http://www.nbzfcg.cn/）, 不再另行书面通知参与本项目的所有投标人。

**八、****合同授予**

**（一）签订合同**

1、中标人收到中标通知书后及时与采购人签订合同，所签订的合同不得对招标文件和投标文件作实质性修改。

2、自合同签订之日起七个工作日内，及时将合同上传至政采云平台。

**（二）履约保证**

1、签订合同前，中标人同采购人商定交纳履约保证金的方式等。

2、应按合同约定认真履行规定的义务，如不按合同的约定履约，违约方应承担违约责任。

3、合同履行完毕后五个工作日内退还履约保证金。

**第四章 评标方法及评标标准**

**一、总则**

本评标方法及评分标准仅适用本项目对资格性检查和符合性检查合格的投标文件进行资信商务和技术评估，综合比较与评价。在评标中，不得改变招标文件中规定的评标标准、方法和中标条件。

**二、评标办法**

评标采用综合评分法，总分为100分，由价格分、技术分、资信商务分等组成。对已通过资格性检查和符合性检查的合格投标文件进行资信商务、技术、报价等评估，综合比较与评价。评标总分为各项得分的汇总（总分=价格分+技术分+资信商务分）。按总分由高到低顺序排列，相同的，按投标报价由低到高顺序排列；投标报价也相同的，按技术得分由高到低顺序排列。评分过程中采用四舍五入法并保留小数二位。

三、评标内容及标准

（一）价格分（A=30分）

采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价并得价格分A分，其他投标人的价格分按下列公式计算：价格分=（评标基准价/投标报价）×A%×100。

按政府采购政策本项目对小型和微型企业提供货物或服务的价格给予6%的扣除，以调整后的价格计算评标基准价和投标报价。

投标人的报价均超过招标上限价，采购人不能支付的，本次招标失败。

（二）技术（B=45分）、资信商务（C=25分）按照评标委员会成员的独立评分结果汇总。计算公式：投标人的技术、资信商务分=（评标委员会所有成员评分合计数）/（评标委员会组成人员数）。

1、技术分（B=45分）

|  |  |
| --- | --- |
| 技术分45分 | 技术参数性能指标：标注“▲”的技术指标为负偏离的，每条扣2分，扣完为止。满分20分（须提供相关技术证明材料的复印件并加盖投标人公章；低于招标要求或未按照要求提供响应的视为负偏离） |
| 根据投标方案与需求的吻合程度以及在本项目中的建设优势，包括方案技术架构的先进性、成熟性，业务流程的合理性，充分满足用户当前和未来发展的使用需求情况，进行综合评分。满分15分 |
| 根据投标人提供的项目实施方案的完整性、先进性、合理性进行评分。满分7分 |
| 项目实施团队的成员具有信息系统项目管理师等中高级职称的技术人员，每有一名得1分，最高得3分。（须提供相关资格证明和社保部门出具的在投标单位近半年内缴纳社会保险有效证明复印件，不提供不得分） |

2、资信商务分（C=25分）

|  |  |
| --- | --- |
| 资信商务分25分 | 售后维护方案及承诺：有完整、可行、合理的售后维护措施、服务保障及服务反馈。满分8分。 |
| 投标人售后服务体系的完善性，与本项目实施地点的距离及响应时间、速度情况，售后维护人员的投入情况等进行综合评分。满分5分。 |
| 技术培训方案、计划的可行性及合理性等酌情评分。满分5分。 |
| 投标人近三年内具有相关类似案例，一个得1分，最高得3分。（提供完整合同复印件并加盖投标人公章，否则不得分） |
| 政策性因素加分：投标产品为节能产品，提供有效期内节能产品认证证书的，得1分；投标产品为环境标志产品，提供有效期内环境标志产品认证证书的，得1分。（提供证书复印件并加盖投标人公章）满分2分。 |
| 投标文件编制质量进行评分，2分。 |

**第五章 镇海区政府采购合同（格式）**

项目编号：

合同编号：

采购人（甲方）：

供应商（乙方）：

 根据 项目的采购结果，经双方协商签署本合同。

**一、服务内容**

**二、质量要求、技术标准、乙方对质量负责的条件和期限及售后服务的承诺**

1、乙方应按招标文件规定的技术要求、质量标准向甲方提供服务。

2、乙方应保证所提供的服务任何一部分均不会侵犯任何第三方的知识产权。

3、乙方没有甲方事先书面同意，不得将由甲方提供的有关合同或任何合同条文或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

**三、服务期限和服务地点**

1、期限 年，从 年 月 日至 年 月 日。

2、服务地点：

**四、结算方式及期限**

1、付款方式及期限：

**五、不可抗力事件处理**

1、在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2、不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3、不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

**六、解决合同纠纷方式**

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向合同签订地法院起诉，合同签订地在此约定为镇海区。

**七、合同生效及其它约定事项**

1、合同经双方法定代表人或授权委托代理人签字并加盖单位公章后生效。

2、合同执行中涉及采购资金和采购内容修改或补充的，须经区财政部门审批，并签书面补充协议报镇海区政府采购管理办公室备案。

3、本合同执行中相关的税费均由各方自理。

4、其他约定:

5、乙方交纳合同总金额人民币的 %即 元作为本合同的履约保证金，履约完毕甲方应全额无息退还乙方。

6、本合同正本一式两份，具有同等法律效力，甲乙双方各执一份；合同签订完成后同时上传至政采云平台。

甲方（章）： 乙方（章）：

地址： 地址：

法定代表人： 法定代表人：

委托代理人： 委托代理人：

电话： 电话：

电传： 电传：

开户银行： 开户银行：

帐号： 帐号：

邮政编码： 邮政编码：

签订地点： 签订日期： 年 月 日

**第六章 投标文件格式**

 **一、资信商务文件格式**

1、资信商务文件封面格式：

 **项目资信商务文件**

项目名称：

项目编号：

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

2、资信商务文件目录

（1）资格文件

①法人或者其他组织的营业执照等证明文件，自然人的身份证明；

②投标人声明函、政府采购统计基础信息表；

③法定代表人身份证明书或法定代表人授权委托书；

④最近一个季度财务状况报告、依法缴纳税收完税单和缴纳社会保障资金记录；

⑤具有履行本项目合同所必需的设备和专业技术能力的承诺。

（2）信誉业绩

①具备法律、行政法规规定的信誉、荣誉证书、自主创新、节能环保、认证证书等材料；

②业绩

③参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（债务纠纷、违法违规记录等）；

（3）商务条款

①政府采购合同条款修正条款；

②售后服务措施和承诺给予采购人的各种优惠条件；

③商务响应偏离表。

格式：

**法人或者其他组织的营业执照**

（复印件的加盖单位公章，自然人签字）

项目名称：

项目编号：

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**投标人声明函**

采购人、镇海区政府采购中心：

 （投标人名称）系中华人民共和国合法企业，经营地址 ，自愿参加 项目的投标，为便于贵方公正、择优地确定投标人及其投标产品和服务，就本次投标有关事项郑重声明如下：

1、向贵方提交的所有投标文件、资料都是准确和真实。

2、我单位不是采购人的附属机构；也没有与采购人聘请的提供咨询服务的公司及其附属机构任何联系或利益关系。

3、根据财政部《政府采购促进中小企业发展管理办法》和宁波市财政局《关于政府采购促进中小企业发展若干问题的通知》的规定，本单位按《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》划分标准属（大型、中型、小型、微型）企业，其中所属行业为 ，上年末从业人员 人，上年营业收入 万元、上年资产总额 万元。

4、我单位投标的 项目 标项市场平均成交价格为 万元，我单位投标价格为 万元，由本单位提供服务金额 万元。

5、我单位已详细审查全部“招标文件”，包括修改文件（如有的话）以及全部参考资料和有关附件，现按规定提交资信商务文件、技术文件、报价文件。

6、本投标有效期自开标日起 个日历天。

7、与本投标有关的一切正式往来信函请寄：

地址：

邮编： 电话： 传真：

投标人全称（盖章）：

法定代表人（签名）： 年　 月　 日

说明：

1、根据工信部联企业[2011]300号文件。企业行业分为：农林牧渔业，工业（包括采矿业、制造业、电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，有物业管理，租赁和商务服务业，其他未列明行业（包括科学研究和技术服务业、水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。一般研发、生产、加工型企业填写工业，销售、贸易型企业填写批发，具体行业划分依据国家统计局网站公布的《国民经济行业分类》标准规定。

2、宁波政府采购网注册的供应商须根据上年财务报表等，登录进入供应商平台“供应商账户管理”、“单位信息”模块，对照前款说明，可选择修改“所属行业”，如实填写修改上年末从业人员 人、上年营业收入万元、上年资产总额万元等数据，重新点击会自动显示修改后企业划型信息。

3、有多个标项的，须按每个标标分别填写，无此分类货物金额的应填“零”。

4、如联合体投标的，由联合体牵头方提供本表。

格式：

**政府采购统计基础信息表**

|  |  |  |  |
| --- | --- | --- | --- |
| 采购人 |  | 采购金额 |  |
| 项目名称 |  | 中标金额 |  |
| 是否专门面向中小企业 |  |
| ★以下内容由投标人按实填写，如有虚假，经查实一律记入不良信誉名单。 |
| 投标人名称 |  |
| 投标金额 | 其中： |
| 企业注册地 | 宁波市内（ ） 宁波市外（ ） |
| 企业类别 | 国内企业（ ）中外企业（ ）外资企业（ ） |
| 企业类型 | 大型（ ）中型（ ）小型（ ）微型（ ） |
| 投标的货物是否本企业制造 | 是（ ）否（ ） |
| 投标的工程或服务是否本企业承担 | 是（ ）否（ ） |
| 投标的货物原产地是否在中国境内 | 是（ ）否（ ） |
| 投标的货物原产地是否在宁波 | 是（ ）否（ ） |
| 投标的货物是否节能清单产品 | 是（ ）否（ ） |
| 投标的货物是否环境标志清单产品 | 是（ ）否（ ） |
| 投标的货物是否《宁波市自主创新产品与优质产品目录》内产品 | 是（ ）否（ ） |

投标人全称（盖章）：

法定代表人或被授权人（签名）： 年 月 日

格式：

**法定代表人身份证明书**

×××在我 (单位名称)担任 职务，系我 (单位名称)的法定代表人。

特此证明。

附：法定代表人联系地址：

     联系电话：

身份证正反面复印件：

年 月 日

 (公章)

格式：

**法定代表人授权委托书**

采购人、镇海区政府采购中心：

我 （姓名）系 （投标人名称）的法定代表人，现授权委托 （姓名）以我方的名义参加 单位 项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约、询问质疑等具体事务和签署相关文件。

我方对被授权人的签名负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤销而失效。

被授权人无转委托权，特此委托。

被授权人签名：

被授权人身份证号码：

（须附身份证正反面复印件）

被授权人联系电话：

投标人全称（盖章）：

法定代表人（签名）：

 年 月 日

格式：

**最近一个季度财务状况报告、依法缴纳税收完税单和缴纳社会保障资金记录**

（复印件的加盖单位公章，自然人签字）

格式：

**具有履行本项目合同所必需的设备和专业技术能力的承诺**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**具备法律、行政法规规定的信誉、荣誉证书、自主创新、节能环保、认证证书等材料**

（复印件的加盖单位公章，自然人签字）

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**业绩**

（复印件的加盖单位公章，自然人签字）

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（债务纠纷违法违规记录等）**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**政府采购合同条款修正条款**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**售后服务措施和承诺给予采购人的各种优惠条件**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**商务响应偏离表**

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 招标文件要求 | 是否响应 | 投标人承诺或说明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

**二、技术文件格式**

1、技术文件封面格式：

 **技术文件**

项目名称：

项目编号：

投标人全称（盖章）：

法定代表人或被授权人（签名）：

年 月 日

2、技术文件目录

（1）技术参数性能指标资料；

（2）技术方案资料；

（3）产品配置资料；

（4）项目整体实施方案情况；

（5）项目人员综合实力情况资料；

（6）产品参数响应情况表；

（7）技术响应偏离表；

（8）技术培训方案资料

（9）其他需提供的技术资料

格式：

**技术参数性能指标资料**

项目名称：

项目编号：

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 　年　 月　 日

格式：

**技术方案资料**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

格式：

**产品配置资料**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

格式：

**项目整体实施方案情况**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

格式：

**项目人员综合实力情况资料**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

格式：

**产品参数响应情况表**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

格式：

**技术响应偏离表**

|  |  |  |  |
| --- | --- | --- | --- |
| 招标文件要求 | 投标文件响应 | 偏离情况 | 说明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：投标人应根据投标的实际性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

格式：

**技术培训方案资料**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

格式：

**其他需提供的技术资料**

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

**三、报价文件格式**

1、报价文件封面格式：

 **项目报价文件**

项目名称：

项目编号：

投标人全称（盖章）：

法定代表人或被授权人（签名）：

 年 月 日

2、报价文件目录

（1）开标一览表；

（2）投标报价明细表；

（3）中小企业声明函；

（4）落实政府采购政策的其他材料。

格式：

**开标一览表**

项目名称：网络安全改造

项目编号：ZHZFCG2021004G004 单位：元

|  |  |  |
| --- | --- | --- |
| 内容 | 数量及单位 | 投标报价 |
| 网络安全改造 | 一套 |  |
|  |  |  |
| 投标合计报价（大写）： |  |

注: 1、报价有涂改的，作无效标处理。

2、投标合计报价应包括货款、运输、安装、调试、服务费、维护服务费、税费及其他等一切费用。

投标人全称（盖章）：

法定代表人（签名）：

 年 月 日

格式：

**投标报价明细表**（格式）

项目名称：

项目编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 规格型号  | 数量及单位 | 单价 | 金额 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| 11 |  |  |  |  |  |
| 12 |  |  |  |  |  |
| 13 |  |  |  |  |  |
| 合计金额： ￥  |

注：合计金额应与开标一览表合计金额一致。

投标人全称（盖章）：

法定代表人（签名）： 年 月 日

格式：

**中小企业声明函（货物）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库[2020]46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1、（标的名称），属于（采购人文件中明确的所属行业）行业；制造商为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元1，属于（中型企业、小型企业、微型企业）；

2、（标的名称），属于（采购人文件中明确的所属行业）行业；制造商为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与打企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

1从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

格式：

**落实政府采购政策的其他材料**

投标人全称（盖章）：

法定代表人（签名）：

 年 月 日