**附件1：**

**报 价 函**

江苏省广电有线信息网络股份有限公司盐城分公司：

我方已仔细研究了贵公司“YC-CGXQD-2023078”江苏有线盐城分公司智慧乡镇网络及安全监管平台建设项目”询价公告，我方愿意以：人民币大写 （￥： ）的报价，在工期 个日历日内，完成贵公司所采购的江苏有线盐城分公司购置智慧乡镇网络及安全监管平台建设并提供后续售后服务，详细配置及单价见下表：

报价：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **类别** | **品牌及型号** | **数量** | **单价** | **合计** | **质保期** | **备注/说明** |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |  |
|  | 合计 |  |  |  |  |  |  |

报价人：（盖单位公章）

法定代表人及其委托代理人：（签字）

地址：

电话：

年 月 日

**投标授权函**

本授权委托书声明：我 （姓名）系 （投标人名称）的法定代表人，现授权委托 （单位名称）的 （姓名）为我单位的代理人，以本单位的名义参加 （招标人名称）的 服务项目的投标活动。代理人在开标、评标、合同谈判过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。代理人无转委托权。

特此委托。

代理人姓名： 性别： 身份证号码：

电话： 传真： 手机：

投标人（盖章）：

法定代表人（签字或盖章）：

**法定代表人及委托代理人身份证复印件粘贴处：**

**投标承诺函**

江苏省广电有线信息网络股份有限公司盐城分公司：

1、根据已收到的 询价文件，我单位经研究贵方的询价文件后，决定无保留地接受谈判文件所有条款，愿以：人民币大写 （￥： ），在工期 个日历日内，承担本招标范围内的全部内容，并将按询价文件的规定履行合同责任和义务。

2、一旦我方中标，我方保证在按招标文件约定时间内完成全部工作内容。

3、我方保证设备质量达到询价文件约定的要求 。

4、本次投标，我方将派出 （项目负责人姓名）作为本项目的项目负责人。

5、我方保证：严格遵守《盐城市市场廉政准入规定（试行）》的各项规定。我方响应文件提供的所有资料真实、有效，如有不实，我方将放弃中标的权利，并承担由此产生的责任。

6、我方同意所提交的响应文件中规定的投标有效期内有效，在此期间如果中标，我方将受此约束。严格遵守国家法律、法规及江苏省、盐城市现行招投标管理的规定，如有违反，贵方有权取消我方的投标资格，同时我方愿意接受相关部门的处理。

7、你方的中标通知书和本响应文件将成为约束双方的合同文件的组成部分。

投标人： （盖章）

单位地址：

法定代表人或其委托代理人： （签字或盖章）

日期 年 月 日

**质保期承诺书**

致：江苏省广电有线信息网络股份有限公司盐城分公司：

我单位郑重承诺：如我单位中标，满足询价文件要求：

1. 合同货物的质保期为现场验收合格起算，设备质保期 年；
2. 我方保证提供的合同货物是全新的，未使用的；
3. 我方保证合同货物在正确安装，正确操作情况下，运行安全、可靠；
4. 中标价含现场安装调试及本地现场售后服务；
5. 我方保证在接到贵单位售后电话后，30分钟内响应，2小时内到达现场，4小时内解决问题；
6. 我方保证合同货物的质量及各项技术标准完全满足采购人规定的质量、规格参数和性能要求，并符合国家标准及原厂商检验标准，符合安全使用和说明书载明的基本使用要求；

附加优惠政策：

投标人（盖章）：

法定代表人或授权代表（签字或盖章）：

日期： 年 月 日

**附件2：**

**网络及安全监管平台(物联网安全管控平台+边缘网关)**

**技术要求**

**本章内容为实质性要求，不接受负偏离，否则作为无效响应。请自行制作响应表，标明正偏离、负偏离。**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **技术参数及功能描述** | **数量** | **单位** |
| 1 | 物联网安全管控平台 | 硬件性能：支持≥6个1G电口，≥2个USB2.0接口；≥1个console口；  硬盘容量≥500G固态硬盘；内存≥8G；  最大管理终端数量1024台（含3年免费升级服务）；  旁挂部署；  管理性能：支持HTTPS、HTTP、SSH、Telnet、SNMP、DHCP Server、NTP Client等常用网络通信  支持对接ONVIF协议；  支持主被动结合方式发现资产，支持ARP、ICMP、ONVIF、SNMP、Agent、SDK对接及指纹库识别等多种方式发现及识别资产，支持多种策略的组合配置及统一下发；  支持资产清单列表，支持资产清单手动导出备份；  支持资产的统计分析，包括在线资产、离线资产的数量统计，资产种类、品牌分类统计，网点/区域资产统计，在保、过保、资产上线时长统计等；  支持资产的可视化管理，支持资产基于地理位置可视化（百度地图）、网络位置可视化（拓扑图）、接入位置可视化（交换机端口面板）；  支持动态安全评估，根据整网安全状态（物联网安全、资产状态、网络传输质量）进行动态综合评估并给出评分；  支持全网物联网终端设备安全准入策略的集中配置和统一下发；  支持物联网边界安全风险统计分析，包括已准入、非授权、仿冒接入、非法外联、黑名单等边界安全风险统计分析；  支持全网物联网终端安全风险扫描策略的集中配置和统一下发；  支持物联网终端安全风险/脆弱性统计分析，包括终端弱口令、高危端口、安全漏洞的风险统计分析；  支持内网行为分析与识别策略的集中配置和统一下发；  支持网络行为统计分析，包括视频调阅、非法扫描、设备登陆及其他行为的行为风险统计分析；  支持非法访问行为拦截策略的集中配置和统一下发，拦截私接、仿冒、非法登陆、非法视频调阅等网络行为；  支持私接拦截、仿冒拦截、违规外联的历史防御统计，按当日/本周/本月统计新增防护次数；  支持视频录像完整性检测，能够对摄像头漏录事件进行检测与告警，并支持视频漏录的统计分析；  支持对视频漏录的详情查看，包括：漏录摄像机的IP、设备名称、安装区域、漏录时长的查看，支持图表或列表的形式查看漏录发生的开始时间、结束时间、漏录总时长的查看，并且能够精准到秒级；  支持视频存储天数达标检测，能够对录像保存天数小于指定天数进行检测与告警，并支持存储天数不达标统计分析；  支持视频存储天数不达标详情查看，包括：不达标摄像机IP、设备名称、安装区域、录像存储的天数及达标情况；  支持视频防外泄管控，支持联动防泄密客户端，对屏幕添加水印、对下载的视频/图片添加水印，水印类型支持文字水印和二维码水印，水印支持设置电脑主机名、IP、MAC、日期，也可自定义水印内容；支持对水印字体、二维码像素、透明度、位置等进行设置；  支持对需要外发的视频/图片进行外发加密处理，支持对外发文件设置限制打开次数、使用时间及指定接收终端，确保外发的视频数据不被中途窃取和篡改；  支持终端离线告警、网络设备离线告警、网络故障告警的集中推送与统计分析；  支持生成全网动态拓扑图，支持手动编辑网络拓扑；  支持故障的精准定位，基于百度地图/区域图、动态网络拓扑图、交换机端口的故障定位，实现故障位置从宏观到微观的多维度呈现；  告警内容推送支持弹窗显示、语音播报提醒、短信推送等，及时将告警信息送达给值班人员和运维人员；  支持告警手动确认及解除告警；  支持工单系统，支持售后工单生成、审核、派发，支持工单总数、未处理工单数统计；  支持生成全网安全报告便于对现网运行状况做阶段性小结，包括全网动态安全评估、资产概览、安全风险统计、运维/售后概览等内容；  支持对边缘网关/物联网安全交换机的统一管理，支持对版本批量升级，支持几种配置统一下发；  支持与上级物联网大数据平台对接，将管控平台上的物联网安全、资产数据、智能运维的数据集中上报给上级大数据平台统一呈现；  支持日志记录，包括系统日志和告警日志并进行分类统计，支持可批量或筛选导出相关日志；  产品符合CQC12-045800-2022认证规则要求,并提供相应的证书，提供复印件并加盖厂家公章；；  提供公安部安全防范报警系统产品质量监督检验测试中心颁发的检验检测报告，提供复印件并加盖厂家公章；；  具备“中华人民共和国国家版权局”颁发的计算机软件著作权登记证书，提供复印件并加盖厂家公章；  提供3年原厂免费质保服务，提供复印件并加盖厂家公章；  免费与原智慧乡镇平台进行对接；  甲方保留对上述功能测试验证权利。 | 1 | 套 |
| 2 | 安全边缘网关 | 硬件性能：≥6个千兆电口，≥2个USB接口，≥1个console口；  支持管理终端数量512个;  网络行为分析能力≥1000M流量；  管理性能：支持旁挂部署  支持HTTPS、HTTP、SSH、Telnet、SNMP、DHCP Server、NTP Client等常用网络通信  支持对接ONVIF协议；  支持主被动方式探测发现资产（如ARP、ICMP、SNMP、LLMNR等方式），支持自定义IP段范围扫描发现资产；  支持ONVIF视频协议对接发现，支持基于SDK私有协议对接主流视频监控厂商（海康、大华、宇视、天地伟业等国内主流品牌）识别出安防终端设备；  支持基于内置指纹库识别资产，包括安防设备（IPC、NVR、门禁、对讲、报警等）、网络设备、办公设备、服务器设备、智能终端等；  支持识别出终端的IP、MAC、名称、型号、品牌、交换机位置、流量等信息；  支持资产清单列表统计；  支持资产批量导入识别；  支持资产批量导出备份；  支持资产信息手动录入（资产入网时间、资产质保时长录入）；  支持批量导入新增资产数据；  支持基于IP、MAC、指纹多维度对终端进行准入控制，未授权终端阻断接入；  支持对仿冒IP、MAC、类型的终端进行仿冒识别，告警提醒并阻断接入；  支持黑白名单安全准入策略；  支持常见网络协议的识别，支持基于协议的准入控制；  支持对交换机镜像的内网流量进行网络行为的分析与识别，并跟踪记录日志；  支持对常见的网络行为（设备访问、后台登录、视频调用）的识别，并跟踪记录；  支持自定义安全策略或执行平台下发的安全策略拦截非法行为，支持主动或联动交换机进行拦截；  支持主动检测网络是否外联接入互联网，并告警提示；  支持主动检测内网隔离是否失效，并告警提示；  支持高危端口扫描检测，主动发现终端开启的高危服务端口号；  支持弱口令扫描检测，主动发现常见的弱口令终端，并支持自定义弱口令扫描；  支持安全漏洞扫描，支持查看终端安全漏洞的漏洞风险等级、漏洞名称、漏洞编码等信息，并能够提供对安全漏洞进行验证；  支持终端状态监测：IPC、门禁、对讲、报警、道闸、大屏、广播等物联网终端设备的在/离线状态监测；  支持网络设备状态监测：在线/离线状态、CPU、端口流量、ARP表项等监测  支持网络链路通信质量检测（链路丢包、拥塞、链路协商异常检测）；  支持常见网络故障自动检测，譬如网络环路、广播风暴、IP地址冲突、DHCP-Server冲突检测；  支持生成全网拓扑图，支持手动编辑拓扑图；  支持交换机面板可视化管理，图形化显示交换机端口所接终端的类型、工作状态；  支持POE交换机显示所有端口的供电状态，以及对供电进行开关管理；  支持对前端终端POE供电的智能重启功能，对于检测获取不到终端流量信息的端口，自动重启POE供电功能，达到重启终端的目的；  支持终端状态异常、网络设备异常、网络故障的自动告警；  支持基于拓扑图的告警定位功能；  支持告警内容弹窗推送；  支持WEB、CLI、Telnet管理；  支持安全管控平台/网络管理平台统一管理；  支持边缘网关版本批量升级；  支持本地日志记录，包括系统日志和告警日志，支持日志记录分类统计，支持批量或筛选导出相关日志；  产品符合CQC12-045800-2022认证规则要求,并提供相应的证书，供复印件并加盖厂家公章；  提供3年原厂免费质保，供复印件并加盖厂家公章；  免费与原智慧乡镇平台进行对接；  甲方保留对上述功能测试验证权利。 | 1 | 套 |