采购需求

1.项目说明

1.1 本章内容是根据采购项目的实际需求制定的。

1.2本项目不分包。供应商所报价格应为含税全包价，包含提供相关服务的所有费用，合同存续期间采购人不额外支付任何费用。

2.采购服务要求（包括附件、图纸等）

2.1 项目简介

根据《环境保护部办公厅关于加快重点行业重点地区的重点排污单位自动监控工作的通知》（环办环监[2017]61号）和《青岛市环境保护局关于加快重点行业重点排污单位自动监控工作的通知》(青环发〔2017〕84号)要求，在采购人监控中心建设一套远程视频监控平台（包括软、硬件建设、网络建设等），对前端企业的视频记录进行远程存储及调阅，在采购人处保存至少一个月的连续视频记录，同时采购人下属单位辖区同步监控，实现多级架构的管理平台，实时监控重点污染源自动监控设备运行情况，进一步保障自动监控设备不受干扰，正常运行。

★成交供应商需要根据采购人的要求，结合企业现场端视频设备安装的实际情况，以降低企业成本、保证视频数据正常传输为目的，出具性价比优的联网建设方案，并明确现场已安装视频监控设备的联网协议价格，在采购人要求的时限内及时完成全市的视频联网工作，保证监控系统正常运转。

2.2 项目内容及服务要求

2.2.1 视频信息整合

视频监控平台需实现将全市约400家重点污染源企业800余个视频监控点位联网监控，企业已自行在监控点位的采样口、站房内安装视频系统，即墨区和胶州市等区市已经与辖区视频监控平台集中联网，将以上点位一并联网至采购人监控中心视频监控平台。在采购人视频监控平台用视频方式实时监控全市控及以上排污企业的自动污染源监测站房及排污口的运维及设备运行情况，监控点位的视频信息集中到采购人监控中心远程视频监控平台，采购人下属单位依托市级视频监控平台网路分设视频平台，监控辖区情况。

2.2.2 视频监控平台功能要求

2.2.2.1 实时图像点播

在实时播放的过程中，支持图像的抓拍、录像，并可以将本地抓拍和手动中心存储到存储设备中。

2.2.2.2 云台控制

视频监控客户端选择一个云台摄像机后，可以进行远程控制。

首先系统会判断用户对摄像机是否有控制权限，如果没有，视频管理服务器会拒绝用户的控制请求，并在视频监控客户端上提示出来。

2.2.2.3 历史录像存储

通过视频管理服务器给每一个摄像机配置存储计划，指定存储资源，也可以手动给摄像机配置存储资源，配置时需要指定摄像机对应的 IP SAN 设备、存储空间以及数据保留期（天数或空间大小）及录像存储时段等。同时还支持存储和告警的联动，当用户配置告警联动，指定联动动作为录像存储，告警出发后，则启动执行报警联动录像存储，每次报警联动录像的时间可以配置。

2.2.2.4 历史录像分段下载

录像可按时间段选择进行分段查询，查询到的结果除可进行在线点播回放外，也可直接下载到本地，作为后续取证或其它用途。

2.2.2.5 历史图像的检索和回放

服务器上的数据库中记录了设备、通道、时间、报警同图像存储物理位置的对应关系，通过设备、通道号和时间段（可选），或通过报警信息，用户可以检索到已经录制的历史图像列表，双击即可播放。

2.2.2.6 用户与权限管理

支持多级用户管理，每个用户有用户名和密码，通过 MD5 加密的方式到服务器上进行验证，保证可靠性。

整个系统有一或多个系统管理员，对全网的用户有配置权限，可选的对设备有操作权限。

管理员用户，可以对域内的编解码器、图像采集和显示设备进行增、删、改、查，为云台设置预置位，新增域和子域的新用户。

普通用户对摄像机和显示器的权限包括：查看配置信息，看实时监控，远遥，

看回放，下载录像，配置轮切计划；管理员可以指定某用户对于某摄像机或显示器具有某种权限；为配置方便，也可以指定某用户对于某域内的所有摄像机或显示器具有某种权限（权限的批量配置）。

当某用户需要临时访问非管辖区域内的历史或实时图像时，可以向管理员申请授权。

2.2.2.7 日志管理

整个系统的日志管理分为三类：系统运行日志、操作日志和告警日志

系统运行日志包括：设备启动、保活失败、配置不同步、故障和故障恢复等信息（设备 ID、状态变化、时间）

系统操作日志包括：某用户的登入、退出、对系统配置的修改、控制等

告警日志包括：温度过高、视频丢失报警、遮挡报警、运动检测告警、外部告警、设备离线等。

系统支持针对各种告警信息提供统计报表，基于报表，提供基于告警类型和告警时间等的查询功能。

2.2.2.8 轮切业务

轮切业务基于实时监控，是对多路实况进行轮流查看的业务。

2.2.2.9 视频监控客户端多画面业务

视频监控客户端上，可以实现多画面的显示，多个画面之间的操作相互独立，比如：可以显示多路实况，可以显示多路回放，也可以部分画面显示实况、部分画面显示回放。视频监控客户端根据所配置的计算机性能的不同，可以支持 1\4\9\16 分屏，并可灵活组合为任意多屏显示模式。

2.2.2.10 终端合法性，状态一致性检查

IP 摄像机，编解码器和监控客户端启动后，必须向视频管理服务器发起注册，在注册过程中利用相关协议的安全性机制审计终端的合法性。只有完成了注册过程，终端才能接入到视频监控专网，开展业务。

在运行的过程中，如果终端实时检测到异常，将信息保存到本地，上报到视频管理服务器，在客户端管理界面的告警台上提示给系统管理员。当视频管理服务器管理的域内的服务器类设备（例如数据管理服务器、流媒体服务器、IP-SAN，也包括视频管理服务器自身）出现故障时，视频管理服务器也会及时将告警信息

推送到客户端上，并以稍高级别的告警提示管理员。

终端注册成功后，需要周期性的向视频管理服务器发送保活。保活是为了保证终端与视频管理服务器之间的通讯正常，采用的一种心跳检测机制。各种服务器同数据管理服务器之间也有同样的保活机制。一旦设备检测到心跳断开，说明对端设备出现了问题，此时除了发送告警信息，系统将同时按照预先设定的方案采取措施，例如将业务切换到备份设备上，在数据管理服务器和视频管理服务器进行业务切换的过程中，所有已经建立的实时监控业务和历史回放业务都不受影响。保活的默认周期是 10s（推荐），有时为了提高系统在故障时的恢复速度，也可以将周期适当缩短。

视频管理服务器主动发起的配置轮询，是为了保证服务器上记录的配置与下发到编解码器上实际的配置一致。配置轮询的时候，如果出现配置不一致，将以视频管理服务器记录的配置为准，自动启动配置下发，强制终端更新的配置。同时视频管理服务器将记录日志，并启动告警提示。

2.2.2.11 集中管理和批量配置

视频监控系统需要提供集中的配置管理功能，管理员在权限范围内，对所有终端进行集中的配置，同时支持批量配置管理。解决系统内存在大量终端设备时，管理员不能分别登陆到每个设备上配置各种参数的问题。

2.2.2.12 视频监控系统抓拍提示

视频监控系统需要提供站房人员进出次数、时间、时长等记录统计功能；人员进出需要从平台提供实时提示功能。

2.2.3 建设项目主要技术要求

2.2.3.1 采购人监控中心端视频管理平台

2.2.3.1.1 支持主流品牌的前端设备、管理设备的接入和管理。

2.2.3.1.2 可同时接入多个安防主流厂商的平台，支持同时实现对接上级平台和接入下级平台，监控点位管理能力不低于 3000 路。

2.2.3.1.3 支持 1000 个在线用户同时在线；系统最大注册用户数 3000 个。

2.2.3.1.4 支持对资产进行报表统计功能；具有用户权限管理功能，用户可按角色分配权限，一个用户可以拥有一个或多个角色。

2.2.3.1.5 支持快速定位录像关键节点，可以将录像文件切分成多片，通过切片点的图像差异，迅速启动回放关键录像时段。

2.2.3.1.6 输出支持多网域配置，实现多网融合、跨网段、内外网等灵活部署。

2.2.3.1.7 支持 AR 实景地图，支持视频画面直接调用其他摄像头视频、支持画面内建筑物名称标注;支持实景界面调阅地图，可以展开/关闭二维地图，在地图上显示当前高点相机位置，并可以切换高点相机。

2.2.3.1.8 支持智能拉框放大功能，支持智能降帧存储功能，支持 UDP 网络下单播和组播支持抗 5%的丢包。

2.2.3.1.9 支持录像检索、常规回放、切片回放、逐帧回放、单画面（多画面）回放、预览时的即时回放等功能。

2.2.3.1.10 支持告警联动功能，包括联动到电视墙、联动到客户端、联动抓图、联动到预置位、联动录像、联动发短信发邮件。

2.2.3.1.11 支持出现紧急情况时，能从当前时间即时后退查看录像，回放时间、进度可调节，且可持续回放不限时间。

2.2.3.1.12 支持 GB/T 28181、ONVIF 标准协议。

2.2.3.1.13 支持门禁系统的物联接入，开/关门状态提醒，联动视频输出功能。

2.2.3.1.14 支持第三方品牌系统集成应用。

2.2.3.1.15 以电子地图形式显示设备的实时数据、运行状态，根据终端用户现场酌情使用 GIS 地图或二维图;

2.2.3.1.16 显示所有设备的在线、离线情况，设备离线时触发告警，通知用户处理;

2.2.3.1.17 硬件 CPU≥ 3.5GHz，内存≥2*8GB，硬盘≥2T*2,网口≥2 个千兆电口

2.2.3.2 流媒体转发服务器(一套)

2.2.3.2.1 单台设备支持 1024 路或 1Gbps 输入，单台设备支持 2048 路或 2Gbps 输出

2.2.3.2.2 支持音视频单播流的复制分发

2.2.3.2.3 支持音视频组播流转单播复制分发

2.2.3.2.4 支持对跨域媒体流进行复制分发

2.2.3.2.5 支持负载均衡和动态互备

2.2.3.2.6 单/组播抗丢包功能：UDP 网络下单播和组播支持抗 5%的丢包

2.2.3.2.7 支持 VPN 的部署方式

2.2.3.2.8 为保证系统兼容性及功能完整性，同监控系统硬件配置统一品牌

2.2.3.2.9 硬件 CPU≥ 3.1GHz，内存≥2*8GB,硬盘≥1T，网口≥6 个千兆电口

2.2.3.3 视频接入服务器(一套)

2.2.3.3.1 采用 Linux 操作系统，支持 7×24 小时稳定运行，并且不易受到黑客、病毒的入侵和攻击

2.2.3.3.2 支持域内网络设备 IP 地址统一规划

★2.2.3.3.3 支持页面上添加其他网段的路由可下发给拨号客户端，可配置网关发给客户端

2.2.3.3.4 支持扩展访问控制列表，可根据访问控制列表实现个性化访问控制

2.2.3.3.5 支持 L2TP、SoftVPN 等多种 VPN 的部署方式

2.2.3.3.6 支持 GB28181、Onvif 协议等联网标准，业务的建立和拆除基于 SIP 协议

2.2.3.3.7 支持 NVR、IPC、卡口等社会资源接入

★2.2.3.3.8 支持作为网络中继转发数据流量

2.2.3.3.9 硬件 CPU≥Intel Xeon E3-1275 v5，内存≥1*8GB，硬盘为≥6TB，网口≥3 个千兆电口

标星项需提供公安部检测机构产品专业认证测试报告；

2.2.3.4 视频安全网关(一套)

2.2.3.4.1 能实时发现接入前端网络的网络设备。

2.2.3.4.2 能将发现的网络设备上报后端监控平台，并动态更新该设备

状态。

2.2.3.4.3 能允许或拒绝指定 MAC 地址的设备进行访问

2.2.3.4.4 能允许或拒绝指定 IP 地址的设备对系统进行访问

★2.2.3.4.5 仅转发白名单中的设备发出的数据报文，不转发非白名单中的设备发出的数据报文

2.2.3.4.6 仅对符合标准协议（GB/T 28281、ONVIF）的媒体流进行转发，其余数据报文丢弃

2.2.3.4.7 当且仅当监控平台通过标准协议向前端发起媒体流请求后，对应的媒体流才允许通过

★2.2.3.4.8 支持终端接入数据管控功能，只允许授信数据如控制信令、协商视频流、告警信息等接入网络中

2.2.3.4.9 能实现前端摄像机等设备的准入控制，只允许授信终端接入，阻断非法私接入

★2.2.3.4.10 能对需要访问监控平台的客户端进行身份认证，只有认证通过后的客户端才可以访问平台并获取监控资源

2.2.3.4.11 支持在线和旁挂两种组网模式。

2.2.3.4.12 具有不少于 4 对千兆 Combo 口(光电复用)、10 个千兆电口、1 个 Console 口、1 个 USB 接口；

标星项需提供公安部检测机构产品专业认证测试报告。

2.2.3.5 IPSAN 存储设备(一套)

2.2.3.5.1IP SAN 存储，4U 48 盘位，支持 SATA 盘(1TB/2TB/3TB 4TB/5TB/6TB)、SSD 盘。

2.2.3.5.2 支持冗余电源、冗余风扇、冗余电池。支持电源、电池、风扇热插拔。

2.2.3.5.3 具备数据直存功能，无流媒体服务器，可将视频流直接写入存储。

2.2.3.5.4 具备数据保护功能，异常掉电后存储在缓存中的数据应不丢失，可通过数码管显示缓存数据的保存进度，可查看断电前 1s 的视频录像。

2.2.3.5.5 支持数码管、指示灯、蜂鸣器告警、邮件告警、SNMP Trap、

短信等告警方式对故障进行告警。

2.2.3.5.6 具备视频入侵检测、报警联动、视频信号丢失报警、报警预录功能。

2.2.3.5.7 具备录像的即时倒放、切片功能。

2.2.3.5.8 根据业务压力不同，RAID 阵列可自动动态调整重建速率，RAID 中磁盘发生故障，RAID 处于降级、重建状态时，不影响数据写入

2.2.3.5.9 具备 N+M 集群管理功能，某台主机发生故障时，备用主机可替换记录录像，故障恢复后，可将录像回传。

2.2.3.5.11 产品具备 CE/FCC/CCC/UL/TUV 认证，具有 CQC 节能报告。

2.2.3.6 硬盘（48 块）

2.2.3.6.1 硬盘容量：6TB

2.2.3.6.2 接口类型：SATA

2.2.3.6.3 硬盘转速:7200 转

2.2.3.6.4 缓存容量：128MB

2.2.3.6.5 适用机型：存储服务器

2.2.3.7 运维服务器(一套)

2.2.3.7.1 支持通过设备名称、IP 地址、告警级别、通信状态查询设备信息

2.2.3.7.2 运维报警管理功能：支持多条件查询报警信息，并支持分类显示

2.2.3.7.3 支持手动填写故障保修单，支持自动根据视频质量诊断异常结果生成故障保修单

2.2.3.7.4 支持多条件查询系统故障保修单，支持手动处理报修流程，并支持查看报修流程状态

2.2.3.7.5 设备自动发现功能：具有网段自动发现、路由自动发现、ARP 自动发现设备选项，具有 snmp 设备过滤设置选项

2.2.3.7.6 能够自动发现全网拓扑，自动生成全网拓扑图，且拓扑图可自定义设置，支持在网络拓扑上显示子网的 IP 地址

2.2.3.7.7 高效的录像状态侦测管理：具备智能视频检测服务器进行海

量前端的录像检测、具备根据录像计划智能判断前端录像状态、对未按计划录像的摄像机进行告警上报、具备对智能视频检测服务器的录像分析结果分类统计、查询

2.2.3.7.8 支持按组织区域、设备类型、故障类型查询设备的故障统计情况，支持显示设备在查询时间段内的故障次数，故障时长和最近一次故障起始时间

2.2.3.7.9 支持使用 web 在线升级系统，支持设备配置文件导入导出功能，支持使用 web 远程重启设备，支持设备配置恢复出厂设置功能，支持日志导出功能，支持查看设备的运行状态，CPU 使用率、温度等。

2.2.3.7.10 硬件 CPU≥Intel Xeon E5-2620 v3，内存≥2*8GB，DDR4，硬盘≥1TB*2，网口≥2 个千兆电口

2.2.3.8 核心交换机(一套)

2.2.3.8.1 交换机类型：以太网交换机

2.2.3.8.2 接口数目：24 个电口，4 个光口

2.2.3.8.3 传输速度:1000Mbps

2.2.3.8.4vlan：支持基于端口的 VLAN、支持 GVRP;

2.2.3.8.5 交换容量≥336Gbps

2.2.3.8.6 包转发率≥96Mpps

2.2.3.8.7 聚合：支持链路聚合;

2.2.3.8.8 镜像：支持端口镜像;

2.2.3.8.9 安全：支持 ARP 入侵检测功能、支持防 Dos 攻击;

2.2.3.8.10 组播：支持 IGMP Snooping;

2.2.3.8.11 生成树协议：支持生成树协议;

2.2.3.8.12 网管：支持 SNMP V1/V2/V3，支持通过 telnet 方式进行配置和管理，支持用户的分级分权控制，支持用户访问控制。

2.2.3.9 防火墙(一套)

★2.2.3.9.1 硬件指标：专业防火墙设备，吞吐量≥3Gbps，并发连接数≥200,000，新建连接数≥50000，不少于 6 个千兆电口，1U 机架式机箱。

2.2.3.9.2 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。

2.2.3.9.3支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口。支持链路聚合功能。支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路。

2.2.3.9.4支持静态路由，ECMP等价路由。支持标准MPLS VPN协议。支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议。

2.2.3.9.5访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式。访问控制规则支持数据模拟匹配，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，方便排查故障，或环境部署前的调试。支持根据国家/地区来进行地域访问控制。支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制。支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式。

2.2.3.9.6支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测。支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为。

2.2.3.9.7支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS过滤，文件过滤支持文件上传和下载过滤。

2.2.3.9.8支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤；

2.2.3.9.9 设备具备独立的入侵防护漏洞规则特征库，特征总数在6800条以上。支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能，具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能。

2.2.3.9.10支持同防火墙访问控制规则进行联动，可以针对检测到的攻

击源IP进行联动封锁，支持自定义封锁时间。可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。

2.2.3.9.11设备具备独立的僵尸网络识别库，特征总数在40万条以上。支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。

2.2.3.9.12对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告。支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址。

2.2.3.9.13支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别。支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证。支持以攻击链方式来匹配和展示资产遭受到的攻击行为。

2.2.3.9.14支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式。支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限。支持自动备份配置，最大支持十五天内的配置恢复。

2.2.3.10 服务器机柜(一套)

2.2.3.10.1 机柜类型：服务器机柜

2.2.3.10.2 尺寸：2000mm*600mm*1000mm

2.2.3.10.3 材质：冷轧钢材质

2.2.3.10.4 用途：装载网络设备网络配件等

2.2.3.11 采购人监控中心端 1000M 专线(一条)

租赁通信运营商 1000M 数据专线。

2.2.4 日常运维要求

2.2.4.1 软件（监控平台）运维

主要是对平台设备软硬件维护，对采购人监控中心以及下属单位的平台设备

的维护，软件升级及维护，企业前端设备接入的变更及维护,小型配件的维修更换，平台运维数据的监控及整理。

在运营期间，成交供应商要严格按照采购人制订的操作规范和规章制度，建立对所运维的系统及设备进行规范操作和精心维护及必要维修,保证系统及设备的正常运行，达到采购人提出的系统及设备指标要求，仪器发生故障不能按时修复时直接使用备机替代工作。

每天：驻地人员每工作日通过视频监控平台巡检监控点总数不少于 120 个，并做好进入站点人员及时间记录。成交供应商需收集企业端运维人员的日常工作记录，工作日巡检要求进入站点人员拍照。其中对存在问题点位拍摄问题部位照片，并在巡检报告中进行文字描述，并及时汇报采购人。

每周：成交供应商每周汇总所有点位中人员进入和无运维人员进入情况，在巡检报告中进行统计。

每月：成交供应商需在每个月对所有项目的监控点巡检一次，并做好月度巡检报告。

每年：成交供应商出具日常巡检报告、月度巡检报告、以及月度、年度考核报告,组织相关项目的年度考核会议。每月第一周提交上月巡检结果及情况分析；完成对被考核方的年度考核后 5 个工作日内向招标人提交被考核方的年度考核报告，并保证报告的真实性。

2.2.4.2 硬件运维

7×24 小时硬件保修，系统硬件发生故障时，应以最快速度赶到故障现场进行故障检测、维护，及时更换故障部件恢复系统正常运行。如果故障在短时间内无法排除，需提供替代整机。若发生解决不了的问题，需与产品制造商联系缩短故障排除时间。在做硬件维护前需制定详细可行的计划，确保系统运行的可靠稳定连续。

7×24 小时专线保修，专线光缆发生故障时在 6 小时内完成修复，若无法解决，需有备用可替代路由紧急抢通业务，保障专线安全运行。