**绍兴明晨建设项目管理有限公司关于绍兴市上虞区大数据发展管理中心上虞区公共安全视频监控建设联网应用（雪亮工程）大数据发展管理中心建设项目（一期）的征求意见**

一.   征求意见范围：

1、是否出现明显的倾向性意见和特定的性能指标；

2、影响政府采购“公开、公平、公正”原则的其他情况。

二.   合格投标人：

  1、符合政府采购法第二十二条规定的投标人资格条件；

2、本次招标不接受联合体投标；

3、本次招标需采用资格后审的审查方式，由采购人负责审查。

三.   征求意见回复：

  1、意见递交时间：2019年11月12日17时00分前（节假日除外）递交。

  2、意见递交方式：各供应商及专家提出修改理由和建议的，将书面材料签字（盖章）并密封后送至绍兴明晨建设项目管理有限公司（上虞区城北金城大厦18楼），外地可扫描件发送邮箱至940453120@qq.com扫描件必须签字（盖章）。

  3、意见接收机构：绍兴明晨建设项目管理有限公司 /绍兴市上虞区大数据发展管理中心

  4、联系人：张先生/金先生

  5、联系电话：0575-82181118/0575-82500062

绍兴市上虞区大数据发展管理中心

绍兴明晨建设项目管理有限公司

2019年11月7日

**附件 ： 招标采购内容与技术规格书**

## 第一章　技术规范及要求

1、1建设依据

**（一）政策依据**

（1）《中华人民共和国国民经济和社会发展第十三个五年规划纲要》

（2）《“十三五”国家信息化规划》(国发〔2016〕73号)

（3）《公共安全视频监控建设联网应用“十三五”规划方案》

（4）《中华人民共和国\*\*怖主义法》

（5）《国家创新驱动发展战略纲要》(中发〔2016〕4号)

（6）《关于加强社会治安防控体系建设的意见》

（7）《国家电子政务总体方案》

（8）《政府信息资源共享管理暂行办法》的通知(国发〔2016〕51号)

（9）《关于加强公共安全视频监控建设联网应用工作的若干意见》(发改高技〔2015〕996号)

（10）《浙江省公共安全视频监控建设联网应用工作实施方案》（浙综委〔2016〕11号）

（11）《关于推进社会治安综合治理信息化建设的若干意见》(中综办〔2014〕

27号)

（12）《公共安全视频监控建设联网应用工程示范和重点支持项目管理办法》

（13）关于印发《浙江省公共安全视频建设联网整合共享应用规范》的通知（浙综委办〔2017〕12号）

（14）关于印发《浙江省公共安全视频图像信息共享总平台建设规范》的通知（浙数局发函〔2018〕2号）

**（二）标准规范**

（1）《公共安全视频图像信息联网共享应用标准体系（2017版）》

（2）《安全防范视频监控联网系统信息传输、交换、控制技术要求》（GB/T28181-2016）

（3）《社会治安动态视频监控系统技术规范》（DB33/T502-2018）

（4）《公共安全视频监控联网信息安全技术要求》（GB35114-2017）

（5）《安全技术防范系统建设技术规范》（DB33/T768）

（6）《跨区域视频监控联网共享技术》（DB33/T629-2011）

（7）《公安视频图像分析系统》（GA/T1399-2017）

（8）《公安视频图像信息应用系统》（GA/T1400-2017）

（9）《安全技术防范（系统）工程检验规范》（DB33/T334-2011）

（10）《安全防范监控数字视频音频编解码技术要求》（GB/T25724-2017）

（11）《社会治安综合治理基础数据规范》(GB/T31000-2015)

（12）《视频中物品图像检验技术规范》（GA/T1018-2013）

（13）《视频中人像检验技术规范》（GA/T1023-2013）

（14）《安全防范视频监控摄像机通用技术要求》（GA/T1127-2013）

（15）《安全防范视频监控高清晰度摄像机测量方法》（GA/T1128-2013）

（16）《基于视频图像的车辆行驶速度技术鉴定》（GA/T1133-2014）

（17）《公安视频图像信息联网与应用标准体系表》（GA/Z1164-2014）

（18）《安全防范高清视频监控系统技术要求》（GA/T1211-2014）

（19）《视频安防监控系统技术要求》（GA/T367-2001）

1.2建设目标

到 2020 年 6 月，实现“全域覆盖、全网共享、全时可用、全程可控”的公共安全视频监控建设联网应用。 1.全域覆盖：重点公共区域视频监控覆盖率达到 100%，新 建、改建高清摄像机比例达到 100%；重点行业、领域的重要部位视频监控覆盖率达到 100%；2.全网共享：重点公共区域视频监控联网率达到 100%；重点行业、领域涉及公共区域的视频图像资源联网率达到 100%；3.全时可用：重点公共区域安装的视频监控摄像机完好率达到 98%，重点行业、领域安装的涉及公共区域的视频监控摄像机完好率达到 95%，实现视频图像信息的全天候应用；4.全程可控：公共安全视频监控系统联网应用的分层安全体系基本建成，实现重要视频图像信息不失控，敏感视频图像信息不泄露。

**1.3 视频联网现状**

上虞区视频监控网络已经形成基于三网三平台的视频应用格局，包括：“视频专网”、“公安网”、“互联网”。各政府职能部门均可以按需使用已建的各类视频资源开展相关的视频应用。目前三网三平台各司其职初步实现城市道路交叉口无死角、关键道路关键节点无盲区、人员密集区域无遗漏、要害部门、案件高发区、治安复杂场所全覆盖的要求，基本形成市、县两级，城区重点场所和部位、主干道路、周边交界三层的视频监控网络的全覆盖。

**1.4 总体设计方案**

**1.4.1联网架构设计**

结合上虞区视频图像信息联网系统现状以及后期业务规划需求，以电子政务视联网、公安视频专网、政务外网等多个通道实现政府、企业、社会等视频资源的汇聚整合，形成电子政务视联网、公安视频专网及其他网络的视频联网共享格局，服务于综治、公安和其它职能部门实战应用。



**联网架构图**

系统最终实现将不同网络的视频资源统一汇聚到视频图像共享应用平台上，并可提供各委办局单位基于电子政务视联网的视频图像相关应用。

## 第二章 项目基本要求

上虞区公共安全视频图像共享平台3年服务。服务包括：提供稳定可靠上虞区公共安全视频图像信息共享平台能力、软硬件设备、日常运维、常驻技术人员保障、故障维修、应急处理等。

本项目为交钥匙承包项目，中标单位承包及负责招标文件对中标单位要求的一切事宜及责任。包括设备及软件供应、运输、保管、安装、调试、试运行、验收及售后服务等。

1、总体要求：平台实现与已建的绍兴市电子政务视联网系统无缝对接（无缝接入省、市、区三级防护终端平台，请投标供应商自行到项目现场了解与沟通。）、逐级互联，共享资源，达到一体化的融合系统平台，提供统一的 API 接口，接入绍兴市电子政务视联网平台。提升基层双向通信指挥能力，满足公共安全事务及维稳工作的实战需求。平台需符合浙江省公共安全视频图像信息共享总平台建设规范。

2、扩容要求：视联网核心服务系统作为区电子政务视联网的核心设备，在服务于电子政务视联网日常运行的同时还需满足所有接入监控图像的交换转发工作，故本次需建设区级核心服务器，与原电子政务视联网平台形成资源池，实现区级视频资源负载均衡与备份负载；新建区公共安全视频图像信息共享应用平台，通过电子政务视联网形成覆盖市、县、乡、村四级的视频调度，实现统一管理服务。本次新建的汇聚平台具备较高的扩展性，可以根据实际项目需求对联网性能、流媒体取流性能、级联并发性能、存储性能等进行扩容。

3、联网要求：平台联网需接入公安、综治两个分平台，向上可连接绍兴市公共安全视频图像信息共享应用平台，满足各级平台之间视频图像资源互联互通。平台联网必须遵守GB/T28181《安全防范视频监控联网系统信息传输、交换、控制技术要求》，其功能须满足国家“十三五”规划联网应用的基本业务功能、基本管理功能。平台须符合GB/T31000-2015《社会治安综合治理基础数据规范》、GB/T33200-2016《社会治安综合治理综治中心建设与管理规范》实现现有平台的监控协议转换，并建立监控平台和电子政务视联网平台的若干通道。提供基于SDK、API接口的二次开发。平台汇聚平台应能通过GB/T28181-2016协议接入各自辖区内新建的前端感知摄像机和已建的监控资源平台，一方面为本项目建设的应用系统提供视频能力，另一方面，为其他部门提供视频共享支撑能力。

4、共享要求：平台共享功能需遵守GB/T28181《安全防范视频监控联网系统信息传输、交换、控制技术要求》，其基本业务功能、基本管理功能参照视频图像信息联网平台。共享平台需扩展支持GB/T25724-2010《安全防范监控数字视音频编解码技术要求》（SVAC标准），支持运维管理、安全认证等功能，支持与视频图像信息解析系统等系统的应用对接。平台内部须实现摄像头数据流IP包与MAC地址包相互高效转换，同时符合《GB/T 33200-2016》、《GB/T 31000-2015》。

5、接入要求：要求接入不少于20处场所或监控网络（具体场所和监控网络，由招标人指定），接入视频不少于1.1万路（除公安外）。区内每个场所或监控网络原则上通过裸光纤汇聚至区政务网络核心机房。中标人需做好接入摄像头（除公安外）的点位命名及GPS定位等工作。平台支持多样化的平台或前端接入，可通过国标GB/T28181协议进行接入整合。平台要支持对非标平台或非标前端接入，支持采用非IP技术体系的设备实现平台或前端的接入，并进行标准化改造

6、权限管理要求：平台用户权限分菜单资源权限和设备操作权限两部分，只有被授权的内容方可进行操作，权限可以被赋予，也可以被收回。用户权限按角色管理。所有用户按照所属区域、部门、组织机构和职责分配用户角色，每个不同的角色定义不同的级别和操作权限，对应不同的操作内容，包括可以查看的视频内容、可以播放的录像、对云台镜头的控制、可以编辑和修改的系统信息、对设备的设置和控制等。用户权限分级管理。可以按照部门设置多级管理员，不同部门的管理员可以且只能按照本部门的最高访问控制权限设置、编辑和修改本部门用户的权限。用户权限管理应满足集中统一管理的要求，以业务流程为纵向主线，以行政管理体系为横向主线，无论是上级业务管理部门、主管领导或其它管理单位，均可根据系统授予的权限察看所需要的图像和相关信息。对于像云台控制这样需占有型操作及夺权型操作的权限，需要按照用户权限等级来决定控制策略。平台支持管理至少100000路监控点位，支持历史图像回放并发不小于200路，支持用户数不少于1000个，并发用户数不少于200个，级别较高的用户有优先控制权和优先服务权，并在级别较低用户的界面上给予提示；同级别用户按时间顺序取得控制权；同级别用户以先取得控制权为优先，可以设定停止控制时间限制，假如先取得控制权的用户在一定时限（支持自定义）内没有操作，可以认为主动放弃控制权，由其它同级别用户取得。用户对系统资源的控制能力仅仅受限于其权限和优先级，与资源所处的地域无关。用户权限支持“临时用户”，在设置用户时可以对用户设定有效时间，在有效时间内用户具有正常权限，超过有效时间后用户权限自动失效。用户与资源的交叉分组进行资源和用户的权限管理功能；用户与资源的交叉分组进行资源和用户的权限管理功能。

7、平台安全性要求：采用先进网络技术手段，能够实现所有外部数据体系在系统运行网络环境下无法透传，可同时抵御网络层攻击和应用层攻击，并能将恶意数据包进行丢弃。能够将系统的网络结构、设备信息及状态等对外部均不可见。当利用IP技术进行攻击行为时，无法找到网络中的设备，就等于没有了攻击入口，整个系统网络对攻击者而言是完全空白的。具备结构化安全能力，系统网络设备自身不存在已知安全漏洞和后门，并能有效阻止漏洞攻击和信息泄露。无法从系统提供的服务中获取保密数据，具备针对系统漏洞、协议弱点、病毒蠕虫、DDoS攻击、间谍软件、恶意攻击、流量异常等威胁网络层深度防御能力。

本次汇聚平台系统采用公安部要求安全接入设备包括对媒体流、信令流数据进行严格校验机制内外端机严格控制对外网用户提供的服务，甚至可以不对外提供服务，以减少由于开放知名服务而带来的安全隐患。系统提供管理员身份鉴别功能，并借助强有力的安全策略来保证鉴别的有效性和安全性，例如对口令强度的检测及对鉴别尝试次数的限制等。系统用户登录、操作、配置等功能都采用严格的传输加密机制。同时应在网内重要部位安装网路探测器，发现违规模式和未受权用访问时，报告信息报警通知系统安全管理中心。接受来自网路探测器的信息，根据安全策略进行分析，并作审计、报告、事件记录和报警等处理。要按照GB/T20271-2006《信息安全技术信息系统通用安全技术要求》中4.2.7的要求，对包括计算机病毒在内的恶意代码进行必要的安全防护。

**平台技术参数要求：**

**1）、区公共安全视频图像信息共享总平台部分**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目** | **技术参数要求** | **数量** | **单位** |
| 一、公共安全视频图像信息共享平台 |
| 1 | 核心服务平台系统 | ▲1、符合国家相关文件要求，可与浙江省电子政务视联网系统实现无缝对接，可将整合的视频监控资源和浙江省电子政务视联网应用深度结合。▲2、符合视联网技术（国内自主创新具有完全自主知识产权的交换式视频通信技术），可兼容H.323协议及SIP协议，应支持以太网标准(标准802.3)，实现视频的高效实时传输，具有强大的兼容能力。3、采用嵌入式操作系统；非插板卡式、非PC机架构，非工控机架构(无鼠标键盘和VGA接口），设备应支持7×24小时连续不间断开机运行，稳定性满足99.99%。须提供满足该参数的产品彩页。4、单台设备支持256路2M码流接入，并支持后期通过licence授权的方式进行扩容，在不增加硬件的前提下实现扩容，实现单台设备最大支持512路1080P的高清视频并发接入1080P高清终端接入。支持电视墙功能，同一组会议中支持任意会场配置电视墙；跨级会场画面、辅流画面，PC 端视频、手机端视频可任意加入电视墙灵活组合显示5、不少于2路千兆光口和电口。须提供满足该参数的产品彩页。6、核心视频平台服务器支持级联模式，至少支持6级以上数字级联。7、视频：支持H.265、H.264BP/HP/MP视频协议。支持4K、1080P、720P分辨率，并向下兼容4CIF、CIF图像格式；支持1080p/i 50/60和720P 60帧场视频格式。8、音频：系统应支持G.711a/u和AAC音频格式。时延：整个系统中，任意两点之间延迟小于200ms，保证唇音同步。9、具有结构性安全或其他更优的安全方式，保证平台安全。设备自身结构性不存在已知安全漏洞和后门，可有效阻止漏洞攻击和信息泄露。提供经权威检测机构出具的安全测评报告复印件。10、支持会场视频监播功能，可监播的会场信号可以是固定视频终端信号、移动客户端信号、桌面式电脑客户端信号以及视频监控信号，以方便会议保障者及时发现会场画面异常或调整，同时在视频监播的同时支持监播终端可以与监播画面中的会场进行语音私聊功能，确保面对画面异常或调整时的及时沟通，且不影响当前会议。▲11、承载视频网络的网络结构、设备信息、设备状态对外均不可见，内部结构对外隐藏，具有抗嗅探、抗攻击能力，可有效防御系统漏洞、协议弱点、病毒蠕虫、DDoS攻击、间谍软件、恶意攻击、流量异常等安全威胁。提供经权威检测机构出具的安全测评报告复印件。12、支持级联多通道功能，且级联可实现服务器容量全并发，单台设备支持不少于256个级联通道。13、须提供产品3C认证、电信设备入网证复印件。14、须提供核心视频服务器或视频平台的相关软件著作权证书复印件。15、支持辅流功能，在同一组会议中，多个会场可以同时发起动态辅流。须提供满足该参数的产品彩页。16、支持自主多画面功能，支持全交换功能，一组会议中具有权限的终端可以自由选择自己收看画面的组合显示模式。须提供满足该参数的产品彩页。17、网络接口：2个GE RJ45电口+2个GE 光接口。  | 1 | 台 |
| 2 | 统一视频监控融合调度平台服务系统 | 1、符合国家相关文件要求，可与浙江省电子政务视联网系统实现无缝对接，可将整合的视频监控资源和浙江省电子政务视联网应用深度结合。2、符合视联网技术（国内自主创新具有完全自主知识产权的交换式视频通信技术），应支持以太网标准(标准802.3)，实现视频的高效实时传输，具有强大的兼容能力。3、须支持国标GB/T28181-2016、ONVIF等协议标准，支持IPC、DVR、NVR 等各类IP视频编码设备接入。▲4、支持不少于10万路监控点管理能力，1000个用户注册，200路用户并发。需提供满足该参数的产品彩页。不少于2\*RJ45 10/100/1000Mbit/s自适应网络接口。5、支持结构化抗渗透攻击和信息泄漏，无法从系统提供的服务中获取保密数据，具备针对系统漏洞、协议弱点、病毒蠕虫、DDoS攻击、间谍软件、恶意攻击、流量异常等威胁网络层深度防御能力。提供经权威检测机构出具的安全测评报告复印件。6、须支持统一管理，提供角色管理、用户管理、权限管理等多层次的监控资源权限管理。7、须资源管理功能，可将接入的监控资源进行统一整合，资源编码，统一维护等管理，为联网监控资源按用户需求进行管理提供了数据基础。8、须支持多维分组功能，分组的方式可不局限于监控资源的物理限制。 9、须支持权限管理功能，提供用户权限分配和认证，赋予每个用户特定权限和级别。10、须支持系统配置功能，提供组织结构、用户管理、设备管理、权限管理等管理和配置功能。11、硬件要求：配置2颗 Intel Xeon E5-2620v4(2.1GHz/8c)/8GT/20ML3；配置 2根 DDR4 16GB 内存，可支持8个内存插槽：配置1块2GB 缓存 Raid卡(支持SAS/SATA Raid0,1,10,5,50，6,60）；配置2块4TB 企业级 7.2K 3.5寸 SATA 热插拔硬盘；配置2个千兆以太网口：N+1个冗余系统风扇；1+1冗余电源，支持热插拔。内置DVD-RW，导轨。 | 1 | 台 |
|
| 3 | 统一视频监控接入服务系统A | 1、要求须与核心服务平台系统为同一品牌产品。2、支持视联网技术（国内自主创新具有完全自主知识产权的交换式视频通信技术），支持TCP/IP协议。3、视频编码：至少支持RTP、RTSP、RTMP、HLS协议。至少支持ONVIF、GB/T28181-2016（兼容GB/T 28181-2011）标准。须提供满足该参数的产品彩页。4、单台设备可以对接不少于6万路的监控信号，支持不少于80路2Mbps并发上传到上级平台。须与第三方视频监控系统实现无缝数字对接。须提供满足该参数的产品彩页。不少于2\*10M/100M/1000M自适应以太网口。5、须支持独立的WEB访问、配置、管理界面。6、须支持接入设备状态查看、视频通道状态查看、网络连接状态查看。7、须具备对设备资源总数、设备在线数量的统计功能。8、须具备参数配置、日志获取、系统升级、设备校时等设备远程维护功能。9、硬件要求：配备2 X Intel Xeon Processor E5-2620V4 ;显卡：Intel集成显卡Intel® HD Graphics 500；内存不小于8GB，系统：Windows Server 2008R2以上； 不少于2 x 10/100/1000M自适应以太网口； | 1 | 套 |
| 4 | 统一视频监控接入服务系统B | 1、要求须与核心服务平台系统为同一品牌产品。2、支持视联网技术（国内自主创新具有完全自主知识产权的交换式视频通信技术），支持TCP/IP协议。3、视频编码：至少支持RTP、RTSP、RTMP、HLS协议。至少支持ONVIF、GB/T28181-2016（兼容GB/T 28181-2011）标准。须提供满足该参数的产品彩页。4、单台设备可以对接不少于6万路的监控信号，支持不少于50路2Mbps并发上传到上级平台。须与第三方视频监控系统实现无缝数字对接。须提供满足该参数的产品彩页。不少于2\*10M/100M/1000M自适应以太网口。5、须支持独立的WEB访问、配置、管理界面。6、须支持接入设备状态查看、视频通道状态查看、网络连接状态查看。7、须具备对设备资源总数、设备在线数量的统计功能。8、须具备参数配置、日志获取、系统升级、设备校时等设备远程维护功能。9、硬件要求：配备1X Intel Xeon Processor E3-1231 ;显卡：Intel集成显卡Intel® HD Graphics 500；内存不小于8GB，系统：Windows Server 2008R2以上； 不少于2 x 10/100/1000M自适应以太网口； | 1 | 套 |
| 5 | 视频监控前端汇聚接入服务系统 | 1.必须提供双千兆以太网口，可跨接多个网段，支持多网口技术。2.支持与TCP/IP、CDMA、WCDMA、CDMA2000、802.11x等协议的桥接。3.视频编码：H.264BP、H.264MP、H.264HP。4.音频编码：G.711、AAC。5.视频分辨率：D1、720P、1080P等。6.单台视频监控接入前端服务系统实现对异构异源设备的接入前端，支持GB28181、ONVIF、厂商 SDK 以及其他定制开发方式接入。可对接2000路监控资源（非标协议的IPC可以接入不少于1000路；GB28181标准协议可接入不少于2000路）、支持10路高清监控视频流并发上传。7.可将监控平台中的视频信号，作为视频会议的信号源，加入任意一组会议中。8.采用全中文管理，简单便捷，易学易懂。9.需具备计算机软件著作权证书10.为确保视频资源接入的信息安全和网络安全，需提供非IP技术接入方式，并提供切实可行的接入方案。 | 1 | 套 |
| 二、公共安全视频图像信息共享平台-前置汇聚平台 |
| （一）、前置智能视频汇聚平台软件配置清单 |
| 1 | 视频图像信息应用平台 | 系统支持用户名密码及PKI登录方式，用户首次登陆或重置密码后登陆需强制修改密码，支持密码输入自动隐藏明文功能系统支持防暴力破解登录，遇到暴力破解时支持自动锁定用户ip。当用户连续登录失败次数超过3次时，需要输入验证码；当用户连续登录失败次数超过5次时，用户将被暂时锁定应用支持以标签页方式嵌入显示在门户中，最多支持打开20个标签页；支持刷新、关闭当前标签页，同时支持快速关闭当前标签页左侧或右侧所有应用、关闭除了当前应用外所有应用、以及关闭所有已打开的应用支持创建新的收藏夹分组，并支持编辑、删除收藏夹分组支持查看收藏夹内点位，支持针对收藏夹内点位进行查看详情、预览及回放，并支持添加及删除收藏夹内点位▲支持切换查看基础目录及业务目录，资源以资源树形式展示，点击可查看下层资源及点位，支持点位周边搜索，在地图上自由选择当前等点位周边点位，并支持对所选点位进行预览、回放、收藏、定位到资源树及查看属性（以公安部检测报告为准）支持画面抓图、录像、电子放大、3D放大、云台控制、视频增强、音频播放、对讲（支持国标设备级联对讲），抓图时支持上传至暂存架▲支持录像分段回放功能，可以将录像文件等分成多个片段同时回放，通过分割点的图像差异，快速确定回放关键录像时段（以公安部检测报告为准）▲支持设置是否开启直连云存储高倍速回放，开启后点位可支持32倍、64倍高倍速播放，支持高倍速播放的点位画面上会有图标标明（以公安部检测报告为准）支持画面抓图、录像、电子放大、视频增强、音频播放等功能，抓图时支持上传至暂存架，支持单画面及多画面播放控制，支持画面倒放、逐帧倒放、逐帧前进，支持调整画面播放倍速，支持1倍、2倍、4倍、8倍、16倍快速播放，也支持1/2、1/4、1/8、1/16倍速慢放，支持高倍速回放的点位还支持32倍、64倍播放监控资源、地理资源、视频预案、视频追踪、网格规划、场所规划、轨迹分析、区域碰撞、线路预案、GPS定位、GPS轨迹、告警视图、流量热力图、地图基本操作、地图控件、空间查询、显示控制▲支持查看基础目录及自定义的业务目录树下，监控点、卡口、探针、报警设备、报警输入/输出、移动探针、车载、单兵、无人机等类型资源，同时支持资源的地图展示，提供时空一体化的指挥与作战能力（以公安部检测报告为准）▲支持组件化微服务架构设计，支持系统评分，对服务器在线率、中心服务器资源使用情况、资源运行状态、服务器告警等状态综合评分，可以可视化界面展示及监控服务器及组件服务数量、运行状态、资源状态及告警状态，并支持以颜色区分节点及服务器连接的告警紧急程度（以公安部检测报告为准）支持进行平台安装部署操作，包括软件安装包、资源包、补丁包的安装与管理，提同时支持对单个组件进行安装、卸载、补丁升级和参数配置▲支持单台物理设备自定义多个微服务，包括核心服务、集群代理服务、授时服务、视频点播服务、智能分析服务、智能接入服务、API网关、录像存储服务、媒体网关服务、资源管理服务、数据库服务等，并支持微服务能力快速动态调整（以公安部检测报告为准）▲支持系统备份及还原功能，支持以组件维度进行备份还原，支持查看、维护、还原备份文件（以公安部检测报告为准）支持持用户管理、部门管理、角色管理支持查看系统及各应用当前CPU/内存消耗占比及当前网络传输情况支持用户针对客户端进行锁定，锁定后其他用户需解锁后使用（以公安部检测报告为准）支持修改用户密码、用户切换、下载客户端使用说明书，同时支持支持查看系统名称、系统版本信息以及系统授权有效期支持多机部署，即不同服务器上分别安装一个电视墙服务，在电视墙客户端上支持用户选择要操作的电视墙服务并且支持选择不同解码器添加到不同服务上支持预览上墙、回放上墙、轮巡上墙、报警上墙，支持客户端所在PC机的系统桌面上墙功能支持电视墙单窗口按1/2/4/6/8/9/12/16/25/36多画面分割显示（以公安部检测报告为准）支持根据监控点名字、标签名字和报警名字模糊搜索点位录像，并支持以颜色区分录像类型。红色为报警录像，蓝色为计划录像支持批量下载、锁定或解锁录像，录像被锁定时在存储设备中不会被覆盖支持搜索、查播放、下载标签录像，支持查看录像的标签内容、点位名称、录像开始时间及结束时间支持打开/关闭视频实时报警功能，当打开该功能时，若有新报警产生，页面自动弹出报警联动画面支持查询、删除视频报警记录信息，并根据不同颜色区分报警紧急程度，支持针对报警点位进行预览、回放及临时撤防（以公安部检测报告为准） | 1 | 套 |
| 2 | 视频运维 | 支持视频运维概况；支持视频监测功能；支持设备告警查询；支持视频质量、取流情况等统计报表展示 |
| 3 | 数据库 | 数据存储。数据库软件，系统自带PostgresSQL，可选择自购Oracle数据库 |
| （二）、前置汇聚平台硬件配置清单 |
| 1 | 智能应用服务器/基础服务组件服务器 | 部署智能应用模块，部署名单库管理、数据级联组件、API后端适配器、智能车辆数据服务、联网共享组件、电视墙组件等服务，为应用提供支撑。（1） 机箱：2U（2） 处理器：X86架构，4颗处理器（4114(10核2.2GHz）（3） 内存通道≥6个，支持24个DIMM内存插槽，配置128G （4） 网络：≥4个千兆电口+4个万兆光口（5） 支持≥16块热插拔硬盘位，至少支持4块3.5寸硬盘，配置600GSAS硬盘×4块，支持2个M.2插槽（6） PCIe扩展： 最大支持6个（7） IO：USB 3.0接口≥6个（8） 阵列卡：配置独立的阵列卡，支持RAID 0、1、10（9） 工作温度：可支持45度(TDP≤125W)（10）800W铂金冗电(1+1)（11）可支持中文BIOS界面（二级目录）  | 2 | 台 |
| 2 | 设备接入服务器/智能接入服务器/运维服务器 | 部署设备接入服务，单台设备可以支撑每3000台监控设备/6000视频通道的接入。（1） 机箱：2U（2） 处理器：X86架构，4颗处理器（4114(10核2.2GHz）（3） 内存通道≥6个，支持24个DIMM内存插槽，配置64G （4） 网络：≥4个千兆电口+4个万兆光口（5） 支持≥16块热插拔硬盘位，至少支持4块3.5寸硬盘，配置配置600GSAS硬盘×4块，支持2个M.2插槽（6） PCIe扩展： 最大支持6个（7） IO：USB 3.0接口≥6个（8） 阵列卡：配置独立的阵列卡，支持RAID 0、1、10（9） 工作温度：可支持45度(TDP≤125W)（10）800W铂金冗电(1+1)（11）可支持中文BIOS界面（二级目录） | 2 | 台 |
| 3 | 数据库服务器 | 部署数据库；4114(10核2.2GHz)×2/64G DDR4/600G 10K SAS×4（RAID\_10）/SAS\_HBA/1GbE×2+10GbE×2/Win Svr 2016 简中标版/550W(1+1)/2U/16DIMM | 1 | 台 |
| 4 | 流媒体服务器 | 部署流媒体服务，单台设备可以支撑150路4M码流视频的取流；【4114×1/32GB DDR4/600G 10K SAS×2（RAID\_1）/SAS\_HBA/1GbE×2+10GbE×2】×2/800W (1+1) /2U | 2 | 台 |
| 5 | 联网网关转码服务器 | 部署级联网关服务：单设备可以支撑400路4M码流的视频流并发取流；机箱：1U服务器电源：AC100~240V功耗：≤200W网络接口：8个，千兆以太网口USB接口：2个 USB 3.0VGA接口：1个 VGA输出口MIC：1个音频输入：1个音频输出：1个功能参数：支持GB/T28181标准协议实现平台间联网；平台可通过联网网关实现对级联系统的目录查询、实时点播、云台控制、视音频文件检索、视音频文件回放及回放控制、系统布防撤防、设备信息及状态查询、视音频文件下载、系统设备远程启动等功能；单台联网网关可同时接入多个异构平台，内置多个千兆网络接口，支持端口聚合绑定、负载均衡；支持协议网关与媒体网关分离的工作模式；能将国标码流实现无损转发；▲设备支持同时接入多个异构平台，实现转码、转发功能（以公安部检测报告为准）；设备支持将非GB/T28181-2016中规定的封装格式的码流转码成GB/T28181-2016中规定的封装格式码流；设备内置千兆网口，支持网口的聚合绑定、负载均衡；▲千兆网络环境下，设备单业务板卡应支持1600M码流转发（以公安部检测报告为准）；设备支持将H.265码流转码为H.264码流；▲设备支持将高分辨率、高码率、高帧率视频流转换至低分辨率、低码率、低帧率视频流（以公安部检测报告为准）；设备支持20万个前端监控点资源的容量；多台部署时支持流转发的负载均衡策略；设备支持控制协议网关和媒体网关分离的操作模式；设备支持通过级联方式实现扩容； | 4 | 台 |
| 6 | 运维服务器 | 4114(10核2.2GHz)×2/64GB DDR4/600G 10K SAS×2/SAS\_HBA/1GbE×2+10GbE×2/550W(1+1)/2U/16DIMM | 1 | 台 |
| 三、公共安全视频图像信息共享平台-资源接入部分 |
| 1 | 局办接入服务器-局办点位超过300路 | 部署视频级联服务，单台可以支撑150路4M码流并发；【4110×1/32GB DDR4/600G 10K SAS×2（RAID\_1）/SAS\_HBA/1GbE×2+10GbE×2】×2/800W (1+1) /2U | 4 | 台 |
| 2 | 局办接入服务器-局办点位不超过300路 | 部署视频级联服务，单台可以支撑50路4M码流并发；4110(8核2.1GHz)×1/16GB DDR4/1TB SATA×2/SAS\_HBA/1GbE×2/Win Svr 2016 简中标版/550W(1+1)/2U/16DIMM | 2 | 台 |
| 3 | 局办接入硬盘录像机-32路 | 硬件规格：2U标准机架式2个HDMI，2个VGA,HDMI+VGA组内同源8盘位，可满配6TB硬盘2个千兆网口2个USB2.0接口、1个USB3.0接口1个eSATA接口支持RAID0、1、5、10，支持全局热备盘报警IO：16进4出（可选配8出）软件性能：输入带宽：320M32路H.264、H.265混合接入最大支持16×1080P解码支持H.265、H.264解码Smart 2.0/整机热备/ANR/智能检索/智能回放/车牌检索/人脸检索/热度图/客流量统计/分时段回放/超高倍速回放/双系统备份 | 2 | 台 |
| 4 | 局办接入硬盘录像机-64路 | 硬件规格：2U标准机架式2个HDMI，2个VGA,HDMI+VGA组内同源16盘位，可满配6TB硬盘2个千兆网口2个USB2.0接口、1个USB3.0接口1个eSATA接口支持RAID0、1、5、10，支持全局热备盘软件性能：输入带宽：320M64路H.264、H.265混合接入最大支持16×1080P解码支持H.265、H.264解码Smart 2.0/整机热备/ANR/智能检索/智能回放/车牌检索/人脸检索/热度图/客流量统计/分时段回放/超高倍速回放/双系统备份 | 4 | 台 |
| 5 | 监控硬盘 | 6TB/256MB(6Gb/秒)/7200RPM/SATA3 | 68 | 块 |
| 四、公共安全视频图像信息共享平台-网络交换 |
| 1 | 行业平台接入交换机 | 交换容量≥336Gbps（如官网存在双数值，以较小值为准）；包转发率≥96Mpps（如官网存在双数值，以较小值为准）；固定接口：GE电口≥24,10GE光口≥4；支持IPv4/IPv6静态路由，支持RIP/RIPng，OSPF；设备内置图形化智能管理中心；支持10KV业务端口防雷能力；配置2个单模万兆光模块。 | 8 | 台 |
| 2 | 行业单位接入交换机 | 交换容量≥336Gbps（如官网存在双数值，以较小值为准）；包转发率≥27Mpps（如官网存在双数值，以较小值为准）；固定接口：GE电口≥8,GE光口≥2；支持IPv4/IPv6静态路由，支持RIP/RIPng，OSPF；设备内置图形化智能管理中心；支持10KV业务端口防雷能力；配置2个单模千兆光模块。 | 14 | 台 |
| 3 | 全流量威胁检测系统 | 尺寸 1U架构硬盘容量 系统盘：128G(SSD）数据盘：2T(企业盘 7200转）内存 16G内存接口数量 6个千兆电口、2个SFP光口、1个串口（RJ45）、1个USB口电源 单电源吞吐率 应用层：600Mbps部署模式 旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响设备信息 支持展示CPU、内存、磁盘利用率进行实时监控，同时支持对核心的资源占用率进行实时分析吞吐量 支持实时、24小时、最近一周所有镜像口吞吐率展示安全事件攻击阶段分布 支持通过系统漏洞、遭受攻击、C&C通信、内网探测、内网扩散、盗取数据、黑产牟利等安全事件阶段分布展示和下钻分析安全事件类型分布 支持受影响主机安全事件分类展示业务、终端安全状态分布 支持业务、终端安全状态分布展示，支持弱密码、明文传输等系统脆弱性展示风险业务视角 具备失陷(业务和终端)主机详细分析，包含攻击阶段分布、风险等级趋势、安全事件举证、开放端口等信息。攻击阶段包含存在漏洞、遭受攻击、C&C通信、黑产牟利、内网扫描、内网扩散、盗取数据；存在的漏洞风险包含漏洞风险、配置风险、明文传输、弱密码；支持对每个安全事件详细举证分析，包含风险危害、处置建议、专杀工具等（需提供截图证明并加盖原厂商公章）风险终端视角 支持终端维度展示终端IP、所属终端组、风险等级、安全事件标签、处理状态、联动状态，风险等级包含已失陷、高危、中危、低危、信息等。支持终端的详细分析，包含风险评估、攻击阶段分布、风险等级趋势、安全事件举证等信息。（需提供截图证明并加盖原厂商公章）安全事件视角 支持待处置安全事件描述、事件标签、攻击阶段、事件分类、失陷确定性、威胁等级、风险主机统计、发生时间、处理状态以及自定义待处置事件；支持攻击阶段分布和事件类型分布，热点事件统计。（需提供截图证明并加盖原厂商公章）资产管理 支持感知业务/服务器资产，可定义IP地址、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息。支持感知终端资产，可定义终端/ip组、主机名、用户名、用户邮箱等信息，并支持基于流量自动识别终端。支持受监控内部IP组名、IP范围、IP属性、更新时间、责任人等自定义添加。（需提供截图证明并加盖原厂商公章）。弱密码 支持镜像流量检测业务系统中的弱密码，检测列表包含账号、密码、服务器、所属分析和业务、最近登录源IP、类型、最近发现时间等信息，密码星号显示需超级管理员才可查看，并支持储存数据包内容（需提供截图证明并加盖原厂商公章）。明文传输 支持镜像流量检测web流量中是否存在可截获的口令信息，检测列表包含对应域名/URL、服务器IP，所属分支和业务，数据包举证等信息，避免因明文传输导致信息泄露的风险。（需提供截图证明并加盖原厂商公章）。主机安全风险报告 支持展示需要处理的风险主机与风险状况报告，报告内容包括业务与终端风险、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。综合风险报告 支持完整展示网络的安全态势和详情的综合风险报告，报告内容包括系统说明、安全风险概括、业务与终端安全详情分析、安全规划建设建议等。DNS检测 支持DNSFlow分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意DNS协议。SMB检测 支持SMBFlow分析引擎，发现主机传输可疑文件、恶意软件行为、文件或关键目录的可疑操作行为以及SMB暴力破解等。AD域控检测 支持对AD域控服务器安全检测，发现主机对域控服务器DNS探测、SMB会话枚举、账户探测、暴力破解等攻击行为。同步AD域协议审计日志，主要用于平台AD域分析引擎进行安全分析。文件威胁深度检测 系统具备独立文件威胁鉴定模块，支持基于HTTP、邮件、FTP、SMB等协议的文件检测，系统内置病毒检测引擎、人工智能检测引擎等，支持记录恶意文件、文件名、病毒病毒、发现次数、传播协议、感染源等信息，并支持导出分析结果。邮件深度检测 系统具备独立邮件威胁模块，支持机器学习技术发现主机发送可疑附件的邮件行为、伪造发件人发送邮件、发送钓鱼网站邮件和垃圾邮件等行为，包含接收恶意邮件、恶意附件、危害和处置建议；支持对恶意邮件详情分析，包含收件人账号、恶意邮件数量、发件人账号、附件名称、病毒名称、恶意链接名称等，并支持导出分析结果。威胁情报 系统具备独立威胁情报分析模块，支持自定义威胁情报，可定义域名、IP、URL、文件MD5、确定性等级、威胁等级、事件类型、危害描述、处置建议等信息。基础特征库升级 具备漏洞特征识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、白名单库，其中漏洞特征识别库 9000+以上规则，僵尸网络识别库35万以上规则，支持定期自动升级或离线手动升级（需提供截图证明并加盖原厂商公章）。深度检测引擎升级 支持DNS审计日志，主要用于系统dns flow分析引擎进行安全分析；HTTP审计日志，主要用于系统http flow分析引擎进行安全分析；SMB审计日志，主要用于系统SMB flow分析引擎进行安全分析；同步SMTP、POP3、IMAP审计日志，主要用于系统Mail flow分析引擎进行安全分析。基础检测能力 具备报文检测引擎,可实现IP碎片重组、TCP流重组等,  具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和域名记录。深度监测能力 对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型;支持MYSQL/RDP/SMB/FTP/TELNET/邮件等的暴破检测；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。Web应用安全检测能力 支持HTTP 1.0/1.1，HTTPS协议的安全威胁检测；支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测；支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；支持对被Web网站是否被挂黑链进行检测僵尸网络检测 支持对终端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；具备独立的僵尸主机识别特征库，恶意软件识别特征总数在35万条以上；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，并下发威胁特征；安全组件接入展示 支持接入防火墙、终端EDR（需提供功能截图证明并加盖原厂商公章）EDR组件联动 支持与同品牌终端EDR组件联动响应，禁止攻击流量出站或入站，也可以实现被感染主机IP封锁隔离，防止风险扩展（需提供功能截图证明并加盖原厂商公章）。防火墙设备联动 支持与同品牌防火墙进行联动响应，支持系统下发安全策略到防火墙上，阻断攻击流量。（需提供功能截图证明并加盖原厂商公章）。僵尸网络查杀工具 一款集本地查杀与云查杀功能于一体的恶意软件查杀工具。在云端上具备强大的病毒库，可以识别现有网络上大多数活跃的病毒威胁；在本地中又拥有强大的扫描引擎，通过对程序的静态分析以及动态虚拟执行的方式，让恶意软件无处遁形。（需提供功能截图证明并加盖原厂商公章）威胁维基库 针对主流漏洞、攻击方式等有详细而专业的介绍，并提供了专业实用的安全建议。（需提供功能截图证明并加盖原厂商公章）三年原厂软硬件质保和规则库升级 | 1 | 台 |
| 4 | 视频防火墙 | 设备吞吐量为100Gbps，至少支持同时处理12000路4M码流视频准入控制能力，具备4千兆电口，4个千兆光口，8个万兆光口，2U机架式设备，配置双电源。具备主动探测与被动流量识别技术。开通防火墙基本功能（NAT、路由、访问控制ACL、IPSec VPN、DDoS、会话控制、用户认证、流控、双机等）、URL过滤、邮件安全、僵尸网络检测（含云端沙盒检测）、风险分析、威胁情报功能、入侵防护IPS、Web防护、网关防病毒模块；三年原厂软硬件质保和规则库升级。▲支持视频终端主动扫描，并且扫描间隔时间可设置（需提供相关功能截图证明并加固原厂商公章）支持单向及控制方向的传输支持主流协议：支持SIP协议信令控制；支持识别IPC是否采用GB28181标准接入，对不符合国标的终端可进行告警和阻断；▲支持对<<GB 35114-2017 公共安全视频监控联网信息安全技术要求>>视频协议的信令进行控制，如标准中明确规定的SIP视频协议中注册REGISTER，邀请INVITE等信令的访问控制；（需提供相关功能截图证明并加固原厂商公章）支持访问控制规则支持模拟策略匹配，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(需提供相关功能截图证明)支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制支持接入摄像头如海康、大华等设备安全性检查，弱口令和摄像头高危漏洞等安全风险并提供防御能力支持对防护的服务器安全性检查，能够发现操作系统、中间件、应用漏洞等安全风险并提供防御能力设备具备独立的入侵防护漏洞规则特征库，特征总数在7400条以上；支持自动生成综合安全风险报表，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统计，具备有效攻击行为次数统计和攻击举证；（提供安全报表截图证明）支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机IP地址；（需提供相关功能截图证明）支持高级威胁事件分析，并展示热点事件详情，如全网威胁情报、高级黑客、持续性攻击、网站存在后门（webshell）、黑链、感染流行僵尸网络、大面积病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警；（需提供相关功能截图证明）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；（需提供具备相关云端查杀能力的报告） 支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于AI技术的病毒检测报告； （需提供相关功能截图证明）提供《计算机信息系统安全专用产品销售许可证》，提供复印件并加盖厂商公章；所投产品厂商为国家互联网应急中心CNCERT国家级网络安全应急服务支撑单位，提供证书复印件并加盖厂商公章；所投厂商具备软件开发成熟度CMMI 5级认证，提供证书复印件并加盖厂商公章；所投厂商具备云安全成熟度成熟度模型CSA-CMMI 5认证，提供证书复印件并加盖厂商公章； | 1 | 台 |
| 5 | 核心交换机 | 1.支持最大交换容量≥153Tbps；整机包转发能力≥36000Mpps；业务插槽位数量≥6，主控槽位≥2；支持冗余电源模块≥2；支持主控板1+1冗余以太网支持千兆电口，千兆光口，10GE端口、40G端口、100G端口支持SDN/OPENFLOW标准；支持多控制器；支持多表流水线；支持Group table；支持FCOE、TRILL、EVI和EVB数据中心特性；以上要求提供官网截图。多虚一技术(N:1)；2.支持并配置RRPP（快速环网保护协议）功能支持并配置基于端口、协议、子网和MAC的VLAN划分功能，支持并配置SuperVlan功能；支持并配置Jumbo Frame功能；支持最大VLAN MAPING/灵活QinQ表项；支持VLAN MAPPING能力；支持并配置IEEE 802.1ad（QinQ），灵活QinQ功能；支持并配置IEEE 802.3ad（链路聚合）和跨板链路聚合功能；3．支持并配置RIP、OSPF V2、IS-IS和BGP协议功能，组播协议必须支持IGMP V1/V2/V3 Snooping、PIM-SM、PIM-DM、PIM-SSM和MSDP，支持并配置等价路由功能；支持并配置策略路由和路由策略功能；支持并配置RIPng、OSPF V3、IPv6 IS-IS和IPv6 BGP功能，隧道协议必须支持IPv6手动隧道、6to4隧道和ISATAP隧道，支持PIM-SMv6、PIM-DMv6、PIM-SSMv6；支持并配置DHCPv6、ACLv6等功能；4.支持AC板卡，POE，POE+，支持原生的无线AC功能，无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能。只要保持无线AP的IP可达，拔出任意接口板，均不影响无线AC管理无线AP功能；5.支持FLOGI/PLOGI和DCBX功能6.支持并配置IEEE 802.1x和IEEE 802.1x SERVER功能支持并配置MAC认证功能支持并配置AAA/Radius功能支持SSHv1.5/SSHv2支持ACL流过滤机制支持OSPF、RIPv2 及BGPv4 报文的明文及MD5密文认证7.至少具备8个QoS优先级，通过服务质量策略（特别是优先权规则和算法）为关键业务和特定应用预留带宽；支持Ingress/Egress CAR，粒度可达8Kbps提供广播风暴抑制功能；支持VLAN聚合CAR，MAC聚合CAR功能； | 1 | 台 |
| 五、配套设备 |
| 1 | 会议平板 | 智能交互会议平板需要采用86英寸LED背光源整屏幕分辨率不得低于3840×2160@60HZ，满足超高清4K分辨率显示要求；亮度≥450 cd/㎡，对比度≥4000：1；响应时间不大于6ms，可视角度：水平178°,垂直178°支持接口类型包括：HDMI IN\*2路；HDMI OUT\*1路；VGA 接口\*1路；AUDIO IN\*2 路；AUDIO OUT；SPDIF OUT\*1路，EARPHONE\* 1 路 USB接口： 2个前置，2个后置操作系统 支持Android5.0， Android6.0、Android7.0 及以上采用4核Cortex-A53，主频1.5 GHz，2G内存，32G存储容量，15W\*2，解码支持H.265、H.264，支持UHD60采用红外触控技术，至少支持20点触控，触控精度不大于1mm防眩光防爆钢化玻璃，支持2路RJ45接口，内置网络交换机功能支持无线投屏，可同时支持安卓、Windows任一操作系统下实现联网互通功能会议平板具备在安卓定时开关机功能，提供图形化设置界面，支持用户自定义设置定时循环周期（需要提供第三方检测报告证明） | 1 | 套 |
| 2 | 电视机 | 配套85寸以上电视一台，（1）屏幕尺寸：85英寸。（2）屏幕比例：16：9.（3）cpu核数：4核。（4）运行内存：3GB，存储内存 ：16GB。 | 1 | 台 |
| 3 | 笔记本 | （1）第九代英特尔酷睿i7标压处理器。（2）内存：16GB DDR4 2666MHz 。（3）硬盘：1TB / 512GB PCIe×4 NVMe SSD，预留第二个 M.2 PCIe/SATA SSD 卡位，可与机械硬盘位替换使用。（4）支持双屏显示和4K视频播放。（5）USB-C 和 HDMI 视频输出。 | 1 | 台 |
| 六、运维服务 |
| 1 | 3年驻点服务 | 需要提供2名驻点人员，开展运维服务工作。主要工作内容为平台的运行维护。一、全程参与“雪亮工程”项目建设，在服务期内提供区级雪亮工程平台（上虞）驻场服务。1、具备电子类、计算机类、通信类助工及以上职称，且有3年以上相关工作经验。 2、负责检查雪亮各平台、系统运维情况，并负责管控障碍修复时限，定期形成巡检记录，留档保存，定期向甲方汇报；3、能独立完成雪亮工程相关的软硬件安装、配置、调试等维护工作，对故障问题有一定的分析能力和解决能力，拥有良好服务意识及协调能力；4、平常驻点在甲方正常上班。如遇重要节假日，重大安保事件需要24小时驻点服务的，需进行定期的轮班值班，相关值班人员报备甲方相关人员。有参观、检查等活动需做好系统操作演示、讲解、培训等工作。5、遵守法纪，遵守各项规章和制度；有较强的责任感和事业心，准时到岗到位；了解合同货物的设计，熟悉其结构，有相同或相近维保、现在工作经验，能够正确地进行工作协调、指导；身体健康，适应工作条件。中标方需提供驻场服务人员的简历及相关资格证明文件。二、在服务期内，如发生系统运行故障或出现瑕疵与缺陷，中标方需第一时间提供技术支持和维护服务：驻场人员在系统报修15分钟内进行响应并处理，若现场驻场工程师无法解决问题，1小时内联系原厂服务运维工程师远程解决问题。若远程无法解决的，4小时内联系原厂服务商安排技术人员到达故障现场，设备配置问题在4小时内修复。若因设备硬件本身的问题，在4小时内未能修复货物的，要求为甲方免费提供备用货物。三、如人员配置影响平台运行稳定，或人数不能满足日常需要，甲方有权要求追加人数或更换人员，提高专业水平，且不发生费用；如中标方需更换驻场人员，须提前30天向甲方书面申请，说明更换原因，得到甲方同意后方可更换。 四、驻场人员的保密要求现场服务人员需符合保密法规定，一旦发生泄密涉密事件，中标方负全部责任，并按国家和地方的有关法律法规进行处理。 | 1 | 套 |
| 七、机房租赁 |
| 1 | 机房环境租赁费 | 机房环境租赁 机房应为标准IDC机房，单机柜功耗不低于3000W，双路交流PDU供电；机房系统应包括机房装修工程、电气配电系统、空调系统、消防工程、安防工程、环境监控系统工程、防雷接地系统、机房机柜系统、综合布线系统等；安防和环境监控需提供远程实时查看和≥3个月的历史录像查阅、告警短信通知； | 3 | 年 |
| 2 | 链路租赁费 | 提供不低于1000M带宽，区内局办原则上裸纤接入。 | 22 | 条 |
| 3 | 平台与政务外网互联租赁费 | 需提供至少千兆政务外网出口，按甲方实际需求免费升级 | 1 | 条 |

注：投标供应商必须保证所有设备为原装正规渠道行货,有原厂服务，最终用户为绍兴市上虞区大数据发展管理中心，如有需要则提供正规渠道等证明，所有产品均原包装到用户，当场开箱验货。投标供应商中标后签订合同前必须提供该项目原区电子政务核心机房承建单位租赁意向证明原件，提供视联网核心服务平台系统、视联网/统一视频监控融合调度平台系统视频图像信息应用平台、智能应用服务器/基础服务组件服务器、设备接入服务器/智能接入服务器/运维服务器、视频防火墙等设备的授权代理证书原件，供货前必须提供原厂服务保修承诺原件(复印件无效，服务承诺书要求有明确服务年限与服务级别)。由原厂认证工程师到本地完成系统规划、整改、搭建及测试,不得影响原有业务系统。

## 第三章　供货范围及要求

1　一般要求

1.1　中标人须保证提供货物为全新的、先进的、成熟的、完整的和安全可靠的，且货物的技术经济性能符合本部分第一章规定的要求。

1.2　中标人应提供详细供货清单，清单中依次说明型号、数量、产地、生产厂家等内容。

1.3　除有特别注明外，所列数量均为一套（台）所需。对于属于整套货物运行和施工所必需的部件，即使在本部分第一章中未列出或数目不足，中标人仍须在执行合同时补足。

1.4　中标人应提供所有安装和检修所需专用工具和消耗材料等，并提供详细供货清单。

1.5　提供随机备品备件和　质保期内 运行所需的备品备件，并在投标文件中给出具体清单。

1.6　提供所供货物中的进口件清单。

1.7　中标人提供的技术资料清单。

1.8 投标供应商必须保证所有设备为原装正规渠道行货,有原厂服务，最终用户为绍兴市上虞区大数据发展管理中心，如有需要则提供正规渠道等证明，所有产品均原包装到用户，当场开箱验货。投标供应商中标后签订合同前必须提供该项目原区电子政务核心机房承建单位租赁意向证明原件，提供视联网核心服务平台系统、视联网/统一视频监控融合调度平台系统视频图像信息应用平台、智能应用服务器/基础服务组件服务器、设备接入服务器/智能接入服务器/运维服务器、视频防火墙等设备的授权代理证书原件，供货前必须提供原厂服务保修承诺原件(复印件无效，服务承诺书要求有明确服务年限与服务级别)。由原厂认证工程师到本地完成系统规划、整改、搭建及测试,不得影响原有业务系统。中标方需在合同签订后两个月内确保前端点位接入数大于11000路。设备清单中未包含的部分配套，需由中标方按甲方功能要求自行承担。局办因视频调用影响办公的需免费为局办升级带宽。未尽事宜双方以签署补充协议、备忘录等方式协商解决。

2　供货范围。

2.1 中标人要确认本条所列范围，并提供细化清单

3　特别声明

3.1　在本章中，为了方便起见，可能会采取按某种品牌货物的规格和型号予以表述，但并不因此限制或者拒绝投标人以其他能满足本项目技术需求且性能与所明确品牌相当的货物参加投标。

3.2 其他要求：1、货到现场后由中标方负责安装、保管、费用自负。

3.3 中标供应商在签订合同时必须提供该项目的相关产品原厂保修服务承诺原件。

3.4 中标供应商应配备足够的备品备件不少于3%,保证及时维修和更换设备。

## 第四章　技术资料及交付要求

1　一般要求

1.1　中标人提供的资料应使用国家法定单位制即国际单位制，语言为中文。

1.2　中标人提供的资料须组织结构清晰、逻辑性强，内容要正确、准确、一致、清晰完整，能满足项目要求。

1.3　中标人应在合同签订后　30 天内给出全部技术资料清单和交付进度，并经采购人确认。

1.4　中标人提供的技术资料一般可分为投标阶段，配合项目设计阶段，货物监造检验阶段，安装调试、试运、性能验收试验和运行维护服务阶段等四个方面。

1.5　对于其他没有列入合同技术资料清单，却是项目所必需的文件和资料，一经发现，中标人也应及时免费提供。如本期项目为多种货物构成，且实行分期分批供货，后续货物如有改进时，中标人应及时免费提供新的技术资料。

1.6　采购人要及时提供与合同货物设计制造有关的资料。

1.7　中标人提供的技术资料为每台货物　1　套。

2　资料提交的基本要求

2.1　在投标阶段，采购人可根据具体货物提出清单，中标人补充和细化所列技术资料须满足项目初设要求。

2.2　在配合项目设计阶段，中标人应及时提供满足项目设计的资料和图纸。

2.3　在货物监造检验阶段，中标人应提供满足合同货物监造、检验和见证所需的全部技术资料。

2.4　在安装调试、试运、性能试验和运行维护阶段，所需的技术资料包括但不限于：

2.4.1　提供货物安装、调试和试运说明书，以及组装、拆卸时所需用的技术资料。

2.4.2　安装、运行、维护、检修所需的详尽图纸和技术文件，包括货物总图、部件总图、分图和必要的零件图、计算资料等。

2.4.3　货物的安装、运行、维护、检修说明书，包括货物结构特点、安装程序和工艺要求、起动调试要领。运行操作规定和控制数据、定期校验和维护说明等。

2.4.4　中标人应提供备品、配件总清单和易损零件图。

2.5　中标人须提供的其他技术资料包括以下但不限于：

2.5.1　检验记录、试验报告及质量合格证等出厂报告。

2.5.2　中标人提供在设计、制造时所遵循的规范、标准和规定清单。

2.5.3　货物和备品管理资料文件，包括货物和备品发运和装箱的详细资料（各种清单），货物和备品存放与保管技术要求，运输超重和超大件的明细表和外形图。

2.5.4　详细的产品质量文件，包括材质、材质检验、焊接、热处理，加工质量，外形尺寸，水压试验和性能检验等的证明。

2.6　技术资料由采购人提出要求，中标人予以细化。细化后的技术资料清单，经采购人确定后，由中标人根据项目实际，及时、充分地予以提供，并能满足项目进度的要求。

## 第五章　交货期限及要求

1　货物交货期限具体按以下规定执行：

1.1 合同签订后二个月内完成，试运行一个月后经验收后合格交付使用。

1.2　货物交货顺序要满足项目安装进度的要求。

1.3　交货地点：本项目的设备计划安装于上虞区电子政务网络核心机房，如有调整，会及时告知中标人。

2　货物交货顺序要满足项目安装进度的要求。

2.1　交货进度表（详见下表）：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称及型号 | 数量 | 重量 | 交货时间 | 送达地点 | 备注 |
|  |  |  |  |  |  |  |

2.2　备品备件、专用工具和进口件的交货进度，如双方无特别约定，应视为与主货物的交货进度一致。

2.3　交货进度表的序号要与供货范围分项清单序号保持一致。

## 第六章　监造、检验、性能验收试验及要求

1　概述

1.1　本章的规定适用于合同执行期间对中标人所提供的货物（包括对分包外购货物）进行监造、检验和性能验收试验，确保中标人所提供的货物符合本部分第一章的规定要求。

1.2　中标人应在本合同生效后半个月内，向采购人提供与本合同货物有关的监造、检验、性能验收试验标准。有关标准应符合本部分第一章第4.6条的规定。

2　工厂检验

2.1　工厂检验是质量控制的一个重要组成部分。中标人须严格进行厂内各生产环节的检验和试验。中标人提供的合同货物须签发质量证明、检验记录和测试报告，并且作为交货时质量证明文件的组成部分。

2.2　检验的范围包括原材料和元器件的进厂，部件的加工、组装、试验至出厂试验。

2.3　中标人检验的结果要满足采购人的要求，如有不符之处或达不到标准要求，中标人要采取措施处理直至满足要求，同时向采购人提交不一致性报告。中标人发生重大质量问题时应将情况及时通知采购人。

2.4　工厂检验的所有费用包括在合同总价之中。

3　货物监造

3.1　监造依据。根据本合同和　浙江省　的规定，以及国家有关规定。

3.2　监造方式。具体包括文件见证、现场见证和停工待检三种。每次监造内容完成后，中标人和监造代表均须在见证表上履行签字手续。中标人复印3份，交监造代表1份。

3.3　监造内容（详见下表）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 监造部套 | 监造内容 | 监造方式 | 检验数量 |
| 文件见证 | 现场见证 | 停工待检 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

3.4　中标人必须配合监造的要求。

4　性能验收试验

4.1　性能验收试验的目的为了检验合同货物的所有性能是否符合本部分第一章规定的要求。

4.2　性能验收试验的地点由合同确定：采购人现场。

4.3　性能试验的时间：具体试验时间由采购人和中标人确定；单台货物的试验供需双方协商确定。

4.4　能验收试验由采购人主持，中标人参加。试验大纲由采购人提供，与中标人讨论后确定。如试验在现场进行，中标人要按要求进行配合；如试验在工厂进行，试验所需的人力和物力等由中标人提供。

4.5　性能验收试验的内容，视具体货物而定。

4.6　性能验收试验的标准和方法，按具体货物要求填写。

4.7　性能验收试验所需的测点、一次元件和就地仪表的装设应由中标人提供，参加方配合。中标人也要提供试验所需的技术配合和人员配合。

4.8　性能验收试验的费用。本章第19.7条和中标人试验的配合等费用已在合同总价内。其他费用，如试验在现场进行，由采购人承担；在中标人工厂进行，则已包含在合同总价之中。

4.9　性能验收试验结果的确认。

**4.9.1　采购人在中标人送货后对本项目进行检查验收，如果发现数量不足或有质量、技术等问题，中标人应负责根据合同及使用单位的要求采取补足或更换等处理措施，并承担由此发生的一切损失和费用。验收合格后，采购人在验收单上签字并加盖单位公章。未尽事宜双方以签署补充协议、备忘录等方式协商解决。**

4.9.2　进行性能验收试验时，一方接到另一方试验通知而不派人参加试验，则被视为对验收试验结果的同意，并进行确认签名盖章。

## 第七章　付款方式及要求

付款方式：

**本次项目分设备租赁费用（公共安全视频图像信息建设联网应用总平台设备）及运行维护费（“一总两分”平台驻点维护及链路、机房租赁费）二部分进行分别付款,中标单价一次性包死，不再调整，经采购人分级审批认可的数量增减，在结算时按中标单价按实调整。**

**设备租赁费用所有费用按年支付，租用期限自系统验收合格签订租赁合同之日算起，租赁合同签订后一个月内采购人支付中标项目设备租赁费用的50%并付清配套会议设备采购费用；对系统运行质量、服务质量进行考核后，一年租赁期满后15个工作日内支付中标项目设备租赁费用的20%；对系统运行质量、服务质量进行考核后，二年租赁期满后15个工作日内支付中标项目设备租赁费用的10%；三年期租赁期限满后一个月内经考核合格支付中标项目设备租赁费用的20%。**

**根据财政厅相关文件规定，本租赁项目三年到期后，综合绩效考评较好，经承租方认可后可续租两年。续租满一年后15个工作日内支付中标项目租金总额的17%，续租两年到期后15个工作日内支付中标项目租金总额的17%。**

**运行维护费用按年支付，在每年对系统运行质量、服务质量进行考核后，第一年度租赁期满后15个工作日内支付中标维护费用的34%；第二年度租赁期满后15个工作日内支付中标维护费用的33%；第三年度租赁期满后15个工作日内支付中标维护费用的33%。如租赁项目三年到期后，综合绩效考评较好，经承租方认可后可续租两年，则续签两年每年的维护费用按中标维护费用的33%，在单年度租赁期满后15个工作日内支付。**

## 第八章　售后服务及要求

1　质保要求

1.1　中标人对提供的货物须提供不少于36个月的保修质量保证期限，除不可抗力造成的损坏以外，如续签需提供原厂延保服务等。

1.2　在质量保证期限内双方的权利和义务按第五部分规定执行。

2　安装和调试要求

2.1　货物的安装和调试工作由中标人负责，并承担相关费用。

2.2　中标人应在下列规定时间内完成货物的安装和调试工作：

2.2.1　合同签订后二个月内完成，试运行一个月后经验收后合格交付使用。

3　维修服务要求

3.1　在接到采购人的故障通知后，中标人须在15分钟内作出响应，并在最短的时间内提出解决方案，直至修复货物。

3.2　中标人须按下列规定的要求，为采购人提供维修服务：

投标人须提供经调试、试运行、验收合格后至少3年的质保期(投标人可根据自身实力作出更长时间的质保承诺,各设备及软件指标要求中若有特别要求的还需按指标要求执行)。无论在质保期内还是质保期满后，中标供应商负责对其实施的项目提供现场服务。在服务期内，如发生系统运行故障，或出现瑕疵与缺陷，中标人将按照下列方式提供技术支持和维护服务：系统报修故障响应时间15分钟，若现场驻场工程师无法解决问题，1小时内联系二线运维工程师远程解决问题。若远程无法解决的，4小时内安排技术人员到达故障现场，若因设备配置问题，4小时内修复，若因设备硬件本身的问题，24小时内解决。中标人在保修期限内为采购人提供上门维修服务。在24小时内未能修复货物的情况下，须为采购人免费提供备用货物。中标人在规定时间内无法解决故障，采购人有权自行向第三方服务商寻求技术服务，所产生的一切费用由中标人承担。在服务质量保证期间，中标人应免费提供咨询服务，免费处理因质量、性能、功能等各类影响系统使用发生的故障，免费提供相关软件、系统的小版本升级服务，并进行正常维保服务。每季度需提供运行报告。中标方须制定包含平台与政务外网互联出口带宽，局办视频调用带宽等的维护升级方案、制度，维护升级内容须在测试环境压力测试无问题后晚上调整，与维护本项目相关的所有费用由中标方负责。中标人在项目验收后需将所有设备资料、秘钥等技术资料全数交给甲方，并无条件按要求做好二期扩展支撑工作，因一期中标方不支持不配合等原因造成二期项目延期或无法开展，甲方有权扣除或不支付尾款。未尽事宜双方以签署补充协议、备忘录等方式协商解决。

4　技术服务要求

4.1　中标人须派合格的现场服务人员，为采购人提供上门技术服务，确保所供货物安全、正常投运。在投标阶段应提供包括服务人数的现场服务计划表（详见下表）；如果此人数不能满足工程需要，中标人要追加人数，且不发生费用：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 技术服务内　　容 | 计　划人 数 | 派出人员构成 | 备注 |
| 职称 | 人数 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |

4.2　中标人现场服务人员应具有下列资质：

4.2.1　遵守法纪，遵守现场的各项规章和制度；

4.2.2　有较强的责任感和事业心，按时到位；

4.2.3　了解合同货物的设计，熟悉其结构，有相同或相近机组的现场工作经验，能够正确地进行现场指导；

4.2.4　身体健康，适应现场工作的条件。

4.3　服务人员情况表

4.3.1　中标人要向采购人提供服务人员情况表（详见下表）：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 姓　　名 |  | 性　　别 |  | 年龄 |  | 民族 |  |
| 政治面貌 |  | 学校和专业 |  | 职务 |  | 职称 |  |
| 工作简历 |  |
| 单位评价 |  |

4.3.2　中标人须更换不合格的中标人现场服务人员。在填写时，服务人员的工作简历包括参加了哪些工程的现场服务；单位评价按第21.2条规定的内容逐条作出评价。

4.3.3　服务人员情况表应一人一表，并加盖中标人单位公章。

4.4　中标人现场服务人员的职责。

4.4.1　中标人现场服务人员的任务主要包括货物催交、货物的开箱检验、货物质量问题的处理、指导安装和调试、参加试运和性能验收试验。

4.4.2　在安装和调试前，中标人技术服务人员应向采购人技术交底，讲解和示范将要进行的程序和方法。对重要工序，中标人技术人员要对施工情况进行确认和签证，否则采购人不能进行下一道工序。经中标人确认和签证的工序如因中标人技术服务人员指导错误而发生问题，中标人负全部责任。

4.4.2.1　中标人提供的安装、调试重要工序表（详见下表）：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工序名称 | 工序主要内容 | 备注 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

4.4.3　中标人现场服务人员应有权全权处理现场出现的一切技术和商务问题。如现场发生质量问题，中标人现场人员要在采购人规定的时间内处理解决。如中标人委托采购人进行处理，中标人现场服务人员要出委托书并承担相应的经济责任。

4.4.4　中标人对其现场服务人员的一切行为负全部责任。

4.4.5　中标人现场服务人员的正常来去和更换事先与采购人协商。

4.5　采购人的义务。采购人要配合中标人现场服务人员的工作，并在生活、交通和通讯上提供中标人方便。

5　培训服务要求

5.1　为使合同货物能正常安装和运行，中标人有责任提供相应的技术培训。培训内容应与工程进度相一致。

5.2　培训计划和内容由中标人在投标文件中列出（详见下表）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 培　训内　容 | 计　划人 数 | 培训教师构成 | 培　训地　点 | 备注 |
| 职称 | 人数 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

5.3　培训的时间、人数、地点等具体内容由供需双方商定。

5.4　中标人为采购人培训人员提供货物、场地、资料等培训条件，并提供食宿和交通方便。

6　其他服务要求：　　　　　　　　　 　。