上海市公安局闵行分局视频图像监控租赁经费（2025 年）项目

单一来源采购文件

项目编号：SN20250212

采购人：上海市公安局闵行分局

招标代理机构：上海申诺招标代理有限公司

2025 年 04 月

2025年04月27日

2025年04月25日

目　录

协商邀请函

根据《中华人民共和国政府采购法》之规定，受采购人委托，就上海市公安局闵行分局视频图像监控租赁经费（2025 年）项目进行单一来源采购，欢迎符合报名条件的投标人前来报名。

一、采购内容

上海市公安局闵行分局视频图像监控租赁经费（2025 年）项目采购。（详细要求见采购文件）

本项目系《上海市电子政府采购管理暂行办法》（下称《上海电子政采办法》）所规定的电子政府采购。采购人、招标代理机构、投标人以及招标程序皆应符合《上海电子政采办法》（沪财采[2012]22号）第十七、十八、十九条的规定，由此产生的后果，由投标人自行承担。

二、投标人报名条件

1. 必须按照《上海市政府采购供应商登记及诚信管理办法》完成登记（网址：www.zfcg.sh.gov.cn），未完成登记的供应商，必须按规定完成登记手续，并根据《上海市数字证书使用管理办法》等规定向本市依法设立的电子认证服务机构申请用于身份认证和电子签名的数字证书，并严格按照规定使用电子签名和电子印章；

2. 投标人须为符合《中华人民共和国政府采购法》第二十二条规定的供应商；

3. 根据财政部《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库[2016]125 号）的规定，列入失信被执行人、重大税收违法案件当事人、政府采购严重违法失信行为记录名单的供应商（以在“信用中国”网站（www.creditchina.gov.cn）和中国政府采购网（www.ccgp.gov.cn）查询的记录为准），将被拒绝参加本项目；

4. 投标人的营业执照须含有相应的经营范围；

5. 本项目面向大、中、小企业采购；

6. 本项目**不允许**联合体投标。

三、招标文件的获取

时间：2025-04-28 至 2025-05-07，上午 00:00:00~12:00:00-12:00:00，下午 12:00:00~23:59:59-23:59:59 截止，登录“上海政府采购网”（http://www.zfcg.sh.gov.cn）在网上招标系统中自行下载招标文件。

四、开标时间及地点

1. 投标截止时间：2025 年 05 月 09 日 13:30；

2. 投标地点：本次投标采用网上投标方式，投标人应根据有关规定和方法，在上海市政府采购云平台的门户网站上海政府采购网（http://www.zfcg.sh.gov.cn）（简称：采购云平台）提交；

3. 开标时间：2025 年 05 月 09 日 13:30；

4.开标地点：通过上海市政府采购网（www.zfcg.sh.gov.cn）以线上远程形式开标，不再进行现场开标。投标人应根据有关规定和方法，在采购云平台参加开标会议；

5.协商时间：2025 年 05 月 09 日 14:00

届时请供应商代表持投标时所使用的数字证书（CA 证书）及可以无线上网的笔记本电脑（要求自带 3G/4G 上网卡，能正常登陆上海政府采购网系统）参加投标；

6.协商地点：上海市杨浦区江浦路 1188 号 2 座阳明商务中心二楼 1026 室。

7.组织协商当日，投标人必须派被授权代表按时到现场。

五、发布公告的媒介：

以上信息若有变更我们会通过“上海政府采购网”通知，请供应商关注。

六、电子招投标系统的使用须知

供应商应确保CA证书在本投标项目进行过程自始至终处于有效状态，中途不得对证书进行任何更换及更新，并严格按照《 上海市政府采购云平台 》 电子招投标系统的要求及步骤进行投标，任何由于供应商自身 CA 证书及电子招投标系统信息录入错误等导致的项目挂起均由供应商承担相关责任。

第一章 投标人须知及前附表

前 附 表

序号	内 容
1	项目名称：上海市公安局闵行分局视频图像监控租赁经费（2025 年）项目 项目编号：SN20250212 项目预算：194182445.27 本项目最高限价为：194182445.00 采购标的对应的中小企业划分标准所属行业：租赁和商务服务业 单一来源采购对象：中国电信股份有限公司上海分公司
2	采购人：上海市公安局闵行分局　　地址：银都路 3700 号
3	招标代理机构：上海申诺招标代理有限公司 地址：上海市杨浦区江浦路 1188 号 2 座阳明商务中心二楼 1026 室 联系人：贺贤 电话：55780339-802 传真：55961231
4	响应有效期：开标后 90 天 本项目不收取投标保证金，不收取纸质投标文件。
5	响应截止时间：2025 年 05 月 09 日 13:30（北京时间） 注：供应商上传的投标（响应）文件需在投标(响应)截止时间前在采购平台收到代理机构的签收回执方才生效。未签收的投标（响应）文件视为投标(响应)未完成。
6	开标日期：2025 年 05 月 09 日 开标时间：13:30（北京时间） 开标地点：通过上海市政府采购网（www.zfcg.sh.gov.cn）以线上远程形式开标，不再进行现场开标，投标人应根据有关规定和方法，在采购云平台参加开标会议。
7	交货期：/ 工期：/ 服务期限：一年
8	付款方式：按季度支付。本项目中标方需分包合同金额 40%给中小企业，中标方需提供分包合同给甲方，此合同作为支付最后一季度尾款依据。
9	对单一来源采购文件澄清的提问截止时间：2025 年 05 月 08 日上午 09：00
10	答疑会：本项目是否召开答疑会：（否） 答疑会时间：无　　答疑会地点：无
11	本项目是否现场踏勘（否） 踏勘时间：无 踏勘地点：无
12	本项目是否提供样品：（否） 投标人须按协商文件规定的时间、地点及具体数量、式样等要求送达样品，未按招标文件要求送样或逾期的将做无效标处理。

	中标的投标人样品将由甲方封样。未中标的投标人应在本项目中标公告发布后 10 个工作日内将样品取回，逾期未取回的样品将视作投标人放弃样品处置权，无主样品由代理公司统一处理。
13	资格符合性检查 凡出现下列情况之一者，将予以无效标处理，不进入后续评审： 1.未提供在“信用中国”网站（www.creditchina.gov.cn）和中国政府采购网（www.ccgp.gov.cn）报名当天网页截图证明的； 2.不符合《中华人民共和国政府采购法》第二十二条规定的； 3.所报价格超过本项目预算资金的； 4.投标文件未实质性响应招标文件要求的； 5.投标有效期不足的； 6.招标文件明确规定可以作无效标处理的其他情形。
14	招标服务费：中标方在本项目招标完成后的七天内向招标代理机构支付招标服务费。 服务费金额：人民币陆拾万元整（RMB600000.00）。 账户名：上海申诺招标代理有限公司 开户银行：交通银行股份有限公司上海控江路支行 账号：310066535018120054346 摘要：SN20250212
15	采购项目需要落实的政府采购政策情况：本采购项目执行政府采购有关鼓励支持节能产品、环境认证产品以及支持中小企业、残疾人福利性企业等的政策规定，详见第二章。
16	《中华人民共和国政府采购法》第二十二条规定供应商参加政府采购活动应当具备下列条件： （一）具有独立承担民事责任的能力； （二）具有良好的商业信誉和健全的财务会计制度； （三）具有履行合同所必需的设备和专业技术能力； （四）有依法缴纳税收和社会保障资金的良好记录； （五）参加政府采购活动前三年内，在经营活动中没有重大违法记录； 法律、行政法规规定的其他条件。
17	（六）上海政府采购网电子投标软件平台咨询电话：95763

投标人须知

1.总则

1.1 适用范围

本招标文件适用于本须知前附表第 1 项所列项目的采购。

1.2 投标费用

投标人应承担所有与编写和提交投标文件有关的费用，不论投标的结果如何，采购人和招标代理机构在任何情况下均无义务和责任承担这些费用。

2.招标文件

2.1 本招标文件包括：

（1）投标邀请函

（2）投标人须知及前附表

（3）政府采购主要政策

（4）项目需求

（5）评审办法

（6）投标格式

（7）合同条款及合同格式

2.2 投标人应认真阅读招标文件中所有的章节、条款、格式、图纸、附表和附件。如果投标人没有按照招标文件的要求提交全部资料，或者投标文件没有对招标文件在各方面都做出实质性响应，则属于投标人的风险。根据本须知规定，没有实质上响应招标文件要求的投标将被拒绝。

2.3 投标人应认真审阅招标文件的所有内容，如果在收到招标文件后发现有缺页、印刷不清楚或对其中内容不理解而未向招标机构提出，由此导致投标人的投标文件不符合招标文件的要求，其责任应由投标人自负。实质上不响应招标文件要求的投标文件将被拒绝。

3.招标文件的澄清

3.1 任何要求对招标文件进行澄清的投标人，均应在本须知前附表内所规定的截止时间之前，按投标邀请函中的通讯地址以书面形式（如信函、传真或电子邮件，下同）通知招标代理机构，采购人和招标代理机构将以书面形式予以答复，同时将书面答复发给每个获得招标文件的投标人，答复中包括所提问题，但不包括问题的来源。

4.招标文件的修改

4.1 在投标截止期前的任何时候，无论出于何种原因，采购人和招标代理机构可主动地或在解答投标人提出的澄清问题时对招标文件进行修改。

4.2 对招标文件的修改将以书面形式通知所有购买招标文件的投标人，并对其具有约束力。投标人应立即以书面形式确认已收到了修改通知。

4.3 为使投标人在编写投标文件时有充足的时间对招标文件的修改部分进行研究，采购人可以自行决定，酌情延后投标截止期。

5.投标文件的编制

投标人提交的投标文件以及投标人与采购人或招标代理机构就有关投标的所有来往函电均应使用中文。投标人可以提交用其他语言打印的资料，但有关的段落必须翻译成中文，当原文和译文之间存有差异和矛盾时，将以中文为准。

6.投标文件的构成

6.1 投标人编写的投标文件应包括下列部分：

（1）投标函；

（2）报价一览表；

（3）商务、技术规格偏离表；

（4）投标单位基本情况；

（5）投标单位的纳税、社保缴纳、财务情况表；

（6）投标单位项目拟委派人员情况表；

（7）详细项目方案说明；

（8）近几年内完成的类似业绩清单（对其中所列的主要项目应附中标通知书或合同复印件）；

（9）资格证明文件格式；

（10）按招标文件要求提供的其他有关文件。

7.投标函

投标人应按招标文件中所附的“投标函格式”完整地填写投标函。

8.投标

投标人应按照招标文件第五章中所附的“投标表格式”完整地填写投标表，说明所提供货物及服务的详细情况。每种货物及每项服务只允许有一个投标，任何有选择的投标将不予接受。

9.投标货币

本次招标项目的投标应以人民币（RMB）报价。

10.资格证明文件

10.1 按照本须知的规定，投标人应提交证明其有资格参加投标和中标后有能力履行合同的文件，并作为其投标文件的一部分。

10.2 投标人提交的证明其有资格参加投标和中标后有能力履行合同的文件应能使采购人和招标代理机构满意。

11.证明货物或服务合格性的文件

11.1 按照本须知的规定，投标人应提交有关证明文件，证明其按合同要求提供的货物或服务的合格性，并能满足招标文件的要求。证明文件应作为投标文件的一部分。

11.2 证明提供的货物或服务合格性的文件应包括投标表中对标的物内容等的声明。

11.3 证明提供的货物或服务能够满足招标文件要求的文件可以是文字资料、图纸和数据，投标人应提供：

（1）主要技术指标和运行性能的详细说明；

（2）为使采购人能够正常、连续地使用所购货物或服务，投标文件中应提供货物或服务从质量保证期结束后壹年内所需的完整的备件和特种工具清单，包括备件和特种工具的货源及现行价格（如果适用的话）；

（3）逐条对采购人要求的“技术规格”进行评议，说明自己提供的货物或服务是否做出实质性的响应，或逐条填报招标文件第五章中所附的“规格偏离表格式”（如果适用的话）。

11.4 投标人在按照要求进行阐述时应注意：如果采购方在“技术规格”中给出了的工艺、材料和相关的标准或者参照的牌号及分类号，则它们仅仅起说明作用，并没有任何限制性，投标人在其投标文件中可以选用替代的标准、牌号或分类号，但这种替代要实质上优于或相当于“技术规格”中的相关要求，并能使采购方满意。

12.投标有效期

12.1 投标人的投标应从本须知规定的开标之日起，在本须知前附表规定的以日历天计算的投标有效期内保持有效。投标有效期比规定短的可以视为非响应标而予以拒绝。

12.2 在特殊情况下，在原投标有效期届满之前，采购人可征得投标人的同意延长投标有效期。这种要求与答复均应采用书面形式。投标人可以拒绝采购人的这种要求而不被没收投标保证金。同意延长投标有效期的投标人既不能被要求也不允许修改其投标文件，但要相应延长其投标保证金的有效期。

13.投标文件的式样和签署（电子签名）

13.1 投标人应按照“投标人须知”的要求，准备纸质投标文件正本副本套数；每套文件均须清楚地标明“正本”或“副本”；一旦正本和副本内容不符，将以正本内容为准。纸质投标文件与网上上传电子投标文件内容不符的，以上传的电子投标文件为准。

13.2 投标人应先按招标文件要求制作成册的投标文件之后，再通过扫描制成未加密的电子投标文件。制作电子投标文件过程中，由于扫描文件的分辨率不佳、汇标项的相应链接错误等原因导致评标时对投标人不利等后果，由投标人自行承担。

13.3 投标人应在上海政府采购网下载电子招标文件后，应使用上海政府采购网提供的客户端投标工具编制投标文件，并使用其数字证书进行电子签名。

13.4 投标文件的正本和副本均应使用不能轻易擦去且不易褪色的档案墨水书写或用打印机打印，投标文件的副本也可用复印机复制。不论是书写、打印或复制，均应做到清晰、整洁、规范。

13.5 投标文件的正本应由投标人的法定代表人或经正式授权并对投标人有约束力的代表签字。由授权代表签字时，须在投标文件中加附“法定代表人授权书”，其格式应符合招标文件的规定。

13.6 除投标人对错漏之处做必要修改或补充外，投标文件中不得有随意的行间插字、涂改和增删。如

确有错漏之处确需要手工修改或补充，则必须由投标人的法定代表人或其授权代表在修改或补充之处签字和盖章。

13.7 投标文件副本的上述签名及盖章之处既可由投标人的法定代表人或其授权代表亲笔签署，也可以通过复印将上述签名及盖章复制到副本上。

13.8 投标人根据招标文件的要求，在投标文件及相关文件的签订、履行、通知等事项中需单位盖章处，均需加盖单位公章，此单位公章仅指与当事人名称全称相一致的标准公章，不包括投标专用章、合同专用章、财务专用章等带有“专用章”字样的印章,否则将被视为无效。

13.9 各投标人应将纸质投标文件装订成册，编制目录及注明页码，且将目录设置为第 1 页，依次逐页增加页码，所有分隔页包括空白页以及样本或图片等技术资料也必须连续编制页码，且采用胶装密封。并请提供用光盘或 U 盘为载体的包括全部报价文件内容的电子文档 1 份，密封在报价文件的正本内，该电子载体不再退还。

14.投标文件的递交

14.1 投标文件的密封（加密）、标记和发送（上传），投标人应按《上海电子政采办法》规定对制作的电子投标文件进行加密、签名并在规定的投标截止期前上传。由于投标人的原因造成其电子投标文件未能加密而致电子投标文件在开标前泄密的或其他情况，则由投标人自行承担相关责任。

14.2 投标截止期，投标人上传经加密的投标文件及招标代理机构收到书面投标文件时间不得迟于本须知前附表中规定的截止日期和时间。投标截止期后上海政府采购网不再接受投标人上传电子投标文件。

14.3 迟交的投标文件，按照《上海市电子政府采购暂行管理办法》规定执行，招标代理机构将拒收并原封退回在其规定的投标截止期后收到的任何投标文件。

14.4 投标文件的修改和撤回

14.4.1 投标人在递交投标文件后，按照《上海市电子政府采购暂行管理办法》规定可以修改或撤回其投标文件，但必须在规定的投标截止期之前，以书面形式通知招标代理机构。

14.4.2 投标人的修改或撤回通知书应按规定进行签署、密封（加密）、标记和发送（上传）。在纸质投标文件的内层信封上加注“修改”或“撤回”字样。

14.4.3 在投标截止期之后，投标人不得对其投标文件做任何修改。

14.4.4 在投标截止期至采购人和招标代理机构在投标有效期届满之间的这段时间内，投标人不得撤回其投标，否则其投标保证金将被没收。

15.开标

15.1 投标截止，采购云平台显示开标后，投标人进行签到操作，投标人签到完成后，由招标人解除采购云平台对投标文件的加密。投标人应在规定时间内使用数字证书对其投标文件解密。签到和解密的操作时长分别为半小时，投标人应在规定时间内完成上述签到或解密操作，逾期未完成签到或解密的投标人，其投标将作无效标处理。有证据能证实是因系统原因导致投标人无法在上述要求时间内完成签到或解密的除外。如采购云平台开标程序有变化的，以最新的操作程序为准。

15.2 上海政府采购网显示开标之后，由招标代理机构解除上海政府采购网对电子投标文件的加密。所有登陆的投标人应对其上传的投标文件进行解密。由于投标人因自身原因未能将其电子投标文件进行解密的，则视作为该投标人放弃本项目投标。

15.3 投标文件解密后，上海政府采购网将根据投标文件中开标一览表的内容自动汇总生成开标记录表。

15.4 投标人应及时检查开标记录表的数据是否与其投标文件中的投标报价一览表一致，并作出确认。投标人应及时使用数字证书对《开标记录表》内容进行签名确认，投标人因自身原因未作出确认的视为其确认《开标记录表》内容。

16.评审过程的保密性

16.1 公开开标后，直至向中标单位授予合同为止，凡与对投标文件的审查、澄清、评价和比较有关的资料以及授标意见等，均不得向投标人及与评审无关的其他人透露。

16.2 在评审过程中，如果投标人试图在投标文件的审查、澄清、评价、比较及授予合同方面向采购人和招标代理机构施加任何影响，其投标将被拒绝。

17.投标文件的澄清

17.1 为有助于对投标文件的审查、评价和比较，采购人和招标代理机构可要求投标人对其投标文件进行澄清，有关澄清的要求和答复应以书面形式提交，但不得寻求、提供或允许对投标价格或投标文件中的其他实质性内容做任何更改。

18.投标文件的初审

18.1 开标后，招标代理机构将审查投标文件是否完整，有无计算上的错误，是否提交了投标保证金，文件的签署是否合格，投标文件是否大体编排有序。

18.2 在详细评审之前，采购人和招标代理机构将审查投标文件是否实质上响应了招标文件的要求。实质上响应的投标应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离或保留的投标。所谓重大偏离或保留是指实质上影响合同的供货范围、质量和性能，或者实质上与招标文件的要求不一致，而且限制了合同中采购人的权利或减轻了投标人的义务。纠正这些偏离或保留将会对其他实质上响应要求的投标人的竞争地位产生不公正的影响。采购人和招标代理机构判定投标文件的响应性只根据投标文件本身的内容，而不寻求外部的证据。

18.3 如果投标文件实质上没有响应招标文件的要求，采购人和招标代理机构将予以拒绝，投标人不得通过修正或撤销不符合要求的偏离或保留，而使其投标成为实质上响应的投标。

18.4 招标代理机构将对确定为实质上响应的投标进行审核，看其投标是否有计算上或表述上的错误，修正错误的原则如下：

（1）如果用数字表示的金额与用文字表示的金额不一致，将以文字表示的金额为准。

（2）当单价与数量的乘积与总价不符时，将以单价与数量的乘积为准修正总价。

19.资格符合性检查

凡投标人或其递交投标文件出现本须知前附表资格符合性检查所列的情况，则该投标人所递交的投标

文件将予以否决。

20.投标文件的评价和比较

20.1 采购人和招标代理机构将按照本须知的规定，只对确定为实质上响应招标文件要求的投标进行评价和比较。

20.2 评审的基础应是本须知规定的投标及投标文件技术部分。

20.3 在通过实质性响应条款审查的基础上，协商小组根据单一来源采购文件要求和供应商提供响应文件情况，就采购项目需求、合同主要条款及价格与供应商进行协商，商定合理的成交价格并保证采购项目质量。

20.4 协商小组编写协商情况记录，并由协商小组全体人员签字认可，具体操作以上海政府采购网操作系统中单一来源协商程序为准。

20.5 采购人根据协商小组的协商情况记录确定成交供应商。

21.授予合同

采购人应将合同授予被确定为实质上响应招标文件要求，能够满意履行合同义务，经协商小组评审确认的投标人。

22. 签订合同

22.1 中标人与采购人应当在《中标通知书》发出之日起 30 日内签订政府采购合同。

22.2 中标人应根据合同条款的规定，按照招标文件中提供的履约保证金格式向采购人提交履约保证金（如有）。

23.采购人更改采购货物数量的权利

在授予合同时，采购人经财政局同意后对项目服务内容和数量等予以增加或减少，但不得对单价或其他的条款和条件作任何改变。

24.采购人接受和拒绝任一或所有投标的权利

采购人保留在授标之前的任何时候接受或拒绝任一投标、宣布招标程序无效或拒绝所有投标的权利，对受影响的投标人不承担任何责任，也无义务向受影响的投标人解释采取这一行动的理由。

25.中标通知书

25.1 在投标有效期届满之前，招标代理机构将向中标单位发出中标通知书。

25.2 中标通知书将成为合同的组成部分之一。

26.签订合同

26.1 采购人在通知中标单位其投标被接受的同时，将就招标文件中规定的体现双方之间所有协议的合同执行细则和中标单位进行洽谈。

26.2 中标单位在收到中标通知书后十天内应派其授权代表与采购人在规定的地点签订合同。

第二章 政府采购主要政策

根据《政府采购法》等法律法规及相关规定，政府采购应当有助于实现国家的经济和社会发展政策目标，包括保护环境，扶持不发达地区和少数民族地区，促进中小企业发展、促进残疾人就业的作用，进一步保障残疾人权益等。

如上政策适用于不同项目的需求：

1）符合条件的中小企业；

2）符合条件的残疾人福利性单位；

3）列入财政部、国家发展改革委发布的“节能产品政府采购清单”且属于应当强制采购的节能（包括节水）产品，按照规定实行强制采购；

4）列入财政部、国家发展改革委发布的“节能产品政府采购清单”的非强制采购节能产品；

5）列入财政部、环保总局发布的“环境标志产品政府采购清单”的环境标志产品。

上述“节能产品政府采购清单”、“环境标志产品政府采购清单”，在采购公告发布前已经过期的以及尚在公示期的均不得作为评标时的依据。如果有国家或者上海市规定政府采购应当强制采购或优先采购的其他产品和服务，按照其规定实行强制采购或优先采购。

对于参与投标的中小企业以及残疾人福利性单位，按照国家和上海市的有关政策规定，评标时在同等条件下享受优先待遇，实行优先采购（残疾人福利性单位属于小型、微型企业的，不重复享受政策）。政府采购对于非专门面向中小企业采购，对小型和微型企业投标人产品的价格给予 10%的扣除，用扣除后的价格参与评审。如果政府采购非专门面向中小企业采购且接受联合体投标，联合协议中约定小型或微型企业的协议合同金额占到联合体协议合同总金额30%以上的，给予联合体4%的价格扣除，用扣除后的价格参与评审。联合体各方均为小型或微型企业的，联合体视同为小型、微型企业。组成联合体的大中型企业或者其他自然人、法人或其他组织，与小型、微型企业之间不得存在投资关系。

根据财库〔2020〕46 号，符合条件的中小企业在参加政府采购活动时，应当提供《中小企业声明函》（见格式），并对声明的真实性负责。

根据财库〔2017〕141 号，符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》（见格式），并对声明的真实性负责。

第三章 项目要求

采购需求

一、项目概述

1、项目建设背景

近年来，公安图像监控系统建设规模日益扩大、功能不断完善，在道路交通管理、社会治安防控、处置突发事件、重大安全保卫等各项工作中得以广泛应用并发挥了重要作用,视频监控逐渐成为维护国家安全和社会稳定、预防和打击暴力犯罪、提升城市管理水平及创新社会治理体系的重要手段。当前，视频监控信息已成为信息化、智能化条件下支撑上海各项城市管理工作的重要基础信息资源。加强公共安全视频监控建设联网应用工作，最大限度发挥公共安全视频监控应用效能是提升社会治安防控能力与水平、推进平安上海建设的重要抓手和措施。目前，本区监控探头数为 9780 个，占全市已建总量的 10.8%，覆盖率为 26.4 个/平方公里，在全市处于中下游水平。为落实中央综治办部署的“雪亮工程”建设任务，根据上海市公安局“智慧公安”建设规划，我区将进一步提升本区图像监控设备的质量、数量及智能化水平。

2、项目建设目标

本项目在现有公安标准及技术框架下，对原一期建设的模拟标清视频监控等视频监控资源进行改造，整合区内多年以来城市治安电子防控系统建设中的电子警察、高清治安卡口等视频图像资源，在城市交叉路口、公共区域临街面、制高点和治安复杂的重点区域新建一批数字高清摄像设备，从而为公安的视频侦查、治安管理以及刑侦追逃提供有效的实战帮助和解决方法，实现闵行区“重要部位全覆盖、重点路口全摄入、社会管理联成网、侦查办案有证据、维稳防控有实效”的建设目标。

3、服务范围、内容

3.1 服务范围

向闵行区提供视频图像监控设备。

3.2 服务内容

（1）监控前端，提供一期存量高清点位 1163 路、存量卡口点位 862 路、存量车载（无线）移动视频图像 12 路、存量移动终端功能费 408 路、二期新建高清视频点位 1659 路、二期改造高清监控点位 7932 路、二期卡口点位 438 路、二期监控点位 2057 路、二期高空瞭望点位 16 路、二期车载（无线）移动视频图像点位 60 路、二期数据处理能力达到 12500 路、二期前端接入（即社会图像接入）1481 个、二期水域瞭望点位（60 倍）14 个、二期水域瞭望点位（30 倍）7 个。

（2）网络服务，为本项目提供专用网络，由前端汇聚至附近的分控中心机房，各分控中心通过万兆链路组成环网，并通过双万兆链路上联至分局机房。

（3）应用系统服务，包括高清视频监控应用子系统、高清治安卡口应用子系统、视频云子系统、警务终端 APP、运维管理子系统、云计算资源池、存储资源池、GIS 子系统、信息安全子系统及区级视频共享平台建设等。

（4）分控中心机房建设，包括四个分控中心的电源、空调、装修、机架等配套建设。

（5）通信线路建设，包括配套光缆、立杆、管道、引电等内容。

二、总体要求

1、建设原则

高清视频监控系统的建设以“统一标准、技术先进、突出应用、稳定可靠、资源共享、信息安全、经济适用”为原则，确保系统满足闵行城市管理的全局需求。

（1）统一标准

系统建设在符合国家和行业相关标准及地方标准的建设要求基础上，“统一编解码标准、统一联网协议、统一控制协议、统一编号规则、统一图像标注、统一位置标识”，采用先进的技术手段和系统架构，整合治安监控资源、道路监控资源、市政监控资源、社会监控资源和已建视频资源，在同一的标准框架下实现统一部署、资源共享、平台共用，构建全网各种设备接入、各子系统互联互通、区域视频信息系统互联共享的可扩展规模和可升级应用的视频信息管理系统。

（2）技术先进

采用主流的、先进的技术构建系统平台，满足可视化社会治安防控需要，为城市数字化管理、公安治安监控、政府市政管理、应急联动指挥等业务提供支撑，促进城市图像信息综合应用，使闵行区城市可视化管理、应急指挥和治安防控数字化水平进入全市先进行列。

（3）突出应用

系统的建设必须突出应用，鉴于系统技术复杂，投资巨大，在建设中应以现实需求为导向，以有效应用为核心，以技术建设与工作机制的同步协调为保障，确保系统能有效服务于公安和政府工作的需要，充分利用视频信息资源，结合各种应用业务，围绕打造“智慧城市”、创造“平安城市”、保障和谐的城市环境和良好的社会治安条件，不断提高公安机关预防打击犯罪、加强治安管理和维护社会稳定的能力，不断提高城市管理中的行政执法水平。

（4）稳定可靠

本系统的建设不是各种视频资源的简单组合，而是统一标准构架下的有机组成，系统采用的软硬件根据统一的规范、协议和要求选型，根据最新的标准规范，并经过具有相应资格的软件评测中心、产品检测中心的测试，质量达标，性能稳定，能够持续有效运行，满足公安监控 7*24 小时不间断持续运行的需要。

（5）资源共享

系统的建设应满足公安各部门、各应用系统对监控图像共享的需求，为监控资源数字化整合共享提供接口支持。视频信息不仅要满足治安管理、城市管理、交通管理、应急指挥等的需求，而且还能兼顾灾难事故预警、安全生产监控、环境等方面对视频图像的需求。

（6）信息安全

通过 VPN 或政务外网等非公安网络接入时，需采用严格的网络隔离和安全措施，确保公安专网的信息安全。

（7）经济实用

设计合理、构架简洁、功能完备、切合实际，能有效提高工作效率，满足治安动态监控和公安业务工作需求。在先进、可靠和充分满足系统功能的前提下，体现高性价比。采用经济实用的技术和设备，充分利用现有设施和资源，综合考虑系统的建设、升级和维护费用，实现经济效益和社会效益最大化。

2、建设依据及遵循标准规范

《公共安全视频监控联网系统信息传输、交换、控制技术要求》(GB/T 28181-2016)；

《城市监控报警联网系统技术标准》（GA/T 669-2008）

《公共安全视频监控联网系统信息传输、交换、控制技术要求》(GB/T28181)；

《安全防范视频监控摄像机通用技术要求》(GA/T1127)；

《公安视频图像信息系统安全技术要求第 2 部分:前瑞设备》(GA/T1788.2)；

《公共安全视频监控边界安全交互技术要求》征求意见稿；

3、业务需求要求

（1）治安管理业务

目前，通过有限地增加治安管理基层单位的警力资源已经无法有效应对目前治安管理新局面和新要求。通过增设视频监控设备、联网共享政府部门视频资源，加强治安防控体系建设。

从治安业务管理需求的角度出发，新建系统强调增强监控覆盖密度，重点监控目标，重点关注。治安管理单位在实战过程中迫切需要道路交叉路口的实时和历史视频图像，可以有效回溯治安事件过程。重点区域和重要路段还需要进一步加强监控的覆盖，做到缺遗补漏，同时扩大政府部门监控信息的接入融合，强化视频信息数据的共享。

（2）刑侦管理业务

刑事案件过程的线索追踪和历史复现还原，通过视频图像网络密集的监控前端可以尽可能多地提供图像信息，对刑侦单位侦查破案至关重要。此外，互联共享政府部门自建视频，为应急事件的联动处置，准确判断与指挥提供必要的现场信息资源。在治安卡口应用业务中，结合高清治安卡口采集车辆号牌数据信息，可有效提高涉车案件的侦破效率，提高破案率。

（3）交通管理业务

城市道路交叉口是交通事故、交通肇事逃逸等事件多发地点，目前闵行区已经建成一定数量的电子警察设施和治安卡口设施，但是还有很多的新建道路或路口未部署相应的设施，对深入开展交通管理工作带来一定的影响。

在已有信息化项目应用基础上，本工程将对区内、区界道路尚未建设高清治安卡口的路段进行增补，借助治安卡口杆件同步安装高清全景摄像机，实现对道路断面通行车辆的全车道视频记录，服务于治安业务管理的同时，也可以为交警车辆管理、交通管理提供服务。

（4）消防管理业务

消防监控的侧重点在于通过制高点部署远距离大范围的摄像机，对制高点周边区域火警信号的及时发现和灾情的掌握，为及时扑灭火情提供研判参考。本工程将选取重要高层建筑安装制高点视频监控，进行全方位、立体、动态监控，为火灾险情的及时预报、过程跟踪、事后分析提供现场实时与历史回放视频图像。

（5）保卫管理业务

随着举办的各类综合性大型活动日益增多，需要通过安防系统展现现场实况，实现“扁平化”的协同指挥调度，可以有效帮助警卫部门减轻压力，提升处置应急突发事件的响应能力。

（6）城市管理需求

包括市政、城管、绿化市容、水务、民防等城市管理职能部门通过视频监控系统可及时发现城市管理中存在问题，所获取的图像信息通过与行业应用系统的结合，实现城市管理问题早发现、早解决、早反馈、快速汇总分析，提高管理效率，提升公众满意度。

（7）警务终端 APP 需求

公安民警在开展日常巡检、外勤调用图像、雪亮工程社会点位信息采集、警员运维报障、流程跟踪等工作中，需要访问图像管理、调用及运维系统，在浏览视频的过程中流量需求较大。同时，根据统一要求，警员的 PDA 设备将更换为手机，并通过轻应用来实现管理。

4、 整体功能要求

（1）严格执行相关标准和规范，在分局建设区公安图像联网平台，实现区内跨行业的图像资源接入、共享，尽快形成规模效应，并实现与市级图像联网平台的对接。

（2）新建系统全部为高清视频监控联网系统，扩大和增强视频监控覆盖范围密度，实现全区主要道路路口、重点目标出入口及主要交通节点的监控全覆盖。

（3）在统一部署区图像联网平台，各派出所部署监控客户端，通过区图像联网平台授权，实现对前端授权视频监控点的察看、录像检索、业务数据查看等功能。接入各委办局、街镇村居建设的视频监控资源，为全区的视频监控资源共享创造条件。

（4）实现区图像联网平台与上级相关系统的对接，服务公安业务管理和决策支持，将 GIS 技术与公安信息系统相结合，拉动公安信息整合，全面提升公安信息化应用水平。

（5）通过中心区图像联网平台将治安监控、电子警察等原来各自具有的功能整合，实现其与智能分析等业务子系统的无缝整合，通过统一界面和统一权限管理实现对各业务功能的管理与浏览，同时平台应具有很强的业务扩展能力，能与公安各业务系统实现对接，保证在发生案情时，实现警情互动，视频与数据信息同步。

（6）建设公安分局的图像联网平台及区总平台，其它相关政府部门可通过区总平台实现共享信息，查看视频资源，最大限度实现社会视频监控资源的有序共享。

（7）为满足视频监控业务应用需求，本工程中需完善视频 IP 交换专网，保证大量高清视频监控的联网需求。

（8）对各类智能前端的设备运行状态进行实时监测，自动对前、后端设备的工作状态进行远程巡检，自动识别比较简单的故障类型，具备故障自动告警和日志记录等功能。实现 IT 运维监控，实现对网络、应用系统的全面监控，建立起统一、完善、科学的运维管理流程，逐步实现运维模式由被动式支持转为主动式服务，最终实现一体化的运维监控和管理体系。通过网络对系统设备进行远程升级维护，如智能前端算法的调度、升级、远程软件升级、用户权限更改、中心系统设置配置等。

（9）针对事件等事项属性特点，能通过数据挖掘的方式分析其通过多个智能前端的位置，确定相应相互关系，锁定相应事件的规律。利用大数据系统开放、共享、兼容的特点，灵活开展不同业务系统之间的数据碰撞，智能拓展跨业务系统的多元化应用功能，提升系统的实战成效。可实现对前端智能采集设备所采集的视频片段等资源进行统一管理，并对数据进行转发。可实现对前端智能采集设备所采集的视频片段、将处理后数据统一上传并进行集中存储。

3、存储时间

各类数据存储时间，统一按照国标要求：

（1）基础视频存储时间至少 1 个月，重要目标至少存储 3 个月。

（2）提取类算法的图片至少保存 90 天、视频片段至少保存 30 天，二级处理数据 、图片、附属信息至少保存 1 年。

（3）事件检测类算法的事件截图至少保存 90 天、视频片段至少保存 30 天，报警信息、附属信息等至少保存 1 年。

（4）各类专题库、长期保存。

3、时钟同步

必须配备可以接收 GPS 或北斗等系统授权的 NTP 时间服务器，时钟精度应小于 100ms，应采用 NTP 协议或 SIP 协议对所有设备（包括前端摄像机、管理转发机、存储、子系统服务器等）进行时钟同步，确保全网时间统一。

2.6 存储要求

高清视频监控采用集中存储方案，全部存储于存储分中心。根据规定，高清码流 8Mbps（H.264 编码）估算，每路高清监控视频保存时间 30 天需要约 8*30*60*60*24/8/1024/1024=2.592TB/路。

根据文件要求，图像信息存储采用前端存储和接入平台存储相结合的分布式存储策略，前端和接入图像信息存储时间不小于 30 天，其中重点区域与重要部位的视频信息存储期限应达到 90 天。

高清视频监控系统的高清摄像机按照同时输出以 H.264 编码的高清、标清双码流功能考虑，高清摄像机传输带宽：主码流，高清 1080P，1920×1080 逐行扫描，25 帧，带宽 8Mbps，600 万及以上像素的高清摄像机带宽按照最大码流计算；副码流，标清码流，640×480，25 帧，带宽 2Mbps。

具体存储信息的存储周期要求如下所示：

NVR 存储，高清视频监控文件，存储周期为 30 天；

云存储，高清视频监控文件，存储周期为 7 天；

高清视频二级处理大图，存储周期为 90 天；

高清视频二级处理小图，存储周期为 1 年；

高清视频二级处理数据 ，存储周期为 1 年；

卡口图片（均为大图），存储周期为 90 天；

卡口数据，存储周期为 1 年；

大图数据，存储周期为 90 天；

小图数据，存储周期为 1 年；

相关数据，存储周期为 1 年。

2.7 性能要求

（一）、高清视频监控系统性能要求

1）用于管理公安数字高清监控设备的 PVG 配置要求不低于：

标配 1 颗 Intel 至强 E3 1200 系列 CPU，主频不低于 3.3G；

内存：4G DDR3 1333，最大支持 32G，支持 ECC；

硬盘：不低于 250G；

网络接口：RJ45(10M/100M/1000M Base-T)×2；

USB：外置 USB 2.0，前后面板各 2 个；

串行接口：RS-232×2。

原则上，分县局需配置两台用于管理公安数字高清监控设备的 PVG，互为备份；同时，按每个派出所配置一台，集中部署在分控中心。

2）接入高清探头的 NVR 存储应满足以下性能要求（同时并发所需要的最低处理能力）：

存储所连接的实时高清图像；

同时转发所连接的实时高清图像给本地高清流媒体转发节点；

同时供视频 IP 专网用户调看至少 16 路回放高清图像。

3）高、标清流媒体转发节点

在配置性能上，单节点至少应达到 2 颗六核 E5 系列 2.4GCPU、32G DDR4 内存，1TB 硬盘，双千兆网口、双电源冗余的要求。

流媒体转发单节点转发码流不低于 500Mbps,可转发 60 路 8Mbps 码流的 1080P 高清图像或 240 路 2Mbps 码流的标清图像。

（二）高清监控系统网络及时延性能指标要求如下：

（1）网络性能要求

系统各级之间互联的网络性能指标应达到YD/T 1171-2001中规定的0 级服务质量等级。具体指标如下：

1 ）网络时延上限值为150ms；

2 ）时延抖动上限值为50ms；

3 ）丢包率上限值为1 × 10-3

4 ）包误差率上限值1 × 10-4。

（2）时延指标要求

当信息（包括视音频信息、控制信息等）经由网络传输时，时延指标应满足下列要求：

智能前端设备与用户端设备问端到端延迟时间（不含解码缓存的延时），即用户端首次发起点播信令到接收到前端设备视频流数据包的时延，应≤2500ms 。

监控系统用户端与前端设备控制指令响应时延≤300ms 。

智能前端二级处理数据 转发入库延时应≤2000ms 。

（三）治安卡口性能指标要求如下：

实时性指标

号牌识别时间为从车辆图像捕获到至号牌信息提供所需要的时间，要求该时间：≤60ms。

前端信息采集本地写库的时间要求

前端各断面采集设备，在实时采集并处理生成数据和图片信息后，到信息全部实时写入本地数据库所需要的时间，要求该时间小于20ms。

数据采集中心写库的时间要求

前端各断面采集设备，在实时采集、处理信息后，到这些信息全部写入中心计算机系统数据库所需要的时间，要求该时间小于500ms。

信息查询响应时间

精确查询：查询数据库中某一车辆号牌，查询时间范围为连续4h，计算响应时间，其响应时间应小于3s；

模糊查询：输入连续三位为任意数字的车辆号牌，查询时间范围为连续32天，计算查询响应时间，其响应时间应小于6s。

准确性指标

车辆图像捕获率指所记录的有效车辆数（指车辆图像中包含特写图像要求的车辆数）与实际通过断面车辆数的百分比：≥99%(5～120km/h)，≥97%(120～200km/h)；

号牌识别准确率指号牌信息识别正确（指单排字符结构的号牌信息识别结果全部与实际号牌信息相符；其识别结果为下排序号的识别结果与实际号牌信息相符；对应号牌信息识别结果为序号的识别结果与

实际号牌信息相符）的车辆数与断面号牌信息有效（指车辆号牌完整、安装规范，且无遮挡、无污损）的车辆总数的百分比：白天≥95%，夜间≥90%；

号牌颜色识别准确率指号牌颜色识别正确的车辆数与断面号牌信息有效的车辆数的百分比：白天≥99%，夜间≥97%；

号牌结构识别准确率是指号牌结构识别正确的车辆数与断面号牌信息有效的车辆数的百分比：≥95%

车身颜色识别准确率指车身主体颜色识别正确的车辆数与断面所记录的有效车辆数的百分比：白天≥70%，夜间≥65%；

车辆类型识别准确率指车辆类型识别正确的车辆数与断面所记录的有效车辆数的百分比：≥90%；

信息存储

前端摄像机对本地图片和数据信息至少应保存 15 天。

高清治安卡口中心存储的信息主要包括前端所有治安卡口的图片、数据和系统业务数据信息。其中在磁盘阵列上图片至少可保存 3 个月的信息量，数据信息至少可保存半年的信息量，关键数据和报警数据保存 3 年。

高清全景视频监控在分中心存储的图像视频信息，保存时间不少于 30 天。

其他

同步要求

中心计算机设备与外场设备的时钟达到同步，同步误差控制在 100ms 以内。

图像分辨率：不低于 200 万像素。

色彩模式：RGB，24 位真彩色。

压缩格式：JPEG。

数据格式：车辆经过时间、地点、车道、行驶方向、号牌号码、号牌颜色、车辆图像、车身颜色、车辆类型等。

在通信中断时，前端设备能完整保存相关数据信息，一旦通信恢复正常，设备能自动恢复上传数据信息的功能。

外场设备正常工作环境要求

正常工作温度：－20℃～＋70℃；

正常工作湿度：≤95%；

电源范围：AC 220V 50Hz ±10%；

防护等级：符合 IP65 标准；

抗静电放电、电快速瞬变脉冲、浪涌、电压短时中断等干扰；

具有过载，漏电和短路保护装置，使用快速熔断器来保护内部电路，外壳等金属零部件均与保护接地端子连接并保证各部件的接地连续性，具有专门保护接地端子，室外设备使用避雷器与防雷接地作为防止雷击保护措施，专用接地电阻≤4 欧姆，综合接地电阻≤1 欧姆。摄像机和控制主机之间采用光电隔离方式进行防雷；

设备应节能、环保、易于维护；

系统能连续 7*24h 连续工作，同时在不同光照和环境条件下能正常工作。

系统可靠性要求：系统平均无故障时间（MTBF）大于 30000h。

卡口应用性能

应用系统应满足用户的要求，稳定、可靠、实用；

人机界面友好，输出、输入方便，图表生成灵活美观，检索、查询简单快捷，系统便于维护、扩充；

采用分层数据系统设计技术，使应用系统具有良好的可扩展性、可移植性和可升级性。

（四）区共享平台性能要求

为了确保区级共享平台与市级共享平台之间的视频联网相互兼容，互联互控，安全有序和统一摄像机编号，要求区级共享平台的中心管理设备与上级平台中心管理设备选型一致。每个区共享平台要求配置 2 台双机热备中心管理服务器用于管理本平台的视频资源，同时向上对接市总平台，且要求配置配套的流媒体转发设备，流媒体转发设备按照最高峰值配置相应数量的流媒体转发设备并留有一定的余量，要求至少满足向市总平台上传 100 路高清视频（以 8Mbps 计算）的性能需求。

按照国标 GB/T 28181-2016 要求，联网系统应采用 NTP 协议或 SIP 协议进行时钟同步。区级共享平台应配备可以接收 GPS 或北斗等系统授权的 NTP 时间服务器，时钟精度应小于 100ms。要求配置 2 台双机热备时钟同步服务器。

2.8 信息安全保障要求

本工程信息安全系统的建设应与闵行公安现有安全机制保持一致。根据公安信息系统的业务特点和需要，以及现有的安全状况，系统应建立一个合理、实用、先进、可靠、综合、统一的安全保障体系。

1、身份认证：系统对不同岗位人员实行分级授权，对用户的访问权限实行有效的管理。

2、访问控制：设置隔离网闸、防火墙和网段划分，实现有效的安全隔离和访问控制。

3、入侵检测：在系统关键环节设置入侵监测系统，有效防止非法入侵，及时采取措施。

4、漏洞扫描：采用专业漏洞扫描工具，定期对网络系统及计算机系统进行漏洞扫描，及时发现潜在安全隐患，加以防范处理。

5、病毒防范：在服务器端安装防病毒系统，以提供对病毒的检测、清除、免疫和对抗能力；在客户机和主机安装单机防病毒软件，将病毒在本地清除而不至于扩散到其他机器。

6、数据安全交换：在系统和网络安全的基础上，实现内网和专网间的数据安全交换。

7、安全防护体系：信息系统仅有安全技术防护，而无严格的安全管理相配合，是难以保障网络系统运行安全的。必须建立完善的安全防护系统，从安全规章制度建设、安全管理手段建设等方面保障系统的安全可靠、稳定运行。

2.9 运维要求

随着信息化应用的不断深入，系统管理员将面临管理复杂的、异构的网络系统和主机系统、海量的数据和众多的终端用户，这就要求运行维护管理系统，提高对系统故障的快速响应能力，规范计算机部门的工作流程和规程，保障业务系统安全可靠地运行。除了借助信息化系统来辅助高效、高质地完成

运维管理工作外，高清视频监控系统的建设拟采用运维服务外包的方式，增强政府与企业合作模式，公安民警专注自身业务，实现规模效益最大化。

2.10 测试要求

监控系统有关测试报告需至少包括系统的工程施工质量、系统图像质量的主观评价和录像回放功能测试等三项测试内容，作为系统验收的必要材料。系统图像质量的主观评价和录像回放功能测试必须在已建成的全局统一的管理系统上进行，分局将所建监控系统的所有高清图像资源接入统一上述管理系统，包括高清 IPC、NVR、高标清解码器的国标注册、GIS 电子地图上的摄像机标点（摄像机图标在合适的位置添加、经度纬度输入或批量导入），确保平台上至少能够调用所接入的高清 IPC 的实时流和录像回放流。基于全局信息应用管理系统对分局接入的高清图像资源进行抽查测试，经上级测试通过方后系统方可验收。

1、系统的工程施工质量。系统的工程施工质量测试应依据施工要求，主要以现场观察方式进行。检查完毕后，对该系统总体施工质量情况检测打分。测试结果合格的打“√”，基本合格的打“△”，不合格的打“×”。测试结果记录在《系统施工质量验收表》。

2、系统图像质量的主观评价。在前端监控点接入的首个图像交换系统处用键盘在上屏调看该监控图像高清和标清图像，并在公安视频 IP 专网上通过上海公安图像信息应用管理系统调看和操控高清和标清图像，进行主观评价测试，并检查图像右上角叠加的时间信息是否规范准确。图像质量的主观评价采用五级损伤制评定，由所有评价人员独立打分，取算术平均值为评价结果。功能测试结果合格的打“√”，不合格的打“×”。测试结果记录在《前端图像质量主观评价检测表》。

3、录像回放功能测试。所有的新建前端监控点实现 24 小时实时存储，测试采用现场观察的方式，使用上海图像信息应用管理系统，对录像回放功能进行测试。对输出的图像按五级损伤制评分。通过调阅 30 天前的录像资料或查看硬盘容量的方式确定图像资料保存的期限。测试结果合格的打“√”，不合格的打“×”。测试结果记录在《录像回放功能检测表》。

2.11 GB/T 28181 标准符合性检测要求

本项目涉及的各类国标联网平台必须进行国家标准符合性测试，检测工作须遵照《全国公安机关视频监控系统联网标准符合性检测工作实施方案》进行。国家标准符合性检测包括如下内容：

1、信令一致性检测

分析设备与系统或系统与系统之间的通信数据包，评估 SIP、SDP、MANSCDP、MANRTSP 信令流程及参数的符合性。

2、媒体一致性检测

对视频编解码技术中比特流（编码器）和解码器进行一致性测试，检测编解码的档次和级别、工具选项、码流语法的规定以及媒体流的封装格式。

三、技术要求

3.1 系统总体架构

本期平安闵行二期视频监控系统由前端采集层、网络传输层、数据处理与存储层、应用子系统层、大数据融合层和运维管理体系以及安全管理体系组成，软硬件基础设施主要由云计算和云存储系统提供。系统总体架构分层如下图所示：

1）前端采集层：

本期主要包括前端的监控摄像机、治安卡口等图像信息采集设备。

2）网络传输层：

是指利用光纤链路资源和网络设备建设的万兆 IP 图像专网系统，为数字视频信号、图像业务数据提供传输网络。

3）数据处理与存储层：

实现各类视频设备的联网管理，实现视频直播、点播、转发、录像等视频服务；实现各类视频的二级处理；根据业务需求提供视频数据及二级处理数据的存储。

4）系统层

针对不同的前端设备以及应用场景，对于实时性要求较高的业务提供实时信息，对于实时性要求不高的业务场景向上对视频云子系统输出数据。本期主要包括高清视频监控应用子系统、高清治安卡口应用子系统等。

5）云子系统层

结合视频、卡口等数据实现大数据分析、警情预警和可视化调度、统一展现等功能，为分局总控中心、派出所、业务单位提供图像综合应用。提供图像智能分析和图像智能搜索的功能界面，对涉案视频资源进行管理。

6）管理体系

对项目设备、通信链路进行统一管理，对系统进行监控，实现统一管理、统一告警、故障处理等功能。

7）管理体系

提供系统安全运行机制，通过物理安全、网络安全、主机安全、数据安全、应用安全、虚拟化安全等安全建设，确保满足包括国家信息安全等级保护三级等有关要求。

3.2 逻辑架构

系统逻辑架构由 6 个部分组成，分别为：前端智能采集、接入端管理转发、分析及存储、布控、智能算法调度、综合应用。同时，所有数据通过接入端转发或中间库，汇聚上传，接受全市范围内智能视频资源的管理调度，以及全市范围内的视频图像二级处理数据的存储和智能化应用。

（1）前端智能采集

前端智能采集设备主要有 3 种形态：第 1 种是直接采用智能监控 IP 摄像机，实现轻量化智能算法部署；第 2 种是高清 IP 摄像机加前端智能分析模块，实现标准化智能算法部署；第 3 种是在后端部署智能化分析工具，实现复合型多样化智能算法部署。采集的数据类型应至少包括：视频及多类型图片、必要数据、智能算法的厂商和版本等。

（2）接入端管理转发

前端采集的视频流接入现有的图像监控联网系统，实现视频信号的管理转发；前端采集的多类型图片和视频片段，直接存入分局总控中心的一级处理数据存储模块，汇聚系统可以按需访问获取分局数据存储中多类型图片和视频片段；前端采集的多类型图片和数据通过管理转发设备份两路转发，一路提供给分局，另一路用于上传，提供给全局应用。同时，分局系统处理产生的图片和处理后数据也全部上传。

（3）分析及存储

智能分析系统，通过后端智能分析工具，对有分析需求的智能监控前端采集的视频、图片信息进行补充分析，满足全局的智能图像识别应用。所有视频、图片、处理后数据进行分级存储：完整的视频录像按照原有高清图像监控系统方式存储，或者在视频云存储系统中存储；图片以及视频片段分布式存储在分局一级处理数据存储模块中；二级处理数据分级存储在相应部门的二级处理数据存储模块中，最终统一汇聚上传。

（4）智能算法调度

智能算法调度可统一调度管理前端智能采集设备上运行的智能算法。可根据业务应用需求，结合前端智能采集设备的智能算法能力集，按照时间和空间对智能算法进行变更设置，运用特定的智能算法。前端智能采集设备可以根据用户需求和自身的能力集运行一种或多种智能分析算法。

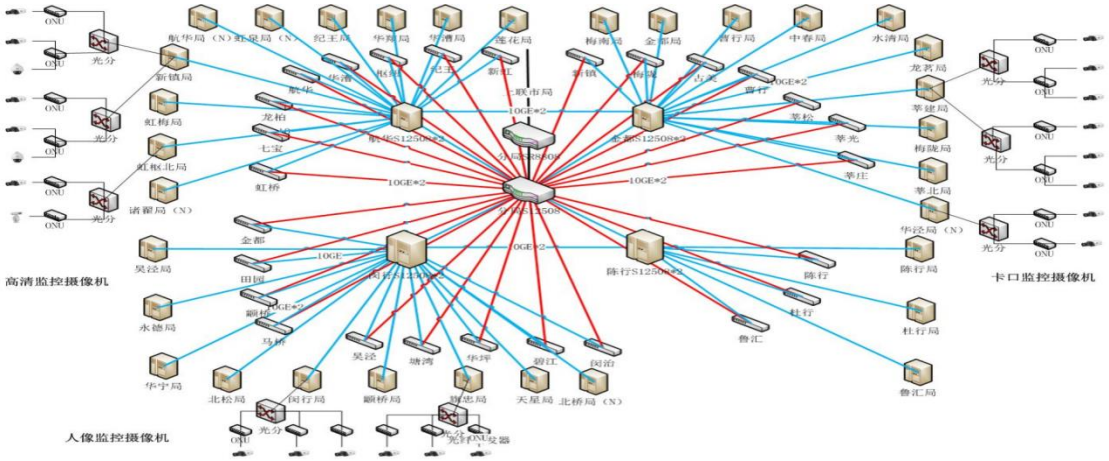
前端智能采集设备需要具备开放性和扩展性，可以运行不同厂家的智能算法，并可以进行智能算法的远程升级。

（5）综合应用

综合应用需要统一监测前端智能采集设备的智能算法，包括获取智能算法的能力集、智能算法的状态、智能算法消耗的资源等信息。

3.3 总体网络架构

本期工程总体网络架构如下图所示：



前端高清摄像机、治安卡口摄像机通过 PON 网络接入所属端局并上联对应分控中心，航华与金都、闵行与陈行增加双万兆链路进行保护，四个分中心均通过双万兆链路上联至分局机房机房之间双万兆链路均采用两条不同光缆路由，保证 99.9%的网络可靠性。四个分控中心部署在莘闵电信的闵行、航华、陈行和金都局。另外，本项目还需新增一条光缆链路（至少保证二芯可用），约 28 公里。

分控中心负责各类视频数据存储及基本管理同时进行一级数据处理；总控中心负责汇聚各子系统二级数据处理之后的数据，进行统一的分析处理和展现，实现基于大数据分析的视频智能应用和警情分析及预警，同时提供可视化调度展现平台。

3.4 系统组成

本期视频监控系统硬件设备部署物理位置见下表：

序号	设备名称	部署地点	备注
1	核心交换机	总控中心	
2	网络安全设备	总控中心	防火墙、入侵防御、防病毒、防篡改等
3	安全管理设备	总控中心	4A、日志审计、数据库审计等
4	云计算资源池	总控中心	高清视频、高清卡口、视频云子系统、运维管理子系统等
5	存储资源池	总控中心	图片存储、数据存储、备份设备
6	汇聚交换机	分控中心	
7	接入交换机	分控中心	
8	网络安全设备	分控中心	防火墙、入侵防御、防病毒等
9	云计算资源池	分控中心	流媒体转发等
10	存储资源池	分控中心	视频云存储

序号	设备名称	部署地点	备注
11	NVR 存储设备	分控中心	
12	视频数据处理设备	分控中心	
13	高清转发服务器	分控中心	
14	高清节点管理服务器	分控中心	
15	解析服务器	分控中心	
16	比对服务器	分控中心	
17	接入交换机	派出所	
18	OLT 设备	电信端局	
19	摄像机及 ONU	前端点位	

3.5 业务流程

1、实时监控业务流程

派出所高清实时监看流程：

高清摄像机将采集的视频信号进行 H.264 编码，码流通过以太网光端机接入相应的分控中心以太网交换机，进入图像专网后在 NVR 和云存储中存储；

派出所通过流媒体服务器从 NVR 获取高清摄像机监看码流输送到通用解码器进行解码上墙；电脑客户端通过流媒体服务器从云存储获取高清摄像机监看码流实现实时监看。

派出所对于其他派出所图像，由分局分配权限，通过骨干网络传输进行图像查看。

指挥中心高清实时监看流程：

总控中心通过骨干网络利用分控中心流媒体服务器调用高清数字视频到指挥中心，既可提供座席终端实时监看，也可直接解码上墙。

2、录像存储及检索回放流程

分控中心监控录像流程：

高清摄像机采用全天高清视频录像的模式，将采集的视频信号转换为 H.264 码流，通过以太网光端机将码流接入相应的分控中心以太网交换机，进入图像专网；

在分控中心，将高清摄像机的 H.264 码流分别存储在 NVR（录像数据 30 天循环覆盖）和云存储中（录像数据 7 天循环覆盖），并自动生成相应的索引数据备查。在分控中心的点播服务器提供视频点播服务。

派出所、指挥中心检索回放派出所、分控中心录像流程

派出所、指挥中心从分控中心检索 7 天以内的 H.264 存储资料；

通过分控中心 H.264 流媒体服务器进行视频回放。

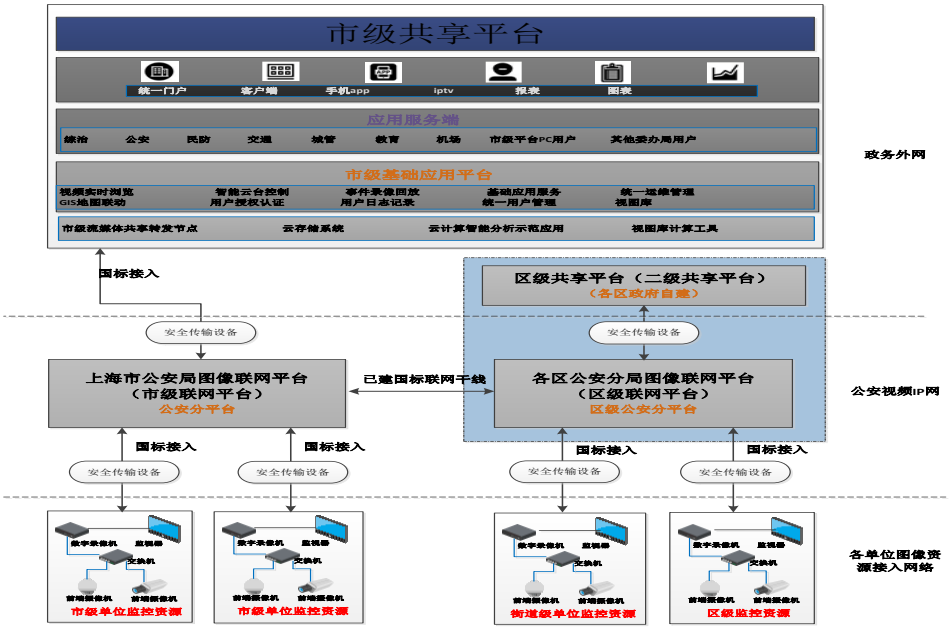
3、智能分析和检索

高清摄像机输出的高清码流可以用于视频智能分析，由流媒体转发服务器将高清视频流转发至高清视频数据处理平台，对视频内容进行处理并保存到图像数据库中，用于检索。

4、大数据融合处理及展现

高清视频监控应用子系统、治安卡口应用子系统等均通过各自管理平台与视频云子系统对接，向视频云子系统输出数据，由视频云子系统结合视频、卡口等数据实现大数据分析、警情预警和可视化调度、统一展现等功能。

3.6 与外部系统的关系上海市公共安全视频监控联网应用采用市、区两级架构，遵循 GB/T 28181 标准开展联网共享，其总体架构如下图所示：



公共安全视频监控联网应用总体架构

本项目建设内容包括区级图像联网平台和区级共享平台两部分。区级联网平台统一采用 GB/T 28181 联网对接各委办局或相关单位联网平台，即各委办局或相关单位联网平台的图像资源就近接入派出所、分控或分（县）局，通过公安数模兼容、三级架构、上下一体、统一管理的图像监控基础联网平台汇聚，再上传至对应的区级共享平台。

视频互联采用的技术手段应是公安现有联网管理手段的延伸，应能融入到公安三级架构体系，与公安已有的 PVG 设备实现无缝对接。

视频联网过程中，应确保信息传输安全，监控资源接入网络必须与公安视频 IP 专网之间实现逻辑隔离，各行业单位图像资源接入公安视频 IP 专网需使用具有访问控制功能的设备实现单向接入，不得将公安视频 IP 专网直接延伸至各行业单位。

1）社会单位监控资源与区级联网平台对接方式

各委办局或相关单位联网平台接入区级联网平台时，各委办局或相关单位网络通过光缆连到公安节点，通过汇聚交换机及访问控制安全设备接入公安视频 IP 专网，并配置安全设备。

采用千兆工业级网络光纤收发器或以太网光端机等实现各委办局或相关单位联网平台至区级联网平台的监控资源传输，端口数量根据接入视频的规模配置单路或多路。

采用访问控制安全设备负责完成社会单位监控资源的传输安全，应通过国家权威机构的测评认证，取得相关资质证书，并获得公安部计算机信息系统安全专用产品销售许可证，支持 TCP/IP 控制协议传输功能、国标联网协议透传功能、UDP 视频流传输功能，包过滤与内容过滤等访问控制功能，支持网管功能，社会单位网络至公安视频 IP 专网的 IP 地址转换功能。

2）区级联网平台与区级共享平台对接方式

区级联网平台通过上海公安视频 IP 专网与政务外网互联，实现图像至区级共享平台的网络连接，通过具有访问控制功能的安全设备实现内外网的逻辑隔离，并配置入侵检测设备。

3）区级共享平台与市级共享平台对接方式

区级共享平台要求部署在政务外网，视频监控部分通过政务外网上联市总平台。

3.7 系统功能

3.7.1 高清智能视频监控

为支撑视频图像信息应用和公安实战业务应用，提高案件侦破效率，提高视频监控系统的应用效能。应用功能需求如下：

1）实时监控：能全帧显示现场探头采集的实时图像，根据实战需要，能看清图像的基本特征。

2)图像控制:授权用户能对任意一路前端高清图像进行切换显示,对带云台探头可进行 PTZ 操作。

3）图像存储与回放：每个监控点的高清图像必须全帧存储 30 天以上，授权用户可调阅指定探头某一时间段的回放录像。

4）流媒体转发：高清 IPC 编码输出的流媒体可通过具备转发能力的节点设备，转发到其他转发设备、显示终端或解码设备。

5）上墙显示：授权用户可以通过图像监控操控键盘或应用软件将高清探头的高清或标清图像切换至监视墙上显示。

6）在线运维：充分利用高清设备网络化和数字化的特点，基于产品已有功能，按需开发运行维护系统，实现对前端探头、网络存储设备、网络交换设备等本系统主要设备的故障实时告警和性能管理，更可以结合自身的业务流程，整合形成完整的巡检、运维和分析功能，有效提升运维工作水平。

7）用户管理：应具备科学分类、合理分级、灵活扩展的特点，既要符合公安用户严格管理的行业需要，又要满足日常便捷设置的操作要求，可实现公安图像监控对内、对外共享过程中用户和资源的安全和高效管理。

扩展应用功能（智能视频分析功能）需求如下：

1）视频信息数据转换：对前端智能采集设备所覆盖区域的车、物等进行多类型图片及二级处理数据 的采集和识别，实现一级处理数据 的转换。

2）行为事件检测：对前端智能采集设备所覆盖区域的特定行为及异常事件等进行检测，并提取视频片段、多类型图片及报警数据。

3)统一管理转发：可实现对前端智能采集设备所采集的视频片段、多类型图片和二级处理数据 进行统一管理，并对图片和二级处理数据 进行转发。

4）数据分布式存储：可实现对前端智能采集设备所采集的视频片段、多类型图片集中存储到一级处理数据 存储模块中，将二级处理数据 统一上传并集中存储。

5）预警信息上传：前端智能采集设备所产生的报警信息及数据布控指令所产生的报警信息，应逐级上传，以实现统一展示。

6）一机一档：对所有前端智能采集设备的基础信息进行采集，建立数据档案，并逐级上传。

7）查询检索：可对所使用的智能算法种类、各种算法的前端数量、报警信息分布情况等各类数据进行精确或模糊查询，对查询结果进行统计。

8）信息展示：可在电子地图上直观地快捷监视、查看、展示信息，丰富系统展示信息量，特别是对于智能的分类统计、报警量的分级分类统计，并生成统计报表。

高清智能视频监控子系统需求如下：

1）联网标准：根据本市公安机关的实际情况开展分级建设，实现三级平台的分层级应用，三级平台逐级级联构成联网系统，必须严格遵循国家标准 GB/T 28181-2016（以下简称国标）要求开展跨域联网。

2)资源管理:依托全局统一的图像监控管理平台,分局通过配置软件独立维护各自监控资源信息,这些信息应统一汇聚到数据库。

3）注册认证：为实现对监控设备的有效管理，建设单位负责对本系统 IPC、网络存储和高标清解码等设备统一编码和注册，编码规则遵照国标附录 D.1 中的编码规则 A，应具有全局唯一性，注册过程严格按照国标要求。建设单位负责入网设备的注册以及有关信息的录入工作，上级负责审核，只有通过审核的监控设备才允许入网正常工作。

4）统一编号：切换监控图像时，高清 IPC 的切换编号延续模拟系统的 8 位编号规则，使用独立的二级编号区分数字高清与模拟标清探头。高清 IPC 的切换编号由建设单位负责分配与管理，应具有全局唯一性。本地高清监视器的编号从 MON 501 开始区分，用户操作键盘时，输入监视器与数字探头编号，系统根据监视器的编号分辨监视器类型，并自动调用高清或标清流解码显示。即用户调阅同一高清监控的高清或标清码流时，仅需要输入同一个监控点编号，系统可根据监视器 MON 号自动识别。

5）两级管理：全局应建立统一的用户认证机制，所有联网用户按照规定流程由上级统一开设。经授权后，有关业务单位可具备管理员权限，可开设本单位用户，并设置共享范围和应用权限。

6）权限分配：图像监控系统建设经费庞大，探头数量、网络传输和运算交换能力都属稀缺资源，需要根据公安的业务特点对每个用户权限内容进行分配。依据建设原则，用户权限的分配应沿用原有模拟系统的分配方式，采用继承的方式进行配置。

7）用户分级：被赋予权限的用户，同时使用同一资源（如前端云台、图像干线等）时，应根据优先级别进行管理。用户级别可量化，每个用户被赋予一个数值属性来表示其级别。高级别用户可以按照一定规则抢占低级别用户的在用资源，相同级别的用户对同一资源同时使用时，最后使用资源的用户获得使用权。

8）日志记录：系统保留用户调用与管理操作的所有痕迹，具备查询、统计和导出等必要功能，可以实时监测系统状态，分析应用绩效和系统性能，并可对违规操作和非法攻击开展倒查。

3.7.2 视频图像联网系统要求

区级联网应配置数字联网接口设备，包括公安视频网关和配套流媒体转发节点。所涉及接入的派出所（分控中心）、公安分局要视实际接入的图像资源数量配置相应数量的公安视频网关和流媒体转发节点以满足对视频接入管理，配置的设备必须完成联网安装调试。

为保障分局视频图像系统的安全性、稳定性、可靠性，及对分局所需视频等的运维管理，视频互联的技术手段采用公安现有联网管理手段的延伸，必须能无缝融入到上海市公安视频联网三级架构体系，与公安已有的联网设备无缝对接。

3.7.3 高清治安卡口监控

系统可对断面进行24小时数据捕获,能提供高清晰的图片。所提供的图片能够清晰辨认车辆类型、车身颜色、所载货物和所处位置，还可提供完整的车头信息，包括完整的牌照，清晰可辨的牌照颜色等。

1)图片信息提。

2)车辆基础信息提取。

3)车辆动态信息提供。

4)交通流参数检测。

5)非机动车信息提取。

6）取机非乱行、非正常运动对象信息。

8)全景视频图像回传：对于安装断面全景摄像机的高清治安卡口，须能实现全景视频图像的实时回传功能，并在上联派出所或分局中心平台进行存储，并通过网络上的互联满足高清治安卡口中心平台的调用与检索，且提供的全景视频图像在清晰度达到1920*1080、流畅度达到25帧/s。全景断面高清摄像机具有高、低双码流（H.264编码）输出能力。

9)提供前端采集设备实时运行状态信息与故障报警信息的：采集范围包括触发单元、抓拍单元、传输单元与预处理单元等设备。

10)数据过滤预处理：为避免不必要的通信、存储与中心数据处理压力，需对采集数据进行初步过滤处理，剔除定义的无效图片，且应能够在保证不丢失有效信息的前提下，对每一抓拍对象所拍摄的图片进行过滤筛选，仅将一张信息完整、质量符合要求的图片上传。

11)数据通信传输：系统记录的车辆信息数据保存在本地的数据库中，同时向中心工作平台传递数据。如果遇到网络故障，则在网络通讯恢复时自动将未传递的数据上传到中心工作平台。或者用户可根据业务的需要，选择实时传输、或者周期传输。用户可根据具体的业务需求，自己选择设置如何传输图片和数据。

12)异常自动诊断及自动恢复：系统具有异常自动诊断及自动恢复功能，传感器异常自动诊断及自动恢复功能。系统能自动检测到系统故障并恢复正常工作。前端控制器采用模块插卡式设计，能自动

侦错报错，可以针对系统软件崩溃，硬件故障等事件做出恰当的处理，保证系统在出现意外情况时实现最大限度的可用性。路口停电后再来电，系统能自动重新启动恢复正常。

13)防盗报警：为了防止违法犯罪分子破坏，设备具备防盗检测功能，具有报警保护措施，当机箱门被非正常打开时，能够进行声音报警和向中心系统发送报警信息。

14)数据存储：为满足通信中断故障造成数据丢失问题，治安卡口前端需对采集的车辆识别数据与图片信息进行本地存储。提供前端数据的存储冗余，在通信链路故障恢复后，实现采集信息的历史补传。

治安卡口子系统需要完成如下功能：

1)基本信息处理：对获取信息的有效组织与存储管理。信息的二次处理功能。信息的统计分析与查询检索：可对记录的数据进行统计与分析，生成统计报表、平面图或三维图（饼图、折线图、直方图等）。系统支持按时刻、时间段、特定号牌、颜色等条件查询以及带通配符的模糊查询；支持 B/S 架构下的中央远程查询。

2)信息互联与交换：为实现公安治安卡口数据共享，系统须预留与以下系统进行信息互联和数据交换的接口。

3)与治安卡口信息综合管理平台的接口：图像专网接入。

4)与电子警察综合应用系统的接口：图像专网接入。

5)与道口车驾查控系统的接口。

6)与闵行区图像监控系统的接口：图像专网接入。

7)扩展业务：统一预警功能、套牌车辆检测功能、车辆区域关联性查询分析功能、车辆数据查询功能、交通流参数检测功能、信息展示功能等。

8)系统校时：能通过时钟服务器（不在本项目内）对治安卡口系统内的所有服务器和外场设备进行时钟同步。

9)远程维护管理：用户可以在系统运行现场进行控制操作，又能通过网络进行数据传输、远程访问、远程维护管理等，并提供方便的数据搜索与浏览等操作手段。

10)设备状态监测：系统可对每个设备进行状态监测，实时、定时或以远程检测的方式向中央系统提供设备运行状态。

11)设备防盗监测：前端系统需采取开门监测、断线监测以及剧烈震动监测等防盗监控设计，可在设备非法开门、设备支撑杆件被锯、设备被恶意敲砸等情况下，向中央进行报警。

12)通信状态监测：系统应能对通信状态进行监测，当网络故障或其他通信故障时，系统应能进行日志记录，并备份存储数据，当通信恢复时，所有临时备份数据应能及时上传中心。

13)设备管理：系统设备状态能在 GIS 界面以颜色显示，同时在操作界面以数据报表的形式显示。点击 GIS 治安卡口点图标能够查看设备信息和状态：设备信息包括路段交通组织及渠化情况，经纬度坐标定位信息，设备编号，设备配置文件等；设备状态包括机箱状态，控制主机状态，摄像机状态，

通信状态等。对即将到达保养期、超过保养期的设备，能够通过弹出框或者短信（需要手机短信模块支持），通知设备维护人员进行检修。

14)安全管理：包括前端设备安全、数据安全和后端系统安全三个部分。前端设备安全是当前端设备检测到敲砸、异常开门、非法 IP 接入等状态时进行中心实时报警，并联动治安卡口设施附近道路监控摄像机到相应的预置位查看；数据安全指的是系统支持数据加密，数字水印功能，防止电子图片被非法篡改。

15)权限管理：系统可以按照功能模块为系统管理者、使用者、操作者、维护者进行个性化的权限设定，根据权限设定不同的登陆界面。

16)日志记录：系统应提供 Log 管理功能，包括系统事件的记录和存储，具体的事件有：系统故障信息记录、报警记录、故障处理情况记录、系统开机记录、方案调用记录、人工干预记录、系统登录和退出记录、操作员修改系统数据和键入命令的记录等。

其他要求：

1)需在完成下发的车辆二次识别设备的部署及数据上传有基础上，增配设备实现本分局车辆识别采集图片的全量二次识别；

2)新建或改建的车辆识别采集设备（治安卡口、电子警察、违停、小区微卡口、加油站微卡口等），应通过管理转发机实现数据实时上传。

3.7.5　数据接入、转发要求

1、智能前端接入、转发

前端智能采集设备应通过 GB/T28181-2016 协议和 GA/T 1400.4 接口协议接入、转发到智能图像识别系统。

具体的接入、转发包含以下信息：

（1）视频数据：前端采集的视频流按照《高清技术规范》接入现有的高清图像监控系统，实现视频信号的管理转发。

（2）视频片段、

图片数据：前端采集的视频片段、图片数据、数据管理转发设备对其进行统一管理，数据流无需转发，直接存储到数据存储设备中。

（3）图片数据：前端采集的图片、数据管理转发设备一分为二，一路给分局，另一路上传。

（4）视频数据：前端采集的数据通过数据管理转发设备一分为二，一路给分局，另一路上传。

（5）预警数据：前端采集分析出来的预警数据通过图片、视频数据管理转发设备分别转发。

（6）配置数据：前端智能采集设备的配置数据应逐级汇聚至分局智能图像识别系统，并可按照权限级别通过智能图像识别系统、分局的智能图像分析子系统对前端智能采集设备进行算法设置或对算法进行变更。

2、图片、数据管理转发设备

图片、数据管理转发设备负责对前端智能采集设备所采集的视频片段、图片及二级处理数据 进行统一接入、管理，对前端设备状态进行监测及校时，并对图片和二级处理数据 进行数据分发后再入库，以确保数据上传的及时性。

3.7.6 时钟同步及字符叠加要求

1、时钟同步要求：高清智能监控 IP 摄像机、前端智能分析模块、后端智能化分析工具，图片、数据管理转发设备，一级处理数据 存储模块，以及布控及智能算法调度模块等均应具备时钟同步功能。应配置带 GPS 校准的时钟同步服务器，保持全网智能图像监控设备时间同步。

2、字符叠加要求：字符叠加应遵循《高清技术规范》中的字符叠加要求。

3.7.7 数据融合共享及统一管理调度

建设视频云子系统，进一步提高视频侦查工作效率和全流程可视化，整合多元化资源，统一界面查询，集成所有可接入的平台系统，实现集成化应用和管理，利用云计算技术进行底层碰撞，提供指导意见和可用情报，提升数据利用率。应实现复杂网络下的多元数据统一采集。应提供标准的数据服务接口和分析接口，为上层应用平台提供开放、高效的多资源数据共享与分析服务。具体功能需求如下：

3.7.8 GIS 子系统

系统将采用指定的高德地图数据接口，WGS-84 坐标系，建立统一的二三维一体化的 GIS 基础数据服务平台。提供 GIS 空间数据集、影像数据集、警务业务数据集等。其中 GIS 空间基础数据集包括行政区划、水系、国省县乡道、城市道路、地铁、桥梁、路口、派出所、医院，商场、遥感影像等图层。警务业务数据集，遵照“唯一数据产生源”的基本原则，由业务系统维护数据。三维空间数据集包括道路及沿线附属设施对象，包括：场地、道路、设施设备、绿化等全景影像和空间数据。应用功能需求如下：

1)二位地图服务：提供预先编制地图的浏览服务，包括政区图、交通图、影像图以及各类专题地图等。创建地图服务之前，需指定矢量和栅格数据源，预先对数据进行符号化配置，设置注记，创建专题图。

2)三维地图服务：提供多分辨率遥感影像、DEM 构建的三维地形，以及利用三维建筑物模型和纹理构建的三维道路模型。

3)平台数据管理服务：实现整个平台的统一登录、统一权限管理、统一用户管理。并实现移动版的监测、协同客户端。支持对数据的复制、查询和更新，并支持空间数据的编辑。

4)数据应用分析：实现某些特定的空间应用模型分析和数据处理的服务，主要包括常用的空间分析和计算服务。

5)二维功能接口：包括地图标注、地图测量、图层目录、空间查询、缓冲分析、叠加分析等功能性接口。

6)三维功能接口：包括三维空间查询、视图控制、地图定位、查询检索、空间测量、飞行浏览、空间分析、标注控制、动态模型管理、模型搜索等功能性接口。

同时，系统通过统一的标准地址库，在地图上展示区域内对应、实有房屋、实有单位、实有安防设施、实有安防力量的位置和信息；当发生实有警情时，在地图上对应位置进行实时告警展示；具体包括以下内容：

1） 标准地址库

支持将感知点位标注到高德二三维地图上，点位包括：动态感知、责任区、实有房屋、实有单位、实有安防设施、实有警情；

2)实有房屋

支持实有房屋地理详细位置信息在高德二三维地图上标注；

支持地图，可展示该户信息，包含该户地址所对应的人员信息、水电煤用量、车辆信息等；

3） 实有单位

支持实有单位的地理详细位置信息在高德二三维地图上标注；

支持在地图上以及单位列表上查看实有单位详细信息，包括单位名称、地址、照片及从业人员列表等；

4） 实有安防力量

支持警务人员、电台在高德二三维地图上标注详细地理位置信息；

支持警务人员、电台在地图上位置展示以及人员基本信息列表查询；

5） 实有安防设施

支持柱状图分类型显示目前区域内实有安防设施的数量，分为监控点、道路卡口、wifi 探针、消防栓等；

支持实有安防设施详细地理位置在高德二三维地图上进行标注与查看；

6） 实有警情

支持实有警情在高德二三维地图上的实时位置告警；

支持实有警情分类与基本信息查询；

3.7.9 运维管理

运维管理子系统对平安闵行二期视频监控项目涉及的基础设备（摄像头、交换机、存储、服务器、虚拟化等）、通信链路（有线、无线、PON 接入等）、传输数据（数据库类二级处理数据 、日志类一级处理数据 、图像音频类非二级处理数据 ）、运行业务（支撑业务的中间件、数据库，对业务的请求、访问、时延等）进行智能扫描、智能分析、智能告/预警，全面涵盖设备管理、链路管理、数据管理、业务管理、大数据分析、数据可视化，实现一套系统统一管理、统一告警、统一分析、统一展现，有效减少了重复建设管理平台的情况，降低了人员投入、提高了运维效率。

子系统分为：部署层、基础管理层、数据处理层、算法应用层和展现层。

部署层：对其上部署的应用实现自动化部署、升级和可视化组件状态运维管理，且需提供自动化的调度和负载分担的机制，对匹配调度和负载分担策略逻辑的应用进行自动化操作，确保整体系统的高可用性和高稳定性。

基础管理层：通过物联协议、IT 网络协议、数据协议或接口，对摄像头、卡口、网络链路、交换机、服务器、数据库、中间件、虚拟化、业务系统、日志、位置等进行综合数据采集和管理。

数据处理层：基于大数据技术将采集或对接的多类型、多格式的海量数据进行统一存储、挖掘和标准化，设备类数据：如摄像头、卡口、交换机、服务器等设备的运行状态、指标、告警等，业务支撑类数据：如业务关联的中间件、数据库、日志、访问行为等，其他数据：如业务数据或其他软件数据等。

算法应用层：提供算法库和模型库，通过对海量数据的分析，实现如对历史故障的原因分析、现有设备的风险识别、未来系统的预警预测，通过多维数据训练和算法应用，适配各类应用场景，如通过设备故障频次、原因与设备位置之间的关联关系，智能优化巡检线路，减少无目的地毯式巡检造成的资源浪费，提高效率，节约成本。

展现层：通过丰富的数据展现方式，通过模块化门户构建、2D/3D 全景呈现、资产管理、拓扑连接、设备告警、业务保障、报告推送和手机 APP 的方式，以全局的、统一的风格呈现在管理者面前，真正做到了统一管理、统一告警、统一分析、统一呈现。

3.8 前端采集系统技术要求

3.8.1 布点原则

1）治安视频监控的建设位置主要位于路口或一些重点部位、重点区域，以视频形式掌握一定区域内的情况。

2）治安视频监控密度要相对较高，确保实现点位置间的监控“接力”，重点区域的治安视频监控点位要与治安卡口系统形成彼此呼应、支撑的分布格局。

3）结合实战需求、按照一定比例，治安视频监控系统分为数字固定高清、数字可控高清球机和数字可控高清枪型摄像机（含高孔瞭望，水域瞭望）三类，分别进行分类建设。

4）视频监控点位分布在两个区域内，即中心城市化区域、外环至郊环区域。以路面道路为主体，以交叉口为重点，以小区、政府部门等出入口红线范围以外为目标，有层次地完成布点及建设工作。

对辖区内重点场所的建设规模进行预估和现场排摸，并综合考虑警情数量、人口密度、商业繁华程度等因素确定拟建设高清监控的具体点位，为全面开展高清监控建设提供依据。对分布于闵行区城市主干道、重要交通路口、特定公共场所、要害部位、重要设施的由机关、团体、企事业等单位自建的、用于公共场所和内部监控的图像监控资源进行预估和现场排摸，并对收集的数据进行分类汇总。

3.8.2 安装要求

安装时，应综合考虑地点、周边环境、光线照度及监控目的等因素，避免遮挡，全天候、全季节取得较好图像质量。

3.8.3　前端智能采集设备建设

建设功能复合型智能前端，每一个采集端必须配置一一对应的智能算法，并同时具备事件检测（或行为分析）和解析等功能，逐步实现视频智能功能前置化。并视情集成音频、手机 MAC 地址、射频等多维数据采集功能。

复合型智能前端主要有三种实现方式，具体要求如下：

1、新建监控摄像机及现有模拟监控摄像机的更新，应优先采用高清智能监控 IP 摄像机，实现轻量化智能算法部署；

2、已建的高清监控 IP 摄像机，优先通过配置对应的具备智能算法的前端智能分析模块，实现标准化智能算法部署；

3、如不采取上述方式，则通过后端部署智能化分析工具，按需配置所需的智能算法，实现复合型多样化智能算法部署；

4、高清智能监控 IP 摄像机、前端智能分析模块和后端智能化分析工具都需满足《上海公安智能摄像机、智能分析设备接入管理协议规范》的要求，并通过兼容性测试（通过兼容性测试的产品将及时在公安信息网上公布）。各类数据格式及要求参见《上海公安智能摄像机、智能分析设备接入管理协议规范》。如已建设备不符合上级部门的要求则必须予以更换。

3.8.4 智能监控 IP 摄像机技术要求

1、分辨率：新采购的智能监控 IP 摄像机分辨率不小于 200 万像素；

2、音频输入：前端都需具备音频输入接口，可外接有源拾音器；

3、IPv4/IPv6 互联网协议：智能前端都需支持 IPv4 和 IPv6 互联网协议；

4、数据流：智能监控 IP 摄像机应能输出视频图像、多类型图片和二级处理数据 。

3.8.5 前端智能分析模块要求

1、音频输入：前端都需具备音频输入接口，可外接有源拾音器；

2、智能功能：前端智能分析模块需具备接入高清监控 IP 摄像机后实现检测

3、分辨率、帧率适应性：前端智能分析模块至少能支持 25fps 的帧率下 1920x1080、2048x1536、2560x1440、2592x1944、3072x2048、3840x2160 等分辨率；

4、IPv4/IPv6 互联网协议：智能前端都需支持 IPv4 和 IPv6 互联网协议。

同时，可视情增加音频智能分析模块。即通过以视频监控系统为载体，利用网络摄像机音频输入接口、音频输出接口、RS485 总线接口融合接入专业拾音器，并通过音视频同步码流 NVR，实现音视频同步信息存储与转发。在指挥中心引入音视频同步监管和音频智能分析功能，利用从音视频同步监控系统中分离出来的音频流，实现对拾音器采集到音频信息的智能判断分析，并通过音频智能分析功能进行综合态势判断后，联动音视频同步监管功能进行联动预处置。

3.9 网络系统技术要求

3.9.1 前端传输要求

前端监控摄像机至 OLT 设备间路由距离控制在 10 公里范围内。

由于本次建设规模庞大，可根据实际情况分别选择使用二级及二级光分，光分路器放置在就近的光交接箱，总光分比为 1：32，但今后仅使用其中的 25--30 路，动态扩容。

鉴于实际监控点位分布情况，在 ONU 设备选型上，宜全部采用 4 口的 ONU 设备；建议每台 ONU 设备仅使用 2 口，另外作为备用端口，主用端口故障时启用同时为后续发展业务作预留。

本项目 ONU 带宽需满足摄像机 8M 双码流并发上传的要求并考虑一定冗余，并满足卡口图片、二级处理数据 等上传的带宽需求。

3.9.2 网络系统技术要求

根据闵行区现有视频 IP 网络现状及应用状况，结合上述章节对信息传输量的分析，为确保闵行区视频高清监控应用顺利实施，更好地为公安及其他政府部门实战应用服务，需对现有视频监控交换专网进行重新组建及改造。按照“既满足需求，又适度超前”的设计原则，以光纤网络为基础，实现全数字化信号传输。

存储分中心与分局总控中心节点交换机采用光纤互联，网络主干达到双 10GE，并预留 40GE 端口，确保监控数量后续增加时整个监控网络的带宽和速率。

1、分局总控中心

总控中心新建 2 台核心交换机，对内负责接入数据中心内部服务器、存储、网络安全设备等，对外负责与总平台、区级共享平台、分控中心等对接。

2 台核心交换机互为热备，当主用核心交换机发生硬件故障，数据流可以自动切换到备份核心交换机，这样保证了平台应用的持续稳定运行。

核心设备之间应该具有最高速的链路和可靠的冗余性能；比较细的 QoS 控制粒度；最高的路由前缀；支持 MPLS、IPV6、QING、组播路由；为网络其他模块提供互联。

2、四个分控中心

分控中心配置核心交换机对内负责接入数据中心内部服务器、存储、网络安全设备等，对外负责与总平台、总控中心、派出所、前端摄像机（通过 PON 网络或光纤直连方式）等对接。核心交换机需选用高性能框式交换机，每个分控中心需配置 2 台核心交换机，每台核心交换机配置冗余主控、电源，并提供多个业务槽位。智能分析服务器、虚拟化服务器及云存储通过万兆光口至连核心交换机，NVR 存储通过千兆电口上联接入交换机汇聚后通过万兆光口上联核心。

3.10 存储系统技术要求

智能图像监控系统的存储主要包括：基础视频存储、一级处理数据 存储（有价值视频片段、多类型图片）和二级处理数据存储。

（1）基本要求

应支持对存储对象的分类存储管理，并符合以下要求：

1、支持设置自动采集视频图像信息对象的存储时间及周期；

2、支持设置视频分析规则对象的存储时间及周期；

3、支持存储容量的平滑扩展；

4、支持配置数据导入与导出；

5、支持业务数据备份与恢复。

（2）基础视频存储

基础视频主要是前端智能摄像机 24 小时不间断记录的视频资料，对于基础视频的存储遵循《高清技术规范》的相关存储要求，存储时间至少一个月，重要目标至少存储 3 个月。

本项目采用 NVR+集中存储相结合的方式，NVR 存储时长为 30 天，集中存储存储时长为 7 天。

（3）一级处理数据存储

一级处理数据 主要包括用于存储包括按照智能分析规则认为有价值的视频片段、多类型图片等，对于视频片段、图片采用直存方式存储在各分局和业务单位的一级处理数据 存储模块中，经图片、数据管理转发设备分发后进行存储。因此，一级处理数据 存储模块应支持数据直存，为数据转发设备提供标准的服务接口，并支持存储容量的平滑扩展。

视频片段、图片的存储侧重于海量一级处理数据 的高频次写入与读取，对存储设备的容量和 I/O 读写性能要求均较高，应采用目前较成熟的横向节点扩展存储设备。存储架构可以是 SAN 架构也可以是 NAS 架构。存储模块应具备以下功能：

1、数据预览：支持根据视频片段、图片 URL 进行预览；视频片段、图片预览支持百分比压缩、大小压缩、宽高压缩等多种图片压缩方式。

2、检索下载：支持根据视频片段、、图片 URL 进行指定视频片段、、视频片段、、图片下载；支持根据摄像机编号、时间段、图片、二级处理数据 对视频片段、图片批量下载；视频片段、图片下载时支持百分比压缩、大小压缩、宽高压缩等多种图片压缩方式。

3、数据锁定：支持数据锁定，锁定后的数据不被循环覆盖；支持根据摄像机编号、时间段、图片、二级处理数据 对视频片段、图片批量锁定；支持已锁定的视频片段、图片锁定时长到期后自动解锁。

4、数据覆盖：按策略支持按周期、容量进行视频片段、场景数据的周期覆盖式存储。

5、存储时间：图片至少保存 90 天，视频片段至少保存 30 天。

（4）二级处理数据存储

二级处理数据可按照不同智能算法进行分类存储管理，并支持存储容量的平滑扩展。二级处理数据存储为数据转发设备提供标准的服务接口，允许数据转发设备将分析得到的二级处理数据存储到二级处理数据存储中，同时在全文检索中建立索引，并可向外提供标准的查询服务接口。

由于二级处理数据 存储侧重海量二级处理数据的高频次写入与读取，而大量的查询检索调用性能和效率依托于存储设备性能，应采用高性能全闪存阵列存储二级处理数据 ，可集群部署。

1、并发性能：二级处理数据存储支持不少于 100 路并发服务请求。

2、检索性能：二级处理数据存储数据精确检索须在 3 秒内返回结果，数据模糊检索须 5 秒内返回结果。

3、存储时间：二级处理数据至少保存 1 年。

3.11 虚拟机子系统技术要求

本项目参考业内成熟商用案例，引入虚拟化技术，建设虚拟化资源池，可以快速提供弹性的 IT 基础设施资源，更好地支撑未来快速发展的业务应用，同时提供多层面、多方向的数据安全保障。为快速响应、安全可靠的公安信息化发展趋势奠定坚实的基础。

本项目建设目标如下：

通过虚拟化技术实现数据中心资源共享，提高资源利用率。摒弃原有物理硬件的束缚，通过虚拟化技术实现跨站点的资源池。实现现有业务从现有数据中心到新数据中心的平滑迁移：在最小化影响业务运行的前提下，通过合理的规划、设计迁移方案，利用虚拟化技术方便快捷的实现机房搬迁，将目前在运行的传统物理环境搬迁到云平台环境。灵活、便捷的实现可视化运维。通过分布式架构，避免单点故障，提升平台的可靠性、稳定性。

本项目拟在 4 个分控中心部署 2vCPU 的服务器，并部署云计算、虚拟存储、虚拟网络、虚拟防火墙等软件，并在上层部署视频流媒体转发软件；在总控中心部署 4vCPU 的服务器，并部署云计算、虚拟存储、虚拟网络、虚拟防火墙等软件，并为视频云子系统、运维管理子系统、卡口子系统、无线监控管理等提供基础资源。

3.12 区共享平台技术要求

区级共享平台部署在政务外网，视频监控部分通过上联区总平台，并与公安视频 IP 专网对接，将闵行区各单位监控资源转发至区总平台，服务于各区的应用。各区用户调看本区范围内的监控资源通过区级共享平台实现。

区共享平台要求配置 2 台双机热备中心管理服务器 用于管理本平台的视频资源，同时向上对接市总平台，且要求配置配套的流媒体转发设备，流媒体转发设备按照最高峰值配置相应数量的流媒体转发设备并留有一定的余量，要求至少满足向市总平台上传 100 路高清视频（以 8Mbps 计算）的性能需求。区级共享平台应配备可以接收 GPS 或北斗等系统授权的 NTP 时间服务器，时钟精度应小于 100ms。要求配置 2 台双机热备时钟同步服务器。

3.13 配套附属设施建设

3.13.1 分控机房建设

为配合整个项目的正常实施，中标方需在闵行辖区内设置若干个分控中心机房，前端监控点位网络就近汇聚各分控中心，根据分控中心所在辖区接入的前端监控点位规模，每个分控中心的机房可使用面积不小于 100 平方米。

机房设计必须符合国家相关机房工程标准，按精密机房的要求进行建设，对电磁干扰、静电危害等进行隔离、消除；同时应保证业主方开展各项业务的需要，以实用、简洁、美观为原则，机房布局要美观大方。

分控中心机房保密性、安全性等同于公安办公场所。系统的安全性按照三级等保的要求来保证；机房租赁的安全性通过公安挂牌、设公安值班点，同时公安派专人 24 小时职守来保证。

3.13.2 通信线路及立杆建设

所有配套光缆、立杆、管道等，应在明显处做好公安及维护公司标识标志，包括且不限于外观设计、专用外漆涂画、铭牌标识、二维码标识等。

原则上新建点位网络均采用 PON 承载方式接入系统，传输网络稳定可靠，在网络通道上应与电信其他业务的网络物理隔离。

3.13.3 现场施工及供电条件

本项目外场所安装设备用电及施工取电由中标人就近取电，取电费用全部由中标方支付，取电应确保安全规范。

施工用水由中标人自行解决。

3.14 系统安全技术要求

3.14.1 软件平台安全要求

1、行为审计

系统软件必须对所有登录用户进行自动的审计跟踪，并保存审计记录。

审计的内容应包括用户注册、验证、权限设置、注销等；系统对所有用户的所有操作过程进行记录，记录的内容应包括登录时间、重要控制动作、修改设置、报警处理、退出时间等。重要控制动作包括对前端设备的启动、关闭、重启等控制、对其它用户控制有影响的控制（控制权限发生冲突时）及对设备的开始控制和结束控制动作。系统管理员可以设置平台系统的操作审计策略。系统对记录的资料采取严格的防护措施，不允许更改和删除；支持记录数据的备份与恢复，导出/导入。

2、操作记录

系统记录全部的登录用户的操作记录。记录的内容包括登录者名称、时间、IP 地址/或者主机名称、重要控制动作、修改设置、报警处理、退出系统的时间等。重要控制动作包括对前端设备的启动、关闭、重启等控制、对其它用户控制有影响的控制（控制权限发生冲突时）及对设备的开始控制和结束控制动作。对录像资料的处理，包括回放、下载、上传、剪辑等。

3、权限设定

支持精细化权限设定，可针对任何一个用户，针对任何一个图像资源进行精细权限设置，比如可为每个用户设置对每个摄像头的权限（是否可以实时监控、录像文件点播、云台控制等），权限类型和用户级别数量都没有限制；支持自动同步功能，授权用户对系统进行设置修改后，系统可将自动对全网进行更新。

4、其他安全要求

1）平台可提供多级用户管理架构，每级用户具有不同的管理权限，根据所赋予的权限可以进行相应的系统访问和监控操作，以防止非法登录和越权操作。

2）系统能对所有操作键盘和用户进行管理，能设置不同的权限。不同的权限对不同的资源有不同的监控级别，系统管理员可以将用户及权限自由组合成各种“角色”以方便管理。

3）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。

4）用户权限管理应满足集中统一管理的需要，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。

5）多个用户可以同时监看任意的同一个前端图像，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；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内没有操作，可以认为主动放弃控制权，由其它用户取得。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。

6）平台系统的用户数目不受限制，但可以该根据网络带宽状况和服务器的性能提供平台所容许的最大用户数，当同时登录用户数超过设计用户数后，禁止低级别用户进入，高级别用户可以取代低级别用户，将某低级别用户挤出，并给出相应提示信息。

7）平台可以根据用户的级别、业务种类、所处的物理位置来对其权限进行限制。

8）平台能够对系统所有设备中可远程设置的参数采取严格的保护措施，防止被非法或无意删改。

9）平台系统可以对视频监控资源的使用情况进行有效的管理，可以根据设备、网络预定的极限工作临界阀值自动采取流量带宽控制、设备功能抑制等措施，防止过载。

10）各级视频图像中心的后台管理软件能保证当管理子系统出现故障时不影响系统中各业务功能子系统、各级子网络的运行，某一子系统、子网络发生故障时，不影响其他子系统、子网络的运行。

3.14.2 前端设备安全要求

1、温湿度监测系统：实时监测并回传前端设备的温度和湿度，并在超过阈值时进行告警。

2、防水功能：良好的防水功能，使监控产品可以适应更恶劣的户外监控环境。

3、防暴功能：采用耐震加固的设计，铝合金结构持久耐用高强抗冲击外壳；以有效的防范恶意破坏。

4、防盗功能：新建的视频监控点因其前端采集、网络设备放置在室外，采取在设备的外部机箱内安装报警器，一旦有人非法开启机箱就马上产生报警。

5、系统前端硬件设备支持在线升级。设备异常时能向系统发送报警信息，并自动重新启动或后端远程启动。

3.14.3 中心设备安全要求

中心平台关键设备能保障系统正常运行或快速恢复。根据中心规模等级和重要程度采用双机热备、冷备份或备件的方式，确保系统的持续稳定运行。

数据库服务器是平台集中处理单元，接收处理大吞吐量的数据流，对各应用服务器的数据访问请求进行及时的处理应答，它的性能对系统的可靠性、可用性、可服务性以及资源的利用率有很大的影响，因此建议配置 2 台互为热备的数据库服务器，使系统具有很高的吞吐量、负载均衡和快速响应能力。

所有的应用请求都将通过请求接收层，即 Web 服务器转给应用处理层中的应用服务器处理。考虑到系统将存在大量的应用请求，建议采用两台 WEB 服务器互为热备，负载均衡。

WEB 服务器和数据库服务器采用双机集群方式。

中心系统硬件设备的平均无故障时间不小于 20000 小时。

关键设备根据系统规模宜采用冷备份或设置备品备份方式，采用冷备方式时系统恢复时间应≤30min。

3.14.4 网络传输与接入安全要求

本次建设系统的用户涉及相关政府部门用户，上述用户都基于政务网实现信息传送和交换。而视频监控系统运行在公安自建的视频 IP 专网。由于政务网与公安图像网有不同的安全要求，所采取的安全措施也不同，因此需要考虑一定的数据传输安全措施以及平台的性能，保证实时视频数据传输的效果。

本方案遵循公安部最新发布的《公安信息通信网边界接入平台安全规范（试行）——视频接入安全部分》草案，遵循《公安信息通信网边界接入平台安全规范（试行）》规范，视频接入链路的体系架构必须符合《公安信息通信网边界接入平台安全规范（试行）》的 3.2 节的要求。在公安图像网于政务网的网络边界上安装安全设备，并配置相应策略进行防护。

3.15 基础保障要求

为了保障本工程各类设备正常运转，租用的存储分中心机房必须满足行业标准机房的要求，而且必须为公安专用、独享的独立标准机房，装修、照明、空调通风、门禁、环境监控、防雷、防震、静电释放、消防、机房监控、供配电系统、UPS 系统和接地系统的要求不得低于以下要求。

1、装修工程

主要包括：主机房和辅助工作间的布局设计；机房的密闭和保温；吊顶装修（空调管道、照明灯具和走线、消防报警、保温、防尘、空调回风）；机房活动地板（布线、空调送风）；机房内墙、柱面装修；机房隔断；机房门窗。

2、屏蔽系统

主要包括：防止外界强电磁干扰机房内部的计算机和其它电子信息处理设备；防止机房内部的计算机和其它电子信息设备产生的信息以电磁波外泄，造成失密；采用金属板式屏蔽。

3、电力系统

(1)供配电系统

1）市电双回路：日常供电模式。

2）UPS 不间断电源：在市电停电时，采用 UPS 集中供电。

3）供电总功率冗余设计为 30%，配电系统频率 50Hz，电压 380/220V。

(2)UPS 不间断电源系统

UPS 采用双总线冗余方式进行设计。

(3)接地系统

机房接地系统有两种：单独接地和联合接地，建议采用联合接地的方式，交流工作接地、直流工作接地、安全保护接地与大楼的防雷接地共用一组接地装置，其接地电阻不大于 1Ω；交流工作接地，接地电阻不应大于 4Ω；安全工作接地，接地电阻不应大于 4Ω；直流工作接地，接地电阻应按计算机系统具体要求确定；防雷接地，应按现行国家标准《建筑防雷设计规范》执行。

设备机房接地等电位连接带应采用铜质线，其截面积不应小于 16mm2，设置的接地汇集环或汇集排宜采用裸铜线，其截面积不应小于 35 mm2。

(4)防雷系统

保护机房的重要设备不被雷击和浪涌损坏，是机房设计首要考虑的问题。充分考虑用户设备的安全，结合业内领先的防雷和防浪涌技术，为用户关键设备提供安全保障。

1）机房电源总开关加装电源避雷器作为电源第二级保护。

2）UPS 进线端加装电源避雷器作为电源第二级保护。

3）服务器、交换机柜加装防雷插座，达到第三级防护。

根据本工程的特点，要求 4 个存储分中心单独申请用电、单独计量核算。

4、空气调节系统

(1)机房空调系统：机房空调系统具有送风、回风、加热、加湿、冷却、减湿和空气净化的能力。考虑到存储分中心的重要性，存储分中心机房建议采用两套互为备用的恒温恒湿精密空调系统；空调考虑 20%的余量。根据国外资料介绍，计算机房热负荷按 300～600Kcal/h·m2 计算。而我国，由于机器利用率一般为 60-80%，装机密度小。因此，热负荷选 300～550Kcal/h·m2。

(2)机房新风系统：机房内新排风系统的风量根据空调送风量大小而定。

(3)环境监控系统：环境监控系统主要是监控电力系统、环境系统、消防系统、门禁保安系统等系统的运行情况。要求在机房部署环境监控系统。

5、综合布线系统

(1)综合布线采用千兆多模光纤和全六类非屏蔽产品。

(2)机房内设计采用金属网格桥架上走线方式，机房内敷设双绞线沿机架安装，信息插座均布在机柜内，采用标签加以识别。

6、门禁系统

采用非接触式 IC 卡门禁系统。

7、消防系统

(1)火灾自动报警系统

机房安装烟感、温感探测器及火灾自动报警系统。火灾报警系统与空调电源及配电电源连动，当有火灾报警时，自动切断供电回路。机房的消防报警系统当发生火警时，监控系统能实行语音报警。

(2)气体自动灭火系统

根据机房建设规范要求，本工程采用七氟丙烷气体灭火系统。七氟丙烷灭火装置分为有管网和无管网（柜式）两种。

1）有管网七氟丙烷灭火系统

有管网七氟丙烷灭火系统的灭火剂储存瓶平时放置在专用钢瓶间内，通过管网连接，在火灾发生时，将灭火剂由钢瓶间，输送到需要灭火的防护区内，通过喷头进行喷放灭火。

其中，有管网系统又分为内贮压系统和外贮压系统，其主要区别为灭火药剂的传送距离不同。内贮压系统的传送距离一般不超过 60m，外贮压系统的传送距离可达 220m。

2）无管网（柜式）七氟丙烷灭火系统

气体灭火剂储存瓶经过包装成灭火柜，外形美观，平时放在需要保护的防护区内，在发生火灾时，不需要经过管路，直接就在防护区内喷放灭火。无管网（柜式）七氟丙烷气体灭火系统，其灭火效能高，灭火速度快、毒性低、对设备无污损，灭火装置性能优良，其控制部分可与消防控制中心相衔接。

本工程中机房采用无管网（柜式）七氟丙烷灭火系统。灭火剂用量依据《气体灭火系统设计规范》（GB50370-2005）中有关规定，灭火浓度取 C=8%。

8、智能中央集中控制系统

在机房设置集中控制器，进行设备状态监测，在机房门口及走廊设置视频监控设备，通过相应传感器、监控等设备，在无人值守的情况下，实现突发情况报警（可通过短信等功能实现远程报警）。

3.16 土建及其他配套工程要求

3.16.1 供电

1、取电

由于前端摄像机数量多、分布广，不可能采用统一集中的集中供电方式，所以前端监控点的供电采用分散集中及就近取电的方式。

位于方便取电附近的可提供稳定电源的摄像机可采用共源方式，单杆或就近几支杆共用取电。

当前端监控点附近又找不到适合的稳压电源时，可考虑选取一些可提供稳压电源的地方设置一定数量的集中供电点（汇聚点），将距离在 50 米内的多个摄像机（或多个立杆）的电源连同信号线拉到集中点，图像和控制信号统一用光纤传回监控中心。这样即保证了供电，同时又降低了线路传输造价。

在视频监控系统中前端设备一般都采用单相交流供电方式，标称值为 AC220V，50HZ。

系统供电质量应该满足电压传输损耗小、电压稳定、谐波分量小等要求，一般来说电压波动不大于±10%,频率变化不大于 1HZ，波形失真率不大于 20%。

对于电缆传输方面，应该估算设备功率和传输距离，使得所选择的电源电缆能够满足电压、电流损耗等方面的要求。

2、电缆线

(1)电缆线的要求

电缆线的型式、规格应与设计规定相符。

线缆进场用于工程之前应进行验收，验收的程序、内容和方法应符合 GB50303-2002 中 3.2.12 条的规定。

(2)电缆线敷设原则

线缆的布放应自然平直，不得产生扭绞、打圈接头等现象，不应受到外力的挤压和损伤。

同一根电缆线两端应贴有标签，应标明编号，标签书写应清晰、端正和正确。标签应选用不易损坏的材料。

穿过管道的所有线缆截面积之和在设备机箱及杆件等末端处不应超过管道截面积的 90%，其他地方不应超过管道截面积的 60%。

(3)地下电缆线的敷设

地下敷设的电缆线不得有接头。

每根电缆线应留有 2m～4m 的余量。

(4)架空电缆线的敷设

确实无法采用地下敷设电缆线方式时，需严格遵循《上海市城市道路架空线管理办法》、《上海市人民政府办公厅印发<关于开展本市架空线入地和合杆整治工作的实施意见>的通知》（沪府办【2018】21 号）。对于《关于印发 2018 年本市架空线入地和合杆整治计划的通知》（沪指【2018】2 号）文件范围内一律不得使用架空线。

架空电缆线最低净空高度≥6m。架空电缆线跨度超过 30m 时应使用钢绞线将电缆线吊起。

架空电缆线在杆件引下处 2.5m 以下应使用钢管穿线套管。钢管穿线套管的顶部应有半月型防水弯或安装防水出线管帽。

(5)桥梁上电缆的敷设

敷设于桥梁上的电缆应穿管敷设。

在经常受到震动的桥梁上敷设的电缆，应有防震措施。

桥梁两端和伸缩缝处的电缆应留有松弛的部分。

线缆在桥梁上敷设时应事先征得桥梁管理部门的同意后方可施工。

3.16.2 防盗、电气保护和防雷

1、户外机箱需符合 IP65 或以上防护等级标准。

2、监控设备机箱应具有防盗措施，具有监控防盗报警装置，通过现场通信系统将报警信号传送至控制中心。

3、外场设备所用的电路板应进行抗盐雾腐蚀的处理。

4、设备电源提供漏电保护。

5、安装高度超过 5 米的外场设备，必须采取防雷措施。

6、电气保护接地电阻≤4Ω，防雷接地电阻≤10Ω，联合接地电阻≤1Ω。

7、实行高、低频信号隔离，设备保护接地分别连至各自的公共接地排。

8、所有重要设备的接口板和功能板均采用高速光电隔离技术，以减弱浪涌对集成电路芯片的损坏。

9、电子设备设有防过电压措施，长距离的电源线、视频线、数据传输电缆的入口接线安装相应的浪涌抑止装置。

3.16.3 管道

1、横穿机动车道的地下管道埋设

(1)敷设在机动车道上的管道宜采用镀锌钢管或聚丙乙烯管等高强度管材，口径宜为 50 ㎜～110㎜，管与管接头处应使用套管固定，在进、出窨井端应使用防鼠护套。

(2)钢管进/出窨井端宜烧制喇叭口并应去除毛刺，以便于线缆敷设。

(3)管道埋深应≥ 300mm。

(4)检查管道以保证管道内通畅、清洁无砂石、管口无毛刺。

2、非机动车道、人行道或绿化带下的地下管道埋设

(1)敷设在非机动车道、人行道或绿化带下的管道宜使用硬质塑料管或镀锌管，口径宜为 50mm ～110mm，管与管的接头处应使用套管固定，在进、出窨井端应使用防鼠护套。

(2)穿越非机动车道下的硬质塑料管周围应包有足够强度的混凝土防护层。

(3)管道的埋深应≥300mm。

3、管道引上处处理及路面恢复

(1)管道在引上处的弯曲半径不得小于四倍的管道直径。

(2)管道铺设完成后必须按原道路标准恢复路面。

3.16.4 预埋件

(1)预埋件有地脚螺栓、带锚板与锚筋的预埋件和钢构件等，建议采用 Q235-B.F 钢，焊条采用 E43。

(2)所有预埋件在预埋前均应进行防腐处理，施工时应按批准的施工设计图纸，密切配合土建施工，严格控制预埋件平面位置、埋入深度、朝向和标高，严格控制预埋地脚螺栓的垂直度，保证工程误差在许可范围之内。具有良好的接地措施。

3.16.5 基础

(1)采用钢筋混凝土基础。

(2)基础应根据具体要求进行设计。

(3)基础的浇注、混凝土强度等级必须符合 GB50204-2015 的要求。

⑷基础内预埋穿线管内径大于 50mm，弯曲角度大于 120° 。

3.16.6 杆件

对于《关于印发 2018 年本市架空线入地和合杆整治计划的通知》（沪指【2018】2 号）文件范围内的监控点位应尽量合杆建设。

(1)立杆与基础间连接采用法兰连接，法兰间加防水措施，立杆底端应设有走线、维修用手孔。

(2)立杆、法兰盘、柱帽、加劲肋及连接螺栓、螺母、垫圈等钢铁件，采用热浸镀锌进行防锈处理，镀锌层均匀且厚度 100μm。立杆、悬臂采用双面焊，所有的对接焊缝和贴角焊缝，其厚度和强度应与被焊构件相等，焊缝应打磨光滑。

(3)立杆挑臂长度根据现场环境定制，挑臂安装牢固且能确保摄像机在风速 35m/s 时不发生抖动或有明显的偏离。

(4)立杆采用热镀锌管，使用下部蓝色、上部白色的统一配色，其中必须具备一根接地桩和接地导线。监控立杆高度通常不应低于 6 米，立杆壁厚不低于 6mm；立杆可使用不锈钢立杆，不做着色要求。

3.16.7 窨井

窨井的设置通常应该注意以下几点：

(1)管道拐弯处或长度＞50m 时应设置窨井。

(2)公安交管用杆件附近 2m 范围内，公安交管用设备机箱附近 2m 范围内应设置窨井。

(3)窨井底部应设有渗水孔。

(4)窨井中管道到井底的距离≥20cm。

(5)井口应与地面持平。

(6)不应在临河、临沟处设井。

(7)窨井应设置有交通设施或公安专用标记的窨井盖，窨井盖材质宜采用复合材料。

本项目建设过程中建议大窨井一般设置在设备机箱附近或管道汇集处，井口面积不宜小于 0.6m2，深度应≥ 700mm。小窨井一般设置在人行道、渠化岛或绿化带上，井口面积不宜小于 0.15m2，深度应≥ 500mm。

四、主要设备技术参数

4.1 高清智能视频监控

4.1.1 高清固定摄像机

摄像机	传感器类型	不小于 1/2.8 英寸 CMOS
	传感器有效像素	1920×1080
	电子快门	1/3 秒至 1/100000 秒;可手动或自动调节
	最低照度	0.002Lux@F1.2(彩色模式);0Lux@F1.2(黑白模式)
	日夜转换	IR-CUT 自动切换
	扫描方式	逐行扫描
	降噪	3D 降噪
	宽动态	120dB
	信噪比	≥56dB
	增益控制	手动/自动
	白平衡	手动/自动
	背光补偿	支持,可选择区域
	强光抑制	支持
	聚焦功能	手动
	后焦调节	支持(ABF)
	外调焦	支持
镜头参数	镜头接口	C/CS
	光圈控制	自动
	变焦类型	手动
音频参数	音频输入	至少 2 路,3.5mm JACK LINE IN 内置 MIC

	音频输出	至少 1 路,3.5mm JACK LINE OUT
	音频压缩标准	MP2L2;G.711Mu;G.711a;G.726;G.722;AAC;G729
	音频采样率	8Kbps/64Kbps
视频参数	视频压缩标准	H.265;H.264;H.264B;H.264H;MJPEG
	视频码率	24kbps~11Mbps，可自定义
	视频帧率	50Hz:主码流(1920×1080@25fps),辅码流(704×576@25fps),第三码流(1920×1080@25fps) 60Hz:主码流(1920×1080@30fps),辅码流(704×480@30fps),第三码流(1920×1080@30fps)
报警参数	报警输入	2 路以上
	报警输出	2 路以上
	报警联动	支持无 SD 卡;SD 卡空间不足;SD 卡出错;网络断开;IP 冲突;非法访问；动态检测;视频遮挡;
功能	图像设置	亮度;对比度;锐度;饱和度;伽马
	OSD 信息叠加	时间;通道;地理位置;图片;客流量统计;
	图像镜像	支持
	心跳机制	支持
	录像模式	手动录像;视频检测录像;定时录像;报警录像 录像优先级从高到低依次为手动/外部报警/视频检测/定时
	存储功能	支持 Micro SD 卡存储,最大容量 128GB 以上
	预览最大用户数	20 个以上
	恢复默认	支持一键恢复默认配置
	浏览器	支持 IE7;IE8;IE9;Chrome8+;Firefox3.5+;Safari5+ 浏览器
	用户管理	至少支持 20 个用户,多级用户权限管理
	安全模式	授权的用户名和密码;MAC 地址绑定;HTTPS 加密;IEEE 802.1x;网络访问控制
	透雾	支持
	电子防抖	支持
	智能功能	虚焦侦测;区域入侵;拌线入侵;物品遗留/消失;场景变更;徘徊检测；人员聚集；快速移动；非法停车；音频异常侦测;外部报警；客流量统计；热度图

	隐私遮挡	4 块区域以上
	走廊模式	支持
接口	网络接口	10/100M 以太网口
	RS485 接口	至少 1 个
	网络协议	HTTP;TCP;ARP;RTSP;RTP;UDP;RTCP;SMTP;FTP;DHCP;DNS;DDNS;PPPOE;IPv4/v6;SNMP;QoS;UPnP;NTP
	接入标准	ONVIF;GB/T28181;CGI;PSIA
	模拟输出	至少 1 路,支持 HDCVI/CVBS 两种模拟视频输出,BNC(1.0Vp-p,75Ω)
	电源返送	支持 12V（2W）电源输出
常规参数	供电	AC24V
	工作温度	-30℃~+60℃
	工作湿度	≤95%
	安装方式	壁装,吊装
其他	需通过上海市公安局兼容性测试	

4.1.2 高清固定摄像机镜头

像素	500 万		
日夜	支持		
规格	1/1.8"		
接口	C/CS		
焦距 (mm)	12.5-50mm(4x)		
光圈范围	F1.6~T360		
操作方式	变焦	手动	
	聚焦	手动	
	光圈	DC 自动	
视 角 (H x V) 4 : 3	1/1.8"	广角端	35° 54’ × 24° 37’
		长焦端	8° 14’ × 6° 13’
	1/2"	广角端	29° 32’ × 22° 7’
		长焦端	7° 26’ × 5° 36’
视 角 (H x V) 16 : 9	1/1.8"	广角端	35° 52’ × 20° 6’
		长焦端	8° 57’ × 5° 5’
	1/2"	广角端	32° 12’ × 18° 3’
		长焦端	8° 5’ × 4° 35’

最小物距（M.O.D）		0.8m	
最小物距下的物体大小 (H x V) 4 : 3	1/1.8"	广角端	461 × 345 mm
		长焦端	115 × 86 mm
	1/2"	广角端	409 × 307 mm
		长焦端	102×73 mm
最小物距下的物体大小 (H x V) 16 : 9	1/1.8"	广角端	496 × 279 mm
		长焦端	124 × 70 mm
	1/2"	广角端	446 × 251 mm
		长焦端	111 × 63 mm
后焦距（空气换算长）		MIN.7.7mm	
出射光瞳（从成像面）		-36mm	
接品材质		金属接口	
备注		ND 滤光片	

4.1.3 固定高清摄像机防护罩

材料：主体铝合金，视窗：透明

防护等级：IP66

视窗面积：不小于 67mm*57mm

镜头视窗面积：不小于 28.5mm

工作温度：-35℃-+65℃

具备遮阳罩

4.1.4 高清可控球型摄像机

不小于 1/2.8 英寸，逐行扫描 CMOS；

4.3-129mm 镜头/F1.6-4.7 自动对焦，自动日夜转换，30 倍光学变焦，12 倍数字变焦；

支持至少 2 个独立可配置 1080P(1920x1080)分辨率，30/25 帧速码流；或 3 个独立可配置高清(1280x720)分辨率，60/50 帧速并发码流；

最低照度：彩色小于等于 0.2lux/F1.6 30IRE；黑白小于等于 0.01lux/F1.6 30IRE；

支持 120dB 动态范围；

摄像机具备 SDHC UHS-I/SDXC UHS-I 插槽用于本地存储；

摄像机必须支持 NAS 存储

摄像机必须支持 360° 水平旋转；垂直旋转 180°，转速范围 0.2 - 350/每秒；

摄像机支持 256 个或以上预置位；

支持音频输入输出接口；

支持 4 个可配置的 I/0 报警输入、输出；

支持移侦测、震动侦测、音频侦测、门卫值守功能等；

同时支持自有的前端嵌入式智能分析和第三方智能分析上传。

支持 High PoE，24V DC 或 24V AC 供电

工作温度范围-30℃ to +55℃

支持 IP66、IK10 防护标准

摄像机必须符合国际相关标准，并完全采用国际标准开放协议，并提供开放的接口，投标方必须提供摄像机原厂 SDK 开放承诺书；

摄像机必须支持原厂 3 年质保；投标方必须提供摄像机 3 年质保承诺书/承诺函。

平均无故障时间 MTBF 球机必须大于等于 100000 小时。

通过上海市公安局兼容性测试

4.1.5 高清可控云台一体机

不小于 1/2.8 英寸，逐行扫描 CMOS；

4.3-129mm 镜头/F1.6-4.7，30 倍光学变焦,自动对焦,自动日夜转换；

支持产生 HDTV 1080P (1920x1080)分辨率的 50/60 帧/每秒的 H.264 或 Motion JPEG 视频流。

支持至少 2 个独立可配置 1080P(1920x1080)分辨率，30/25 帧速码流；或 3 个独立可配置 HDTV 720P (1280x720)分辨率，30/25 帧速并发码流

彩色时感光度支持要求小于等于 0.1lux/F1.6 30IRE；黑白时感光度支持要求小于等于 0.05lux/F1.6 30IRE；

支持 microSD/microSDHC/microSDX 插槽用于本地存储，至少支持 64GB；

支持 120dB 宽动态；

支持 360° 不间断水平旋转，参考转速范围 0.05 - 80/每秒；+40°~-75° 垂直旋转，转速范围 0.05 - 60/每秒；

支持 255 个或以上预置位；预设速度：水平 110°/s，垂直 60°/s，预设精确度：± 0.1；

支持音频输入输出接口；

支持报警输入输出接口；

支持 3D 隐私遮挡；

支持电子防抖功能；

支持自动透雾功能；

支持移动侦测、门卫、主动防篡改报警等功能；

支持自带智能分析功能，同时可支持第三方智能分析上传功能；

可支持密码保护、IP 地址过滤、IEEE 802.1X 网络访问控制、HTTPS 加密、摘要式身份验证；

抗风性：大于 12 级，可在 140 kph 风速条件下保持运行；

支持 IP66 防护标准；

支持 24V DC/24V AC 供电

工作温度范围至少-30℃ to +50℃.

通过上海市公安局兼容性测试

4.1.6 高空瞭望高清云台摄像机

类别		名称	参数
可见光部分	机芯	图像传感器	1/1.8”CMOS
		有效像素	207 万
		最低照度	彩色模式：0.01Lux
			黑白模式：0.001Lux
		白平衡	自动/手动
		增益控制	自动
		信噪比	≥50dB
		背光补偿	自动
		日夜转换	自动、手动、报警触发转换、定时转换等多种切换模式
		数字降噪	支持
		强光抑制	支持
		宽动态	支持
		图像调节	色调、锐度、亮度、对比度和饱和度等多种参数可调
		光圈控制	支持自动光圈、手动调节光圈
		聚焦模式	自动跟焦/电动聚焦
	镜头	焦距	变焦 12.5-775mm
		光学变倍	62 倍
		x2 扩展器（选配）	支持
		光圈数	F3.5-close
		滤光镜	光学透雾
红外部分	机芯	探测器类型号	非制冷非晶硅型
		像素	384×288
		像元尺寸	25um
		光谱响应范围	8～14um
		非均匀矫正	电磁阀快门矫正
		电子放大	2×、4×
		图像增益	多级增强细节参数可调节
		数字降噪	多级去噪细节参数可调节

类别		名称	参数
		极性	支持白热、黑热、红热、铁红、黑红、彩虹、冷热、墨褐、多层、多彩等 14 种显示模式
		调光	支持直方图、线性和混合调光算法
	镜头	聚焦方式	一键聚焦/电动聚焦
		焦距	定焦 150mm
		光圈数	F1.0
功能		水平范围	360° 连续旋转
		水平速度	水平键控速度：0.005° /s~90° /s
			水平预置点速度：90° /s
		垂直范围	+90～-90°
		垂直速度	垂直键控速度：0.005° /s~90° /s
			垂直预置点速度：90° /s
		设备精度	0.0038°
		转台位置校准	支持
		自动跟焦	支持
		3D 定位	支持
		抓图功能	支持
		预置点个数	2048 个，可订制增加。
		巡航扫描	16 条，可订制增加。
		温度控制系统（选配）	支持
		自动标定地理正北	支持
		自动标定地理坐标	支持
		气压实时监测	支持
		存储	支持 Mirco-SD 卡本地存储，最大支持 128G
		断电保护	断电后能自动保存断电前的配置参数，软件升级过程中断电，重新加电后可恢复到升级前的软件版本
		上电恢复	支持巡航方案及记忆点上电恢复业务
		自动看守	支持按巡航方案及保护模式等类型开启和关闭自动看守
		定时任务	支持按业务类型定时开启和关闭设备功能
		远程升级	支持设备控制程序、图像处理程序、烟火识别程序远程

类别	名称	参数
		程序升级与远程维护管理
网络	可见光最大图像尺寸	1920×1080
	红外光最大图像尺寸	384×288
	可见光主码流分辨率及帧率	50Hz： 25fps （1920×1080）
		60Hz： 30fps （1920×1080）
	可见光子码流分辨率及帧率	50Hz： 25fps （704×576）
		60Hz： 30fps （704×576）
	热成像主码流分辨率及帧率	50Hz：50fps （384×288）
		60Hz： 60fps （384×288）
	视频压缩	H.264，H.264 编码支持 Baseline/Main/High Profile
	ROI 编码	支持
	语音压缩	G.711
	网络协议	TCP/IP, UDP, RTSP, RTP, RTCP, HTTP, PPPoE, DHCP,NTP, FTP
	同时预览视频数	最多 10 路
	用户权限	可设置
系统集成	报警输入	支持，2 路
	报警输出	支持，8 路
	报警联动	支持
	音频输入	LINE_IN
	音频输出	可驱动 8Ω，15～50W/4Ω，30～50W
	网络接口	内置 RJ45 网口，支持 10M/100M 网络数据
	控制接口	RS422/RS485/RS232
	对外供电接口	DC12V/1A
	应用编程接口	支持软件集成的开放式 API，支持标准协议(ONVIF)、支持 SDK 和第三方管理平台接入、支持 GB/T28181 协议
	客户端	支持
	浏览器	支持
一般规范	电源	DC48V±20%
	工作温度和湿度	-40℃~70℃(室外)
		湿度小于 85%

类别	名称	参数
	防护等级	IP67
	防雷等级	具备多级防雷，抗雷击能力达±6000V
	电磁兼容性	符合 GB/T 17626.2、GB/T 17626.3、GB/T 17626.4、GB/T 17626.5、GB/T 17626.6 相关规定
	防凝露	支持
	除雪	支持
	安装方式	座装

4.1.7 高空瞭望高清云台摄像机（3000 万像素）

传感器：3000 万像素逐行扫描 CMOS 传感器

镜头：单镜头，采用 35mm 全画幅传感器

分辨率：最高达 7360 x 4128 分辨率

低照度：最低照度达 0.005Lux（F1.4）（彩色）

视频压缩：H.264 或 MJPEG 压缩

支持移动侦测

自动或手动曝光控制与光圈控制

自动聚焦，或者软件远程控制对焦

本地 SD 卡存储，最大支持 256GB 容量

兼容各种 EF 卡口单反镜头

以太网 POE 供电，或者 24 VAC 或 12 VDC 外部电源

外部输入/输出接口，以及 RS-485 云台反向控制接口

Mini jack 3.5mm 端子可同时支持音频输入与输出，G.711 PCM 音频压缩

多达 4 个隐私区域

焦距不低于 28-300mm

水平范围：360° 连续旋转；

水平速度：0.01～20° /s；

垂直范围：-45° ～ +45° ；

垂直速度：0.01～15° /s；

角度回传：支持；

预置点个数：256 个；

巡航、扫描：1 条；

守望功能：预置位/自动扫描/自动巡航；

云台最大承载 35Kg 及以上，室外大型防护罩；

温度与湿度：-45℃～+65℃＜90%RH;

防护等级：IP66。

4.1.8 水域瞭望高清云台摄像机（30 倍）

可见光摄像机技术参数

摄像机传感器类型：1/2.8″ 逐行扫描 CMOS

最低照度：彩色：0.01Lux

黑白：0.001Lux

快门速度：1/100000s - 1s

日夜切换模式：IR-CUT 双滤光片自动切换

数字降噪：3D 数字降噪

宽动态范围：数字宽动态，≥120dB

镜头焦距：f4.5-135mm，支持自动聚焦

光圈：F1.6 - F5.0（广角 - 望远）

水平视角：61.9°-2.3°（广角 - 望远）

视频压缩标准 H.264（BaseLine Profile/Main Profile/High Profile）/MJPEG

音频压缩标准 G.711/AAC

分辨率与帧率 最大支持 1920x1080@30fps

多路码流 支持四路 H.264 独立码流实时编码

支持透雾（手动/自动），支持背光补偿

支持协议：IPv4, HTTP, FTP, RTSP, UPnP, DNS, NTP, RTP, TCP,UDP, IGMP, ICMP, ARP, SOCKS

安全性 用户权限分级，密码保护，用户访问日志

行为分析：越界侦测,区域入侵侦测，物品看守

异常侦测：音频门限检测、音频陡升检测、音频陡降检测、音频突变检测

红外摄像机技术参数

红外：非制冷焦平面

波长范围：7.5~14μm

像素数：384 x 288

像素尺寸：17μm

帧率：50Hz

镜头焦距：15mm 定焦

视场角(°)：26 x 20

探测/识别/辨认距离：540m/140m/70m

车辆探测距离：1100m

测温范围：-20~150℃

测温精度：2℃或 2%

测温环境温度：-10~50℃

根据输入发射率和背景温度自动校正，发射率 0.01~1 可调

根据输入透过率自动校正

根据气象参数自动计算大气透过率并校正温度

实时显示光标点温度

支持全局高低温追踪、全局平均温度、点、线、矩形、圆、椭圆、多边形等多种测温模式，最多可添加 100 个测温对象。所有测温对象可独立设报警阈值范围、采样周期、绘制历史温度曲线图

控制端声光报警，并记录日志，触发报警时可自动存储温度数据和图像快照。相机端报警输出电平指示

相对温度分析、温度直方图分析，历史温度曲线图，线上温度曲线图

自动拉伸，带 DDE，图像亮度对比度可调，支持手动平台拉伸

白热、黑热、铁红、彩虹等 10 种调色方式

重型云台技术参数

水平范围：0°~360°连续旋转

垂直范围：-90°~50°

水平速度：0.5°~90°/s

垂直速度：0.1°~20°/s

预置点：256

巡航扫描：6 条巡航路径，每条可添加 18 个预置点

云台控制：机械 + ePTZ

守望功能：支持

方位角显示：支持

断电记忆：支持

音频接口：1 对 3.81pitch2pin 音频输入/输出端子

通讯接口：1 个 RJ45 10M/100M 自适应以太网口，1 个 RS-485 接口

报警输入：1 路

报警输出：1 路

防护等级：IP65

4.1.9 水域瞭望高清云台摄像机（60 倍）

可见光摄像机技术参数

摄像机传感器类型：1/2.8″ 逐行扫描 CMOS

最低照度：彩色：0.01Lux，黑白：0.001Lux

快门速度:1/100000s - 1s

日夜切换模式:IR-CUT 双滤光片自动切换

数字降噪:3D 数字降噪

数字宽动态，≥120dB

镜头焦距:f5－300 mm

聚焦:自动聚焦

光圈:F1.8 － F6.1（广角 － 望远）

水平视角:56.7°-1.0°（广角 － 望远）

视频压缩标准:H.264（BaseLine Profile/Main Profile/High Profile）/MJPEG

视频压缩码率:32Kbps~8Mbps

音频压缩标准:G.711/AAC

分辨率与帧率:最大支持 1920x1080@30fps

支持四路 H.264 独立码流实时编码

走廊模式，饱和度，锐度，亮度，对比度

支持透雾，支持背光补偿

支持协议：IPv4, HTTP, FTP, RTSP, UPnP, DNS, NTP, RTP, TCP,UDP, IGMP, ICMP, ARP, SOCKS

行为分析：越界侦测,区域入侵侦测，物品看守

异常侦测：音频门限检测、音频陡升检测、音频陡降检测、音频突变检测

报警触发：支持，可以实现联动告警，并进行响应的动作

报警联动：报警信号上传,触发 Micro SD/SDHC 录像,一路开关量输出

智能报警：音频异常,移动侦测,视频遮挡,断网录像

红外摄像机技术参数

红外探测器类型：非制冷焦平面

波长范围：7.5~14μm

像素数：384 x 288

像素尺寸：17μm

帧率：50Hz

镜头焦距：15mm 定焦

视场角(°)：26 x 20

探测/识别/辨认距离：540m/140m/70m

车辆探测距离：1100m

测温范围：-20~150℃

测温精度：2℃或 2%

测温环境温度：-10~50℃

根据输入发射率和背景温度自动校正，发射率 0.01~1 可调

根据输入透过率自动校正

根据气象参数自动计算大气透过率并校正温度

鼠标测温：实时显示光标点温度

测温模式：支持全局高低温追踪、全局平均温度、点、线、矩形、圆、椭圆、多边形等多种测温模式，最多可添加 100 个测温对象。所有测温对象可独立设报警阈值范围、采样周期、绘制历史温度曲线图

高低温报警：控制端声光报警，并记录日志，触发报警时可自动存储温度数据和图像快照。相机端报警输出电平指示

辅助温度分析：相对温度分析、温度直方图分析，历史温度曲线图，线上温度曲线图

图像冻结：支持

显示增强：自动拉伸，带 DDE，图像亮度对比度可调，支持手动平台拉伸

调色板：白热、黑热、铁红、彩虹等 10 种

重型云台技术参数

水平范围：0°~360°连续旋转

垂直范围：-90°~50°

水平速度：0.5°~90°/s

垂直速度：0.1°~20°/s

预置点：256

巡航扫描：6 条巡航路径，每条可添加 18 个预置点

云台控制：机械 + ePTZ

守望功能：支持

方位角显示：支持

断电记忆：支持

音频接口：1 对 3.81pitch2pin 音频输入/输出端子

通讯接口：1 个 RJ45 10M/100M 自适应以太网口，1 个 RS-485 接口

报警输入：1 路

报警输出：1 路

工作温度/湿度　　-10 ℃～+50℃ / 20%～80% RH

防护等级　IP65

4.1.10 高清治安卡口监控摄像机

相机应采用不小于 1/1.2 英寸的百万像素传感器，图像有效分辨率不低于 200 万；

成像传感器，彩色 0.008Lux@F1.2；

支持自动、手动光圈调节；

内置补光灯，一体化结构设计；

具备 GPS 定位功能；

相机应支持同步输出图片和视频流，并且图片和视频流的快门可设置不同值；

视频流编码格式支持 H.264、MJPEG 等标准格式，帧率支持 1~25 帧/秒可调；

支持前缓存补录功能，存储容量不小于 32GB；

支持偏振镜的自动切换功能

相机应支持 TCP/IP、HTTP、UDP、DHCP、PPPOE 等协议；

应具有电源同步接口，支持 12VDC/24VAC±10%；

摄像机应能在-20℃～+70℃正常启动和长期工作；

智能识别软件应内置于智能相机中，支持内置车牌识别算法、车身颜色识别算法和车型识别算法等；

整机一体化交付，防护罩支持自动温控加热、风扇，防护等级不低于 IP66，具备全网口防雷设计，防雷能力达到 6KV；

设备应具有 GA/T497-2009《公路车辆智能监测记录系统通用技术条件》公安部交通安全产品质量监督检测中心的系统检测报告；

4.1.11 监控摄像机

图像传感器	1/1.9″ 2.1 MP Sony 逐行扫描 CMOS
解析度	水平≥1000TVL,垂直≥1000TVL
最低照度	彩色：0.005Lux @ F1.2；黑白：0.005Lux @ F1.2
镜头	1/2″，1″，4/3″200 万像素及以上级别高清镜头
镜头接口	CS/C 接口
日夜转换模式	自动日夜型 ICR 红外切换滤片式
宽动态范围	128dB
信噪比	63.8dB
延时	150ms
定码率均值	4Mbps
灰度等级	11 级
数字降噪	3D-MCTF 数字降噪
快门速度	100000s to 1/25s
4A 控制	自动白平衡，自动增益，自动曝光，自动光圈控制
视频压缩标准	H.264/MJPEG
H.264 编码级别	Main Profile @ Level 5.1
压缩输出码率	32 Kbps~12Mbps
音频压缩标准	G.711/ AAC / MP2

音频压缩码率	G.711(64Kbps) /MP2(16kHz 16bit 32kpbs)
最高分辨率	Full HD/1080P(1920x1080)
帧率	在高帧率模式下最高位 120fps；其它所有分辨率下均可达 25fps
多码流	在高帧率模式下为单码流；四码流：FHD/1080P+720P+FULL D1+CIF；三码流：1080P+FULL D1+ CVBS/HDMI
视频流	在最大分辨率下以全帧速同时输出多路视频流，帧速和带宽可调整，H.264 支持 VBR/CBR
图像设置	可调节图像格式、码率、亮度、对比度、饱和度、锐度、白平衡 多区智能 OSD 图像翻转和镜像（走廊模式） 自动、手动或预定日/夜模式 多场景定时切换模式 经纬度图像模式
日夜转换方式	自动，定时，手动，报警触发
离线存储	支持至少 1 个 microSD/SDHC 卡扩展
背光补偿	开/关
强光抑制	开/关
曝光模式	暗曝光、中心点曝光、平均曝光、指定区域曝光等可选
透雾	支持
感兴趣区域 ROI	支持分别设置固定区域或动态跟踪
ePTZ	支持，需要 inControl 客户端配合
智能报警	图像侦测，移动侦测，传感器联动报警，网线断，IP 地址冲突，存储器满，存储器错
报警联动	通过 FTP、HTTP 和图片服务器上传报警信息和录像文件;启动 SD/SDHC 存储卡录像；继电器输出
其他功能	一键恢复出厂设置，抗闪烁，四码流，心跳，图像旋转，隐私区遮盖，水印技术，设置访问端口
支持的协议	IPv4, TCP/IP, UDP,HTTP, DHCP,RTP/RTCP/RTSP,FTP, DHCP, DDNS, NTP, IGMP, ICMP
兼容协议	ONVIF，GB/T28181
安全	密码保护，多用户访问控制
API 集成	提供 SDK 开发包、移动应用 APP HD Live 以及配套 NVR 和 CMS 管理平台软件

视频输出	1 路 CVBS 标清复合视频输出（BNC 接口，1.1Vp-p±10%，RL=72)；1 路 HDMI 1.4a 高清数字视频输出；RJ45
音频接口	3.5mm 线性音频输入输出接口（Line In/Out)，外接有派麦克风或者线性输入
通讯接口	1 个 RJ45 10M/100M 自适应以太网口；1 个 RS-485 接口
报警输入	1 路，低电平有效，Vin<=0.3V
报警输出	1 路，开关量信号，1A/125VAC,1A/30VDC
本地存储	支持至少 1 个 microSD/SDHC 存储卡插，最大支持 64GB
USB 接口	标准 USB2.0 扩展接口
工作温度和湿度	-20℃～55℃, 20-80% RH (无凝结)
功耗	＜5W
电源	AC24V /DC12V 交流供电; PoE 以太网供电(选配)
图像传感器	1/1.9″ 2.1 MP Sony 逐行扫描 CMOS
解析度	水平≥1000TVL,垂直≥1000TVL
最低照度	彩色：0.005Lux @ F1.2；黑白：0.005Lux @ F1.2
镜头	1/2″，1″，4/3″200 万像素及以上级别高清镜头
镜头接口	CS/C 接口
日夜转换模式	自动日夜型 ICR 红外切换滤片式
宽动态范围	128dB
信噪比	63.8dB
延时	150ms
定码率均值	4Mbps
灰度等级	11 级
数字降噪	3D-MCTF 数字降噪
快门速度	100000s to 1/25s
4A 控制	自动白平衡，自动增益，自动曝光，自动光圈控制
视频压缩标准	H.264/MJPEG
H.264 编码级别	Main Profile @ Level 5.1
压缩输出码率	32 Kbps~12Mbps
音频压缩标准	G.711/ AAC / MP2
音频压缩码率	G.711(64Kbps) /MP2(16kHz 16bit 32kpbs)
最高分辨率	Full HD/1080P(1920x1080)

帧率	在高帧率模式下最高位 120fps；其它所有分辨率下均可达 25fps
多码流	在高帧率模式下为单码流；四码流：FHD/1080P+720P+FULL D1+CIF；三码流：1080P+FULL D1+ CVBS/HDMI
视频流	在最大分辨率下以全帧速同时输出多路视频流，帧速和带宽可调整，H.264 支持 VBR/CBR
图像设置	可调节图像格式、码率、亮度、对比度、饱和度、锐度、白平衡 多区智能 OSD 图像翻转和镜像（走廊模式） 自动、手动或预定日/夜模式 多场景定时切换模式 经纬度图像模式
日夜转换方式	自动，定时，手动，报警触发
离线存储	支持至少 1 个 microSD/SDHC 卡扩展
背光补偿	开/关
强光抑制	开/关
曝光模式	暗曝光、中心点曝光、平均曝光、指定区域曝光等可选
透雾	支持
感兴趣区域 ROI	支持分别设置固定区域或动态跟踪
ePTZ	支持，需要 inControl 客户端配合
智能报警	图像侦测，移动侦测，传感器联动报警，网线断，IP 地址冲突，存储器满，存储器错

4.1.12 补光灯设备

色温支持不大于 6700K，最高功率不大于 95W，实际功率与控制方式有关；

在无环境光照明的情况下，可拍摄到清晰的车牌图像；

响应时间：≤20μs，可与相机进行频率同步；

采用大功率白光 LED，光通量≥1800LM，发光角度不低于 30 度，有效照射距离 16-24 米；

LED 补光灯灯珠数量不少于 16 颗；

对人眼无刺激，不影响行车安全；

白天可平抑逆光，夜间可压制车大灯眩光；

触发方式：电平量触发，4V~6V；

支持 IP66 防护等级；

工作寿命大于 50000h；

工作温度：-40℃~+60℃，10~95%RH；

补光灯亮度可调

设备需提供《交通技 术 监 控成像补光装置通用技术条件》的认证测试报告

4.2 中心设备

4.2.1 高端配置服务器

四路 10 核 Xeon E7-4820 v4 处理器(2.0GHz, 25M 缓存)；

2 块 Raid 卡(支持直通模式)，

512GB 内存；

1 块 HGST 800G SSD 卡或盘；

8 块 1.2TB SAS 盘；

4 块 10GE 网卡，

4 块 1GE 网卡；

五年原厂 7*24 小时现场服务，硬件不返还服务

4.2.2 普通配置服务器

双路 10 核 Xeon E5-2640 v4 处理器(2.4GHz, 25M 缓存)；

2 块 Raid 卡(支持直通模式)，

256GB 内存；

1 块 HGST 800G SSD 卡或盘；

4 块 900G SAS 盘；

4 块 10GE 网卡，

4 块 1GE 网卡；

五年原厂 7*24 小时现场服务，硬件不返还服务

4.2.3 图片解析服务器

机框式服务器，提供 8 个 GPU 插槽

CPU：E5 2680 V4 *2

GPU：Nvidia P4 *8

内存：512G Mem(DDR4/ECC/REG)

硬盘：480G SSD*1(系统盘)1T SSD * 8(数据盘) RAID5

网卡：万兆网卡

软件基础配置：

操作系统：Ubuntu 14.04

数据库：MongoDB

中间件：Kafka

其他支撑软件：tomcat

4.2.4 基础信息中间库专用设备

基础信息中间库接口服务专用设备

提供基础信息中间库安全 API 调用接口服务

4.2.5 服务器

处理器：一颗高性能 Intel E3-1225 四核 CPU，16 颗英伟达 TX1 系列 GPU，共 4096 核 CUDA 处理器；

内存：8GB DDR3 内存，64GB LPDDR4 内存；

硬盘：120G SSD 固态硬盘；

数据接口：4 个千兆自适应网络接口，1 个 VGA 接口，4 个 USB 3.0 接口和 2 个 USB 2.0 接口；

可支持 16 路 1080P 实时流并发分析

4.2.6 二级处理数据 库/视频基础应用/大数据应用服务器

处理器：E5-2640 V3(8 核 2.6GHz)×2

内存：16GB DDR4×2

硬盘：300GB SAS×2

带 DVD 光驱，4 个 1GbE×4 接口。

Windows Server 2008 R2 操作系统

4.2.7 大数据检索服务器

冷数据存储：不带轨迹 10 亿/带轨迹 2 亿

热数据存储：3500 万

3500 万热数据单个以图搜图：5S 内

5 亿冷数据单个属性检索：5S 内

CPU:2*E5-2630 V4 CPU，2*10=20 核

内存：8*32G=256G

硬盘：2*240G SSD，6*480G SSD，2*4T SATA

4.2.8 网络硬盘录像机（NVR）

系统参数	**主处理器**	工业级嵌入式微控制器
	操作系统	嵌入式 Linux 操作系统
	系统资源	支持 512Mb 接入
	操作界面	WEB 方式;本地 GUI 操作
音频参数	**音频输入**	至少 1 路
	音频输出	至少 1 路
视频参数	**视频输入**	最大支持 128 路

	视频输出	至少 1 路 VGA 输出,3 路 HDMI VGA 与 HDMI1 同源 HDMI1/HDMI2/HDM3 异源 4K 显示输出 HDMI3 最大支持 4K@60hz
	画面分割	任意分割，最大支持 64 路画面
报警参数	**报警输入**	至少 16 路
	报警输出	至少 8 路，继电器输出
解码参数	**解码类型**	H.264,H.265,SVAC,MPEG4,JPEG
	解码能力	至少 24 路 1080P
功能	**录像模式**	手动录像;事件报警录像;定时录像;
	多路回放	至少支持同时 16 路 D1;8 路 720P;4 路 1080P 回放
	移动侦测	每画面可设置 396（22×18）个检测区域，可设置多级灵敏度，1～6 档可调
	区域遮挡	每路支持 4 个区域遮挡块
	备份方式	U 盘，eSata
接口	**网络协议**	SNMP,FTP,ISCSI,UPNP
	SATA 接口	至少 16 个 SATA3.0/SAS
	SAS 接口	至少 2 个 SAS3.0
	eSATA 接口	至少 1 个
	RS232 接口	至少 1 个，用于调试及透传串口数据
	RS485 接口	至少 1 个，用于控制外部云台等，支持多种协议
	USB 接口	至少 2 个 USB2.0,2 个 USB3.0
	HDMI 接口	至少 3 个,HDMI1/HDMI2 4K@30HZ,HDMI3 4K@60HZ
	网络接口	至少 4 个 RJ45 10/100/1000Mbps 自适应以太网口 至少 4 个 1000Mbps 光口
常规参数	**供电**	AC100V～240V 50+2% Hz
	功耗	＜120W（不含硬盘以及智能模块）
	工作温度	0℃～+50℃
	工作湿度	10％～90％
	安装方式	台式/机架安装
其他	需通过上海市公安局兼容性测试	

4.2.9 集中存储服务器

（一） 集中视频存储设备（7 天视频）

4 个分控中心，每个配置 1 台全对称分布式横向扩展集群 NAS 存储设备，要求如下：

指标项	技术规格要求
品牌	1.国际知名品牌，非 OEM 产品，拥有自主知识产权，非开源软件开发，如使用开源 Lustre 和 Ceph 软件等。 2.存储国内市场发货套数和发货容量排名前三，并出具 IDC 官方证明； 3.全球知名存储品牌，进入 Gartner 领导者象限，提供 Gartner 或 IDC 同类产品关键竞争力排名证明。
案例证明	需有用户容量 10PB 以上案例至少 5 个。
体系架构	存储系统要求产品采用基于云存储技术，支持横向扩展技术的全对称分布式架构，非开源软件加服务器方式实现； 无独立的元数据服务器和管理服务器（非文件引擎和 SAN 引擎组装架构），提供技术说明； 分布式文件系统具有软件著作权登记证书；
协议支持	操作系统要求为专业存储操作系统。 支持 NFS(V3 或者以上)，SMB(V1/V2)，支持 NIS，Microsoft Active Directory，LDAP，SNMP
总体要求	支持最少 3 台存储节点即可构建云存储，系统支持≥288 节点线性扩展。 **单一文件系统存储容量可扩展至≥100PB**
实配容量	**本次配置≥15 个节点，其中两个节点是做为备件，交付到分控中心** **每节点配置 ≥1*900G SSD 硬盘** **≥35*8TB SATA 硬盘**
性能指标	**投标产品提供 SPEC SFS2008≥100 万 OPS 的材料，提供证明材料；** **1TB 数据恢复时间不超过 1 小时，提供技术说明；**
数据可靠性	支持 N+1 到 N+4 的数据保护策略，最大支持任意 4 个节点故障，数据不丢失，提供基于目录的冗余配比策略，提供不同的数据保护级别； 本次配置软件系统要求每套设备支持故障节点数大于等于 1 个，或集群任意故障 2 块硬盘的数据保护策略，系统出现以上故障后仍旧稳定运行。 支持视频监控图像修复功能；
组网模式	支持 Infiniband 组网或者万兆。 前端业务网络与管理网络物理隔离，为了避免数据重构，动态分级等内部流量对前端业务产生影响，同时基于网络安全等因素，必须独配置独立的后端网络接口卡(以太网）和交换机承载内部流量。

节点互联交换机	配置用于节点间内部数据交换的交换机 **配置 2 台 48 口万兆后端以太网交换机**，要求交换容量≥1.28Tbps，转发性能≥480Mpps **配置 1 台 48 口千兆管理以太网交换机**，要求交换容量≥256Gbps，包转发率≥138Mpps 配齐本次节点间互联所需的线缆和模块
硬件设备	每节点配置处理器数目≥2 个八核处理器。 单节点内存可扩展至 256GB（该内存须系统自带，不能以插 PCI 卡和闪存盘方式扩充，且必须是读写双向内存），**本次配置 64GB**
保电缓存	**单节点配置保电缓存 NVDIMM≥8GB**
支持的硬盘类型	2.5 寸 200GB、2.5 寸 600GB SAS、900GB SAS； 3.5 寸 200GB、3.5 寸 4TB/6TB/8TB SATA 设备需支持不同型号硬盘混插。
存储单元主机接口	**本次单节点配置 2*10GE 后端接口，2*10GE 前端接口**,1 个管理网口
客户端连接负载均衡	1.支持并配置客户端连接负载均衡软件,负载策略支持 CPU 占用率、网络带宽、TCP/IP 连接数、轮询、节点能力值。 2.如果不支持负载均衡，则必须在投标设备中增加第三方商用的负载均衡设备。
动态分级存储功能	支持基于文件级的动态分级存储功能，分级策略支持基于 I/O 热度自动分级。
空间配额管理	**配置基于用户、用户组、目录的空间配额管理，支持文件数量配额管理。**
自动精简配置	支持自动精简配置，可按需动态分配存储空间，保证存储资源的最大化利用。
Worm	支持企业级 Worm 功能
全局缓存	系统支持全局缓存，提高存储访问效率。
管理软件	支持并提供功能全面的图形化管理软件，同时提供中文和英文管理界面，支持 Web 或其它图形化方式进行远程管理，可视化系统结构图，提供对整个存储系统各个部分的监测； 管理软件具备对集群内部组网交换机的管理能力，支持查询端口状态和告警转发；
服务	需有原厂商针对该项目授权书； 需有原厂商针对该项目**三年**质保函； 提供**三年**免费软硬件原厂技术支持与售后服务； 提供**三年**介质保留服务； 设备生产商需在国内设有 400/800 技术服务热线。

(二)大图片存储设备

配置 1 套横向扩展集群 NAS 存储设备，要求如下：

指标项	技术规格要求
品牌	1.国际知名品牌，非 OEM 产品，拥有自主知识产权，非开源软件开发，如使用开源 Lustre 和 Ceph 软件等。 2.存储国内市场发货套数和发货容量排名前三，并出具 IDC 官方证明； 3.全球知名存储品牌，进入 Gartner 领导者象限，提供 Gartner 或 IDC 同类产品关键竞争力排名证明。
案例证明	需有用户容量 10PB 以上案例至少 5 个。
体系架构	存储系统要求产品采用基于云存储技术，支持横向扩展技术的全对称分布式架构，非开源软件加服务器方式实现； 无独立的元数据服务器和管理服务器（非文件引擎和 SAN 引擎组装架构），**提供技术说明；** **分布式文件系统具有软件著作权登记证书；**
协议支持	操作系统要求为专业存储操作系统。 支持 NFS(V3 或者以上)，SMB(V1/V2)，支持 NIS，Microsoft Active Directory，LDAP，SNMP
总体要求	支持最少 3 台存储节点即可构建云存储，系统支持≥288 节点线性扩展 **单一文件系统存储容量可扩展至≥100PB**
实配容量	**本次配置≥22 个节点；** **每节点配置 ≥1*900G SSD 硬盘** **≥35*6TB SATA 硬盘**
性能指标	**投标产品提供 SPEC SFS2008≥100 万 OPS 的材料，提供证明材料；** **1TB 数据恢复时间不超过 1 小时，提供技术说明；**
数据可靠性	支持 N+1 到 N+4 的数据保护策略，最大支持任意 4 个节点故障，数据不丢失，提供基于目录的冗余配比策略，提供不同的数据保护级别； 本次配置软件系统要求每套设备支持故障节点数大于等于 1 个，或集群任意故障 2 块硬盘的数据保护策略，系统出现以上故障后仍旧稳定运行。 支持视频监控图像修复功能；
可扩展性	横向扩展支持≥280 节点线性扩展， 单节点扩展支持节点在线平滑扩展，后续添加新节点后，存储系统能够自动识别所加入的节点的容量，并自动合并所加入的空间。
组网模式	支持 Infiniband 组网或者万兆。

	前端业务网络与管理网络物理隔离，**提供技术说明**
节点互联交换机	配置用于节点间内部数据交换的交换机 **配置 2 台 48 口万兆后端以太网交换机**，要求交换容量≥1.28Tbps，转发性能≥480Mpps **配置 1 台 48 口千兆管理以太网交换机**，要求交换容量≥256Gbps，包转发率≥138Mpps 配齐本次节点间互联所需的线缆和模块
硬件设备	每节点配置处理器数目≥2 八核处理器。 单节 96GB 内存可扩展至 256GB（该内存须系统自带，不能以插 PCI 卡和闪存盘方式扩充，且必须是读写双向内存），**本次配置 96GB**
保电缓存	**单节点配置保电缓存 NVDIMM≥8GB**
支持的硬盘类型	2.5 寸 200GB、2.5 寸 600GB SAS、900GB SAS； 3.5 寸 200GB、3.5 寸 24TB/6TB/8TB SATA 设备需支持不同型号硬盘混插。
存储单元主机接口	**本次单节点配置 2*10GE 后端接口，2*10GE 前端接口**,1 个管理网口
客户端连接负载均衡	1.支持并配置客户端连接负载均衡软件,负载策略支持 CPU 占用率、网络带宽、TCP/IP 连接数、轮询、节点能力值。 2.如果不支持负载均衡，则必须在投标设备中增加第三方商用的负载均衡设备。
动态分级存储功能	支持基于文件级的动态分级存储功能，分级策略支持基于 I/O 热度自动分级。
空间配额管理	**配置基于用户、用户组、目录的空间配额管理，支持文件数量配额管理。**
自动精简配置	支持自动精简配置，可按需动态分配存储空间，保证存储资源的最大化利用。
Worm	支持企业级 Worm 功能
全局缓存	系统支持全局缓存，提高存储访问效率。
管理软件	支持并提供功能全面的图形化管理软件，同时提供中文和英文管理界面，支持 Web 或其它图形化方式进行远程管理，可视化系统结构图，提供对整个存储系统各个部分的监测； 管理软件具备对集群内部组网交换机的管理能力，支持查询端口状态和告警转发；
服务	需有原厂商针对该项目授权书； 需有原厂商针对该项目**三年**质保函； 提供**三年**免费软硬件原厂技术支持与售后服务； 提供**三年**介质保留服务；

	设备生产商需在国内设有 400/800 技术服务热线。

(三)小图片存储设备

配置 1 套横向扩展集群 NAS 存储设备，要求如下：

指标项	技术规格要求
品牌	1.国际知名品牌，非 OEM 产品，拥有自主知识产权，非开源软件开发，如使用开源 Lustre 和 Ceph 软件等。 2.存储国内市场发货套数和发货容量排名前三，并出具 IDC 官方证明； 3.全球知名存储品牌，进入 Gartner 领导者象限，提供 Gartner 或 IDC 同类产品关键竞争力排名证明。
案例证明	列出用户容量 10PB 以上案例至少 5 个。
体系架构	存储系统要求产品采用基于云存储技术，支持横向扩展技术的全对称分布式架构，非开源软件加服务器方式实现； 无独立的元数据服务器和管理服务器（非文件引擎和 SAN 引擎组装架构），**提供技术说明；** **分布式文件系统具有软件著作权登记证书；**
协议支持	操作系统要求为专业存储操作系统。 支持 NFS(V3 或者以上)，SMB(V1/V2)，支持 NIS，Microsoft Active Directory，LDAP，SNMP
总体要求	支持最少 3 台存储节点即可构建云存储，系统支持≥288 节点线性扩展。 **单一文件系统存储容量可扩展至≥100PB**
实配容量	**本次配置≥12 个节点；** **每节点配置 ≥1*900G SSD 硬盘** **≥35*4TB SATA 硬盘**
性能指标	**投标产品提供 SPEC SFS2008≥100 万 OPS 的材料，提供证明材料；** **1TB 数据恢复时间不超过 1 小时，提供技术说明；**
数据可靠性	支持 N+1 到 N+4 的数据保护策略，最大支持任意 4 个节点故障，数据不丢失，提供基于目录的冗余配比策略，提供不同的数据保护级别； 本次配置软件系统要求每套设备支持故障节点数大于等于 1 个，或集群任意故障 2 块硬盘的数据保护策略，系统出现以上故障后仍旧稳定运行。 支持视频监控图像修复功能；
可扩展性	横向扩展支持≥280 节点线性扩展， 单节点扩展支持节点在线平滑扩展，后续添加新节点后，存储系统能够自动识别所加入的节点的容量，并自动合并所加入的空间。

组网模式	支持 Infiniband 组网或者万兆。 前端业务网络与管理网络物理隔离，**提供技术说明**
节点互联交换机	配置用于节点间内部数据交换的交换机 **配置 2 台 48 口万兆后端以太网交换机**，要求交换容量≥1.28Tbps，转发性能≥480Mpps **配置 1 台 48 口千兆管理以太网交换机**，要求交换容量≥256Gbps，包转发率≥138Mpps 配齐本次节点间互联所需的线缆和模块
硬件设备	每节点配置处理器数目≥2 个八核处理器。 单节点内存可扩展至 256GB（该内存须系统自带，不能以插 PCI 卡和闪存盘方式扩充，且必须是读写双向内存） **本次配置 160GB**
保电缓存	**单节点配置保电缓存 NVDIMM≥8GB**
支持的硬盘类型	2.5 寸 200GB、2.5 寸 600GB SAS、900GB SAS； 3.5 寸 200GB、3.5 寸 4TB/6TB/8TB SATA 设备需支持不同型号硬盘混插。
存储单元主机接口	**本次单节点配置 2*10GE 后端接口，2*10GE 前端接口**,1 个管理网口
客户端连接负载均衡	1.支持并配置客户端连接负载均衡软件,负载策略支持 CPU 占用率、网络带宽、TCP/IP 连接数、轮询、节点能力值。 2.如果不支持负载均衡，则必须在投标设备中增加第三方商用的负载均衡设备。
动态分级存储功能	支持基于文件级的动态分级存储功能，分级策略支持基于 I/O 热度自动分级。
空间配额管理	**配置基于用户、用户组、目录的空间配额管理，支持文件数量配额管理。**
自动精简配置	支持自动精简配置，可按需动态分配存储空间，保证存储资源的最大化利用。
Worm	支持企业级 Worm 功能
全局缓存	系统支持全局缓存，提高存储访问效率。
管理软件	支持并提供功能全面的图形化管理软件，同时提供中文和英文管理界面，支持 Web 或其它图形化方式进行远程管理，可视化系统结构图，提供对整个存储系统各个部分的监测； 管理软件具备对集群内部组网交换机的管理能力，支持查询端口状态和告警转发；
服务	需有原厂商针对该项目授权书； 需有原厂商针对该项目**三年**质保函；

	提供**三年**免费软硬件原厂技术支持与售后服务； 提供**三年**介质保留服务； 设备生产商需在国内设有 400/800 技术服务热线。

(四)数据库存储设备

配置 1 套高端全闪存光纤存储设备，要求如下：

指标项	指标要求
品牌	1.国际知名品牌，非 OEM 产品，拥有自主知识产权，非开源软件开发，如使用开源 Lustre 和 Ceph 软件等。 2.存储国内市场发货套数和发货容量排名前三，并出具 IDC 官方证明； 3.全球知名存储品牌，进入 Gartner 领导者象限，提供 Gartner 或 IDC 同类产品关键竞争力排名证明。
体系架构	全闪存固态存储系统，不接受可配置传统机械硬盘的存储系统；
	多控全交换架构，最大可扩展至 16 控制器 本次配置控制器数≥2
	控制器之间采用高带宽、低时延的 PCI-E、Rapid-IO 或 IB 高速总线互联方式，非 FC、IP 协议或者 FC、IP 接口互联
存储缓存容量	系统实际配置总缓存容量≥2TB （不含任何性能加速模块、FlashCache、PAM 卡，SSD Cache 等）
主机接口类型	支持 8Gbps FC、1Gbps iSCSI、10Gbps iSCSI、10Gbps FCoE,16Gbps FC，56Gb IB
前端主机通道接口	支持≥4 个 8Gb FC 主机接口，每个 IO 模块支持热拔插功能。 本次配置 32 个 16Gb FC 主机接口
配置硬盘	本次配置 41 块 1.92TB 企业级 SSD 硬盘（SAS 接口，非 SATA 接口）
最大硬盘数	最大支持磁盘插槽个数≥1800，本次配置 24*4*12G SASSAS3.0 磁盘通道
支持 RAID	支持 RAID 1、RAID3、RAID 10、RAID50、RAID 5、RAID6 等可选配置
冗余性	冗余电源、风扇、控制器、缓存断电保护功能
在线压缩	支持 SAN 存储在线压缩功能（不接受后压缩即 Post 压缩），同时实际配置改功能（无限容量许可，扩容不需要再次购买软件 license），提升存储效率。
在线重删	支持 SAN 存储在线重删功能（不接受后重删即 Post 重删）

SAN 异构虚拟化技术	支持异构虚拟化技术 1）支持异构虚拟化功能，能够提供异构存储虚拟化整合功能，能接管现网异构存储，无需破坏或者改变现有数据格式，构成异构资源池，进行统一的资源调配和管理。 2)异构虚拟化兼容业界主流存储（如 EMC、HP、HDS、IBM、Huawei、NetApp 等多个厂家的阵列） 3）通过全闪存本身软件实现，无需外加网关
在线不停业务的数据迁移	存储系统支持基于异构虚拟化功能的不停业务的在线数据迁移，支持 EMC、HDS、IBM、HPE 等主流存储厂商的设备。
关键业务保障	实配 QoS 功能，提供图像化管理界面，能够按照 IOPS、吞吐量、响应时间等维度进行策略调整
	配置服务质量管理按优先级控制功能
	配置数据销毁功能，通过全 0 或随机数据覆盖写来销毁数据；
远程容灾保护	支持基于磁盘阵列自身的容灾复制软件许可，提供同步和异步方式的数据复制，能够提供 FC 和 IP 复制；
	支持存储 SAN 双活功能 1）提供双活架构，实现两套核心存储数据双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。 2） 双活架构需要具备独立的第三方仲裁设备。仲裁设备故障时，不影响业务运行，同时双活卷仍能保持数据实时一致； 3） 双活引擎数据传送必须采用 FC 协议和链路双活（非 IP 协议或者 IP 链路） 4）不需配置额外的网关，即可实现双活能力，提供产品彩页。 5）支持双物理仲裁设备（非虚拟机仲裁）的冗余，任何一个仲裁故障和站点故障业务均可正常运行
NAS 功能	支持 SAN 和 NAS 一体化，不需额外配置 NAS 网关，存储操作界面同时支持快存储和文件系统服务
可管理性	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储的图形化管理配置和监控软件。
安装服务	三年 7*24 原厂现场服务，三年介质保留服务，提供原厂售后服务承诺函盖鲜章原件和授权书盖鲜章原件；设备生产商需在国内设有 400 技术服务热线

Gartner	近三年入选 Gartner 通用磁盘阵列存储魔力四象限； 近三年入选 Gartner 通用磁盘阵列存储魔力四象限领导者象限
IDC	整体外部磁盘存储市场国内排名前三（2017Q1、2017Q2）的专业存储厂商，并出具 IDC 官方证明

(五)业务数据备份设备

配置 1 套支持重复数据删除功能的备份存储，要求如下：

指标项	指标要求
品牌	1.国际知名品牌，非 OEM 产品，拥有自主知识产权，非开源软件开发，如使用开源 Lustre 和 Ceph 软件等。 2.存储国内市场发货套数和发货容量排名前三，并出具 IDC 官方证明； 3.全球知名存储品牌，进入 Gartner 领导者象限，提供 Gartner 或 IDC 同类产品关键竞争力排名证明。
体系架构	SAN 和 NAS 统一存储，同时支持 NAS、IP SAN 和 FC SAN；
统一存储控制器	多控架构，最大可扩展为 8 个控制器。 本次配置 2 个控制器，双控之间（含 SAN 和 NAS）采用 PCI-E 互联
一体化统一存储	支持 SAN 和 NAS 一体化，不需额外配置 NAS 网关，存储操作界面同时支持快存储和文件系统服务
存储缓存容量	控制器缓存≥128GB,（不含任何性能加速模块、FlashCache、PAM 卡，SSD Cache 等）；NAS 缓存具备 UPS 断电保护功能， 在出现电源故障时，可提供充足的电源，将高速缓存内容转储至非易失性内部存储设备上（非通用服务器架构）
前端主机通道接口	本期配置 8 个 16Gb FC 端口+8 个万兆网络接口
主机接口类型	支持 8Gbps FC、1Gbps iSCSI、10Gbps iSCSI、10Gbps FCoE,16Gbps FC，56Gb IB 以及智能 IO 卡(4 口，支持 8/16Gb FC、10GE 和 FCoE)
后端磁盘通道	本次双控配置≥4*4*12Gbps SAS3.0 磁盘通道
配置硬盘	本次配置 48TB 裸容量，可用容量 34TB 左右
最大硬盘数	最大支持磁盘插槽个数≥730
支持 RAID	支持 RAID 1、RAID3、RAID 10、RAID50、RAID 5、RAID6 等可选配置
可维护性	磁盘、电源、IO 模块都可以不停机热插拔
故障快速恢复	故障快速恢复： 提供快速恢复技术，能够保障硬盘失效后的故障时间最短，减少风险；
可维护性	磁盘、电源、IO 模块都可以不停机热插拔

SAN 异构虚拟化技术	支持异构虚拟化技术 1）支持异构虚拟化功能，能够提供异构存储虚拟化整合功能，能接管现网异构存储，无需破坏或者改变现有数据格式，构成异构资源池，进行统一的资源调配和管理。 2）异构虚拟化兼容业界主流存储（如 EMC、HP、HDS、IBM、Huawei、NetApp 等多个厂家的阵列） 3）提供快速回退功能，即被接管的阵列可直接映射给业务主机使用，防止由于虚拟化失败或者虚拟化不能快速回退造成的数据丢失，导致业务系统不可恢复； 4）异构虚拟化平台支持提供异构存储之间的数据镜像功能； 5）异构虚拟化平台支持提供异构存储之间的双活应用； 6）支持对异构存储创建 FC 和 iSCSI 链路，进行数据传输，并管理异构 LUN
关键业务保障	支持 Cache 缓存分区功能，保障关键业务资源使用；
	支持 QoS 功能，提供图像化管理界面，能够按照 IOPS、吞吐量、响应时间等维度进行策略调整
	支持服务质量管理按优先级控制功能；
资源使用效率提升	配置自动精简配置，可实现存储资源的按需分配，实现零检测和已删除空间的回收，提高空间利用率
	支持块重删功能（非零界面删除），提升空间的有效利用率
	支持自动分级存储，能够以 512 KB～64MB 的热点颗粒度为单位进行自动分级调整，提供图形化的自动分层策略调整工具，能够对数据分层的时间窗口和分层方式进行调整，提高存储资源利用效率，即支持在特定的时间段（定时），开启 I/O 监控热点数据，自动进行数据迁移；具备至少 3 层分级（SSD、SAS、NL-SAS）。
	支持多租户功能，实现隔离租户间的资源，分权分域
本地数据保护	支持数据快照功能，恢复某个时间点的快照，其他时间点快照不丢失；

	支持存储 SAN 双活功能 1）提供双活架构，实现两套核心存储数据双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。 2） 双活架构需要具备独立的第三方仲裁设备。仲裁设备故障时，不影响业务运行，同时双活卷仍能保持数据实时一致； 3） 双活引擎数据传送必须采用 FC 协议和链路双活（非 IP 协议或者 IP 链路） 4） 双活引擎采用冗余架构，提供四坏三节点故障业务不停顿的冗余配置 5）双活配置容量许可，容量不少于实配硬盘； 6）提供异构虚拟化双活能力，对于异构整合后的第三方存储，能够建立双活镜像对
	可通过图形化管理界面自定义远程数据异步传输时间间隔，异步传输时间间隔可达到≤10 秒，可通过阵列异步复制功能把主中心数据复制到异地中心
NAS 基础软件包	支持 NAS 功能，提供 NFS、CIFS、NDMP、多租户、目录配额功能
专用操作系统	采用专业存储操作系统提供文件系统服务，不接受采用服务器+Windows storage server 操作系统的方式提供文件系统服务。
重删压缩	支持文件系统在线重删以及在线压缩功能用于节省存储空间
一体化备份	支持不需要备份软件直接将文件系统备份到备份存储
Worm	支持 Worm 特性，满足一次写入不可修改和删除，满足关键业务文件信息安全以及法规遵从的要求
一体化双活	支持 SAN 双活和 NAS 双活的统一存储双活架构，并能进行统一管理；
安装服务	三年原厂 7*24 小时现场服务，三年介质保留服务，提供原厂售后服务承诺函盖鲜章原件和授权书盖鲜章原件；设备生产商需在国内设有 400 技术服务热线。
可管理性	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储的图形化管理配置和监控软件。
Gartner	近三年入选 Gartner 通用磁盘阵列存储魔力四象限； 近三年入选 Gartner 通用磁盘阵列存储魔力四象限领导者象限
IDC	整体外部磁盘存储市场国内排名前三（2016 年全年）的专业存储厂商，并出具 IDC 官方证明

(六)数据备份软件

指标项	参数要求(一体化备份，Pro：1TB~64TB)
支持的备份容量	配置不少于 34TB 用户数据备份的授权 License
功能特性	支持主流操作系统及文件系统备份，包括 Windows、Linux 下的各操作系统以及国产中标麒麟和红旗操作系统备份。
	支持多平台下的主流数据库和应用在线备份，包括：Oracle、SQL Server、SAP HANA、MySQL、GBase、达梦、Exchange、Domino 等应用。
	支持主流虚拟化平台备份，包括：VMWare、Hyper-V、FusionSphere、H3C CAS、云宏、InCloudSpere、RHEV 虚拟化平台备份。
	结合 RMAN 对 Oracle 数据进行备份，无需使用任何脚本，提供 Oracle 单表恢复能力。
	针对 Exchange Server 提供数据库级别备份的同时，实现单个邮件恢复。
	支持 VMware 虚拟机中单文件恢复能力，整个过程无需任何脚本工作。
	支持断点续传，支持 Oracle，Exchange，主流文件系统的数据备份作业和恢复作业自动从断点继续工作，不需要用户干预。
	支持华为 OceanStor V3、V5 和 OceanStor Dorado V3 系列存储快照管理和快照备份。
	备份一体化节点默认配置源端重复数据删除功能。
	支持系统管理员、普通管理员和审计管理员三员管理。支持自定义角色。
	支持自动演练恢复，无需任何脚本，支持文件、SQL Server 和 Oracle 备份数据根据预设定的策略全自动（非同步）恢复到指定的目标位置。
	支持自备份管理，针对备份存储系统自身的数据进行备份保护，并支持离线导出，当备份存储系统自身发生故障时，可通过备份数据进行还原。
	支持远程复制，支持将本地备份数据 1 对 1、1 对多、多对 1，级联方式进行远程复制，复制支持断点续传，流量限速及固定时段暂停传输，异地备份数据具有安全管理机制，异地备份存储系统需要得到本地授权许可后，才可以浏览、恢复本地传输过去的备份数据，最大限度避免备份数据的泄密可能
	支持备份数据一致性校验，确保备份数据的可用性。
产品资质	1、 服务器通过 CCC、CB、FCC、REACH、ROHS 等国际认证。 2、存储产品进入 Gartner 存储魔力四象限。
软件资质	备份软件通过 CCC、ISCCC、公安部销售许可、涉密信息系统等认证。
公司资质	1、国内排名前三，具备 IDC 官方出具的证明； 2、具备 ISO9001、ISO27001、具备环境认证 14001 认证； 3、具备 SNIA 存储网络工业协会 Vendor Large 最高投票权厂家。

(七)光纤交换机

指标项	技术规格要求
品牌	与存储同一品牌
硬件特性	
端口数	交换机模式：最大支持 48 个端口，可通过按需增加端口许可证，以 12 端口的增量增加为 24、36 和 48 个通用(E、F、M、D 或 EX)端口； **本次激活≥48 端口（含 48 个 16Gb 多模 SFP 模块)；** **本次配置≥48 根 3M 多模光跳线；**
端口类型	D_Port（诊断端口)、E_Port、EX_Port、F_Port 和 M_Port（镜像端口)； 基于交换机类型的自我发现(U_Port)； 接入网关模式中的可选端口类型控制：F_Port 和使用 NPIV 技术的 N_Port。
端口速率	2、4、8 和 16 Gbps 端口速率自动感应； 10 Gbps ，可选择性编程为固定端口速率。
ISL 链路聚合	基于帧的链路聚合，每条 ISL 链路最多 8 个 16 Gbit/sec 端口； 每条 ISL 干线速率最高 128 Gbit/sec； 运用 Fabric OS 中所包括的 DPS，实现基于交换的跨 ISL 负载平衡； 对交换机内可配置的聚合链路集没有数量限制；
软件特性	
可视化用户界面	所有关键部件 LED 指示灯、基于 Web 的管理界面和故障定位指示；
互操作性与认证	与设备兼容，包括主流厂商服务器、存储系统、HBA 卡等设备和应用软件；
服务与安装	
安装材料	配置机架安装套件，支持标准 19 英寸机架式安装；
服务	需有原厂商针对该项目授权书； 需有提供原厂商针对该项目 **3 年**质保函； 提供 **3 年** 7x24 小时软硬件原厂技术支持与售后服务； 提供安装服务； 设备生产商需在国内设有 400 技术服务热线。

4.2.10 核心交换机

交换架构：采用多级多平面正交交换架构，能够配置独立的交换网板，控制引擎和交换网板硬件相互独立，设备为 CLOS 架构设计，基于网元转发，采用无中板技术，主控板 1+1 冗余，支持大于等于 8 个业务扩展槽位。

机框散热设计：风扇框居中，对应单板芯片位置加强散热，风扇扇叶大，节能高效。线卡、网板严格前后风道，支持电源 N+N 冗余，万兆单板功耗<=4.5W，提供权威测试机构的第三方测试报告

交换容量>=230Tbps

包转发率>=230000Mpps

支持 ACL 能力

MAC 表项>=750K

ARP 表项>=370K

路由转发表容量>=250K

单槽位 48 口 100G 单板线速，需提供第三方测试报告

单槽位 48 口 40G 单板线速，需提供第三方测试报告

板卡配置：支持 GE(光/电)、10GE（光/电)、40GE(光)、100GE(光)

单槽位千兆端口密度≧48，单板最大 10G 端口数≧48，单板最大 40G 端口数≧48，单板最大 100G 端口数≧48

支持将 N 台物料设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合

支持将一台物理交换机虚拟化成 N 台逻辑交换机，交换机间硬件独立且相互隔离；

支持 OPENFLOW 1.3 标准，支持多控制器（EQUAL 模式、主备模式），支持多表流水线，支持 Group table，支持 Meter，支持 VxLAN 二层网关，支持 VxLAN 三层网关，支持 FCoE，支持 DCB

支持数据中心内大二层技术和跨数据中心的二层互联技术

支持基于端口的 VLAN，802.1q Vlan 封装，最大 Vlan 数>=4096，支持 GVRP　远程端口镜像（RSPAN），流量控制/802.3x，　支持链路聚合能力，　聚合组内最大成员端口数量>=32，　最大聚合组数量>=128

支持 STP/RSTP/MSTP 协议，符合 IEEE802.1D、IEEE802.1W、IEEE802.1S 标准

QOS 支持优先级队列，支持 SP、WRR、SP+WRR 队列调度算法

支持 PIM-DM、PIM-SM、PIM-SSM、MSDP、MBGP 、Any-RP、IGMPv1/v2/v3 等协议

支持 PIM6-DM、PIM6-SM、MLDv1 等协议

路由协议　支持静态路由、RIP V1/V2、OSPF、BGP，支持策略路由和 VRRP

IPv6 特性　支持 IPv4 和 IPv6 双协议栈

支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+，

支持 IPv4 向 IPv6 的过渡技术，包括：IPv6 手工隧道、6to4 隧道、ISATAP 隧道、GRE 隧道、IPv4 兼容自动配置隧道等

支持基于标准、扩展、VLAN 的 ACL 报文过滤

支持 OSPF、RIPv2 及 BGPv4 报文的明文及 MD5 密文认证

支持 IP 地址、VLAN ID、MAC 地址和端口等多种组合绑定

支持广播风暴抑制，支持主备数据备份机制

支持不间断转发技术 NSR，双引擎快速倒换，实现 50ms 的引擎故障主备切换时间，需提供第三方测试报告

MPLS VPN　　支持 MPLS VPN

支持 MCE/VPN

SNMP V1/V2/V3；RMON 1/2/3/9；Syslog，SSHv2；支持 WEB 网管，支持 MIB-II；中文图形化管理

4.2.11 视频管理控制服务器（公安视频联网网关）

支持管理基础联网平台相关服务，需与上下级联网控制、管理、认证和日志，集群管理，支持 GB/T 28181 设备接入、支持双机热备。通过加载中间件模块，支持选配异构模拟矩阵、异构设备（硬盘录像机、视频服务器、网络摄像机、网络硬盘录像机等）、异构视频监控平台、报警主机、与各类异构资源的接入管理。系统应至少包括以下功能：

系统应能够满足数字方式、网络方式的前端接入。应通过加载视频中间件模块实现用户权限管理、视频流直播、录像、点播、矩阵控制等功能。

系统软件模块应包含基础授权模块、管理配置模块和用户权限模块。

系统应支持分布式系统数据同步，在全局同步协议基础上实现局部数据同步，确保数据一致性。

系统应支持分布式数据安全通信机制，应采用基于非对称加密和签名技术实现数据安全通信。

系统应支持粒度资源权限控制机制，权限控制资源数须达到万级，控制粒度应可细化到单用户对单资源的独立操作。

系统应具备自动连接功能，同时具备高可靠的安全机制。系统客户端应具有良好的操作界面，具有图像窗口、通信连接窗口、控制窗口等辅助界面。

系统应同时具备数字干线和模拟干线管理能力。

系统应按照实用性、兼容性、灵活性、可靠性等要求进行构建。应具有清晰的整体架构，采用组件复用技术，提高软件平台的可维护和可升级能力。

系统应具备较强的扩容性，能随着前端接入点的增加对平台进行硬件和模块的扩容，具备服务器集群管理能力。

系统应能够兼容前端各类图像视频设备，能支持市场主流品牌不少于 80 个（如：大华、海康、SONY、三星、ACTI 等）。实现多种模式的图像采集、压缩、显示、报警联动、控制、远程存储回放、远程管理。支持用户指定任意品牌的前端设备以国标方式接入。

系统应严格按照国标 GB/T 28181-2011 及补充协议的要求。

系统应根据服务的实际负载、系统的网络状况，动态调整接入任务调度和媒体转发路由，具备保持系统压力平稳的能力。

系统应实时监测各服务单元状态，即使在部分服务异常时，在未超出负载限额情况下，仍应能正常响应用户请求。

系统应支持各服务单元故障自动恢复机制，具备多机热备、跨区域灾备的系统能力。

系统应至少支持创建一万个用户的数量，支持移动端拓展应用，并支持至少 300 个用户的同时在线。

系统应支持分布式单点登录机制，应满足用户只需要登录一次就能访问集群系统中任何应用系统。
提供公安部安全防范系统产品质量检测权威报告。
支持各品牌前端接入设备超过 5 万个的公安案例，提供用户证明报告三份。
硬件配置：
标配 1 颗 Intel 至强 E3 1200 系列 CPU；
芯片组：Intel C202，
内存：4G DDR3 1333,支持 ECC，
硬盘：标配 1 块 500G 硬盘，
网络控制器：RJ45(10M/100M/1000M Base-T)*2，
USB：外置 USB 2.0 接口 *4，
串行接口：2 个 RS-232，DB9 接口。
4.2.12 高清转发服务器（流媒体转发节点）
支持前端设备接入、流媒体的转发。将流媒体实时图像转发给上下级联网系统、监控客户端、电视墙服务、视频存储服务等。应至少包括以下功能：
单台流媒体转发节点的码流处理能力应不得低于：
支持同时转发 50 路 8Mbps 码流的 1080P H.264 高清图像；
或支持同时转发 100 路 4Mbps 码流的 720P H.264 高清图像；
在实现如上转发应用时，CPU 占用不应超过 40%，内存占用不应超过 4GB（含视频缓存空间）。
视频直播过程中的图像切换响应时间，应不超过 1 秒；
视频流媒体转发节点冗余热备的主备倒换时间，应不超过 10 秒；
视频流媒体转发节点运行期间，应无内存泄漏、无句柄泄漏；
数字码流转发机制，应实现单源能够分发给单源或多源的路由能力，其网络连接方式应支持单播、组播和 TCP；
数字码流在分发过程中，在保证图像质量的前提下，单节点延迟时间应不超过 100ms；
应采用国标 GB/T 28181-2011 及补充协议的要求，对接其他流应用平台；
应具备较强的扩展能力，支持集群负载均衡，应能实现多台堆叠扩容方式。
提供公安部安全防范系统产品质量检测权威报告。
硬件配置
CPU 标配两颗 E5-2600 系列（6 核，主频 2.4GHz）
内存标配 8GB*4
硬盘标配 1TB SATA（企业级）热插拔 3.5’硬盘，最大支持 4T*8；
网卡板载 2x1000Mb 网卡
电源 550W 冗余电源(动态承载)
4.2.13 视频资源整合网关

在不改变原有外部资源网络规划的前提下对外部资源进行接入，同时解决了不同外部资源私有网段的地址冲突问题，减少了外部资源信息泄漏、接入设备安全性、访问策略等安全隐患，实时监测端口和特定接入设备工作状态，主动上报故障及异常信息。

支持 1 个 10/100/1000Base-TX 上行端口和 1 个用户端口。采用高性能多核处理器，专业的综合业务处理引擎，无风扇低功耗设计。

双向 NAT---解决外部资源私有 IP 地址冲突，隐藏两侧网络架构，无需更改路由配置，提高配置便捷性

访问控制---控制访问方向、灵活限制访问和被访问地址（可按独立 IP 地址或 IP 段设限）

接入协议---支持 Onvif、GB/T28181、第三方 SDK 等协议视频编码设备的接入

报文解析---支持国标、支持报文内容过滤或转换

平台支持---支持东方网力、海康威视、大华、宇视、天地伟业、华为、科达等主流平台或私有平台

规模接入---接入的外部资源 IP 地址数量不受限，支持地址一对一映射

工作模式---独立工作，无需服务器支撑，无缝对接主流视频平台

支持协议：

IEEE802.3、IEEE802.3u、IEEE802.3ab、IEEE802.3z、IEEE 802.3x、IEEE802.1q、IEEE802.1p、IEEE802.1x、IEEE802.1ab

VLAN、PVLAN、Telnet、HTTP、HTTPS、SNMPv1/v2/v3、FTP、ARP

技术性能指标：

高性能多核处理器

1000M 吞吐量，支持同时联网高清视频路数≥100

交换方式：存储转发

支持端口隔离，区分上行端口和用户端口

支持 NAT(IP 地址映射)

路由管理：支持静态路由

支持报文重定向

支持流量监控

支持 Ping

支持不少于 100 路高清并发调用

支持专线、VPN、宽带固定地址

管理与维护：支持 HTTP 加载升级

支持命令行接口（CLI），Console 口进行配置

可视化界面管理

网络安全：

防内网攻击、外网攻击

支持路由遮断

控制访问方向、灵活限制访问和被访问地址

权限管理，提供接入权限认证

接入支持内外网隔离

工作环境及安装：

机架式安装

工作温度：-20～70℃

存储温度：-45～85℃

工作湿度：5%～95%（无冷凝）

其他要求：

应通过国家权威机构的测评认证，取得相关资质证书，并获得公安部计算机信息系统安全专用产品销售许可证。

4.2.14 数据接入网关

用于对接获取小区多种传感数据及文件，进行数据清洗和格式适配，转发进入公安网络。

标配 1 颗 Intel 至强 E3 1200 系列 CPU；

芯片组：Intel C202，

内存：4G DDR3 1333，支持 ECC，

硬盘：1 块 500G 硬盘，

网络控制器：RJ45(10M/100M/1000M Base-T)*2，

USB：外置 USB 2.0 接口 *4，

串行接口：2 个 RS-232，DB9 接口

4.2.15 负载均衡设备

序号	项目	指标项
1	设备厂商资质要求	投标设备必须是现有平台销售产品，并在设备厂商官方网站上能找到对应的投标产品型号和详细技术参数，否则为无效投标
		设备厂商拥有中国政府相关部门颁发的《计算机软件著作权登记证书》
2	硬件及软件系统要求	产品形态需采用独立的硬件专用负载均衡机架式设备，由于空间限制及环保要求，单台设备高度为 1U，
		需采用 Intel Quad 四核 CPU，必须支持超线程技术，需配置独立的控制 CPU，控制 CPU 数量≥2 核

序号	项目	指标项
		需采用高速 ECC 纠错内存技术，系统内存≥8GB
		单台设备数据接口总数≥10 个； 提供千兆接口数量≥8 个，其中提供千兆 SFP 光接口数量≥2 个，若光接口和电接口复用，则只能按照 1 个接口进行计算； 必须同时提供 1/10G 自适应 SFP 光接口数量≥2 个； 必须支持 802.3ad 端口聚合功能，支持静态或 LACP 动态链路聚合协议。 需提供投标设备前后面板照片，显示设备端口的详细配置，如设备为插卡式设备，则必须提供与该项目配置型号和模块一致的机框和模块的面板照片。
		需提供至少 1 个 RS232 串口和 1 个带外管理以太网管理接口，提供独立的带外管理功能；同时，需提供 1 个独立的远程控制管理 LOM(Lights Out Management)模块和接口，通过该接口可实现对设备的远程管理、开机、关机等远程操作。 需根据提供的设备前后面板照片，说明设备管理端口的位置和详细的配置方法。
		存储介质要求： 设备需配置固态 SSD 硬盘，以确保系统镜像和日志等信息得到稳定和可靠的存储，容量≥60GB。
		支持并实际配置可热插拔冗余交流电源，必须能够确保在不停机情况下更换电源模块。需配置通过国际 80 Plus“白金”认证电源。
		支持并实际配置可热插拔冗余智能风扇，风扇模块≥2 个，需根据提供的设备前后面板照片，说明设备可热插拔冗余智能风扇的位置
		需采用专用 64 位操作系统，无明显、已知安全漏洞，过去五年内没有被国家级安全机构通告过相关系统安全漏洞；
3	性能要求	四层最大吞吐量≥10Gbps，需提供工信部相关部门的第三方测试报告，如有 License 限制，必须在报价中包含达到该性能指标的 License 费用。
		七层最大吞吐量≥8Gbps，需提供工信部相关部门的第三方测试报告，如有 License 限制，必须在报价中包含达到该性能指

序号	项目	指标项
		标的 License 费用。
		四层每秒新建连接数（L4CPS）≥400K，需提供工信部相关部门的第三方测试报告
		七层每秒新建连接数（L7CPS）≥150K，需提供工信部相关部门的第三方测试报告
		七层每秒新建请求数（L7 RPS）≥450K
		四层并发连接数≥3000 万,需提供工信部相关部门的第三方测试报告
		DNS 每秒新建请求数（QPS）≥1,500K
		支持并实际配置 SSL 硬件加速功能，提供 SSL 加速性能≥20,000 CPS（1K 密钥长度），最大 SSL 吞吐量≥5Gbps； 如有 License 限制,必须包含达到该性能指标的 License 费用。
		防 DDoS 攻击性能(防止 SYN Flood 攻击)≥400 万 Packet/Sec； 如有 License 限制,必须包含达到该性能指标的 License 费用。
		招标方认为在有必要的前提下，在中标后或签订合同之前，有权利针对以上各项性能指标要求，将投标产品送第三方评测机构对其指定的性能指标进行验证，评测费用由投标方负责。
4	基本功能要求	支持并实际配置多条链路的出向链路负载均衡和智能选路功能；支持基于应用的链路健康检查方式；支持内置地址列表的动态更新；支持静态地址列表匹配，带宽使用分配等等丰富的选路和负载分担算法。 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持并实际配置全局负载均衡功能，能够实现多链路和多站点入向访问的容灾备份部署，同时支持智能的 DNS 解析(需至少支持 A、SOA、MX、NS 记录)及 IP anycast(通过 IP 请求)技术的灾备技术;同时支持 DNS Cache 缓存功能,能够至少缓存 DNSA 和 AAAA 记录。 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持并实际配置防火墙负载均衡功能，能够实现异构防火墙的多活部署，包括透明模式部署的异构防火墙等安全设备；需支

序号	项目	指标项
		持双向流量的源进源出功能，确保防火墙的会话粘连。 以上功能如需 License 激活，则需要在报价中体现相应的 License 的费用。
		支持四至七层的应用服务器负载均衡，至少支持 TCP/ UDP/ HTTP/ HTTPS/ SIP/ SMTP/ FTP/RADIUS 等应用协议的负载均衡功能
		支持以下负载均衡算法： 轮询、最小连接、最小响应时间、加权轮询、加权最小连接、URL-Hashing、无状态（Stateless）、动态比例、最小七层请求数目等算法。
		支持以下服务器健康检查方法： ICMP、TCP、UDP、HTTP、HTTPS、FTP、SNMP、WMI、MSSQL 等多种主动式服务器健康检查方法； 支持基于脚本的健康检查方法。即：用户可自定义灵活的健康检查方式和检查内容，根据不同需求自行编制脚本； 支持基于模仿用户实际访问的复杂检查方法。即：可通过设置，模拟一个用户从登录，访问应用，退出等流程准确校验一个用户应用交易的整个过程。
		支持以下会话保持方法： 支持基于源地址、目的地址、Cookie、header、URL、SSL Session ID、用户自定义脚本等多种会话保持方式。
		支持并实际配置静态路由、RIPng、BGP4+、OSPF v2/v3、IS-IS v4/v6 等路由协议的。支持 BFD 快速故障检测机制，支持 BFD 与各种路由协议之间的联动配置。 以上功能如需 License 激活，则需要体现相应的 License 的费用。
5	应用加速和优化功能要求	支持并实际配置基于七层协议的应用交换和 TCP 协议优化功能，包括：TCP 连接复用、Cookie 会话保持、HTTP 压缩、URL 重写、HTTP 头部插入/修改/删除等功能。 以上功能如需 License 激活，则需要体现相应的 License 的费用。

序号	项目	指标项
		支持并实际配置 HTTP 缓存功能，可以将用户访问的热点静/动态内容缓存在设备系统内存中，以减轻 Web 服务器端负载，提高系统的响应速度，内容缓存容量≥2GB 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持并实际配置 DNS 缓存功能，可以将用户查询过的 DNS 域名缓存在内存中，以减轻 DNS 服务器端递归查询的压力，防范恶意攻击，DNS 缓存条目数≥50 万 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持使用工业标准的 GZIP 和 Deflate 压缩算法来压缩 HTTP 流量，降低带宽消耗、缩短最终用户在慢速/低带宽连接条件下的下载时间。 如需 License 激活，则需要体现相应的 License 的费用。
6	应用安全功能要求	需支持基于终端策略限制功能，提供静态/动态更新的黑白名单，限制恶意攻击源；可根据不同要求，针对不同的用户设定多种请求限制，包括每用户四层新建会话数，七层新建会话数，七层新建 HTTP 请求数、总并发数等，并可以在设备全局和每个对外提供的应用端口分别设置实现。
		支持并实际配置 WEB 应用防火墙（WAF）功能，能够对常见的 SQL 注入、跨站脚本攻击、跨站请求伪造等常见的 HTTP 攻击进行阻隔和防护。 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持并实际配置 DNS 应用防火墙（DAF）功能，支持 DNS 协议合规性判断、过滤目标端口 53 UDP 的恶意攻击，能够对常见的 DNS 攻击类型进行阻隔和防护，可根据域名定制不同安全防护策略。 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持应用访问管理（App Access Management）功能，实现对不同应用提供统一的认证访问管理，需至少支持 Logon

序号	项目	指标项
		Portal，OCSP,认证代理以及 AAA 服务器认证方式。 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持敏感信息防护功能，可将服务器端返回的敏感信息，如版本号，应用软件类型、名称等内容进行隐藏或修改后回传到访问端，避免黑客收集服务器的敏感信息。 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持基于用户自定义脚本的安全防护功能，实现灵活和安全的流量过滤和访问过滤策略
		支持灵活的、可定制的地址翻译（NAT）技术，适合各种复杂的网络环境，全面支持 IPv4 和 IPv6，支持 IPv4-IPv4、IPv4-IPv6、IPv6-IPv6、IPv6-IPv4 网关功能
7	应用灵活性和设备虚拟化要求	可编程控制负载均衡及流量处理功能： 提供基于某种编程语言（如 TCL 语言）的可自定义的流量分担和控制方法，可通过自编程方式实现灵活的流量处理需求。支持基于应用内容的强制转发、请求应答内容改写、条件 NAT、路由转发、会话保持、DNS 改写等功能的可编程控制。 必须满足 Oracle Weblogic 应用服务器集群的深层次应用处理与优化、健康检查和集群系统的会话保持； 必须提供设备基于 Weblogic 应用服务器集群的 JSESSIONID 会话保持脚本，以及相关的开发手册说明能够实现的具体功能。
		设备需具备二次开发能力，提供 API/SDK 开发接口，能够通过该 API 接口，实现与第三方管理平台进行无缝整合，实现第三方管理平台对该设备的自动化管理、运行状态监控等功能。 该 API 接口必须能够以下功能的封装：网络接口状态获取和配置，HA 状态获取和配置，服务器状态获取和配置，系统运行状态获取和配置等。所有功能配置都必须能够通过 API 调用的方式实现。
		支持将一台物理设备虚拟为多台设备使用，需支持并实际配置至少 30 个虚拟设备，对于不同实例中的应用部署，必须支持以下功能实现：

序号	项目	指标项
		支持相同 IP 地址的服务器在不同实例的复用。即：相同 IP 地址可配置于不同的实例； 每个实例可限制其资源使用，至少可对以下内容进行限制：并发会话、L4 新建连接数、吞吐量等； 每个实例可单独定义 ARP、路由、负载均衡等配置，每个实例的配置信息和管理互相独立； 以上功能如需 License 激活，则需要体现相应的 License 的费用。
		支持多台设备虚拟成为一台设备使用，支持至少 8 台设备的集群部署，提供统一的管理界面，设备配置和软件版本自动同步，任何一台设备出现故障不影响业务和其他设备的正常使用，并能够提升整体业务处理能力和设备性能。
		同时支持 VxLAN 和 NVGRE 两种封装模式和功能
		能够提供和硬件平台功能一样的虚拟机版本（同时支持 vmware，hyper-v，Xen）做为测试使用，虚拟机版本有效期不少于 30 天。 需根据招标方要求，提供指定虚拟化平台的软件包备案。
8	设备管理和冗余功能要求	提供基于 SSL 加密的系统管理功能，提供基于 SSH 的命令行方式和基于 HTTPS 的中文图形化管理方式。
		无需额外安装客户端软件或插件，就可以利用 Web 浏览器查看设备的实时流量及系统开销统计图表，如：CPU 利用率、流量信息、用户访问量信息等。可以看到 1 个月以内的相关图表信息。同时自带日志报警和输出功能。
		超级管理员可以根据业务、应用的拥有者或者其它分类来设计定制监控和配置管理权限。如：对应用类型 A，在管理域 A 内，管理域 A 内的管理员被分为超级用户，只读用户等。在该管理域的管理员，无权修改其它管理域的的配置。
		设备自身提供实时的抓包工具，即可远程登录设备，运行其自身提供的类似 tcpdump 的实时抓包工具，可以对通过自身设备的数据包进行过滤并抓包分析。必须能够实时显示抓包信息。抓包结果可以导出为标准的文件格式，并可以用通用的分析工具，如 Sniffer, WireShark 等工具打开。

序号	项目	指标项
		设备可与第三方厂商（如 Microsoft、VMwrae 等）的虚拟化平台高度集成，当发现已做负载均衡的虚拟机组性能不足时，负载均衡设备能够自动调度一台或更多的空闲虚拟机加入到原有的组里，当发现虚拟机组性能过剩时则删减相应的资源，实现虚拟机资源的灵活运用，自动实现虚拟机资源的灵活、合理使用。
		支持串联（In-line）和单臂（One-Armed）、服务器直接返回 DSR 方式。
		支持主备设备之间的双机会话同步功能。即实现主备设备 HA 切换时，确保已经建立的 TCP/UDP 会话不丢失。支持基于每个 VIP 单独配置会话同步功能。 如：对 VIP1 启用会话同步功能，而对于 VIP2 则不不启用。对于启用会话同步功能的 VIP，在主备设备切换时，用户会话不丢失。
		支持 Active-Active、Active-Standby 等 HA 部署方式，支持通过网络的心跳检测机制
9	其他要求	要求三年原厂软件升级，故障修复，技术支持等服务，需提供原厂出具的服务承诺函。
		所有软件功能必须在同一台物理设备上实现，以上功能模块如果需要收费，全部需要在设备报价里体现；如果免费，需要提供加盖公章的原厂证明函。

4.2.16 入侵防御服务器

总控中心

功能指标项	功能描述
系统管理	提供管理友好的中文 Web 图形界面配置，支持 Telnet、SSH、串口登陆命令行模式配置。 支持配置管理 IP 控制列表、SNMP 网管协议以及邮件报警。
	支持通过 web 方式调用设备命令行窗口功能，无需登录串口就可对设备进行命令行操作。
接口规格要求	6 个 10/100/1000Base-T 端口；2 个千兆 SFP 光口插槽

机箱电源要求	2U 机箱，冗余电源
IPS 吞吐	1.2Gbps
液晶屏幕	具备液晶显示屏，提供面板照片证明
网络适应性	支持透明、路由、混合多种工作模式。
	支持静态、策略路由、OSPF、BGP4 等动态路由。
	支持端口聚合。
	支持 ALG 应用协议的 NAT 应用和端口重定向，包括 SIP、H.323、XDMCP 等，并支持自定义协议。
安全防护	内置 4000 种以上的攻击，能够检测包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等攻击。
	支持 AV 病毒检测引擎，内置病毒特征不少于 10 万条。
	支持 4 种安全防护模式，基于网络、用户、应用以及云租户。
	支持租户独立的配置和租户间视图的切换。
	支持以多种方式定义租户，如：VLAN、NVGRE、VXLAN。
	支持基于租户的 NAT、IP 地址配置、IP_MAC 绑定、病毒过滤和防挂马、入侵防护、攻击防护、应用识别、文件控制、ARP 防护、内容安全特性（邮件、网页的内容过滤）、策略/静态/多出口路由。
	支持基于租户的安全策略、地址对象/地址组/地址池/权重地址、自定义服务对象/服务组、时间对象/时间组以及 ALG 中常用协议（包括 FTP、TFTP、H323、TNS、MMS、PPTP、XDMCP、SIP 等）隔离。
智能流量控制	支持基于优化的高速流匹配技术，以多种依据（源 IP/目的 IP/IP 范围/源端口/目的端口/端口范围/接口/用户组/安全策略区域对象/应用协议等）对流量进行控制。
用户认证	支持本地认证、Radius 认证、Tacacs+认证、CA 认证、LDAP/AD 认证。
应用管控	内置 URL 分类库，具有不少于 1 万条 URL 地址库。 可对 URL 地址以及域名进行过滤，且支持黑名单和白名单。
	内置 1700 多种应用特征库，可准确识别各种 IM、P2P、网络游戏、流媒体、股票等应用，并可自定义。
	支持基于安卓开发的多种聊天软件和社交软件，如，QQ、微信、新浪微博、YY 语音、糗粑、网易新闻等。
	内容过滤规则可精确到单个用户和每个 IP。

	Web 关键字过滤功能，支持 HTTP1.0 和 HTTP1.1 协议，支持多种编码协议如 UTF8、GB2312 和 BIG5。 可对通过 gzip 或 deflate 的算法压缩的 web 页面进行动态自动解压缩
应用安全防护	内嵌深度包检测引擎，针对数据包进行深度过滤检测。
	可以阻断内部用户访问非法的网址或访问含有非法内容的网页 支持自定义 URL 过滤策略、关键字过滤策略、蠕虫过滤策略 支持攻击邮件告警。
	可以针对 FTP 传输的文件类型（如 mp3、avi…）进行过滤。 支持通过预定义过滤文件名实现对 FTP 数据流的区分控制。
负载均衡	支持基于多种方式划分的负载均衡，如按照服务器、链路、全局等不同方面划分。
	支持服务器、链路、全局负载均衡的健康探测功能。
	支持通过端口号进行负载均衡。 支持通过传输层协议类型进行负载均衡。 支持 8 种调度算法（轮询调度、加权轮询调度、源地址散列调度、目标地址散列调度、最小连接调度、加权最小连接调度、基于局部性的最小连接调度和带复制的基于局部性的最小连接调度）。
	支持根据监测到的链路状态自动备份和出口链路选择，可根据链路探测结果自动进行链路切换。
集群部署	支持 3 台以上设备集群部署，最多可支持 200 台。
	支持设备可自动加入集群，和动态退出集群，在中心设备上能对指定的设备或所有成员设备下发配置。
	管理中心能监控所有成员的状态。
高可靠性	支持主备模式(A/S)、主主模式(A/A)等多种热备方式。
	支持不少于 4 个节点，使用虚拟 IP 地址技术，通过 VRRP 协议实现集群负载均衡。
	能够进行线路/IP 状态检测，并根据检测结果自动切换。
	支持多个心跳口的冗余备份。
	支持将任意物理接口设置为 HA 接口。
	支持电口硬件 Bypass,保证设备在断电或宕机的情况下，不会引起网络中断；
	支持配置同步、session 同步。
安全审计	支持将日志存储在本地，标配不少于 500G 日志存储硬盘。

	支持全部日志按天和统一格式存储，可以通过 web 页面查看历史日志列表，且可以针对列表日志进行删除、导出等操作。
	支持历史日志，保证设备掉电后仍然可以保留上次运行的日志记录。
安全可视	产品可以图形化显示设备接口面板信息，直观查看接口是否联线。
	产品界面可以显示设备当前的系统状况，包括 cpu 使用率、内存使用率、cpu 温度等。
	设备可以图形化展示应用风险指数、网络风险指数便于用户整体了解网络风险等级。
	支持在线帮助说明，每个功能页面都提供当前页面的功能说明。
	可高速分析与统计 2 至 7 层网络流量。
	实时图表显示用户连接数、当前会话数、应用使用排名等信息。
	提供多种统计方式，如基于用户、应用、接口、安全策略等因素进行统计显示。
	提供多种报表，可依据五元组、应用协议、时间点/时间段等元素自定义报表内容并显示。
	可对接口流量/应用/协议的异常状态进行告警，并以 Email/SNMP Trap/声音等方式通知管理员。
服务及其它要求	所提供的产品没有用户数许可限制。
特征库的升级	厂商提供对特征库的升级更新，频率不低于每周一次；
	支持设备在线、离线升级特征库；
产品资质	公安部销售许可证（国标三级） 软件著作权登记证书 国际 CVE 兼容检测资质证书 获得 IPV6 Ready 金牌认证
厂商资质	风险评估服务资质（二级） 应急处理服务资质（二级） 国家信息安全测评信息安全服务资质（安全开发类二级） 国家信息安全测评信息安全服务资质（安全工程类二级） 信息系统安全集成服务资质（二级） 计算机系统集成资质（二级） 具备 CNCERT/CC 颁发的网络安全应急服务支撑单位证书 具备公安部颁发的信息安全等级保护安全建设服务机构能力评估合格证书

分控中心

功能指标项	功能描述
系统管理	提供管理友好的中文 Web 图形界面配置，支持 Telnet、SSH、串口登陆命令行模式配置。 支持配置管理 IP 控制列表、SNMP 网管协议以及邮件报警。
	支持通过 web 方式调用设备命令行窗口功能，无需登录串口就可对设备进行命令行操作。
接口规格要求	6 个 10/100/1000Base-T 端口；2 个千兆 SFP 光口插槽
机箱电源要求	1U 机箱，单电源
IPS 吞吐	200Mbps
液晶屏幕	具备液晶显示屏，提供面板照片证明
网络适应性	支持透明、路由、混合多种工作模式。
	支持静态、策略路由、OSPF、BGP4 等动态路由。
	支持端口聚合。
	支持 ALG 应用协议的 NAT 应用和端口重定向，包括 SIP、H.323、XDMCP 等，并支持自定义协议。
安全防护	内置 4000 种以上的攻击特征，能够检测包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等攻击。
	支持 AV 病毒检测引擎，内置病毒特征不少于 10 万条。
	支持 4 种安全防护模式，基于网络、用户、应用以及云租户。
	支持租户独立的配置和租户间视图的切换。
	支持以多种方式定义租户，如：VLAN、NVGRE、VXLAN。
	支持基于租户的 NAT、IP 地址配置、IP_MAC 绑定、病毒过滤和防挂马、入侵防护、攻击防护、应用识别、文件控制、ARP 防护、内容安全特性（邮件、网页的内容过滤）、策略/静态/多出口路由。
	支持基于租户的安全策略、地址对象/地址组/地址池/权重地址、自定义服务对象/服务组、时间对象/时间组以及 ALG 中常用协议（包括 FTP、TFTP、H323、TNS、MMS、PPTP、XDMCP、SIP 等）隔离。
智能流量控制	支持基于优化的高速流匹配技术，以多种依据（源 IP/目的 IP/IP 范围/源端口/目的端口/端口范围/接口/用户组/安全策略区域对象/应用协议等）对流

	量进行控制。
用户认证	支持本地认证、Radius 认证、Tacacs+认证、CA 认证、LDAP/AD 认证。
应用管控	内置 URL 分类库，具有不少于 1 万条 URL 地址库。 可对 URL 地址以及域名进行过滤，且支持黑名单和白名单。
	内置 1700 多种应用特征库，可准确识别各种 IM、P2P、网络游戏、流媒体、股票等应用，并可自定义。
	支持基于安卓开发的多种聊天软件和社交软件，如，QQ、微信、新浪微博、YY 语音、糗粑、网易新闻等。
	内容过滤规则可精确到单个用户和每个 IP。
	Web 关键字过滤功能，支持 HTTP1.0 和 HTTP1.1 协议，支持多种编码协议如 UTF8、GB2312 和 BIG5。 可对通过 gzip 或 deflate 的算法压缩的 web 页面进行动态自动解压缩
应用安全防护	内嵌深度包检测引擎，针对数据包进行深度过滤检测。
	可以阻断内部用户访问非法的网址或访问含有非法内容的网页 支持自定义 URL 过滤策略、关键字过滤策略、蠕虫过滤策略 支持攻击邮件告警。
	可以针对 FTP 传输的文件类型（如 mp3、avi…）进行过滤。 支持通过预定义过滤文件名实现对 FTP 数据流的区分控制。
负载均衡	支持基于多种方式划分的负载均衡，如按照服务器、链路、全局等不同方面划分。
	支持服务器、链路、全局负载均衡的健康探测功能。
	支持通过端口号进行负载均衡。 支持通过传输层协议类型进行负载均衡。 支持 8 种调度算法（轮询调度、加权轮询调度、源地址散列调度、目标地址散列调度、最小连接调度、加权最小连接调度、基于局部性的最小连接调度和带复制的基于局部性的最小连接调度）。
	支持根据监测到的链路状态自动备份和出口链路选择，可根据链路探测结果自动进行链路切换。
集群部署	支持 3 台以上设备集群部署，最多可支持 200 台。
	支持设备可自动加入集群，和动态退出集群，在中心设备上能对指定的设备或所有成员设备下发配置。

	管理中心能监控所有成员的状态。
高可靠性	支持主备模式(A/S)、主主模式(A/A)等多种热备方式。
	支持不少于 4 个节点，使用虚拟 IP 地址技术，通过 VRRP 协议实现集群负载均衡。
	能够进行线路/IP 状态检测，并根据检测结果自动切换。
	支持多个心跳口的冗余备份。
	支持将任意物理接口设置为 HA 接口。
	支持电口硬件 Bypass,保证设备在断电或宕机的情况下，不会引起网络中断；
	支持配置同步、session 同步。
安全审计	支持将日志存储在本地，标配不少于 500G 日志存储硬盘。
	支持全部日志按天和统一格式存储，可以通过 web 页面查看历史日志列表，且可以针对列表日志进行删除、导出等操作。
	支持历史日志，保证设备掉电后仍然可以保留上次运行的日志记录。
安全可视	产品可以图形化显示设备接口面板信息，直观查看接口是否联线。
	产品界面可以显示设备当前的系统状况，包括 cpu 使用率、内存使用率、cpu 温度等。
	设备可以图形化展示应用风险指数、网络风险指数便于用户整体了解网络风险等级。
	支持在线帮助说明
	可高速分析与统计 2 至 7 层网络流量。
	实时图表显示用户连接数、当前会话数、应用使用排名等信息。
	提供多种统计方式，如基于用户、应用、接口、安全策略等因素进行统计显示。
	提供多种报表，可依据五元组、应用协议、时间点/时间段等元素自定义报表内容并显示。
	可对接口流量/应用/协议的异常状态进行告警，并以 Email/SNMP Trap/声音等方式通知管理员。
服务及其它要求	所提供的产品没有用户数许可限制。
特征库的升级	厂商提供对特征库的升级更新，频率不低于每周一次；
	支持设备在线、离线升级特征库；
产品资质	公安部销售许可证（国标三级）

	软件著作权登记证书 国际 CVE 兼容检测资质证书 获得 IPV6 Ready 金牌认证
厂商资质	风险评估服务资质（二级） 应急处理服务资质（二级） 国家信息安全测评信息安全服务资质（安全开发类二级） 国家信息安全测评信息安全服务资质（安全工程类二级） 信息系统安全集成服务资质（二级） 计算机系统集成资质（二级） 具备 CNCERT/CC 颁发的网络安全应急服务支撑单位证书 具备公安部颁发的信息安全等级保护安全建设服务机构能力评估合格证书

虚拟化防病毒软件（每颗 CPU 一套）

序号	**具体要求**
1.	支持主流虚拟化系统 VMware(ESXi 5.5/6.0/6.5)等版本
2.	软件独立自主可控，完全与 Hypervior 层解耦，不受制于 Hypervior API 影响
3.	可以针对 Windows、Linux、Unix 等广泛平台的虚拟机系统进行病毒扫描和防护
4.	支持 Vmotion 监管，虚拟机热迁移时病毒防护策略自动适应，防护能力不变
5.	安装在虚拟环境中并对虚拟环境中的所有 Guest OS 提供保护
6.	可以有效防止虚机的病毒风暴导致的网络瘫痪、对于病毒样本进行查杀与隔离
7.	支持在现有业务环境上，进行系统部署安装，对业务不造成影响且会话不中断
8.	需要采用先进的、不断更新的病毒库，病毒库不少于 400 万条，支持手动和在线自动升级方式
9.	支持基于状态、精准的高性能攻击检测和防御，支持实时病毒攻击源阻断、IP 屏蔽、攻击事件记录；
10.	针对虚拟系统，通过无代理病毒防护功能，实现针对虚拟系统和虚拟主机之间的全面防护，减少消耗分配给虚拟主机的计算资源，最大化利用计算资源的同时提供全面病毒的实时防护。
11.	支持代理模式和数据流模式两种病毒扫描方式
12.	支持病毒处理动作设置、扫描文件大小设置
13.	支持基于 SMTP、PoP3、SMTP 等协议代理的病毒扫描
14.	协议查毒：支持 ftp、http、smtp、pop3、imap 等协议病毒扫描
15.	支持自定义非标准端口下应用协议的病毒防护，如 qq 特征。
16.	支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病

	毒的阻断隔离
17.	支持所有常见文件格式的病毒查杀，可自定义文件阈值大小、类型
18.	支持新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒
19.	支持对病毒文件指定隔离位置、隔离导出、隔离删除和隔离内容查看
20.	支持病毒样本信息统计及病毒感染事件的可视化界面呈现
21.	支持收集和分析虚拟化环境中虚拟机感染威胁的安全事件
22.	支持设置日志服务器，将病毒等日志发送到网络中统一的日志服务器上，进行统一收集、管理
23.	支持病毒攻击证据提取，可基于五元组、协议、时间对象等自定义抓包任务，抓取指定接口、指定数量的报文，并可以在 web 上面批量导出、批量删除
24.	可以通过 web 页面查看历史日志列表，且可以针对列表日志进行删除、导出等操作

4.2.17 边界防火墙

总控中心

项目	指标	具体要求
硬件规格	多核 AMP+架构，网络处理能力为 14G，并发连接≥300 万，每秒新建连接 22 万/秒，标准 2U 机箱，冗余电源，标准配置 6 个 10/100/1000M 自适应电口，4 个 SFP 插槽，支持两个扩展槽，最大支持 22 个接口，1 个 Console 口，支持液晶屏；报价中包括三年硬件维修服务.配置 2 个万兆光口插槽。	
基础组网	部署模式	产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式；
	地址转换	支持全面的 NAT 转换配置，包括包括一对一，一对多，多对一的源、目的地址转换，并至少支持 FULL_CONE 和 SYMMETRIC 模式
		可对源地址为 IPv6 地址、目的地址为 IPv4 地址的会话执行源地址转换，将 IPv6 地址转换为 IPv4 地址，实现 IPv6 客户端转换为 IPv4 地址后访问 IPv4 资源；
		可对源地址为 IPv4 地址、目的地址为 IPv4 地址的会话执行目的地址转换，将 IPv4 地址转换为 IPv6 地址。实现 IPv4 客户端通过 IPv4 地址访问 IPv6 资源
		可对源地址为 IPv4 地址、目的地址为 IPv4 地址的会话执行目的地址转换，将 IPv4 地址转换为服务器地址，并支持服务器地址探测
	高可靠性	支持 HA 高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步

访问控制	访问控制	支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。要求设备可基于地理区域配置安全策略，并支持地理区域对象的导入。
	应用识别与控制	可实现应用控制，应用特征库包含的应用数量（非应用协议的规则总数）大于 2400 种
	URL 过滤	支持 URL 云服务，设备可与云服务器联动查找本地未识别的 URL
攻击防护	网络攻击防护	支持防御 DNS Flood 攻击，并支持警告、阻断、普通防护、增强防护及授权服务器防护等多种防护措施
		支持防御 HTTP Flood 攻击，并支持警告、丢弃、普通防护、增强防护等多种防护措施
	病毒防护	能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀
		支持对最多 6 级的压缩文件进行解压查杀
		支持自定义病毒签名，可将病毒文件 MD5 值定义为特征签名
		支持设置例外特征，对特定的病毒特征不进行查杀
		支持本地、云端病毒查杀，本地病毒特征库规模大于 3500 万
	入侵防御	支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMTP 等应用协议的漏洞防护和间谍软件防护。可防护的漏洞类型应至少包括：缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等。可防护的间谍软件类型应至少包括：木马后门、病毒蠕虫、僵尸网络等
安全管理	网络异常感知	支持统计网络中确认失陷的主机及有风险但不能完全确认为失陷的主机数量及风险等级状态，并支持查看失陷时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息，并支持一键跳转处置。
	安全事件分析	所投设备需提供关联分析面板，可将 Top 应用、Top 威胁、Top URL 分类、Top 源地址、Top 目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取
		可提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL 过滤、文件过滤等安全模块检查的日志集中显示
协同防御	云端协同	支持与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱、情报云检测等功能。
	威胁感知系统联动	可与方案中配置的网络威胁感知系统联动，将本地终端产生的异常行为、攻击活动等数据上报至网络威胁感知系统，网络威胁感知系统可实时监控网络内的攻击事件并预警可疑的受感染主机，同时支持接收来自网络威胁感知系统推送的情报信息。

	终端安全软件联动	支持与桌面杀毒或终端管理软件联动，增强防火墙对应用特征及木马特征的识别能力。
厂商及产品资质	产品资质	公安部计算机信息系统安全专业产品销售许可证（3 级）； 国家信息安全认证产品型号证书 EAL3+； 中国国家信息安全产品认证证书三级 涉密信息系统产品检测证书 多核并行操作系统软件著作权登记证书； 高性能 IPv6 防火墙系统计算机软件著作权登记证书 高性能一体化智能安全处理引擎计算机软件著作权登记证书 IPv6 Ready 金牌认证资质
	厂商资质	风险评估服务资质（二级） 应急处理服务资质（二级） 计算机系统集成资质（二级） 国家信息安全测评信息安全服务资质（安全开发类二级） 国家信息安全测评信息安全服务资质（安全工程类二级） 信息系统安全集成服务资质（二级） 中国通信企业协会通信网络安全服务能力评定证书（安全设计与集成乙级） 中国通信企业协会通信网络安全服务能力评定证书（风险评估乙级）

分控中心

项目	**指标**	**具体要求**
硬件规格	多核 AMP+架构，网络处理能力为 10G，并发连接≥260 万，每秒新建连接 18 万/秒，标准 2U 机箱，冗余电源，标准配置 6 个 10/100/1000M 自适应电口，4 个 SFP 插槽，支持两个扩展槽，最大支持 22 个接口，1 个 Console 口，支持液晶屏；报价中包括三年硬件维修服务.配置 2 个万兆光口插槽	
基础组网	部署模式	产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式；
	地址转换	支持全面的 NAT 转换配置，包括包括一对一，一对多，多对一的源、目的地址转换，并至少支持 FULL_CONE 和 SYMMETRIC 模式
		可对源地址为 IPv6 地址、目的地址为 IPv4 地址的会话执行源地址转换，将 IPv6 地址转换为 IPv4 地址，实现 IPv6 客户端转换为 IPv4 地址后访问 IPv4 资源；
		可对源地址为 IPv4 地址、目的地址为 IPv4 地址的会话执行目的地址转换，将 IPv4 地址转换为 IPv6 地址。实现 IPv4 客户端通过 IPv4 地址访问 IPv6 资

		源
		可对源地址为 IPv4 地址、目的地址为 IPv4 地址的会话执行目的地址转换，将 IPv4 地址转换为服务器地址，并支持服务器地址探测
	高可靠性	支持 HA 高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步
访问控制	访问控制	支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。要求设备可基于地理区域配置安全策略，并支持地理区域对象的导入。
	应用识别与控制	可实现应用控制，应用特征库包含的应用数量（非应用协议的规则总数）大于 2400 种
	URL 过滤	支持 URL 云服务，设备可与云服务器联动查找本地未识别的 URL
攻击防护	网络攻击防护	支持防御 DNS Flood 攻击，并支持警告、阻断、普通防护、增强防护及授权服务器防护等多种防护措施
		支持防御 HTTP Flood 攻击，并支持警告、丢弃、普通防护、增强防护等多种防护措施
	病毒防护	能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀
		支持对最多 6 级的压缩文件进行解压查杀
		支持自定义病毒签名，可将病毒文件 MD5 值定义为特征签名
		支持设置例外特征，对特定的病毒特征不进行查杀
		支持本地、云端病毒查杀，本地病毒特征库规模大于 3500 万
	入侵防御	支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMTP 等应用协议的漏洞防护和间谍软件防护。可防护的漏洞类型应至少包括：缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等。可防护的间谍软件类型应至少包括：木马后门、病毒蠕虫、僵尸网络等
安全管理	网络异常感知	支持统计网络中确认失陷的主机及有风险但不能完全确认为失陷的主机数量及风险等级状态，并支持查看失陷时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息，并支持一键跳转处置。
	安全事件分析	所投设备需提供关联分析面板，可将 Top 应用、Top 威胁、Top URL 分类、Top 源地址、Top 目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取
		可提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL 过滤、文件过滤等安全模块检查的日志集中显示
防　同	云端协同	支持与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱、情报

		云检测等功能。
	威胁感知系统联动	可与方案中配置的网络威胁感知系统联动，将本地终端产生的异常行为、攻击活动等数据上报至网络威胁感知系统，网络威胁感知系统可实时监控网络内的攻击事件并预警可疑的受感染主机，同时支持接收来自网络威胁感知系统推送的情报信息。
	终端安全软件联动	支持与桌面杀毒或终端管理软件联动，增强防火墙对应用特征及木马特征的识别能力。
厂商及产品资质	产品资质	公安部计算机信息系统安全专业产品销售许可证（3 级）； 国家信息安全认证产品型号证书 EAL3+； 中国国家信息安全产品认证证书三级 涉密信息系统产品检测证书 多核并行操作系统软件著作权登记证书； 高性能 IPv6 防火墙系统计算机软件著作权登记证书 高性能一体化智能安全处理引擎计算机软件著作权登记证书 IPv6 Ready 金牌认证资质
	厂商资质	风险评估服务资质（二级） 应急处理服务资质（二级） 计算机系统集成资质（二级） 国家信息安全测评信息安全服务资质（安全开发类二级） 国家信息安全测评信息安全服务资质（安全工程类二级） 信息系统安全集成服务资质（二级） 中国通信企业协会通信网络安全服务能力评定证书（安全设计与集成乙级） 中国通信企业协会通信网络安全服务能力评定证书（风险评估乙级）

4.2.18 防篡改管理平台

功能	指标项	规格参数
系统配置	**软件规格**	网页防篡改管理平台软件版，提供原厂服务
网站恢复	**网页防篡改系统**	网页防篡改系统综合支持 Windows、linux、AIX 系统网站防篡改
		网页防篡改客户端在卸载时，需要有验证才可以卸载，保证客户端自身安全性
		支持对网页防篡改客户端和的自动探测功能
		采用基于文件过滤驱动保护技术、事件触发机制相结合方式
		支持文件多线程同步，并可以设置文件同步时间周期、发布时间周期等时间设置

		异地备份，两台服务器之间文件同步时，需要使用专用端口进行加密传输
		支持 IIS、Weblogic、Websphere、Apache、Tomcat 等
		应支持支持超过 40GB 以上网页防篡改保护和恢复功能，以适应客户业务发展需要
		支持内核控制、本地备份、异地备份多种安全网页防篡改组合模式
		系统可以从本地或异地备份文件夹自动同步到监测目录中
		系统支持主/备目录和主/备服务器两种备份模式
		提供网页防篡改的发布模式，能和主流的 CMS 系统集成进行内容发布，提供 32、64 位系统集成
		支持对网站服务器的 CPU、内存、收包量、发包量等信息进行实施监控
日志系统	**备份日志**	支持对日志进行手工备份、自动备份、恢复等功能
	系统审计	对与系统自身安全相关的下列事件产生审计记录：管理员登陆后进行的操作行为；对安全策略进行添加、修改、删除等操作行为；对管理角色进行增加、删除和属性修改等操作行为；对其他配置参数的设置或更新等行为
		支持对网页篡改、添加、删除进行日志记录，并针对文件、进程、攻击类型进行详细记录
告警系统	**多种告警方式**	支持 syslog、SNMP 协议、邮件等多种告警方式、短信报警
部署能力	**系统支持**	监控平台支持 windows 版本系统平台安装
	部署方式	旁路部署方式，支持监控平台和客户端进行正常通信即可
集中监控	**集中管理**	防篡改监控平台支持对统一监管平台进行远程管理、策略下发和日志收集
系统管理	**系统管理**	支持分级分权管理，支持 License 控制。
		支持基于 WEB 的 CLI 管理，方便调试
	系统诊断	支持远程技术支持信息提取
		支持 ping,tcpdump,ifconfig,urltest 等调试方式
设备自身安全性	**设备网络管理**	采用 HTTPS，支持中英文多语言管理
	系统保护机制	支持双系统，支持系统回滚，避免单一系统故障而影响正常业务
资质	**产品资质**	公安部销售许可证 多核多平台并行安全操作系统计算机软件著作权登记证书

		中国国家信息安全产品认证证书（增强级） 涉密产品检测证书
	厂商资质	风险评估服务资质（二级） 应急处理服务资质（二级） 计算机系统集成资质（二级） 国家信息安全测评信息安全服务资质（安全开发类二级） 国家信息安全测评信息安全服务资质（安全工程类二级） 信息系统安全集成服务资质（二级）

4.2.19 4A 安全管控平台

类别	指标项	技术要求
形态	产品形态	硬件形态，规格：6 个千兆电口，1TB 硬盘，1U 机箱，单电源。软件采用 B/S 架构。符合公安部“安全管理平台类”产品的检测规范(提供相关证明)。其中，管理中心内嵌数据库，用户无需另外安装数据库管理系统；管理客户端基于浏览器，无需安装其他客户端软件。
功能	管理范围	能够集中监控网络中的主机设备、网络设备、安全设备。具体包括：交换机、路由器、负载均衡设备、防火墙、IDS、IPS、Windows 服务器、AIX 服务器、Linux 服务器、HP-UX 服务器、Solaris 服务器等。
	资产管理	可对网络中的 IP 资产进行管理，支持以安全域的方式对资产进行分组，资产的属性包括安全 CIA 指标，支持自定义资产属性，可根据需要对资产属性进行任意扩展。
	综合拓扑管理	支持网络拓扑发现，自动生成网络拓扑图，支持分层显示和全局显示两种展现方式。在全局显示模式下，能够在一个拓扑图上显示三层、二层网络设备和终端设备。拓扑图上能够显示节点之间的链路连接，并标示流量值。如果节点出现故障，可通过颜色变化直观显示。支持对拓扑图的鸟瞰、缩放、导出、导入、更换底图、编辑。内置 ping、tracerouter、telnet、rdp 等常用工具，可直接调用。通过拓扑地图，用户可以调用设备的 http 接口、telnet 接口、ssh/ssh2 接口实现对设备的直接访问和控制。
	机房物理视图管理	支持机房和机架物理拓扑显示，用户可以直观地看到每个机架上的每台设备的运行状态，出现问题就会闪烁告警。用户点击机架上的每个设备，可以进入这个设备的明细监控界面。支持拓扑图和机架视图中的设备的双向定位。
	设备面板图	用户可以看到设备的面板图，并可以针对面板上的接口进行实时监控和设置，进行形象化管理。

	智能监控频道	智能监控频道为用户提供了一个从总体上把握网络中各种 IT 资源整体运行情况的界面。通过智能监控频道，用户可以快速导航到系统的各个功能界面，可以看到当前企业和组织的整体健康等级。 用户可以自定义频道，每个频道都能够自由组织视图，包括视图的布局和显示的内容。监控频道中的每个窗口都能够移动、放大、缩小，窗口中显示的统计和摘要信息都能够点击、下钻、查看明细。监控频道能够最大化显示，作为运维中心的主控界面，在大屏幕上呈现出来
	主机监控	能对包括服务器和 HP、IBM 小型机在内的各种主机操作系统进行监控。不仅能够检测主机性能，还能够检测主机安装的软件信息、在线用户信息、主机进程信息、主机网络连接信息、主机服务运行信息等 能够对主机运行的进程信息进行实时监控。通过将进程信息与进程黑名单比对，发现主机上正在运行的违规进程。通过将进程信息与进程白名单比对，进行主机进程防御基线管理
	网络和安全设备监控	网络设备属性，网络设备状态监控，网络性能监控，cpu 利用率监控，内存利用率监控，接口监控，IP 表、ARP 表和路由表监控，设备面板管理，端口通断控制。可以下发防火墙和 IDS 联动策略。 可以对重点设备的重点端口进行流量监控，并且可以配置告警阈值。对于端口流量，管理员可以根据自定义的时间段生成流量报表
	告警与响应管理	自动采集和存储 IT 计算环境中的各类告警信息，并将所有的告警记录按发生时间、告警状态、事件类型、事件等级、源设备 IP、源设备类型等信息列表显示，对告警信息进行分析和统计。产生的告警信息能够通过电话响铃、邮件、短信、电脑语音、控制台弹出窗口、snmp trap、防火墙设备联动、执行预定义参数脚本程序的方式进行自动化响应。其中，设备联动是必要条件，即可以在告警后对防火墙设备下发联动策略。
	报表管理	提供了针对全网络运行状态的分析报表。这是进行综合分析的数据报表，可以让管理员了解和评估整个网络系统的运行状态。能够根据用户的需求定制时间，例如生成日报表，周报表，月报表和年报表等；管理员可以根据自定义的时间段生成网络运行报表、性能分析报表和可用性报表。报表可以另存为 HTML、EXCEL、文本、PDF、WORD 等多种格式。 提供大量预定义的报表模板，用户可使用预定义的报表模板生成报表。 具备自定义报表功能，可方便地自己定义各种复杂的报表，包括报表的内容、布局，以及运行调度设置，满足企业和组织自身不断业务发展的需要。 允许用户对报表生成进行日程规划，定期自动生成报表，提供打印、导出以及邮件送达等服务。

	认证管理	可以在一个界面集中管理所有监控对象的认证方式，便于管理员进行统一修改。通过集中管理界面可以实现所有设备和应用管理的入口，从而实现设备统一认证和管理。
	IP 地址管理	将 IP 地址按照子网分类列表；提供 IP 地址查询，IP 地址扫描；提供图形化的 IP 地址分布查询
	系统自身监控	具有完备的自身运行健康状态监视功能，能够实时监测系统自身运行的 CPU 利用率、内存利用率、磁盘利用率、接收事件速度（EPS），等等，方便管理员实时掌握系统当前运行健康状况。
	系统自身日志	用户对本软件系统的操作都记录日志并进行持久化存储，便于追踪、审核和告警。系统日志格式的属性包括：时间、源 IP、用户名、操作类型、操作说明、操作结果（成功/失败）。
	系统自身安全	产品内部的各个组件之间通信都支持加密传输，浏览器访问管理中心支持 HTTPS，多级管理中心之间采用加密协议进行传输
	权限管理	通过角色定义支持多用户访问
	自带数据库	无需另外安装数据库，系统自带数据维护功能，无需另外进行数据库维护。
	语言	全中文软件界面，中文帮助和用户手册
性能	监控节点数	单级部署时最大可监控 1000 节点
	并发访问用户	最大支持 50 个并发访问用户
可扩展性	功能扩展	提供 SNMP Trap、Syslog 事件转发功能，支持对第三方的 Web Service 接口调用，可方便地与第三方系统进行整合。
产品资质		公安部《计算机信息系统专用产品销售许可证》
		国家保密局涉密信息系统产品检测证书
		国家信息安全测评信息技术产品安全测评证书 EAL1
		国家版权局《计算机软件著作权登记证书》
		《软件产品登记证书》
		产品必须为主流产品，有较高的成熟度，有较高的市场占有率，能够提供投标产品国内权威分析机构最近六年的市场占有率排名。
厂商资质		风险评估服务资质（二级） 应急处理服务资质（二级） 信息系统安全集成服务资质（二级） 国家信息安全测评信息安全服务资质（安全开发类二级） 国家信息安全测评信息安全服务资质（安全工程类三级） 计算机系统集成资质（二级）

	中国通信企业协会通信网络安全服务能力评定证书（安全设计与集成乙级） 中国通信企业协会通信网络安全服务能力评定证书（风险评估乙级） 信息系统安全集成服务资质（二级）

4.2.20 数据库审计服务器

4.2.21 日志审计

性能	
事件采集能力	峰值可达 18000 条条
事件存储能力★	内置 4TB 硬盘；
审计数量★	数据库审计数量不受限制
MTBF（小时）	100,000
接口	
网络口	标配 6 个千兆自适应电口，1 个 Console 口，支持 1 个扩展槽位，支持液晶屏
硬件	
机箱	标准 2U 机箱
电源	冗余电源
资质	
公安部《计算机信息系统专用产品销售许可证》增强型	
国家保密局《涉密信息系统产品检测证书》	
中国信息安全认证中心《中国国家信息安全产品认证证书》（3C）增强级	
国家版权局《计算机软件著作权登记证书》	
功能	
项目	**技术要求**
审计范围	审计包括包括 MS SQL Server、Oracle、DB2、Sybase、MySQL、Informix、达梦、Postgresql 等在内的多种数据库
数据库审计	支持 Cache 数据库集成工具 terminal、portal、studio、Sqlmanager、MedTrak 工具的审计，其中 Portal 能审计到 sql 语句、查询 Global、返回结果，Terminal 能审计到 M 语句和返回结果 中间件的支持，支持 COM、COM+、DCOM 组件
数据库安全	支持对 SQL 注入、跨站脚本攻击等 web 攻击的识别与告警
审计策略	支持数据库语句执行时间、语句执行回应、最大操作语句长度等作为分项响应条件；支持数据库操作返回内容、返回行数作为分项响

	应条件
审计查询	审计数据支持 18 种以上查询条件，可支持按数据库操作命令（包括 select、create 等 14 个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间（包括开始、结束日期）等为条件进行查询
审计安全	审计结果隐秘设置，通过*号对审计结果中的重要信息进行隐秘处理，防止非法权限查看
	系统本身具备能发现未知仿冒进程工具、防范非法 IP 地址、防范暴力破解登录用户密码、设置系统黑白名单等安全功能

类别	**指标项**	**指标内容**
形态	产品形态	该系统为一个软硬件一体化产品，采用专用千兆多核硬件平台和安全操作系统。系统内嵌数据库，用户无需另外安装数据库管理系统；管理客户端基于浏览器，无需安装其他客户端软件。
	产品外观	2U 标准机架式
	硬件配置	内置存储总容量 2TB，支持外接存储设备。单电源。**支持双机热备。**
	网络接口	6 个 10/100/1000M Base-T 电口(RJ45)（1 个管理口，5 个侦听口），另外可扩展千兆以太网络模块 2 光\4 光\8 光\4 电\8 电。1 个 Console 口，支持 Console 口管理。
性能	**事件采集性能**	**峰值可达 20000 条**
	事件分析性能	每秒实时关联分析 5000 条事件
	事件采集丢包率	**每秒采集 20000 条事件时，丢包率小于 0.1%**
	事件查询性能	**百 GB 日志量查询平均响应时间不超过 1 分钟**
	事件入库性能	**事件入库性能可达每秒 7000 条；**
	事件存储性能	存储容量仅取决于磁盘空间大小，可以在线分析 600G 的事件量。
	控制台并发数	50 个
部署	部署模式	支持单一部署，也支持级联部署。
	用户使用模式	界面 100%都是 B/S 模式，无需安装客户端，使用 IE 浏览器访问管理中心，**浏览器端无需安装 Java 运行环境。**
功能	管理范围	能够对企业和组织的 IT 资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。

	日志审计对象	支持对各类网络设备（路由器，交换机）、安全设备（包括防火墙，VPN，IDS，IPS，防病毒网关，网闸，防 DDOS 攻击，Web 应用防火墙）、安全系统（Symantec、瑞星、江民、微软 ISA、Windows 防火墙）、主机操作系统（包括 Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）、各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）、各种应用系统（邮件，Web，FTP，Telnet），网管系统告警日志、终端管理系统（或是内网管理系统、桌面管理系统）告警日志，网络综合审计系统告警日志，上网行为审计系统日志，以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。
	日志采集方式	通过 syslog、snmp trap、netflow、netscreem、jdbc、odbc、opensec lea、agent 代理、wmi 等多种方式完成各种日志的收集功能。对 windows 服务器（系统、应用和安全）日志和文件类型日志，可免日志代理或插件；支持用户环境中 EVT 格式的业务系统日志采集。对于保存在日志文件和数据库中的日志使用 agent 采集方便，无需定制开发采集。
	资产管理	按照设备资产重要程度和管理域的方式组织设备资产，提供便捷的添加、修改、删除、查询与统计功能，支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息,并对资产进行关键度赋值。针对资产可以设置允许接收和拒绝接收日志，在资产日志中显示最近一条日志的接收时间,并可以对资产设置一定时间范围内未收到事件后进行主动告警；可以限定资产的管理员（可以设置为多个），该资产日志只允许所添加管理员查看和审计。
	日志归一化处理	日志收集后进行字段和安全等级的归一化处理,系统归一化字段至少应有 50 个,并至少有 5 个可自定义字段,收集并归一化后的日志需保留原始日志，方便用户对关键日志快速定位。系统应提供灵活简单的归一化方式,对系统默认不支持的日志只需修改配置文件即可支持,不需修改系统程序。
	日志审计查询	所有日志采用统一的日志查询界面，用户可以自定义各种查询场景，并以树形结构组织。查询场景可保存，并可支持在查询结果中继续查询。系统内置针对 windows 服务器的各类应用、系统、安全事件的查询场景，查询结果与 windows 事件查看器显示字段一致。支持原始消息中的关键字查询，可进行全文检索，可显示查询记录总数，当前查询耗时，可对查询结果进行分组排序，可对查询结果跳转到指定页数。查询结果可导出。在查询过程中用户转入其他页面时，可以提示用户继续等待或结束当前查询。

		在查询结果中可以选择跳转到指定页数、可以对查询结果任意字段进行排序。
	日志实时监视	系统提供实时的日志滚动显示和查询，可自定义实时监视的日志内容，可查看实时日志详细信息，可通过雷达图等直观显示目前日志量，可以控制日志对管理员账号的可见性管理。
	日志实时分析和统计	可对收集的日志进行分类实时分析和统计，从而快速识别安全事故。分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新，图表数据支持数据下钻。日志实时分析在内存中完成，不需借助数据库和文件系统。
	事件可视化展现	支持通过世界地图定位 IP 地址，通过事件攻击图展示网络安全态势，通过行为分析图展示一段时间内的用户访问行为。
	日志在线挖掘	系统具备事件挖掘能力可通过事件调查工具可以对某条感兴趣的日志中的源 IP 地址、目的 IP 地址、或者目的端口进行相关性日志检索。
	事件分配	用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中。
	趋势分析	可对收集的日志根据过滤条件，针对设备地址、源地址、目标地址等进行事件数量、流量等的趋势分析。
	事件追溯	对于关联告警事件，用户可以进行追溯，查看导致该关联事件的所有原始事件。
	日志关联分析告警	系统应至少默认有 50 条告警规则，系统提供可视化规则编辑器，对告警规则进行增删改查。系统内置针对服务器和其他安全设备的访问 ip 地址、访问账户和访问时间的访问控制规则；告警规则可按照树型结构组织，并可在该树型结构上直接查看该规则的告警信息,对告警日志可按各告警字段进行分组排序。可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则。
	告警和响应管理	通过关联分析，对于发现的严重事件可以进行自动告警。告警方式包括邮件、短信、SNMP Trap、Syslog、MSN、飞鸽传书等。响应方式包括：自动执行预定义脚本，自动将事件属性作为参数传递给特定命令行程序。**此**

		外，还支持设备联动，即可以在告警后对防火墙/NIDS/网络设备下发联动策略，及时阻断威胁。
	告警查询	支持显示所有和按规则树结果分别显示告警事件信息,对告警查询结果字段可以分别二次排序显示。
	统一监控主页	系统应提供从总体上把握日志告警和日志统计分析的实时综合性监控界面。界面由多个监控组件组成，用户可以自定义监控主页。
	报表管理	提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报表，**满足等保等其他合规性要求；**根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础,帮助管理员掌握网络及业务系统的状况。报表可以保存为 html，excel，文本，pdf 等多种格式。提供自定义报表，用户可根据自身需要进行定制。报表可根据设置自动运行,调度生成日报、周报和月报。
	备份归档	支持按日志属性（原始日志、重要日志、告警日志）、日志类型、存储周期的方式选择备份，支持原始日志与分析后日志分离。支持数据库备份；支持历史日志恢复导入；支持各种配置项的备份和导入。**支持各种配置项的一键备份和恢复；当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警；手动备份和恢复时，可以显示恢复和备份的进度。**
	权限管理	采用基于角色的权限管理机制，通过角色定义支持多用户访问。角色能够从设备和功能两个维度进行定义,从而达到控制谁可以对什么设备进行什么操作的控制粒度；支持禁止与允许用户访问日志审计系统的 IP 地址限制。支持限定管理员只允许查看自己所负责设备的日志；
	系统配置	对系统的各项配置工作，包括日志的备份、恢复。无需借助第三方数据库管理系统。
	系统自身监控	系统自身的健康状况监控。包括 CPU、内存、磁盘的利用率。可以对所有注册了的通用日志采集器的工作状态进行实时监控，包括采集器的启动、停止，以及配置采集器发送什么类型的日志到管理中心。
	系统自身日志审计	用户对本软件系统的操作都记录日志并进行持久化存储，便于追踪、审核和告警。系统日志格式的属性包括：时间、源 IP、用户名、操作类型、操作说明、操作结果（成功/失败）。
	系统认证	**支持用户名密码认证方式，认证时需要提供验证码；支持 USB key 双因**

		子身份认证方式。支持动态口令认证。
	系统自身安全	产品内部的各个组件之间通信都支持加密传输,浏览器访问管理中心支持HTTPS，多级管理中心之间采用加密协议进行传输。
	数据安全	对采集到的日志都进行了加密存储，保证数据的完整性和机密性。
	级联管理	能够实现和上级（下级）安管平台的级联，包括上传监控信息和接收来自上级的控制指令。
	与外部系统集成	可以与第三方的工单系统和工作流系统集成。
	IPv6 网络支持	**系统支持 IPv6 网络环境。**
资质其他	产品资质	公安部《计算机信息系统专用产品销售许可证
		国家保密局《涉密信息系统产品检测证书》
		国家信息安全测评中心《信息技术产品安全测评证书》
		《计算机软件著作权登记证书》
		具有《软件产品登记证书》
		专用 SecOS 操作系统，具有《计算机软件著作权登记证书》
		应至少提供三项相关专利
	厂商资质	风险评估服务资质（二级） 应急处理服务资质（二级） 计算机系统集成资质（二级） 国家信息安全测评信息安全服务资质（安全开发类二级） 国家信息安全测评信息安全服务资质（安全工程类二级） 具备 CNCERT/CC 颁发的网络安全应急服务支撑单位证书 具备公安部颁发的信息安全等级保护安全建设服务机构能力评估合格证书 信息系统安全集成服务资质（二级）

4.2.22 虚拟化网络防火墙

序号	**指标项**	**具体要求**	**备注**
1.	部署安装	软件 SDN 设计思想,控制与转发模块分离的分布式架构系统	
		安装部署和业务管理全程图形界面操作	
2.		支持 VMware(ESXi 5.5/6.0/6.5)等版本,无需 vshield、NSX Manager 等组件支持	
3.		无需在 Hypervior 或虚拟机内部安装驱动软件或代理软件	

4.		透明模式部署，无需改变现有的虚拟机配置和网络架构	
5.		不依赖硬件 SDN 交换机等专有硬件设备	
6.		针对 Windows、Linux、Unix 各平台操作系统均支持无代理方式部署，不需要 Agent	
7.		支持 Vmotion 监管，虚拟机热迁移时安全策略自动跟随，防护能力不变	
8.		支持在客户现有业务环境上，进行系统部署安装，对客户业务不造成影响且会话不中断	
9.		支持系统升级既有会话不中断，可以使用 ssh 和 ftp 会话测试	
10.	管理控制	提供 Web 管理控制台，方便管理员实现不局限于特定地点和终端的管理	
11.		仅有一套统一管理界面，不需要对各业务模块单独管理	
12.		支持统一账户的管理方式，同步虚拟化平台管理员账户，可采用同一个账户密码登陆系统	
13.		控制器需要具备冗余备份保障机制，保证控制器高可靠性，当控制器出现异常（宕机等）数据转发不受影响，不会造成业务中断	
14.		物理节点之间数据通信支持 VXLAN、MPLS over GRE 、MPLS over UDP 等三种隧道封装技术（支持三种协议并可以任意选择其中一种协议进行封装）	
15.		支持以逻辑拓扑图的方式展示可视化效果	
16.		可以对边界安全防护和云平台东西向安全防护进行一站式配置和统一管理	
17.		支持对虚拟机流量、应用、威胁的统计	
18.		自动化展示出外部网网络、虚拟网络、虚拟机之间的流量、应用、会话日志、安全攻击、威胁事件等信息	
19.		支持对接入服务的虚拟机进行全方位的网络监控	
20.	东西向流量安全防护	基于安全组白名单的虚拟机安全策略，通过具体的访问控制规则，控制规则配置在虚拟机的接口上，支持任意虚拟机之间的访问控制	
21.		基于访问控制策略的虚拟机连接，通过具体的访问控制规则，支持任意虚拟机之间的访问控制	

22.		对于虚拟机间东西向流量进行深度安全检测，包括但不仅限于入侵防御、应用监控、病毒检测等	
23.		可支持不同虚拟网络互通、隔离基本的访问控制策略	
24.		东西向流量支持管理员自定义虚拟网络、子网、虚拟机配置安全策略	
25.		任意物理主机节点上的虚拟机无论如何动态迁移，其对应虚拟机的安全策略始终跟随，动态适应，无需人为调整	
26.	服务链安全组件	不依赖于 VMware tools，独立安全业务虚拟机实现 2-7 层安全功能防护	
27.		支持防火墙 vFW、入侵检测系统 vIPS、防病毒 vAV 包括但不仅限于三种产品形态作为服务链安全组件进行安全防护	
28.		支持虚拟安全组件（vFW、vIPS、vAV）横向扩展，随需创建和分配	
29.		支持无代理防病毒，不受 vsphere ESX5.5、vsphere ESX6.0、vsphere ESX6.5 版本演进变化影响	
30.		病毒防护功能独立自主可控，完全与 Hypervior 层解耦，不受制于 Hypervior API 影响	
31.		支持低、中、高三种预制配置模板选择	
32.		单台安全组件虚拟机配置最低可支持 2 核 vCPU、4G 内存	
33.	基础安全防护	支持 4 种安全防护模式，基于网络、用户、应用以及云租户	
34.		支持 ARP 防护，包括但不仅限于防护反向 ARP 查询、防护 ARP 洪水，自有定义 ARP 洪水阈值范围、防护 ARP 恶意欺骗（支持广播应答、检察应答、特征检查、禁止更新检查）	
35.		能够在一条策略里配置源/目的 IP 地址、安全域、应用/应用组、时间、用户/用户组、URL 大类引用、安全业务模板组（至少包含但不仅限于入侵防护业务、防病毒业务、文件控制业务、内容过滤业务、细粒度 URL 业务、挂马防护业务、僵尸网络业务）	

36.	IPS 入侵防御模块	能够检测包括木马攻击、拒绝服务攻击、finger 服务攻击、远程访问攻击、安全扫描、间谍软件攻击、恶意攻击、0-Day 攻击、潜在风险、缓冲溢出攻击、蠕虫攻击、漏洞扫描攻击、SQL 注入攻击、跨站脚本攻击、病毒过滤、爬虫攻击、web 扫描等在内的超过 3500 种攻击事件	
37.		支持基于 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别；	
38.		支持模式匹配、异常检测、统计分析，以及抗 IDS/IPS 逃逸等多种检测技术	
39.		可依据端口识别协议类型，可分析 HTTP、SMTP、POP3、FTP、Telnet、VLAN、MPLS、ARP、GRE 等多种协议	
40.		内置攻击特征库，特征数量超过 3,500 条，支持在线、离线升级方式，并可自定义攻击特征，阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等多种攻击	
41.		能够针对攻击目标的类型进行规则分类，如 Server, Client; 操作系统; 应用程序(IIS, Apache 等)	
42.		可对英文、UTF8/GB18030/BIG5 中文编码 GZIP/inflate/trunked 压缩算法的的网页内容进行深度特征码检测的舆　情监 控和报警	
43.		可对告警事件设置丢弃数据包、阻断会话、页面推送、日志/邮件报警、声音、状态灯报警等	
44.	DDoS 防护模块	抗应用型攻击： 包括 Web cc、http get flood、DNS query/reply 泛洪攻击或速率限制、DNS 协议自身安全性、DNS 缓存投毒、域名劫持、容灾恢复等	
45.		抗流量型攻击： 包括 syn flood、udp flood、icmp flood、arp flood、frag flood、stream flood 等攻击	
46.		抗蠕虫连接型攻击： 可基于 ACL 或者源或目地 IP 地址进行连接数统计和控制，支持连接排行榜，可早期预警	

47.		抗普通常见攻击： 包括 ipspoof、sroute、land、fraggle 攻击、sf_scan、null_scan、xmas_scan、smurf 等攻击	
48.		防扫描：TCP 端口扫描、UDP 端口扫描、Ping Sweep 扫描，能够防止主机和端口扫描等	
49.		流量智能分析，支持流量自学习，学习时间可设置，支持对报文、服务、域名多维度的进行统计，自动生成动态的业务场景防护策略模板	
50.		攻击证据提取，可基于五元组、协议、时间对象等自定义抓包任务，抓取指定接口、指定数量的报文，并可以在 web 上面批量导出、批量删除	
51.	防病毒模块	针对虚机采用零信任管理，有效防止虚机的病毒风暴导致的网络瘫痪、对于病毒样本进行查杀与隔离；	
52.		支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀、病毒库自动更新、虚拟脱壳、自定义查杀文件大小、查杀可疑病毒、可疑脚本、图片病毒、查杀邮件正文、附件、网页及下载文件中包含的病毒	
53.		预定义 20 种文件类型，支持自定义扫描文件类型，支持常见的压缩格式文件扫描	
54.		支持 400 万余种病毒的查杀，病毒库支持在线或者离线升级	

4.2.23 虚拟化软件技术指标要求

指标项	指标参数
资质要求	虚拟化平台软件必须具有国产软件自主知识产权，具有自主研发能力，保障后续产品的连续性；提供《计算机软件著作权登记证书》复印件证明。
	虚拟化软件开发企业必须是 OpenStack 基金会金牌会员(Gold Member)，积极支持开源项目，提供有关证明。
	投标厂商必须是主流虚拟机厂商，是 Gartner 服务器虚拟化魔力四象限成员。
计算虚拟化功能要求	虚拟化软件架构须采用裸金属架构，充分利用 Intel VT 和 AMD-V 的硬件虚拟化技术，支持 Intel 扩展页表技术。虚拟化软件必须能直接安装在服务器硬件设备上，不能采用在服务器上先安装操作系统的方式，虚拟化软件要能直接管理硬件资源。
	支持虚拟机生命周期管理，支持查询、创建、删除、启动、关闭、重启、休眠、唤醒、克隆虚拟机。

指标项	指标参数
	支持虚拟机卷的安全删除，要求虚拟机卷在删除时用户可以选择所有 bit 位彻底清零的删除方式，以保证虚拟机卷在删除后不能被恶意恢复数据。
	提供系统运行记录仪功能，能够在虚拟化系统死机时，记录系统死机时的故障信息如 BMC 截屏、CPU 传感器信息、BMC 日志等异常情况，供故障定位使用。
	支持虚拟机之间亲和性部署规则设置： 1、支持虚拟机聚合规则，即多个虚拟机必须运行于同一个主机的物理 CPU 上； 2、支持虚拟机互斥规则，即多个虚拟机必须运行于不同主机，不能同时运行同一主机；
	“数据安全”的虚拟机 HA。社区 OPENSTACK 删除 VM 数据，创建一个新的 VM，会丢失故障 VM 的磁盘运行数据。要求厂商规避该问题， VM 故障能够重新生成 VM，同时不丢失 VM 磁盘运行数据。
	支持动态电源管理（DPM），动态电源管理(DPM:DynamicPower Management)支持对服务器负载进行检测，实现轻载合并，对不使用的物理机进行并下电节能；重载分离，并对空闲物理机上电分担负载。优化数据中心的能耗，达到节能减排的目的。
	支持动态资源调度 DRS，动态资源调度 (DRS) 动态分配和平衡资源，采用智能调度算法，根据系统的负载情况，对资源进行智能调度，达到系统的负载均衡，保证系统良好的用户体验。
网络虚拟化功能要求	支持服务器节点集成虚拟交换机（OVS）功能；虚拟交换机支持端口聚口、虚拟端口管理、VLAN 管理、DHCP 隔离、QoS(流量整形和限速)设置，提供实现网络数据包的收发与中转。
	支持 SDN 功能，提供自动化网络部署功能，提供 SDN 高级网络服务能力(vFW，vRouter、vLB、VPN)，包括： SDN 功能够同时支持 FusionSphere/XEN/KVM/Vmware 虚拟化平台平台 支持完整的 L2-L7 层能力，支持 vFW，vRouter、vLB、VPN 等高级网络能力，并支持网关集群部署，支持弹性扩展功能 支持全网可视能力，逻辑、虚拟、物理网络统一 TOPO，UnderLay 网络路径可视化 支持物理机、虚拟机统一自动化发放功能，包括物理服务器网络自动化配置 支持通过基于 Openstack 的云管理平台实现计算、网络资源统一自动化发放 提供灵活的 SNAT 和 VPN 多子网能力，提供灵活的基于 Subnet 使能 SNAT 访问外网的能力，提供单个 IPSec 连接保护多个本地子网的能力
	SDN 系统必须基于开放架构的 ODL 平台，便于第三方集成开发
存储虚拟化功	虚拟化平台使用存储设备时，须支持本地存储、IP-SAN、FC-SAN、NAS 等不同类型的

指标项	指标参数
能要求	存储设备。支持这些存储资源的添加、删除、查询、扫描。
	支持多台虚拟机共享同一磁盘卷进行读写，方便 rac 类业务部署
	删除用户磁盘时，支持选择是否彻底清除磁盘数据，避免利用工具对数据进行恢复，以保证数据的安全。
	本次利用物理主机本地磁盘形成高可靠的分布式虚拟存储系统。分布式虚拟存储系统可以支持不少于 128 个资源池，49152 块本地硬盘、4096 个物理主机节点。支持全 SSD 盘部署。
	分布式存储软件支持虚拟化方式部署，虚拟化平台至少支持如下 3 种：VMWARE、KVM、XEN
	分布式存储软件支持 SSD Cache 加速特性，应包括写缓存、预读、读热点三种 Cache 能力（依赖 RAID 卡的 Cache 能力不算）。
	分布式软件系统中支持按照指定刀片或者服务器范围，按冗余方式（副本）、组网方式、加速方式（cache 介质）、存储介质等属性灵活组成多个不同的存储资源池，向上层业务提供大容量、性能和可靠性差异化的存储能力。
	分布式软件系统单卷最大容量可以支持扩充到 256TB
	分布式软件系统重建 1TB 数据小于 15 分钟，并且能现场测试。
兼容性与扩展性要求	虚拟化平台须支持主流设备厂商提供的 X86 服务器，支持基于业界标准的 IPMI 接口的管理硬件设备。
	虚拟化平台须支持主流设备厂商提供的 IPSAN、FCSAN、NAS 存储设备。
	虚拟机平台须支持主流的 X86 架构的操作系统，包括 Windows Server 2003 /2008 R2 及以上版本服务器操作系统，Windows XP、Windows 7 操作系统， Redhat、SUSE、CentOS、中标普华、中标麒麟、Ubuntu、Fedora 等多个发行版本的 Linux 操作系统。
系统可靠性功能要求	OpenStack 管理节点支持负荷分担部署模式，在保障系统运行的可靠性的情况下，可以平滑扩容管理节点，以便管理更大规模的集群。
	系统提供 Openstack 及虚拟化平台管理节点的数据备份与恢复操作界面。支持每日备份、立即备份。备份介质支持第三方 FTP 或对象存储。备份周期更灵活。
	支持虚拟机 HA 功能，虚拟化系统在服务器硬件故障导致虚拟机宕机的情况下，可自动地将虚拟机在其它正常的服务器启动，或者当虚拟机的操作系统出现故障，导致虚拟机无法正常运行时，虚拟化系统可自动将故障虚拟机在其它服务器上启动，尽快恢复虚拟机上业务运行。可支持不依赖于管理模块集中控制式 HA 功能。
	支持虚拟机热迁移（VM Motion）功能。在虚拟机运行期间，通过手工或自动地实现虚拟机在集群之内的不同物理机之间迁移，保障业务连续性。

指标项	指标参数
	支持存储迁移功能：支持虚拟机关机或开机情况下，虚拟机的卷迁移至其他存储单元中，可以在存储虚拟化管理下的同一个存储设备内、不同存储设备之间进行迁移。
	支持无共享存储的虚拟机热迁移功能，虚拟化平台可以让不同存储介质上的虚拟机，在不同的节点之间无缝地进行热迁移，支持带快照的虚拟机的无共享存储热迁移，摆脱共享存储的限制。
	系统备份方案支持无代理备份，不需要在虚拟机内安装备份代理软件。
规格要求	每台物理服务器最大上电 VM 数量无论是 Linux 或 Windows 操作系统的可达 2048 台。
	每台物理服务器最大逻辑 CPU 核数可达 4095。
	每台被虚拟化的物理服务器最大物理内存可达 16TB。
	一台虚拟机最大须可以使用不小于 160 个虚拟 CPU（vCPU）的处理能力；一台虚拟机须可以与其它虚拟机共享物理 CPU 资源。
	每台虚拟机最大须支持 6TB 内存。
	每台虚拟机的虚拟网卡可达 12 块。
	虚拟机的单个虚拟磁盘最大容量可达 64TB。
	同一时刻，单个服务器上进行迁入和迁出的虚拟机数量可达到 8 台。
	单 OpenStack 实例支持最大物理主机数 1,000，支持大资源池，减少资源碎片，提升资源利用率。
	单 OpenStack 实例支持最大虚拟机数 10,000，支持大资源池，减少资源碎片，提升资源利用率。
配置	本次配置 88CPU 虚拟化及 173TB 分布式存储软件许可
服务	提供安装服务，五年维保服务，需有原厂售后服务承诺函盖鲜章原件和授权书盖鲜章原件；设备生产商需在国内设有 400 技术服务热线。

五、设备清单

以下附本项目设备清单，

5.1 视频云平台

序号	**服务项目**	**数量**	**说明**
一	**视频云存储服务（私有云）硬件**		
1	集中视频存储	4	分控中心 7 天视频
2	大图片存储	1	
3	小图片存储	1	
4	数据库存储设备	1	
5	业务数据备份设备	1	

6	数据备份软件	1	
7	光纤交换机	2	
二	**云计算硬件服务**		
1	云计算服务器(高端)	30	
2	云计算服务器（中端）	28	
三	**后端设备租赁服务**		
1	核心交换机	4	
2	48 端口万兆以太网光接口模块	8	
3	48 端口千兆以太网电口模块	8	
4	40KM 万兆光模块	150	
5	40KM 千兆光模块	60	
6	接入交换机	4	
7	联网光缆	28	总长约 28 公里
四	**视频云存储服务（私有云）软件**		
1	企业级备份软件	1	
2	多路径切换和负载均衡	1	
五	**管理平台服务**		
1	数据对接	1	
2	大数据清洗及资源池建设	1	
3	大数据融合实战平台	1	
4	三维 GIS 平台	1	
5	“一标六实”管理及应用系统	1	
六	**云计算虚拟化服务**		
1	云计算虚拟化计算服务	132	
2	云计算虚拟化运维管理平台	1	
3	虚拟化网络及防火墙	132	
4	虚拟化存储服务	76	按高端服务器 CPU 数量核定
七	**视频及数据接入服务**		
1	视频资源整合网关	5	
2	数据接入网关	5	

5.2.高清摄像机

序号	**服务项目**	**数量**	**说明**

一	**高清监控前端点位硬件及配套服务**		
1	固定摄像机	4925	
2	可控枪型摄像机	2152	
3	热成像 60 倍云台一体机（水域瞭望）	14	
4	热成像 30 倍云台一体机（水域瞭望）	7	
5	高空瞭望云台摄像机	30	
6	可控球型摄像机	2514	
7	稳压电源	2700	
8	整流变压器	7013	
9	电源防雷器	2700	
10	网络防雷器	9591	
11	环境监测器	7673	
12	背包箱	1800	
13	补光灯	447	
二	**高清监控前端点位取电服务**		
1	前端点位取电测算	1659	
三	**高清监控前端点位立杆服务**		
1	6 米监控杆	1659	
2	立杆挑臂	1659	
3	立杆喷漆	1659	
4	立杆基础	1659	
四	**流媒体转发服务**		
1	高清转发服务器	50	
2	高清节点管理服务器	23	
3	高清转发服务器(共享平台）	4	
4	高清节点管理服务器(共享平台）	2	
5	边界防火墙(共享平台）	2	
6	千兆电口接入交换机(共享平台）	2	
7	时钟同步服务器(共享平台）	2	
五	**视频 NVR 存储服务（30 天）**		
1	视频 NVR 服务器(含企业级硬盘）	284	至少满足 12123 路视频

			存储 30 天
六	**维护一体化服务平台**		
1	基础信息管理平台	1	
2	故障流转平台	1	
3	备品备件管理平台	1	
4	视频诊断平台	1	
5	运维管理 APP	1	
七	**流媒体转发软件服务**	**300**	

5.3.卡口部分

序号	服务项目	数量	说明
一	**300 万高清卡口前端点位硬件及配套服务**		
1	摄像机	250	
2	稳压电源	200	
3	整流变压器	200	
4	电源防雷器	200	
5	网络防雷器	250	
6	背包箱	200	
7	LED 车牌检测补光灯	375	
8	环境监测器	200	
二	**600 万高清卡口前端点位硬件及配套服务**		
1	摄像机	250	
2	稳压电源	225	
3	整流变压器	225	
4	电源防雷器	225	
5	网络防雷器	250	
6	背包箱	225	
7	LED 车牌检测补光灯	750	
8	环境监测器	225	
三	**高清卡口前端点位取电服务**		
1	卡口前端取电	425	
四	**高清卡口前端点位立杆服务**		

1	L 型卡口立杆	425	
2	L 型卡口立杆基础	425	
五	**卡口图片接收服务**		
1	卡口图片接收服务器	8	
六	**高清卡口流媒体软件服务**		
1	卡口流媒体服务	8	
七	**高清卡口数据库**		
1	高清卡口数据库	3	

5.45.5.数据转换

序号	项目	数量	说明
一	**高清视频硬件服务**		
1	视频服务	218	
2	视频基础应用服务	1	
3	视频联网网关服务	10	
4	数据通信服务	12	
5	数据管理服务	18	
二	**高清视频集群管理服务**		
1	云管理服务	4	
2	云存储服务	3	
3	视频集群服务	20	
4	LISCENCE 管理服务	5	
5	运维管理集群服务	5	
6	系统监控服务	1	
7	视图库应用管理服务	4	
三	**高清视频大数据服务**		
1	视频大数据应用服务	1	
2	视频大数据检索服务	37	
3	数据管理服务	14	
4	数据应用服务	5	
四	**高清视频软件服务**		
1	高清平台服务	1	
2	视频系统授权	12500	

3	图像基础应用服务	2	

5.6.机房等保

序号	名称	单位	数量	说明
一	**硬件**			
1	边界防火墙（分控中心）	台	8	
2	入侵防御（分控中心）	台	8	
3	负载均衡（分控中心）	台	8	
4	入侵防御（总控中心）	台	1	
5	负载均衡（总控中心）	台	2	
6	4A 安全管控平台（总控中心）	台	2	
7	日志审计（总控中心）	台	2	
8	数据库审计（总控中心）	台	1	
二	**软件**			
1	防病毒（分控中心）	套	8	
2	防病毒（总控中心）	套	2	
3	防篡改（总控中心）	套	4	

第四章 评审办法

1.评审原则

本项目评审原则将以《中华人民共和国政府采购法》和上海市相关文件规定为主要依据，由评委对各投标人的响应文件进行认真分析。对各响应文件的价格、技术、财务状况、信誉、业绩、服务、对协商文件的响应程度等内容综合评定。严格遵守公开、公平、公正的原则。

2.评审工作的组织领导

2.1 评审工作由代理机构负责组织，具体评审事务由依法组建的评审委员会负责。评审委员会由有关专家等三人以上单数组成，其中专家的人数不少于成员总数的三分之二。

2.2 评审委员会履行下列职责：

（1）按协商文件确定的有关规定对响应文件进行详细评审；

（2）审查响应文件是否符合协商文件要求，做出书面评价；

（3）要求投标供应商对响应文件有关事项做出解释或者澄清；

（4）向采购人或者有关部门报告非法干预评审工作的行为。

3.评审总则

3.1 采购人和招标代理机构将按照本须知的规定，只对确定为实质上响应招标文件要求的投标进行评价和比较。

3.2 评审的基础应是本须知规定的投标及投标文件技术部分。

3.3 在通过实质性响应条款审查的基础上，协商小组根据单一来源采购文件要求和供应商提供响应文件情况，就采购项目需求、合同主要条款及价格与供应商进行协商，商定合理的成交价格并保证采购项目质量。

3.4 协商小组编写协商情况记录，并由协商小组全体人员签字认可，具体操作以上海政府采购网操作系统中单一来源协商程序为准。

第五章 投标格式

投标函格式

致：_____（采购人、招标代理机构）

根据贵方_____项目投标邀请书(项目编号为:_____),现正式授权的下列签字人_____(姓名和职务）代表投标人_____（投标人的名称），提交下述投标文件正本 1 份，副本__份，光盘__张：

1.投标一览表；
2.报价明细表；
3.资格证明文件；
4.“投标人须知”要求投标人提交的全部文件。

据此函，签字人兹宣布同意如下：

（1）按招标文件的规定提交货物及提供伴随服务的投标总价为：
人民币_____元（RMB_____）。

（2）我们将按招标文件的规定，承担完成合同规定的责任和义务。

（3）我们已详细审核了全部招标文件，包括招标文件的修改通知（如果有的话）、我们知道必须放弃对上述文件中所有条款提出存有含糊不清或不理解之问题的权利。

（4）我们同意在“投标人须知”所述的开标日期起遵循本投标文件的规定，并在“投标人须知”规定的投标有效期届满之前对我方均具有约束力，而且有可能中标。

（5）如果在开标后规定的投标有效期内撤回投标，我们的投标保证金可被贵方没收。

（6）如果贵方有要求，我们愿意进一步提供与本投标有关的任何证据或资料。

（7）我们完全理解贵方不一定要接受最低投标的投标或收到的任何投标。

与本投标有关的正式通讯地址为：

地址：

邮政编码：_____

电话号码：_____

传真号码：_____

电子信箱：_____

投标人代表姓名：_____

投标人（公章）：_____

日期：____年____月____日

投标报价一览表格式

序号	项目名称	投标总价	服务期/供货期
		人民币： RMB：	

注：

1.上表中“投标总价”为所报费用应包含整个项目过程中可能发生的所有费用。投标人在投标时必须充分考虑本项目所需要求，如果在投标中有缺项和漏项，则将被认为该项的价格已经包含在其他项中。采购人在签订合同的时候，不会对投标人缺漏项的金额给予补偿。

2.若本表与投标书格式其他部分在内容上有出入，以本表为准。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

投标货物或服务清单、报价明细表格式

注：表格投标人可自拟，须加盖公章。

资格证明文件格式

1 营业执照、组织机构代码证、税务登记证或营业执照三证合一件；

2.信用查询记录证明；

3.根据项目需求提供必要的各类资质文件；

4.供应商认为需要提供的文件和资料。

财务状况及税收、社会保障资金缴纳情况声明函格式

我方（供应商名称）符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1. 具有健全的财务会计制度；

2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

投标文件主要内容索引表

序号	主要内容	详细内容所对应电子投标文件页码	备注
1			
2			
3			
4			
……			

此表须编入投标文件内，并放置于目录后。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

商务、技术规格偏离表格式

序号	招标规格	投标规格	正（负）偏离

注：商务及技术规格偏离内容适用于同一张表格格式，但须分开填写。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

公司承接项目一览表格式

序号	用户单位	项目名称	合同日期	合同价格

注：1、本表格主要为投标人的项目业绩（提供中标通知书或合同复印件）

2、如本表格内容不能满足需要，投标单位可根据此表格格式自行划表填写。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

节能清单和环保清单说明表（如需）

序号	品牌	投标型号	节能产品认证清单				环保产品认证清单			
			已取得证书日期	清单型号	证书编号	位于节能产品政府采购清单页次	已取得证书日期	清单型号	证书编号	位于环境标志产品政府采购清单页次
1						第 XX 页第 XX 大行第 XX 行				第 XX 页第 XX 大行第 XX 行
2										
3										
4										
5										
6										
7										
8										
9										

备注：

1、上述“节能产品政府采购清单”、“环境标志产品政府采购清单”、以相关职能部门正式发布的最新一期为准。

2、投标人需填写本表，并按以上序号循序在该表后提供《节能产品政府采购清单》和《环境标志产品政府采购清单》中该产品所在页的复印件（用颜色笔标识一一对应的认证型号）。

法定代表人授权书格式

我_____（姓名）系_____（投标人名称）的法定代表人，现授权委托本单位在职职工_____（姓名，职务）以我方的名义参加_____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、投标文件澄清、签约等一切具体事务和签署相关文件。

本授权书于____年___月___日签字生效，有效期为____天。

特此声明。

提供被授权人身份证复印件（正反面）

法定代表人代表签字：_____

投标人授权代表签字：_____

投标人（公章）：_____

地　址：_____

日期：_____年_____月_____日

主要从业主管人员及其技术资格一览表格式

项目经理简历表

姓　名		性　别		年　龄	
职　务		职　称		学　历	
项目经理资格等级		项目经理资格证书编号			
参加工作年限		从事项目经理工作年限			
已 完 项 目 情 况					
用户单位	项目名称	合同价格	合同时间	其他	

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

拟投入项目团队人员情况表格式

序号	姓　名	年龄	性别	职务	职称 （附证）	持证情况 （附证）	经历
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

服务/技术及售后服务方案

包括本项目的设计方案等。说明与“项目要求”的满足程度，并提供深化设计的方案及实施计划，优惠措施，售后服务等。）

公司综合情况

请介绍公司规模、人员、场地、成立时间、获奖情况（公司获得的荣誉证书）等。

中小企业声明函格式

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，提供的货物或服务全部由符合政策要求的中小企业承接。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*（采购文件中明确的所属行业）*；承接企业为*（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*（采购文件中明确的所属行业）*；承接企业为*（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）*；

……

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，也不存在与大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：

说明：

（1）本声明函所称中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

（2）本声明函所称货物或服务由中小企业采购或承接，是指在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。否则不享受中小企业扶持政策。

（3）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。

（4）中标人为中小企业的，本声明函将随中标结果同时公告。

（5）投标人未按照上述格式正确填写《中小企业声明函》的，不享受中小企业扶持政策。

注：各行业划型标准：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人

员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

残疾人福利性单位声明函格式（如需）

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

参加政府采购活动前三年内，在经营活动中没有重大违法记录
声明函格式

致：_____（招标人名称）

我们_____（投标人名称）是按中华人民共和国法律正式成立的一家公司，主要营业地点设在_____（投标人地址）。

我司在参加本次招标采购活动前三年内，在经营活动中没有重大违法记录，无利用不正当竞争手段骗取中标，无重大经济刑事案件。

特此声明。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

第六章 合同条款及合同格式

包 1 合同模板：

[合同中心-合同名称]

合同统一编号： [合同中心-合同编码]

合同内部编号：

合同各方：

甲方：[合同中心-采购单位名称]

地址：[合同中心-采购单位所在地]

邮政编码：[合同中心-采购人单位邮编]

电话：[合同中心-采购单位联系人电话]

传真：[合同中心-采购人单位传真]

联系人：[合同中心-采购单位联系人]

乙方：[合同中心-供应商名称]

地址：[合同中心-供应商所在地]

邮政编码：[合同中心-供应商单位邮编]

电话：[合同中心-供应商联系人电话]

传真：[合同中心-供应商单位传真]

联系人：[合同中心-供应商联系人]

法人姓名：[合同中心-供应商法人姓名]

性别：[合同中心-供应商法人性别]

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1．乙方根据本合同的规定向甲方提供以下服务：

1．1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见合同附件。

2. 合同价格、服务地点和服务期限

2．1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2．2 服务地点：根据招标文件要求。

2．3 服务期限：根据招标文件要求。

3．质量标准和要求

3．1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3．2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4．权利瑕疵担保

4．1 乙方保证对其交付的服务享有合法的权利。

4．2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

4．3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权利。

4．4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5．验收

5．1 服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5．2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

5．3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定

的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

5．4 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

6．保密

6．1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7．付款

7.1 根据招标文件要求支付。

8．甲方（甲方）的权利义务

8．1 甲方有权在合同规定的范围内享受，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。

8．2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8．3 由于乙方服务质量或延误服务的原因，使甲方有关或设备损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8．4 甲方在合同规定的服务期限内有义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。

8．5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8．6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知乙方涉及合同服务范围调整的，应与乙方协商解决。

9．乙方的权利与义务

9．1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9．2 乙方为了更好地进行服务，满足甲方对服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时，可以要求甲方进行合作配合。

9．3 如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。

9．4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、

或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9．5 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9． 6 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9．7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供服务的费用。

9．8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10．2 在服务期限内，如果乙方对提供服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）根据服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低服务的价格。

（2）乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供服务。

11．2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11．3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面

形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

12．误期赔偿

12．1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期服务的服务费用的百分之零点五（0.5%）计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13．不可抗力

13．1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13．2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13．3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14．履约保证金(如有)

14.1 在本合同签署之前，乙方应向甲方提交一笔按照 招标文件规定金额的 履约保证金。履约保证金应自出具之日起至全部服务按本合同规定验收合格后三十天内有效。在全部服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14．2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行负担。

14．3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

15．争端的解决

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一

切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。

15．2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15.3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16．违约终止合同

16．1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

（2）如果乙方未能履行合同规定的其它义务。

16．2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17．破产终止合同

17．1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18．合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19．合同生效

19．1 本合同在合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19．2 本合同一式叁份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20．合同附件

20．1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20．2 本合同附件与合同具有同等效力。

20．3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21．合同修改

21．1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）：　　乙方（盖章）：

法定代表人或授权委托人（签章）：　　法定代表人或授权委托人（签章）：

日期：[合同中心-签订时间]　　日期：[合同中心-签订时间_1]

合同签订点:网上签约

包 2 合同模板：

[合同中心-合同名称]

合同统一编号： [合同中心-合同编码]

合同内部编号：

合同各方：

甲方：[合同中心-采购单位名称]

地址：[合同中心-采购单位所在地]

邮政编码：[合同中心-采购人单位邮编]

电话：[合同中心-采购单位联系人电话]

传真：[合同中心-采购人单位传真]

联系人：[合同中心-采购单位联系人]

乙方：[合同中心-供应商名称]

地址：[合同中心-供应商所在地]

邮政编码：[合同中心-供应商单位邮编]

电话：[合同中心-供应商联系人电话]

传真：[合同中心-供应商单位传真]

联系人：[合同中心-供应商联系人]

法人姓名：[合同中心-供应商法人姓名]

性别：[合同中心-供应商法人性别]

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1．乙方根据本合同的规定向甲方提供以下服务：

1．1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见合同附件。

2．合同价格、服务地点和服务期限

2．1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2．2 服务地点：根据招标文件要求。

2．3 服务期限：根据招标文件要求。

3．质量标准和要求

3．1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3．2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4．权利瑕疵担保

4．1 乙方保证对其交付的服务享有合法的权利。

4．2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

4．3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权利。

4．4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5．验收

5．1 服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5．2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

5．3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

5．4 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

6．保密

6．1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7．付款

7.1 根据招标文件要求支付。

8．甲方（甲方）的权利义务

8．1 甲方有权在合同规定的范围内享受，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。

8．2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8．3 由于乙方服务质量或延误服务的原因，使甲方有关或设备损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8．4 甲方在合同规定的服务期限内有义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。

8．5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8．6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知乙方涉及合同服务范围调整的，应与乙方协商解决。

9．乙方的权利与义务

9．1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9．2 乙方为了更好地进行服务，满足甲方对服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时，可以要求甲方进行合作配合。

9．3 如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。

9．4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9．5 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9． 6 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9．7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供服务的费用。

9．8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10．2 在服务期限内，如果乙方对提供服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）根据服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低服务的价格。

（2）乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。

如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供服务。

11．2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11．3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

12．误期赔偿

12．1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期服务的服务费用的百分之零点五（0.5%）计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13．不可抗力

13．1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13．2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13．3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14．履约保证金(如有)

14.1 在本合同签署之前，乙方应向甲方提交一笔按照 招标文件规定金额的 履约保证金。

履约保证金应自出具之日起至全部服务按本合同规定验收合格后三十天内有效。在全部服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14．2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行负担。

14．3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

15．争端的解决

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。

15．2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15.3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16．违约终止合同

16．1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

（2）如果乙方未能履行合同规定的其它义务。

16．2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17．破产终止合同

17．1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18．合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19．合同生效

19．1 本合同在合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19．2 本合同一式叁份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20. 合同附件

20. 1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20. 2 本合同附件与合同具有同等效力。

20. 3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21．合同修改

21．1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）： 乙方（盖章）：

法定代表人或授权委托人（签章）： 法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]** 日期：[合同中心-签订时间_1]

合同签订点:网上签约