

嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026年度运行维护项目）

招标文件

采购单位：上海市公安局嘉定分局

采购代理机构：上海定佳商务咨询有限公司

编制日期：2026年04月

2026年04月08日

2026年04月08日

目录

第一章：招标公告

第二章：投标人须知

第三章：政府采购主要政策

第四章：项目招标需求

第五章：评标方法与程序

第六章：投标文件有关格式

第七章：合同文本

第八章：质疑、未中标结果询问受理要求及附件

第一章 招标公告

根据《中华人民共和国政府采购法》及相关法律、法规之规定，上海定佳商务咨询有限公司受**上海市公安局嘉定分局**委托，对**嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026年度运行维护项目）**进行公开招标采购，特邀请合格的供应商前来投标。

一、项目基本情况

项目编号：**310114000251219161656-14302737**

项目名称：**嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026年度运行维护项目）**

预算编号：**1426-00005459**

预算金额（元）：**1960000.00元**（国库资金：**1960000.00元**；自筹资金：0元）

最高限价（元）：**包1-1960000.00元**

采购需求：

包名称：**嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026年度运行维护项目）**

数量：1

预算金额（元）：人民币**1960000.00元**

简要规格描述或项目基本概况介绍、用途：**项目运维内容包括智能分析系统、视讯通系统、嘉定分局数字化勤务系统、智能图像算力支撑和功能开发配套系统、智能图像防控能力支撑配套系统、AR全景超融合系统和视频监控轻应用配套系统、基于全局智能视频监控的动态应用服务系统、融合承载网、防控中心配套系统、网络升级服务、感知网分控中心安全加固、安全管理平台及配套设备升级、感知网安全监测、运维系统、嘉定分局视频图像能力及共享平台，共计15个子系统。**

合同履行期限：**自合同签订之日起至2026年12月31日**

本项目**不允许**联合体投标。

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：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、残疾人福利性单位等的政策功能。

3.本项目的特定资格要求：1、符合《中华人民共和国政府采购法》第二十二条的规定。

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

3、提供财务状况及税收、社会保障资金缴纳情况声明函及没有重大违法记录的声明；

4、本次招标 接受 不接受 联合投标。

5、本项目专门面向 中小企业 小微企业 预留采购份额。

本项目非专门面向中小企业预留采购份额。

注：①中小企业参加政府采购活动，应当出具《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的《中小企业声明函》，否则不得享受相关中小企业扶持政策。②非专门面向中小企业预留采购份额的项目如允许分包，大中型企业向一家或者多家小微企业分包的，拟享受价格扣除优惠的必须在投标（响应）文件中提供完整准确《分包意向协议书》，否则不予认可。

6、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

三、获取招标文件

时间：**2026-04-10 至 2026-04-17**，每天上午 **00:00:00~12:00:00**，下午 **12:00:00~23:59:59**（北京时间，法定节假日除外）

地点：上海市政府采购网

方式：网上获取

售价：0 元

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：**2026-05-06 10:00:00**

投标地点：上海政府采购网（<http://www.zfcg.sh.gov.cn>）

开标时间：**2026-05-06 10:00:00**

开标地点：上海市嘉定区嘉罗公路 1661 弄盛创企业家园 31 号 3 层。投标供应商可于开标时间来现场开标，也可通过上海政府采购网开标室远程开标。届时请投标人代表持投标时所使用的数字证书（CA 证书）参加开标。

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

根据上海市财政局《关于上海市政府采购信息管理平台招投标系统正式运行的通知》（沪财采[2014]27 号）的规定，本项目招投标相关活动在上海市政府采购信息管理平台（简称：电子采购平台）（网址：<http://www.zfcg.sh.gov.cn>）电子招投标系统进行。投标人应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知项目负责人进行签收，并及时查看电子采购平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

七、对本次采购提出询问，请按以下方式联系

1.采购人信息

名 称：上海市公安局嘉定分局

地 址：上海市嘉定区永盛路 1300 号

联系方式：021-22172161

联系人：陈诚

2.采购代理机构信息

名 称：上海定佳商务咨询有限公司

地 址：上海市嘉定区嘉罗公路 1661 弄盛创企业家园 31 号 3 层

联系方式：021-69521888

3.项目联系方式

项目联系人：周悦

电 话：021-69521888

第二章 投标人须知

前附表

本附表是对投标人须知说明，与“投标人须知”部分具有同等的法律效力，务请各投标人注意。

序号	内容提要	内容规定
1	项目名称	嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026年度运行维护项目）
2	项目预算	1960000.00元
3	招标文件下载时间、地址	时间：2026-04-10至2026-04-17，每天上午00:00:00~12:00:00，下午12:00:00~23:59:59（北京时间，法定节假日除外） 下载地址：上海政府采购网 www.zfcg.sh.gov.cn
4	书面疑问	书面疑问提交截止时间：报名截止期后一个工作日中午12:00前 书面疑问提交地点：上海市嘉定区嘉罗公路1661弄盛创企业家园31号3层、 dingjiasw@163.com 联系人：周悦 电话：021-69521888
5	答疑会	如有，另行通知
6	投标截止/开标日期、时间、地点	投标截止时间：2026-05-06 10:00:00 开标时间：2026-05-06 10:00:00 投标地点：上海政府采购网（ http://www.zfcg.sh.gov.cn ） 开标地址：上海市嘉定区嘉罗公路1661弄盛创企业家园31号3层。投标供应商可于开标时间来现场开标，

		<p>也可通过上海政府采购网开标室远程开标。届时请投标人代表持投标时所使用的数字证书（CA证书）参加开标。</p> <p>开标所需携带其他材料：可无线上网的并可登陆上海市政府采购信息管理平台的笔记本电脑。注意事项：投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在电子采购平台上的签收情况，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。</p>
7	投标有效期	不少于 90 日历日
8	服务期限	自合同签订之日起至 2026 年 12 月 31 日
9	投标保证金	不收取
10	履约保证金	不收取
11	踏勘现场	不组织，投标人可自行对现场和周围环境进行踏勘
12	分包	<p>本项目是否允许分包</p> <p><input checked="" type="checkbox"/>不允许</p> <p><input type="checkbox"/>允许，具体要求：</p> <p>（1）可以分担保履行的具体内容：_____；</p> <p>（2）允许分包的金额或者比例：_____；</p> <p>（3）接受分包合同企业应具备资格条件（如有）：_____；</p> <p>（4）其他要求：_____。</p>
13	转包	不得转包。

14	政采贷	有需求的供应商可登陆上海市政府采购网政采贷金融服务模块获取“政采贷”信息、在线办理贷款业务。
15	是否专门面向中小企业	不专门面向中小企业
16	小微企业价格扣除百分比	10%
17	采购标的对应的中小企业划分标准所属行业	软件和信息技术服务业
18	代理服务费	<p>本项目的招标代理服务费由中标人支付。代理服务费参照国家计委计价格（2002）1980号文，关于印发《招标代理服务收费管理暂行办法》的通知收费标准规定收取，以中标金额为计费基数。</p> <p>服务招标：100 万以下，1.5%；100-500 万，0.8%。注：采用累进制计价</p>

投标人须知

一、总则

1. 概述

1.1 根据《中华人民共和国政府采购法》、《中华人民共和国招标投标法》等有关法律、法规和规章的规定，本采购项目已具备招标条件。

1.2 本招标文件仅适用于《招标公告》和《投标人须知》前附表中所述采购项目的招标采购。

1.3 招标文件的解释权属于《招标公告》和《投标人须知》前附表中所述的招标人。

1.4 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其它依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

1.5 根据上海市财政局《关于上海市政府采购信息管理平台招投标系统正式运行的通知》（沪财采[2014]27号）的规定，本项目招投标相关活动在上海市政府采购信息管理平台（网址：www.zfcg.sh.gov.cn）电子招投标系统进行。

2. 定义

2.1 “采购项目”系指《投标人须知》前附表中所述的采购项目。

2.2 “服务”系指招标文件规定的投标人为完成采购项目所需承担的全部义务。

2.3 “招标人”系指《投标人须知》前附表中所述的组织本次招标的采购人和代理机构。

2.4 “投标人”系指从招标人处按规定获取招标文件，并按照招标文件向招标人提交投标文件的供应商。

2.5 “中标人”系指中标的投标人。

2.6 “甲方”系指采购人。

2.7 “乙方”系指中标并向采购人提供服务的投标人。

2.8 招标文件中凡标有“★”的条款均系实质性要求条款，投标供应商必须满足的条款。

2.9 “电子采购平台”系指上海市政府采购信息管理平台的门户网站上海政府采购网（www.zfcg.sh.gov.cn），该平台是由市财政局建设和维护。

3. 合格的投标人

3.1 符合《招标公告》中规定的合格投标人所必须具备的资质条件和特定条件。

3.2 《招标公告》规定接受联合体投标的，除应符合本章第 3.1 项要求外，还应遵守以下规定：

（1）联合体各方应按招标文件提供的格式签订联合体协议书，明确联合体各方权利义务；联合体协议书应当明确联合体主办方、由主办方代表联合体参加采购活动；

（2）联合体中有同类资质的供应商按联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级；

（3）招标人根据采购项目的特殊要求规定投标人特定条件的，联合体各方中至少应当有一方符合采购规定的特定条件。

（4）联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

4. 合格的服务

4.1 投标人所提供的服务应当没有侵犯任何第三方的知识产权、技术秘密等合法权利。

4.2 投标人提供的服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准，均有标准的以高（严格）者为准。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采购目的的特定标准确定。

5. 投标费用

不论投标的结果如何，投标人均应自行承担所有与投标有关的全部费用，招标人在任何情况下均无义务和责任承担这些费用。

6. 信息发布

本采购项目需要公开的有关信息，包括招标公告、招标文件澄清或修改公告、中标公告以及延长投标截止时间等与招标活动有关的通知，招标人均将通过“上海政府采购网”（网址：www.zfcg.sh.gov.cn）公开发布。投标人在参与本采购项目

目招投标活动期间，请及时关注以上媒体上的相关信息，投标人因没有及时关注而未能如期获取相关信息，及因此所产生的一切后果和责任，由投标人自行承担，招标人在任何情况下均不对此承担任何责任。

7. 询问与质疑

7.1 投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.2 投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。按照本项目责任分工，质疑事项涉及招标组织程序、中标结果等的，投标人提出质疑的对象为采购代理机构；质疑事项涉及项目采购需求的，投标人提出质疑的对象为采购人；投标人提出质疑但无法区分质疑对象的，先交由采购代理机构梳理区分再行使质疑。其中，对招标文件的质疑，应当在其获得招标文件之日（以电子采购平台上显示的报名时间为准）起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。

投标人应当在法定质疑期内一次性提出针对同一采购程序环节的质疑，超过次数的质疑将不予受理。以联合体形式参加政府采购活动的，其质疑应当由组成联合体的所有供应商共同提出。

7.3 投标人可以委托代理人进行质疑。代理人提出质疑应当提交投标人签署的授权委托书，并提供相应的身份证明。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

7.4 投标人提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

- (1) 供应商的姓名或者名称、地址、邮编、联系人及联系电话
- (2) 质疑项目的名称、编号
- (3) 具体、明确的质疑事项和与质疑事项相关的请求
- (4) 事实依据

(5) 必要的法律依据

(6) 提出质疑的日期

投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖红色公章。

质疑函应当按照招标文件提供的格式填写，范本格式可通过中国政府采购网（<http://www.ccgp.gov.cn>）右侧的“下载专区”下载。

7.5 投标人提起询问和质疑，应当按照《政府采购质疑和投诉办法》（财政部令第94号）等的规定办理。质疑函或授权委托书的内容不符合《投标人须知》第7.3条和第7.4条规定的，招标人将当场一次性告知投标人需要补正的事项，投标人超过法定质疑期未按要求补正并重新提交的，视为放弃质疑。

质疑书的提交方式可以为当面提交、快递、电子邮件等，质疑联系方式详见第八章。

7.6 招标人将在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知提出质疑的投标人和其他有关投标人，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.7 对投标人询问或质疑的答复将导致招标文件变更或者影响招标活动继续进行的，招标人将通知提出询问或质疑的投标人，并在原招标公告发布媒体上发布变更公告。

8. 公平竞争和诚实信用

8.1 投标人在本招标项目的竞争中应自觉遵循公平竞争和诚实信用原则，不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。“腐败行为”是指提供、给予任何有价值的东西来影响采购人员在采购过程或合同实施过程中的行为；“欺诈行为”是指为了影响采购过程或合同实施过程而提供虚假材料，谎报、隐瞒事实的行为，包括投标人之间串通投标等。

8.2 如果有证据表明投标人在本招标项目的竞争中存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为，招标人将拒绝其投标，并将报告政府采购监管部门查处；中标后发现的，中标人须参照《中华人民共和国消费者权益保护法》第55条之条文描述方式双倍赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。

8.3 招标人将在开标后、评标结束前，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站（www.creditchina.gov.cn）失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动。以上信用查询记录，招标人将打印查询结果页面后与其他采购文件一并保存。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

9. 其他

本《投标人须知》的条款如与《投标邀请（招标公告）》、《项目招标需求》和《评标方法与程序》就同一内容的表述不一致的，以《投标邀请（招标公告）》、《项目招标需求》和《评标方法与程序》中规定的内容为准。

二、招标文件

10. 招标文件构成

10.1 招标文件由以下部分组成：

- （1）投标邀请（招标公告）
- （2）投标人须知
- （3）政府采购主要政策
- （4）项目招标需求
- （5）评标方法与程序
- （6）投标文件有关格式
- （7）合同文本
- （8）质疑、未中标结果询问受理要求及附件
- （9）本项目招标文件的澄清、答复、修改、补充内容（如有的话）

10.2 投标人应仔细阅读招标文件的所有内容，并按照招标文件的要求提交

投标文件。如果投标人没有按照招标文件要求提交全部资料，或者投标文件没有对招标文件在各方面作出实质性响应，则投标有可能被认定为无效标，其风险由投标人自行承担。

10.3 投标人应认真了解本次招标的具体工作要求、工作范围以及职责，了解一切可能影响投标报价的资料。一经中标，不得以不完全了解项目要求、项目情况等为借口而提出额外补偿等要求，否则，由此引起的一切后果由中标人负责。

10.4 投标人应按照招标文件规定的日程安排，准时参加项目招投标有关活动。

11. 招标文件的澄清和修改

11.1 任何要求对招标文件进行澄清的投标人，均应在投标截止期 15 天以前，按《投标邀请（招标公告）》中的地址以书面形式（必须加盖投标人单位公章）通知招标人。

11.2 对在投标截止期 15 天以前收到的澄清要求，招标人需要对招标文件进行澄清、答复的；或者在投标截止前的任何时候，招标人需要对招标文件进行补充或修改的，招标人将会通过“上海政府采购网”以澄清或修改公告形式发布。如果澄清或修改的内容可能影响投标文件编制的，且澄清或修改公告发布时间距投标截止时间不足 15 天的，则相应延长投标截止时间。延长后的具体投标截止时间以最后发布的澄清或修改公告中的规定为准。

11.3 澄清或修改公告的内容为招标文件的组成部分。当招标文件与澄清或修改公告就同一内容的表述不一致时，以最后发出的文件内容为准。

11.4 招标文件的澄清、答复、修改或补充都应由采购代理机构以澄清或修改公告形式发布和通知，除此以外的其他任何澄清、修改方式及澄清、修改内容均属无效，不得作为投标的依据，否则，由此导致的风险由投标人自行承担，招标人不承担任何责任。

11.5 招标人召开答疑会的，所有投标人应根据招标文件或者招标人通知的要求参加答疑会。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。

12. 踏勘现场

12.1 招标人组织踏勘现场的，所有投标人应按《投标人须知》前附表规定

的时间、地点前往参加踏勘现场活动。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。招标人不组织踏勘现场的，投标人可以自行决定是否踏勘现场，投标人需要踏勘现场的，招标人应为投标人踏勘现场提供一定方便，投标人进行现场踏勘时应当服从招标人的安排。

12.2 投标人踏勘现场发生的费用由其自理。

12.3 招标人在现场介绍情况时，应当公平、公正、客观，不带任何倾向性或误导性。

12.4 招标人在踏勘现场中口头介绍的情况，除招标人事后形成书面记录、并以澄清或修改公告的形式发布、构成招标文件的组成部分以外，其他内容仅供投标人在编制投标文件时参考，招标人对投标人据此作出的判断和决策负责。

三、投标文件

13. 投标的语言及计量单位

13.1 投标人提交的投标文件以及投标人与招标人就有关投标事宜的所有来往书面文件均应使用中文。除签名、盖章、专用名称等特殊情形外，以中文以外的文字表述的投标文件视同未提供。

13.2 投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，一律采用中华人民共和国法定计量单位（货币单位：人民币元）。

14. 投标有效期

14.1 投标文件应从开标之日起，在《投标人须知》前附表规定的投标有效期内有效。投标有效期比招标文件规定短的属于非实质性响应，将被认定为无效投标。

14.2 在特殊情况下，在原投标有效期期满之前，招标人可书面征求投标人同意延长投标有效期。投标人可拒绝接受延期要求而不会导致投标保证金被没收。同意延长有效期的投标人需要相应延长投标保证金的有效期，但不能修改投标文件。

14.3 中标人的投标文件作为项目服务合同的附件，其有效期至中标人全部合同义务履行完毕为止。

15. 投标文件构成

15.1 投标文件由商务响应文件（包括相关证明文件）和技术响应文件二部分构成。

15.2 商务响应文件（包括相关证明文件）和技术响应文件应具体包含的内容，以第四章《项目招标需求》规定为准。

16. 商务响应文件

16.1 商务响应文件由以下部分组成：

- (1) 《投标函》；
- (2) 《开标一览表》（以电子采购平台设定为准）；
- (3) 《投标报价分类明细表》等相关报价表格详见第六章《投标文件有关格式》；
- (4) 《资格条件响应表》以及《符合性要求响应表》；
- (5) 《与评标有关的投标文件主要内容索引表》；
- (6) 第四章《项目招标需求》规定的其他内容；
- (7) 相关证明文件（投标人应按照《项目招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同）。

17. 投标函

17.1 投标人应按照招标文件中提供的格式完整地填写《投标函》。

17.2 投标文件中未提供《投标函》的，为无效投标。

18. 开标一览表

18.1 投标人应按照招标文件和电子采购平台电子招投标系统提供的投标文件格式完整地填写《开标一览表》，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

18.2 《开标一览表》是为了便于招标人开标，《开标一览表》内容在开标时将当众公布。

18.3 投标人未按照招标文件和电子采购平台电子招投标系统提供的投标文件格式完整地填写《开标一览表》、或者未提供《开标一览表》，导致其开标不成功的，其责任和风险由投标人自行承担。

19. 投标报价

19.1 投标人应当按照国家和上海市有关行业管理服务收费的相关规定，结合自身服务水平和承受能力进行报价。投标报价应是履行合同的最终价格，除《项目招标需求》中另有说明外，投标报价应当是投标人为提供本项目所要求的全部服务所发生的一切成本、税费和利润，包括人工（含工资、社会统筹保险金、加班工资、工作餐、相关福利、关于人员聘用的费用等）、设备、国家规定检测、外发包、材料（含辅材）、管理、税费及利润等。

19.2 报价依据：

- （1）本招标文件所要求的服务内容、服务期限、工作范围和要求。
- （2）本招标文件明确的服务标准及考核方式。
- （3）其他投标人认为应考虑的因素。

19.3 投标人提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。

19.4 除《项目招标需求》中说明并允许外，投标的每一种单项服务的报价以及采购项目的投标总价均只允许有一个报价，投标文件中包含任何有选择的报价，招标人对于其投标均将予以拒绝。

19.5 投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，招标人均将予以拒绝。

19.6 投标人应按照招标文件第六章提供的格式完整地填写各类报价分类明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

19.7 投标应以人民币报价。

20. 资格条件及符合性要求响应表

20.1 投标人应当按照招标文件所提供格式，逐项填写并提交《资格条件响应表》及《符合性要求响应表》，以证明其投标符合招标文件规定的所有合格投标人资格条件及实质性要求。

21. 与评标有关的投标文件主要内容索引表

21.1 投标人应按照招标文件提供的格式完整地填写《与评标有关的投标文件主要内容索引表》。

21.2 《与评标有关的投标文件主要内容索引表》是为了便于评标。《与评

标有关的投标文件主要内容索引表》与投标文件其他部分就同一内容的表述应当一致，不一致时按照《投标人须知》第 30 条“投标文件内容不一致的修正”规定处理。

22. 技术响应文件

22.1 投标人应按照《项目招标需求》的要求编制并提交技术响应文件，对招标人的技术需求全面完整地做出响应并编制服务方案，以证明其投标的服务符合招标文件规定。

22.2 技术响应文件可以是文字资料、表格、图纸和数据等各项资料，其内容应包括但不限于人力、物力等资源的投入以及服务内容、方式、手段、措施、质量保证及建议等。

23. 投标文件的编制和签署

23.1 投标人应按照招标文件和电子采购平台电子招投标系统要求的格式填写相关内容。

23.2 投标文件中凡招标文件要求签署、盖章之处，均应由投标人的法定代表人或法定代表人正式授权的代表签署和加盖红色公章。投标人应写明全称。如果是由法定代表人授权代表签署投标文件，则必须按招标文件提供的格式出具《法定代表人授权委托书》并将其附在投标文件中。投标文件若有修改错漏之处，须加盖投标人公章或者由法定代表人或法定代表人授权代表签字或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人自负。

其中对《投标函》、《开标一览表》、《法定代表人授权委托书》、《资格条件响应表》、《符合性要求响应表》以及《财务状况及税收、社会保障资金缴纳情况声明》、《无重大违法记录的声明》，投标人未按照上述要求显示公章的，其投标无效。

23.3 建设节约型社会是我国落实科学发展观的一项重大决策，也是政府采购应尽的义务和职责，需要政府采购各方当事人在采购活动中共同践行。目前，少数投标人制作的投标文件存在编写繁琐、内容重复的问题，既增加了制作成本，浪费了宝贵的资源，也增加了评审成本，影响了评审效率。为进一步落实建设节约型社会的要求，提请投标人在制作投标文件时注意下列事项：

(1) 评标委员会主要是依据投标文件中技术、质量以及售后服务等指标来

进行评定。因此，投标文件应根据招标文件的要求进行制作，内容简洁明了，编排合理有序，与招标文件内容无关或不符合招标文件要求的资料不要编入投标文件。

(2) 投标文件应规范，应按照规定格式要求规范填写，扫描文件应清晰简洁、上传文件应规范。

四、投标文件的递交

24. 投标文件的递交

24.1 投标人应按照招标文件规定，参考第六章投标文件有关格式，在电子采购平台电子招投标系统中按照要求填写和上传所有投标内容。投标的有关事项应根据电子采购平台规定的要求办理。

24.2 投标文件中含有红色公章，防伪标志和彩色底纹类文件（如《投标函》、营业执照、身份证、认证证书等）应清晰显示。如因上传、扫描、格式等原因导致评审时受到影响，由投标人承担相应责任。

招标人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供，否则视作投标人放弃潜在中标资格，并且招标人将对投标人进行调查，发现有欺诈行为的按有关规定进行处理。

24.3 投标人应充分考虑到网上投标可能会发生的技术故障、操作失误和相应的风险。对因网上投标的任何技术故障、操作失误造成投标人投标内容缺漏、不一致或投标失败的，招标人不承担任何责任。

25. 投标截止时间

25.1 投标人必须在《投标邀请（招标公告）》规定的网上投标截止时间前将投标文件在电子采购平台电子招投标系统中上传并正式投标。

25.2 在招标人按《投标人须知》规定酌情延长投标截止期的情况下，招标人和投标人受投标截止期制约的所有权利和义务均应延长至新的截止时间。

25.3 在投标截止时间后上传的任何投标文件，招标人均将拒绝接收。

26. 投标文件的修改和撤回

在投标截止时间之前，投标人可以对在电子采购平台电子招投标系统已提交的投标文件进行修改和撤回。有关事项应根据电子采购平台规定的要求办理。

五、开标

27. 开标

27.1 招标人将按《投标邀请（招标公告）》或《延期公告》（如果有的话）中规定的时间在电子采购平台上组织公开开标。

27.2 开标程序在电子采购平台进行，所有上传投标文件的供应商应登录电子采购平台参加开标。开标主要流程为签到、解密、唱标和签名，每一步骤均应按照电子采购平台的规定进行操作。

27.3 投标截止，电子采购平台显示开标后，投标人进行签到操作，投标人签到完成后，由招标人解除电子采购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。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。

如电子采购平台开标程序有变化的，以最新的操作程序为准。

27.4 投标文件解密后，电子采购平台根据投标文件中《开标一览表》的内容自动汇总生成《开标记录表》。

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。

六、评标

28. 评标委员会

28.1 招标人将依法组建评标委员会，评标委员会由采购人代表和上海市政府采购评审专家组成，其中专家的人数不少于评标委员会成员总数的三分之二。

28.2 评标委员会负责对投标文件进行评审和比较，并向招标人推荐中标候选人。

29. 投标文件的资格审查及符合性审查

29.1 开标后，招标人将依据法律法规和招标文件的《投标人须知》及资格条件对投标人进行资格审查。确定符合资格的投标人不少于3家的，将组织评标

委员会进行评标。

29.2 在详细评标之前，评标委员会要对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。评标委员会只根据投标文件本身的内容来判定投标文件的响应性，而不寻求外部的证据。

29.3 符合性审查未通过的投标文件不参加进一步的评审，投标人不得通过修正或撤销不符合要求的偏离或保留从而使其投标成为实质上响应的投标。

29.4 开标后招标人拒绝投标人主动提交的任何澄清与补正。

29.5 招标人可以接受投标文件中不构成实质性偏差的小的不正规、不一致或不规范的内容。

30. 投标文件内容不一致的修正

30.1 投标文件内容出现前后不一致的，按照下列规定修正：

(1)《开标记录表》内容与投标文件中相应内容不一致的，以《开标记录表》内容为准；

(2) 投标文件的大写金额和小写金额不一致的，以大写金额为准；

(3) 单价金额小数点或者百分比有明显错位的，以开标记录表的总价为准，并修改单价；

(4) 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照上述规定的顺序修正。修正后的内容经投标人确认后产生约束力，投标人不确认的，其投标无效。

30.2 投标文件中如果有其他错误或矛盾（明显的文字和计算错误除外），将按不利于出错投标人的原则进行处理，即对于错误或矛盾的内容，评标时按照对出错投标人不利的情形进行评分；如出错投标人中标，签订合同时按照对出错投标人不利、对采购人有利的条件签约。

31. 投标文件的澄清

31.1 对于投标文件中含义不明确或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清。投标人应按照招标人通知的时间和地点委派授权代表向评标委员会作出说明或答复。

31.2 投标人对澄清问题的说明或答复，还应以书面形式提交给招标人，并应由投标人授权代表签字。

31.3 投标人的澄清文件是其投标文件的组成部分。

31.4 投标人的澄清不得超出投标文件的范围或者改变其投标文件的实质性内容，不得通过澄清而使进行澄清的投标人在评标中更加有利。

32. 投标文件的评价与比较

32.1 评标委员会只对被确定为实质上响应招标文件要求的投标文件进行评价和比较。

32.2 评标委员会根据《评标方法与程序》中规定的方法进行评标，并向招标人提交书面评标报告和推荐中标候选人。

33. 评标的有关要求

33.1 评标委员会应当公平、公正、客观，不带任何倾向性，评标委员会成员及参与评标的有关工作人员不得私下与投标人接触。

33.2 评标过程严格保密。凡是属于审查、澄清、评价和比较有关的资料以及授标建议等，所有知情人均不得向投标人或其他无关的人员透露。

33.3 任何单位和个人都不得干扰、影响评标活动的正常进行。投标人在评标过程中所进行的试图影响评标结果的一切不符合法律或招标规定的活动，都可能导致其投标被拒绝。

33.4 招标人和评标委员会均无义务向投标人做出有关评标的任何解释。

34. 异常低价投标审查

34.1 评标中出现下列情形之一的，评标委员会应当启动异常低价投标审查程序：

(1) 投标报价低于全部通过符合性审查投标人投标报价平均值 50%的，即 $\text{投标报价} < \text{全部通过符合性审查投标人投标报价平均值} \times 50\%$ ；

(2) 投标报价低于通过符合性审查的次低报价投标人投标报价 50%的，即 $\text{投标报价} < \text{通过符合性审查的次低报价投标人投标报价} \times 50\%$ ；

(3) 投标报价低于采购项目最高限价 45%的，即 $\text{投标报价} < \text{采购项目最高限价} \times 45\%$ ；

(4) 评标委员会基于专业判断，认为投标人报价过低，有可能影响产品质量或者不能诚信履约的其他情形。

34.2 评标委员会启动异常低价投标审查后，属于前述第（1）项至第（4）项情形的，应当要求相关投标人在评标现场合理的时间内对投标价格作出解释，

提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等。其中，属于第（3）项情形，投标人已随投标文件一并提交相关书面说明及必要的证明材料的，在评标现场可不再重复提交。

34.3 投标人在编制投标文件时认为自身报价可能存在前述第(1)项至第(4)项情形的，可提前准备相关书面说明及必要的证明材料，以便按照评标委员会要求在规定的时间内提供。属于第（3）项情形的，投标人可随投标文件一并提交相关书面说明及必要的证明材料。

34.4 投标人不能按时提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

七、定标

35. 确认中标人

除了《投标人须知》第 37 条规定的招标失败情况之外，采购人将根据评标委员会推荐的中标候选人及排序情况，依法确认本采购项目的中标人。

36. 中标公告及中标和未中标通知

36.1 采购人确认中标人后，招标人将在两个工作日内通过“上海政府采购网”发布中标公告，公告期限为一个工作日。

36.2 中标公告发布后，招标人将及时向中标人发出《中标通知书》通知中标，向其他未中标人发出《中标结果通知书》。《中标通知书》对招标人和投标人均具有法律约束力。

37. 投标文件的处理

所有在开标会上被接受的投标文件都将作为档案保存，不论中标与否，招标人均不退回投标文件。

38. 招标失败

在投标截止后，参加投标的投标人不足三家；在资格审查时，发现符合资格条件的投标人不足三家的；或者在评标时，发现对招标文件做出实质性响应的投标人不足三家，评标委员会确定为招标失败的，招标人将通过“上海政府采购网”发布招标失败公告。

八、授予合同

39. 合同分包

39.1 在采购人允许项目非主体、非关键性工作分包的前提下，投标供应商拟中标后采取分包方式履行合同的，必须在投标（响应）文件中提供完整准确《分包意向协议书》。

39.2 接受分包合同的中小企业与分包企业（投标供应商）之间不得存在直接控股、管理关系。

39.3 接受分包合同的企业不得再次分包。

39.4 《中小企业声明函》中需要填写分包企业与接受分包合同企业的相关信息。

40. 合同授予

除了中标人无法履行合同义务之外，招标人将把合同授予根据《投标人须知》第34条规定所确定的中标人。

41. 签订合同

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。

42. 其他

电子采购平台有关操作方法可以参考电子采购平台（网址：www.zfcg.sh.gov.cn）中的“在线服务”专栏。

第三章 政府采购主要政策

根据政府采购法，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，促进中小企业发展等。对列入财政部、发展改革委、生态环境部等部门发布的“节能产品、环境标志产品品目清单”且属于应当强制采购的产品，按照规定实行强制采购。对列入财政部、发展改革委、生态环境部等部门发布的“节能产品、环境标志产品品目清单”优先采购的产品；对于参与投标的中小企业、监狱企业以及福利企业，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。

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。

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。关于中小企业的判定依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）等文件执行。

在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的中小企业扶持政策：（一）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；（二）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；（三）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。在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受办法规定的中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，

以及预留份额项目中的非预留部分采购包,对符合本办法规定的小微企业报价给予 10%的扣除,用扣除后的价格参加评审。

接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目,对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的,采购人、采购代理机构应当对联合体或者大中型企业的报价给予 4%的扣除,用扣除后的价格参加评审。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。

组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的,不享受价格扣除优惠政策。在政府采购活动中,监狱企业和残疾人福利性单位视同小型、微型企业,监狱企业应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件,残疾人福利性单位应当提供《残疾人福利性单位声明函》。

中小企业参加政府采购活动,应当出具《政府采购促进中小企业发展管理办法》(财库〔2020〕46号)规定的《中小企业声明函》,否则不得享受相关中小企业扶持政策。

第四章 项目招标需求

一、项目基本情况

项目名称：嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026 年度运行维护项目）

招标金额：人民币 1960000.00 元

服务周期：自合同签订之日起至 2026 年 12 月 31 日。

项目概况：项目运维内容包括智能分析系统、视讯通系统、嘉定分局数字化勤务系统、智能图像算力支撑和功能开发配套系统、智能图像防控能力支撑配套系统、AR 全景超融合系统和视频监控轻应用配套系统、基于全局智能视频监控的动态应用服务系统、融合承载网、防控中心配套系统、网络升级服务、感知网分控中心安全加固、安全管理平台及配套设备升级、感知网安全监测、运维系统、嘉定分局视频图像能力及共享平台，共计 15 个子系统。

二、项目背景

由于整体项目将质保到期，为保障后续使用的可靠性，亟需由专业单位提供系统的维护保养服务，确保系统正常运行，延长系统的使用寿命。

本次招标旨在筛选具备专业技术能力、丰富运维经验及完善服务体系的运维服务供应商，为嘉定公安智慧安防体系提供全方位、高质量的运维服务，保障各系统模块持续稳定运行，提升系统应急处置能力与综合应用效能，支撑公安业务高效开展。

三、运维服务内容及清单

本项目运维服务范围涵盖 15 个子系统/模块，具体包括：

- 1.智能分析系统
- 2.视讯通系统
- 3.嘉定分局数字化勤务系统
- 4.智能图像算力支撑和功能开发配套系统
- 5.智能图像防控能力支撑配套系统
- 6.AR 全景超融合系统和视频监控轻应用配套系统
- 7.基于全局智能视频监控的动态应用服务系统

- 8.融合承载网
- 9.防控中心配套系统
- 10.网络升级服务
- 11.感知网分控中心安全加固
- 12.安全管理平台及配套设备升级
- 13.感知网安全监测
- 14.运维系统
- 15.嘉定分局视频图像能力及共享平台

上述子系统/模块作为核心基础设施，其质保期逐渐到期，为保障长效运行、减小故障概率，需建立长效维护制度，结合现有技术优化运行方案，全面落实运维工作。

（一）智能分析系统

智能分析系统是用于对视频/图像等数据进行信息提取、存储与智能分析，实现数据检索等功能。

系统主要分为两大模块：

1.信息提取设备

负责从原始数据中提取信息。包含智能分析节点、任务策略节点、资源调度节点、运行检测节点、流量控制节点、算法调度节点，协同完成特征提取、任务分配、资源调度、流量管控与算法调度。

2.信息存储设备

负责存储提取后的信息数据，支撑后续检索与分析。按类型与数据维度分类存储，保障数据高效检索。

具体运维内容包含 6 台智能分析节点、1 台任务策略节点、3 台资源调度节点、1 台运行检测节点、7 台流量控制节点、3 台算法调度节点、17 台信息存储设备、7 台多维信息存储设备、16 台二维信息存储设备。

运维服务要求

围绕硬件、软件、网络三大核心维度开展运维工作，硬件层面定期检查设备状态、备份数据并保障机房环境稳定；软件层面监控节点运行、更新算法补丁并

优化资源调度；网络层面保障带宽稳定并配置安全策略，同时做好运维日志记录与应急预案制定，全方位保障系统稳定高效运行。

（二）视讯通系统

视讯通是一套视频资源安全与转发管理系统，核心用于视频数据的安全传输、统一管理与可靠分发，保障视频流的安全、稳定、高效流转。

系统核心设备及作用：

1. 综合型视频资源安全网关：负责视频数据的安全接入、加密传输、访问控制，是系统的安全“门户”。

2. 视频转发管理设备：实现视频流的统一调度、分发与管理，支持多终端、多平台的视频调用。

3. 数据转发管理设备：负责视频及相关数据的转发、缓存与路由优化，提升数据传输效率。

4. 128G 存储卡+电池：为前端视频采集设备提供本地存储与断电续航，保障数据不丢失、设备持续运行。

具体运维内容包含 2 台综合型视频资源安全网关设备、1 台视频转发管理设备、一台数据转发管理设备、1800 台 128G 内存卡、1800 台电池。

运维服务要求

需围绕系统的硬件、软件、网络及日常管理四大板块展开，硬件上定期检查网关、转发设备等硬件状态，维护存储卡与电池，保障供电稳定；软件上监控视频转发与数据传输服务，更新安全策略和系统补丁，优化转发调度策略；网络上保障带宽稳定，配置安全防护策略，排查链路故障；同时做好运维日志记录、应急预案制定及前端设备巡检工作，全面保障系统稳定高效运行。

（三）嘉定分局数字化勤务系统

嘉定分局的数字化勤务管理系统，核心是通过数字化手段实现勤务工作的流程化、智能化、可视化，提升警务勤务的管理效率与响应能力。

系统核心模块及作用：

1. 勤务业务（数据汇聚清洗、基础支撑、勤务事前、勤务服务赋能）：负责勤务数据的统一汇聚、清洗与标准化，提供基础技术支撑；覆盖勤务事前规划、事中执行、事后赋能全流程，实现勤务任务的智能分配、资源调度与效果评估。

2. 用户及权限：实现系统用户的身份认证、权限分级管理，保障数据安全与操作合规。

3. 技术架构及引擎：作为系统底层支撑，提供稳定的运行环境、数据处理引擎与接口能力，保障各模块高效协同。

4. 嘉定“e嘉人”轻应用：面向民警、群众的轻量化应用，实现勤务信息查询、业务办理、便民服务等功能，提升警务服务的便捷性。

5. 轻应用和隐患清零：通过轻量化应用快速落地勤务场景，同时实现安全隐患的排查、上报、整改与闭环管理，保障勤务安全。

运维服务要求

本次运维需聚焦勤务相关系统，从系统、数据、应用及日常管理四个维度开展工作，系统运维需监控模块运行、更新优化系统并管控用户权限；数据运维要保障数据汇聚清洗的准确实时，做好备份恢复并优化存储查询效率；应用运维需确保轻应用正常访问，推动隐患清零全流程闭环；同时完善运维日志、应急预案并定期巡检评估，全面保障勤务工作高效稳定开展。

（四）智能图像算力支撑和功能开发配套系统

智能图像算力支撑与功能开发配套任务，核心是为视频图像业务提供底层算力、软件授权与上层应用开发能力，支撑视频流解析、基础应用、智能大数据分析等全链路功能落地。

核心内容及作用：

1. 视频流全解析软件授权：提供视频流解析的软件许可，支持对各类视频流进行解码、解析等基础处理，是智能图像应用的“入口”。

2. 视频图像基础应用模块：开发视频图像的基础功能，如实时预览、录像回放、云台控制、告警联动等，满足日常视频监控的基础操作需求。

3. 视频图像智能大数据应用模块：基于算力与解析能力，开发智能分析与大

数据应用，如数据检索、态势研判等，实现视频数据的深度挖掘与价值转化。

运维服务要求

本次运维要求围绕视频解析与智能分析类系统展开，涵盖软件与授权、算力与模块、数据与应用三大核心运维维度，软件与授权层面需监控授权有效性、更新版本补丁并优化配置参数；算力与模块层面要管控算力资源、保障模块稳定运行并优化协同效率；数据与应用层面需保障数据质量、做好备份恢复并优化模型算法，同时完善运维日志、应急预案制定及定期性能评估工作，全面保障系统稳定运行并提升业务支撑价值。

（五）智能图像防控能力支撑配套系统

智能图像防控能力支撑配套任务，核心是为安防场景提供基于智能图像的防控管理能力，实现安全管控。

核心内容及作用：

1. 防控中心管理服务：作为系统的中枢管理平台，负责防控策略的统一配置、下发、监控与管理，实现全市/区域级防控的集中管控。
2. 防控轻应用 - 应用功能：面向一线人员的轻量化应用，提供便捷的防控操作，支持一键防控、分区防控、定时防控等功能，提升防控操作效率。

运维服务要求

运维要求围绕智能防控能力支撑系统展开，从平台与应用、防控管理、数据与安全及日常管理与应急四个维度推进工作，平台与应用层面需监控服务与轻应用运行、更新版本补丁；防控管理层面要保障智能分析与告警功能正常、优化防控策略并推动告警处置闭环；数据与安全层面需监控数据采集存储、做好数据备份并强化安全防护；同时完善运维日志记录、应急预案制定及定期巡检评估，全面保障系统稳定运行与安防管控效能。

（六）AR 全景超融合系统和视频监控轻应用配套系统

AR 全景超融合系统是通过 AR 技术实现全景可视化监控，实现“全景可视、

一键调看、快速处置”。

通过接入分局建设的前端 AR 全景摄像机视频，实现视频联动、录像回溯、视频地图、移动警力可视化、视觉展示、标签配置、自动标签下载导入、系统管理等多种功能。

通过建设区级以及市级的 **AR 全景超融合系统**，实现分局与市局的系统级联，并通过对接实现接入市局现有系统，满足全市各分局指挥中心用户的使用，全面提高全市公安用户在实战指挥工作中的感知能力、预警研判能力和应急处置能力。

1. AR 全景超融合系统

- 业务应用开发：开发 AR 全景核心业务功能，如全景拼接、AR 标签标注、定位、事件联动、态势展示等，实现“一张图”全景监控。
- 系统管理开发：开发系统后台管理功能，包括设备管理、权限管理、配置管理、日志管理等，保障系统稳定运行与安全管控。
- 系统对接开发：实现与现有视频监控平台、物联网设备、应急指挥系统等对接，打通数据与业务链路，实现跨系统协同。

2. 视频监控轻应用

- 应用功能软件：面向一线人员的轻量化前端应用，提供实时预览、录像回放、云台控制、告警查看、一键呼叫等便捷操作，支持移动端/网页端快速访问。
- 后台管理软件：轻应用的后台管理模块，负责用户管理、权限分配、设备配置、告警策略设置等，实现轻应用的统一管理。
- 系统对接软件：实现轻应用与 AR 全景超融合系统、智能图像系统、告警系统等对接，确保数据互通、功能联动。

运维服务要求

运维需要围绕 AR 全景超融合监控系统展开，从系统与应用、对接与数据、性能与安全及日常管理与应急四个维度开展工作，系统与应用层面需监控各模块及轻应用运行、更新版本补丁；对接与数据层面要保障系统与外部平台数据传输畅通、校验数据准确性并做好数据备份；性能与安全层面需监控核心性能指标、强化安全防护并优化算法与转发策略；同时完善运维日志记录、应急预案制定及

定期巡检评估，全面保障系统稳定运行与监控指挥效能。

（七）基于全局智能视频监控的动态应用服务系统

目前，市局依托已建成的智能图像基础应用框架，包括智能图像综合应用系统（PC 端）、移动服务应用基础版（涵盖用户身份验证、静态特征比对、基础信息查询、备案信息调取、数据溯源标识、预警信息展示等功能），已完成对各分局现有智能分析子系统解析整合复用，并与对应对象关联特征数据建立映射关系，形成标准化的个体特征档案。该建设成果有效支撑全市各业务部门通过智能图像 PC 端及移动服务应用。

运维服务要求

运维需要围绕全局智能视频监控系统展开，从数据采集与归档、解析与应用、数据安全与权限及日常管理与应急四个维度开展工作，数据采集归档层面需监控提取上传状态、校验归档数据质量并管理存储资源；解析应用层面要保障模块运行、优化算法参数并支撑数据联动应用；数据安全权限层面需加密存储传输数据、审计权限操作并强化安全防护；同时完善运维日志记录、应急预案制定及定期性能评估，全面保障系统稳定合规运行与安防业务支撑能力。

（八）融合承载网

市局融合承载网项目，嘉定分局负责配套设备：2 套汇聚层设备和 2 套接入层设备。满足市局业务的高带宽、多接口、稳定可靠的传输需求，构建分层级、高适配的融合承载传输链路，支撑全局视频监控、数据交互、业务系统联动等全场景网络传输。

1. 每套汇聚层设备配置如下：

- 平台（主设备），包含：电子架+交叉板+光层
- 线路侧端口配置需求：2 波 100G+2 波 10G
- 业务侧端口配置：32*E1+16*STM1+10*FE+5*GE+4*10GE

2. 每套接入层设备配置如下：

- 平台（主设备），包含：电子架+交叉板+光层

- 线路侧端口配置需求：4波 10G
- 业务侧端口配置：32*E1+6*STM1+10*FE+5*GE+4*10G

运维服务要求

运维需要围绕光传输设备系统展开，涵盖硬件、传输性能、配置调度、保修故障及环境安全五大维度，硬件层面定期巡检核心部件并储备备件；传输性能层面实时监控带宽、误码率等指标并优化资源分配；配置调度层面做好参数备份并按需调整调度策略；建立故障快速报修通道，及时响应现场故障；环境安全层面保障设备运行环境稳定并强化物理与接入安全防护，全面保障光传输系统稳定可靠运行。

（九）防控中心配套系统

基于“一中心一平台”建设，为防控系统提供业务支撑、平台管理与系统对接能力，实现防控业务的统一管理、高效运行与跨系统协同。

核心内容及作用：

1. 业务服务：为防控业务提供底层支撑，包括数据服务、算法服务、接口服务等，保障防控业务稳定运行、数据流转畅通。
2. 对接平台资源管理：统一管理与防控中心对接的各类平台资源（如视频监控平台、智能图像平台、指挥平台等），实现资源的统一接入、配置与调度。
3. 对接现有系统：实现防控中心与现有业务系统（如警务系统、智能图像系统、指挥调度系统等）的对接，打通数据与业务链路，实现跨系统协同处置。

运维服务要求

运维需要围绕防控系统展开，从业务、服务与资源、系统对接及安全与日常管理四个维度推进工作，业务层面监控防控模块运行；服务与资源层面保障业务服务稳定、管理对接平台资源并优化调度分配；系统对接层面监控链路状态、校验数据准确性并做好配置备份；同时强化安全防护策略、完善运维日志记录与应急预案制定，全面保障防控系统稳定高效运行与业务安全。

（十）网络升级服务

本次网络升级服务涵盖感知网扩容、分局光网扩容及通信链路三大核心板块，运维工作整体遵循“预防为主、防抢结合”“预检预修”原则，围绕各系统全流程运维需求，多维度筑牢运行保障防线，确保网络系统稳定、高效、安全运转，持续支撑公安各类业务（含现有业务及多媒体宽带等新业务）24小时不间断开展。

感知网扩容需要维护的内容包括：在汇聚层至核心层8个40GB光口和40G万兆接口板的运维工作。在徐行派出所、南翔派出所、安亭派出所三个网络节点6台现有交换机上各有一块40G万兆接口板，共有10km单模40G光模块4块，40km单模40G长距光模块44块，万兆接入交换机8台。

分局光网扩容需要维护的内容包括：对嘉定分局大楼网络2台核心交换机、15台接入交换机的运维工作。

通信链路需要维护的内容为嘉定分局至南翔分控点的光缆链路。

运维服务要求

具体运维要求聚焦四大核心方向推进：一是保障感知网系统，从线路系统、系统状态、网络系统、日常设施设备维度开展维护；二是保障分局光网系统，围绕硬件、传输性能、保修故障、环境安全维度推进工作；三是保障光缆传输链路，从线路物理、光链路性能、敷设环境与安全、台账与应急管理维度落实责任；四是建立健全全流程运维管理体系，完善巡检、测试、维护及应急处理机制，及时消除各类安全隐患，保持设施设备及线路完整良好。

（十一）感知网分控中心安全加固

感知网分控中心安全加固运维，核心围绕边界防火墙（含分局及各派出所分控与数据中心边界、分控中心数据缓存区边界）、安全管理平台及配套流量采集、探针等设备系统开展，整体目标是筑牢分控中心与数据中心、感知网内网的安全防线，保障各类安全设备与平台稳定运行，为公安业务数据传输、安全预警等工作提供可靠支撑。

运维服务要求

运维工作重点从两大维度推进：一是聚焦边界防护设备，围绕日常监控与巡

检、配置与升级管理、故障处置及安全管理四大方向，建立完善的监报告警、变更管理和安全管控体系，确保访问控制、透明部署等安全策略有效落地；二是聚焦安全管理平台及配套设备，从硬件运行、软件功能、数据安全三大维度落实运维责任，健全监控预警、备份恢复、安全审计机制。同时，全面排查各类安全隐患，保障全链路安全设备协同运转，持续提升分控中心安全防护能力。

（十二）安全管理平台及配套设备升级

系统采用技术+服务方式开展嘉定公安节点数据共享及数据安全防护方案设计，具体包括先进的零信任数据安全架构、数据安全采集分析及数据安全渗透服务。

（1）在数据中心部署零信任核心组件包括：可信应用代理 TAP、可信访问控制台 TAC、可信终端环境感知系统 TESS。

（2）部署数据安全态势感知系统，系统基于“持续自适应风险与信任评估（CARTA）”的安全理念，使用统一的数据安全态势感知平台，构建面向数据安全的四个核心能力，即发现能力、防护能力、检测能力、响应能力。

（3）配备专业的安全服务人员，通过远程或现场渗透方式，开展数据安全风险评估，发现潜在的数据安全防护薄弱点。

具体运维内容包含 1 台统一身份认证网关、2 套控制中心、2 台可信访问网关、2 台数据采集器、1 套数据安全分析平台。

运维服务要求

运维要求围绕数据安全与身份认证类系统展开，从设备、功能、安全三个维度推进工作，建立完善的监控预警、安全防护和审计追溯体系，全面保障系统稳定、合规运行。

（十三）感知网安全监测

具体运维内容包含 3 台 40G 安全监测设备、5 台 40G 安全监测控制设备、18 台 20G 安全监测设备、5 台 20G 安全监测控制设备、2 台流量监测主机。

运维服务要求

运维要求围绕安全监测类设备系统展开，从硬件、性能与功能、数据与安全三个维度开展工作，硬件层面定时巡检、定时进行全面检测相关设备状态并储备配件，同时保障设备部署环境与供电稳定；性能与功能层面实时监控设备重要指标，定期更新安全策略与特征库，确保各项核心功能及分析成功率达标；数据与安全层面监控数据全流程状态，定期开展安全审计并留存操作日志，全面保障系统稳定安全运行。

（十四）运维系统

通过运维管理系统的建设，已实现对视频图像资源的建设、使用和运行维护状况进行有效管理和评价，从而推进与督导公安视频监控系统的建设与维护工作，同时满足公安部门及上级单位对日常维护工作的综合考核需求。

运维服务要求

运维要求围绕运维管理系统展开，从系统运行、功能、数据安全三个维度推进工作，需实时监控系统运行状态并定期更新补丁、优化性能，保障设备监控、日志管理等核心功能正常运行且日志留存达标、报表导出成功率 100%，同时对系统数据加密防护并按季度开展安全扫描，全面保障系统稳定、安全运行。

（十五）嘉定分局视频图像能力及共享平台

具体运维内容包含 1 台能共享管理网关节点、4 台多协议视频共享转发节点、1 台感知设备信息采集节点、3 台公安城市快照管理节点、1 台城市快照轮巡节点、5 台精细化场景分析节点。

运维服务要求

运维要求围绕视频汇聚共享与智能分析平台展开，从硬件、软件与功能、数据与安全三个维度开展工作。硬件要求定时检测节点设备状态，确保低故障率与稳定供电散热；软件需实时监控各项功能，确保接入成功与系统畅通；数据与安全则强调备份监控、权限管控与审计，保证数据完整与访问安全，全面保障平台稳定高效、安全合规运行。

四、运维服务设备型号主要参数

序号	项目名称	详细描述	数量	单位	型号
一	智能分析系统				
1	智能分析节点	Intel 至强可扩展系列处理器;16GBDDR4 x 12;24 根 DDR4 ECC RDIMM 插槽;1 个 480GB SSD;系统兼容 Cent os 7.x 最大支持 8 块 3.5/2.5 寸 SATA 硬盘或 SSD, 支持热插拔;前置 2 个 USB3.0 接口, 后置 2 个 USB3.0 接口;4 个千兆自适应网络接口 支持对视频、图片进行信息的全分析	6	台	DS-IF2006-A3 H/NF
2	任务策略节点	支持高性能多核处理器, 高速 UPI 互连总线(10.4/9.6 GT/s, 依 CPU 型号不同而不同),大容量三级缓存(15/20/25/30/35 MB, 依 CPU 型号不同而不同);TDP 最大支持 125W; 16 根内存插槽;最大可扩展至 2TB 内存;支持单条容量 16GB/32GB/64GB/(128GB LRDIMM); 内存频率支持 2666/2400/2133MHz(工作频率依 CPU 和内存配置不同而不同);支持内存 RAS 技术(内存镜像, 内存等级保护) 最高支持 12 块 3.5 寸(兼容 2.5 寸)热插拔 SAS/SATA 硬盘;支持可选 2 块后置热插拔 2.5 寸硬盘;可选支持 4 块 NVME U.2 热插拔硬盘;支持 1 个 M.2 插槽支持 1 个 TF 插槽	1	台	DS-VE22S-B
3	资源调度节点	支持高性能多核处理器, 高速 UPI 互连总线(10.4/9.6 GT/s, 依 CPU 型号不同而不同),大容量三级缓存(15/20/25/30/35 MB, 依 CPU 型号不同而不同);TDP 最大支持 125W; 16 根内存插槽;最大可扩展至 2TB 内存;支持单条容量 16GB/32GB/64GB/(128GB LRDIMM); 内存频率支持 2666/2400/2133MHz(工作频率依 CPU 和内存配置不同而不同);支持内存 RAS 技术(内存镜像, 内存等级保护) 最高支持 12 块 3.5 寸(兼容 2.5 寸)热插拔 SAS/SATA 硬盘;支持可选 2 块后置	3	台	DS-VE22S-B/ CS

		热插拔 2.5 寸硬盘; 可选支持 4 块 NVME U.2 热插拔硬盘; 支持 1 个 M.2 插槽支持 1 个 TF 插槽			
4	运行检测节点	支持高性能多核处理器, 高速 UPI 互连总线(10.4/9.6 GT/s, 依 CPU 型号不同而不同), 大容量三级缓存(15/20/25/30/35 MB, 依 CPU 型号不同而不同); TDP 最大支持 125W; 16 根内存插槽; 最大可扩展至 2TB 内存; 支持单条容量 16GB/32GB/64GB/(128GB LRDIMM); 内存频率支持 2666/2400/2133MHz(工作频率依 CPU 和内存配置不同而不同); 支持内存 RAS 技术(内存镜像, 内存等级保护) 最高支持 12 块 3.5 寸(兼容 2.5 寸)热插拔 SAS/SATA 硬盘; 支持可选 2 块后置热插拔 2.5 寸硬盘; 可选支持 4 块 NVME U.2 热插拔硬盘; 支持 1 个 M.2 插槽支持 1 个 TF 插槽	1	台	DS-VE22S-B/ CMM
5	流量控制节点	支持 V3/V4 系列多核处理器, 高速 QPI 互连总线(9.6/8.0/6.4GT/s, 依 CPU 型号不同而不同, 大容量三级缓存(15/20/25 MB, 依 CPU 型号不同而不同) 16 根内存插槽机型; 最大可扩展至 1TB 内存; 最大 24 根内存插槽; 最大可扩展至 1.5TB 内存; 支持 DDR42133/2400 ECC 内存(工作频率依 CPU 和内存配置不同而不同) 8 盘位机型最高支持 8 块 3.5 寸或 2.5 寸热插拔 SAS/SATA 硬盘 12 盘位机型最高支持 12 块 3.5 寸或 2.5 寸热插拔 SAS/SATA 硬盘; 24 盘位机型最高支持 24 块 2.5 寸热插拔 SAS/SATA 硬盘; 以上均支持 SAS/SATA 硬盘混插, 支持可选 4 个后置热插拔 2.5 寸硬盘	7	台	DS-VE2224W -KLG/5
6	算法调度节点	支持多核处理器 Socket-SP3, 大容量三级缓存(16/32/48/64 MB, 依 CPU 型号不同而不同); TDP 最大支持 180W; 支持 HG7000/5000 系列兼容 AMD EPYC 系列多核处理器 32 根内存插槽, 最大可扩展至 4TB 内存; 支持单条容量 16GB/32GB/64GB/(128GB LRDIMM);	3	台	DS-VM22S-B

		内存频率支持 2666/2400MHz(工作频率依 CPU 和内存配置不同而不同) 支持内存 RAS 技术(内存镜像, 内存等级保护) 最大可选支持 12 块 3.5 寸(兼容 2.5 寸)热插拔 SATA/SAS 硬盘最大可选支持 24 块 2.5 寸热插拔 SATA/SAS 硬盘; 可选支持 2 块后置 2.5 寸热插拔 SATA/SAS 硬盘; 选择 12 盘位时可选支持 8 块 NVMe U.2 热插拔硬盘支持 2 个 M.2 插槽; 支持 2 个 TF 插槽			
7	信息存储设备	10 亿条信息数据; 支持 3500 万条信息数据加速检索; 两额 4114; 256G DDR4; 240G M2x1 (系统) +240G SSDx1+ 480G SSDx6+2T 7.2K SATAx4 (RAID10)	17	台	DS-VE2212X-K08/HD
9	多维信息存储设备	数据查询:支持通过时间段、监控点、属性等条件进行模糊查询 以图搜图:支持通过模型数据进行相似度匹配检索 区域碰撞:支持通过数据特征进行区域内数据碰撞, 检索符合条件的数据 CPU: 4210R*2 (10C,2.4GHz) 内存: 256G DDR4 硬盘: 240G SSD*1 (系统) +240G SSD*1 + 480G*6 SSD +4T*4 SATA	7	台	DS-VBD0AH-3DU/4S
10	二维信息存储设备	数据查询:支持通过时间段、监控点、属性等条件进行模糊查询 以图搜图:支持通过模型数据进行相似度匹配检索 区域碰撞:支持通过数据特征进行区域内数据碰撞, 检索符合条件的数据 CPU: 4210R*2 (10C,2.4GHz) 内存: 256G DDR4 硬盘: 240G SSD*1 (系统) +240G SSD*1 + 480G*6 SSD +4T*4 SATA	16	台	DS-VBD0AH-3DU/3S
二	视讯通系统				

1	综合型视频资源安全网关设备	<p>1.功能要求 支持对分局现有 4G 执法记录仪终端的状态检测支持对分局现有 4G 执法记录仪终端的有效管理，只有通过审核的设备才能授权正常入网工作 支持对分局现有 4G 执法记录仪终端的认证注册、设备认证、资源汇聚、视频转发</p> <p>2.硬件特性 CPU：不低于 Intel E-2176G @3.7GHz 6核 内存：不低于 32G 网口：不少于 2 个</p>	2	台	DS-A72024R H-CVS
2	视频转发管理设备	<p>1.功能要求 支持将分局现有 4G 执法记录仪非标媒体流进行转码并推送至嘉定智能图像实战应用系统 最大视频转码输出带宽≥80M（最大支持路数根据单路视频码流大小计算）</p> <p>2. 硬件特性 CPU：不低于 4116×2 内存：不低于 64G 硬盘：不低于 1.8T</p>	1	台	DS-AN2110S-DAC
3	数据转发管理设备	<p>1.功能要求 支持将分局现有 4G 执法记录仪终端信息（包含设备状态、经纬度）推送至嘉定分局警务中台及市局平台，满足市局考核要求</p> <p>2.硬件特性 CPU：不低于 4116×2 内存：不低于 32G 硬盘：不低于 1.8T</p>	1	台	DS-VE22S-B
4	128G 存储卡	<p>1.功能要求 适配分局现有 4G 执法记录仪终端</p> <p>2.硬件特性 容量：不低于 128G 读取速度：不低于 128MB/秒</p>	1800	台	128G 存储卡
5	电池	<p>1.功能要求 适配分局现有 4G 执法记录仪终端</p> <p>2.硬件特性 电池容量：不低于 3500mAh</p>	1800	台	/
三	嘉定分局数字化勤务系统				

1	勤务业务	<p>数据汇聚清洗模块: 系统应具有数据汇聚清洗模块，完成数据汇聚及清洗计算。</p> <p>基础支撑模块: 系统应支持将 4A 嘉定分局民警数据同步至嘉定勤务系统，在系统中实现民警的查询、导出、纠偏等勤务管理功能；同时，需支持民警跨单位借调，并支持根据警员实际出勤情况进行是否排班的标记功能及不排班的原因报备。</p> <p>勤务事前模块: 1) 勤务任务 系统应实现任务流程数字化管理，支持嘉定分局下发任务。 2) 民警精细化岗位排班 系统应支持可视化排班或生成排班模块智能排班。</p> <p>勤务服务赋能模块: 系统应提供本局实时在岗警员派勤工作安排数据接口。</p>	1	项	/
2	用户及权限	<p>1、 组织管理 系统应支持用户对警员所属组织进行检索、查询、添加、修改及删除等功能，实现服务于嘉定分局勤务系统的警员所属组织的基础数字化管理。</p> <p>2、 用户管理 系统应支持用户对警员进行检索、查询、添加、修改及删除等功能，实现服务于嘉定分局勤务系统的警员基础数字化管理。</p> <p>3、 权限管理 系统应支持通过角色关联的方式对相关页面提供权限管控功能，支持新增、修改、删除及查询角色，并支持在用户管理中进行相关用户的角色分配及调整。</p> <p>4、 操作日志管理 系统应实现用户操作日志的记录与可视化显示，支撑操作日志按特定条件查询、显示及数据导出分享。</p>	1	项	/
3	技术架构及引擎	系统应支具有地图引擎、微服务引擎、大数据计算引擎等。	1	项	/
4	“e 嘉人”轻应用	应包括探望慰问、健康讲座、便警超市、便警洗衣、聚优惠、辅警管理、信息自动推送等功能。	1	项	/

5	轻应用和隐患清零	围绕派出所实战工作需要，建设办案区辨认模块、送押文书模块、办案提醒模块、现场纠纷调处模块、隐患清零模块等功能模块。	1	项	/
四	智能图像算力支撑和功能开发配套系统				
1	视频流全解析软件授权	系统支持前端设备实际接入能力不少于 5 万路，并进行实时解析、检索和防控。系统支持 2MP（1920×1080）、4MP（2592x1520）、6MP（3072x2048）、8MP（3840×2160）分辨率下的视频解析。系统支持分析 H.264、MPEG-4 编码格式的视频流。系统支持对场景照进行缩放查看。系统支持选择最多 5 路卡口设备进行设备订阅。系统支持卡口抓拍平均响应时间不超过 2 秒。	1	项	/
2	视频图像基础应用模块	系统支持建立布控库。 系统支持集群管理功能，可以看到本集群和跨集群总数、本集群人像库数以及集群列表。 系统支持提供标准 API 接口开放，并支持与第三方业务平台进行对接。	1	项	/
3	视频图像智能大数据应用模块	要求支持在 2.5 亿信息库库下的聚档，提供每天至少 1400 万信息聚档能力。	1	项	/
五	智能图像防控能力支撑配套系统				
1	防控中心管理服务	应包括防控任务分发服务、数据校验服务、告警转发服务、告警推送服务、防控接口、告警推送接口、数据查询接口、防控中心对接等功能	1	项	/
2	防控轻应用-应用功能	应包括地图点位、历史防控查询、告警推送查询、告警推送、链路检测等功能	1	项	/
3	防控管理	应包括用户管理、参数配置、日志管理、数据统计、意见收集、系统维护等功能	1	项	/
六	AR 全景超融合系统和视频监控轻应用配套系统				
1	AR 全景超融合指挥系统	业务应用开发： 应包括视频联动应用、录像回溯应用、视频地图应用、移动警力可视化应用、视觉展示应用、标签配置应用、自动标签下载导入应用， 系统管理开发：	1	项	/

		<p>应包括平台级联管理应用（如上下级平台的通讯服务等）、用户并发访问管理系统对接开发：</p> <p>应包括与智能图像系统、识别系统对接、一机一档系统对接、移动警力系统、标签应用系统、一标六实图层等业务系统对接。</p>			
2	视频监控轻应用	<p>视频监控轻应用系统包含轻应用软件和配套视频管理设备两部分。软件应包含 APP 端应用功能和 Web 后台管理功能，其中应用端应面向民警，至少包括智能融合搜索、视频监控、个人用户等功能模块，后台管理应实现各类统计分析、权限管理等系统管理功能，并能对接相关系统接口。投标人自行提供所需硬件，费用包含在投标总价中。</p> <p>应用功能软件：</p> <p>应包括智能融合搜索、视频监控（实时调阅、历史回放、智能快照、视频标注、提取等）、个人用户（用户登录、个人中心、我的收藏、数据水印等）</p> <p>后台管理软件：</p> <p>包括用户管理、日志查询、反馈查询、后台统计（高频用户统计、使用次数统计等）、预留分组、安全功能、适配功能等。</p> <p>系统对接：</p> <p>应包括与识别系统、智能图像系统、视频联网系统、日志审计系统、用户管理系统、一机一档系统、警务微信系统等系统对接。</p>	1	项	/
七	基于全局智能视频监控的动态应用服务系统				
1	个体信息规范化管理	<p>要求通过万兆骨干链路无缝对接分局智能分析子系统，获取由分局上传的解析后的 8 万路信息数据，含 8 万路已有信息特征智能数据；</p> <p>要求无缝对接市局已有个体信息规范化管理体系，形成完整信息档案和相关数据融合应用，对接智能图像系统 PC 端应用和警务微信图像智能轻应用，供上海公安感知网 PC 终端和一线民警移动终端查询调用。投标人自行提供所需硬件，费用包含在投标总价中。</p>	1	项	/

		<p>应处理不少于 1.53 亿抓拍照片与基础信息中间库碰撞聚类归档，时间应不大于 12 小时。</p> <p>要求按照 GA/T 1400 标准协议对接分局智能分析子系统，通过数据管理转发存储设备获取分局解析后的个体信息、抓拍时间、场景图 URL、小图 URL 和设备 ID 等数据等数据。</p> <p>要求与市局现有个体信息智能分析集群设备无缝对接，在聚档分析维度根据接入情况，在原有系统基础上横向扩容，实现新、老集群的统一整合。</p>			
2	场景图像特征智能分析	对采集的场景图片实时解析、汇聚、检索等功能。	1	项	/
八	融合承载网				
1	汇聚层设备	<p>平台（主设备），包含：电子架+交叉板+光层</p> <p>线路侧端口配置需求：2 波 100G+2 波 10G</p> <p>业务侧端口配置：32*E1+16*STM1+10*FE+5*GE+4*10GE</p>	2	台	OptiX OSN 9800
2	接入层设备	<p>平台（主设备），包含：电子架+交叉板+光层</p> <p>线路侧端口配置需求：4 波 10G</p> <p>业务侧端口配置：32*E1+6*STM1+10*FE+5*GE+4*10G</p>	2	台	Optix OSN 1800V
九	防控中心配套系统				
1	防控中心配套系统	<p>1、防控业务 应包括紧急防控、一级防控、二级防控、定向防控等功能。</p> <p>2、业务服务 包括基础服务、核心业务服务。</p> <p>3、提供对接平台资源管理</p> <p>4、对接现有系统（智能助理系统、警务中台系统、智能图像系统、轨交指挥建设综合作战系统、市域卡口系统、二级库）</p>	1	套	/

十	网络升级服务				
1	分控中心 40G 接口板	24 端口 40G 以太网光接口模块 (QSFP+)(HB)	6	台	H3C LSXM1QGS2 4HB1
2	40G 单模 10KM 光模块	QSFP+ 40G 光模块 (1310nm,10km,LR4,LC)	4	块	H3C QSFP-40G-LR 4-WDM1300
3	40G 单模 40KM 光模块	QSFP+ 40G 光模块 (1310nm,40km,ER4,LC)	44	块	H3C QSFP-40G-ER 4-WDM1300
4	万兆接入交换机	以太网交换机主机,支持 48 个 SFP Plus 端口,6 个 QSFP Plus 端口; 单台满配电源模块和风扇模块。 单台包含 44 块多模万兆模块和 4 块 40G 多模模块。	8	台	H3C S6800-54QF
5	核心交换机	主控引擎 2 块; 交换网板 4 块; 集中监控板 1 块; 24 个千兆光和 24 口万兆光口板 2 块; 48 口千兆电口板 1 块; 配置 VXLAN 功能授权; 配置可插拔风扇 2 个; 配置电源 4 个;	2	台	华为 CloudEngine S12700E-8
6	接入交换机	配置主控引擎 2 块; 电源 2 个; 24 口千兆光接口板 1 块; 48 口千兆电接口板 2 块; 配置 VXLAN 功能授权;	15	台	华为 S7703
十一	感知网分控中心安全加固				
1	分局分控与数据中心边界防火墙	网络层吞吐量 $\geq 150G$ 应用层吞吐量 $\geq 100G$ 并发连接数 ≥ 3500 万新建连接数 ≥ 90 万 千兆电口 ≥ 4 个,万兆光口 ≥ 4 个,40G 光口 ≥ 8 个 支持 802.1Q VLAN Trunk、access 接口, VLAN 三层接口,子接口、GRE 隧道; 2、功能要求 支持链路聚合功能; 支持 LACP 协议 支持端口联动功能,当上行/下行链路出现故障时,对应的另一端下行/上行	2	台	AF-2000-B33 00-TX

		<p>端口自动切断链路；</p> <p>支持静态 ARP 、 ARP 代理、 DNS 、 DNS 代理、DHCP server 、DHCP 中继、SNMPV1/V2/V3/Traps、TCP MSS 配置；</p> <p>支持静态路由， ECMP 等价路由；</p> <p>支持 RIPv1/v2, OSPFv2/v3, BGP 等动态路由协议；</p> <p>访问控制规则支持基于源 / 目的 IP, 源端口, 源 / 目的区域, 用户 (组), 应用 / 服务类型, 时间组的细化控制方式, 支持长连接功能并可以配置连接时长</p> <p>访问控制规则支持模拟策略匹配, 输入源目的 IP、端口、协议五元组信息, 模拟策略匹配方式, 给出最可能的匹配结果, 方便排查故障, 或环境部署前的调试</p> <p>支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测</p> <p>支持对终端已被种植了远控木马或者病毒等恶意软件进行检测, 并且能够对检测到的恶意软件行为进行深入的分析, 展示和外部命令控制服务器的交互行为和其他可疑行为</p> <p>具备独立的入侵防护漏洞规则特征库, 特征总数在 7400 条以上</p> <p>支持对常见应用服务 (HTTP、FTP、SSH、SMTP、IMAP、POP3、RDP、Rlogin、SMB、Telnet、Weblogic、VNC) 和数据库软件 (MySQL、Oracle、MSSQL) 的口令暴力破解防护功能；</p> <p>具备防护常见网络协议 (SSH、FTP、RDP、VNC、Netbios) 和数据库 (MySQL、Oracle、MSSQL) 的弱密码扫描功能；</p> <p>支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别, 支持包含敏感数据业务的识别；</p>			
2	南翔/安亭/徐行分控与数据中心边界防火墙	<p>网络层吞吐量 $\geq 80G$ 应用层吞吐量 $\geq 40G$ 并发连接数 ≥ 1600 万新建连接数 ≥ 60 万</p> <p>千兆电口 ≥ 4 个, 万兆光口 ≥ 4 个, 40G 光口 ≥ 8 个</p> <p>支持 802.1Q VLAN Trunk、access 接口, VLAN 三层接口, 子接口、GRE 隧</p>	6	台	AF-2000-B2800-TX

		<p>道； 2、功能要求</p> <p>支持链路聚合功能；</p> <p>支持 LACP 协议</p> <p>支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；</p> <p>支持静态 ARP 、 ARP 代理、 DNS 、 DNS 代理、DHCP server 、DHCP 中继、SNMPV1/V2/V3/Traps、TCP MSS 配置；</p> <p>支持静态路由， ECMP 等价路由；</p> <p>支持 RIPv1/v2, OSPFv2/v3, BGP 等动态路由协议；</p> <p>访问控制规则支持基于源 / 目的 IP, 源端口, 源 / 目的区域, 用户 (组), 应用 / 服务类型, 时间组的细化控制方式, 支持长连接功能并可以配置连接时长</p> <p>访问控制规则支持模拟策略匹配, 输入源目的 IP、端口、协议五元组信息, 模拟策略匹配方式, 给出最可能的匹配结果, 方便排查故障, 或环境部署前的调试</p> <p>支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测</p> <p>支持对终端已被种植了远控木马或者病毒等恶意软件进行检测, 并且能够对检测到的恶意软件行为进行深入的分析, 展示和外部命令控制服务器的交互行为和其他可疑行为</p> <p>具备独立的入侵防护漏洞规则特征库, 特征总数在 7400 条以上</p> <p>支持对常见应用服务 (HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC) 和数据库软件 (MySQL、Oracle、MSSQL) 的口令暴力破解防护功能；</p> <p>具备防护常见网络协议 (SSH、FTP、RDP、VNC、Netbios)和数据库(MySQL、Oracle、MSSQL) 的弱密码扫描功能；</p> <p>支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别, 支持包含敏感数据业务的识别；</p>			
3	分控中心数据缓存区边界防火墙	<p>硬件特性</p> <p>网络层吞吐量$\geq 20G$ 并发连接数≥ 220万新建连接数≥ 20 万</p>	6	台	AF-2000-B21 50-SK

		<p>千兆电口≥6 个，万兆光口≥4 个</p> <p>支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口、GRE 隧道；</p> <p>2、功能要求</p> <p>支持链路聚合功能；支持 LACP 协议</p> <p>支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；</p> <p>支持静态 ARP、ARP 代理、DNS、DNS 代理、DHCP server、DHCP 中继、SNMPV1/V2/V3/Traps、TCP MSS 配置；</p> <p>支持静态路由，ECMP 等价路由；</p> <p>支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；</p> <p>访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用 / 服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；</p> <p>支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测；</p> <p>支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；</p> <p>具备独立的入侵防护漏洞规则特征库，特征总数在 7400 条以上；</p> <p>支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；</p> <p>具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能；</p> <p>支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；</p>		
--	--	--	--	--

4	流量采集器	<p>1、硬件特性</p> <p>吞吐量≥6Gbps，每秒新建连接数≥35w，最大并发连接数≥800w；接口≥8个千兆电口，4个千兆光口，2个万兆光口；</p> <p>硬盘≥1TSATA盘，内存≥16G，CPU核数≥8核；</p> <p>旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响；</p> <p>2、功能要求</p> <p>能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号，参考信息和建议的解决方案；</p> <p>可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内的多场景网络异常通信行为分析能力。</p> <p>支持同步DNS审计日志；</p> <p>支持HTTP1.0/1.1, HTTPS协议的安全威胁检测；</p> <p>支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持对ASP, PHP, JSP等主流脚本语言编写的webshell后门脚本上传的检测；</p> <p>支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测；</p> <p>产品应具备独立的Web应用检测规则库，Web应用检测规则总数在3000条以上；支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；</p> <p>支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；</p> <p>具备独立的僵尸主机识别特征库，恶意软件识别特征总数在35万条以上；</p>	4	台	STA-100-B26 00-TX
---	-------	--	---	---	----------------------

		<p>能够针对 IP, IP 组, 服务, 端口, 访问时间等策略, 主动建立针对性的业务和应用访问逻辑规则, 包括白名单 (哪些访问逻辑是正常的) 和黑名单 (哪些访问逻辑肯定是异常的) 两种方式, 并对检测到的违规访问进行实时告警</p> <p>能够对网络通信行为进行还原和记录, 以供安全人员进行取证分析, 还原内容包括: TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。</p> <p>支持通过设备对流量进行抓包分析, 可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式</p> <p>支持设备内置简单命令行管理窗口, 便于基础运维调试能够提供网络管理功能, 可进行静态路由配置</p> <p>可支持在线升级和离线升级, 并依托安全管理平台进行统一管控可支持用户初次登陆强制修改密码功能。</p> <p>可实时监控设备的 CPU、内存、存储空间使用情况。</p> <p>支持安全管理平台对接入探针的统一升级, 可展示当前所有接入探针的规则库日期、是否过期等, 并支持禁用指定探针的升级</p>			
5	安全管理平台	<p>1、硬件特性</p> <p>硬盘容量≥48TB, CPU≥20 核, 内存≥256G;</p> <p>设备接口≥为 6 个千兆电口, 2 个万兆光口; 1 个串口; 3 个 USB 口; 支持冗余电源;</p> <p>2、功能要求</p> <p>支持自动识别网络内部主机网段和外网网段;</p> <p>支持自动识别资产, 在不影响内部网络的前提下, 通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息, 如: 操作系统、开放的端口号等;</p> <p>能够自主发现伪装的恶意 DNS 协议;</p> <p>能够自主发现主机传输可疑文件、恶意软件行为、文件或关键目录的可疑操作行为以及 SMB 暴力破解等;</p>	1	台	SIP-1000-D60 2

		<p>能够自主发现主机发送可疑附件的邮件行为、伪造发件人发送邮件、发送钓鱼网站邮件和垃圾邮件等行为；</p> <p>能够自主发现绕过防御的 webshell 攻击，并能够大幅度降低传统检测技术带来的误判；</p> <p>能够自主发现是否正在进行 DoS 攻击，进行网络内部的横向探测。支持对服务器、客户端的各种应用发起的漏洞攻击进行检测；</p> <p>具备独立的 Web 应用检测规则库；</p> <p>支持通过 SNMP 协议，获取待监测设备机器名、CPU 负载、内存使用和流量情况，同时也支持 OID 定制</p> <p>支持与单位现网内使用的防火墙设备进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击 IP；</p> <p>支持检索接入设备传输过来的所有安全日志，可基于时间、攻击类型、严重等级等选择项进行组合查询，可基于具体设备、来源/目的所属、IP 地址、特征 ID、URL 进行具体条件搜索；</p> <p>支持通过 syslog 等接收、存储第三方设备的日志，并提供详细的字段搜索能力；</p> <p>支持管控接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；</p> <p>对接入的非探针设备，具备监控能力，包括展示是否在线、日志传输模式、今日传输日志量、当前传输总量等。</p>			
6	流量探针	<p>1、硬件特性</p> <p>应用层吞吐量\geq1Gbps</p> <p>接口\geq4 个千兆电口，2 个千兆光口</p> <p>旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响</p> <p>2、功能要求</p> <p>支持通过系统漏洞、遭受攻击、C&C 通信、内网探测、内网扩散、盗取数据、黑产牟利等安全事件阶段分布展示和下钻分析支持受影响主机安全事件分类展示</p> <p>支持业务、终端安全状态分布展示，支持弱密码、明文传输等系统脆弱性展示</p>	1	台	STA-100-B42 0

		<p>具备失陷(业务和服务)主机详细分析, 包含攻击阶段分布、风险等级趋势、安全事件举证、开放端口等信息。攻击阶段包含存在漏洞、遭受攻击、C&C 通信、黑产牟利、内网扫描、内网扩散、盗取数据支持对每个安全事件详细举证分析, 包含风险危害、处置建议、专杀工具等。</p> <p>支持对终端种植了远控木马或者病毒等恶意软件进行检测, 并且能够对检测到的恶意软件行为进行深入的分析, 展示和外部命令控制服务器的交互行为和其他可疑行为;</p> <p>具备独立的僵尸主机识别特征库, 恶意软件识别特征总数在 35 万条以上;</p> <p>能够针对 IP, IP 组, 服务, 端口, 访问时间等策略, 主动建立针对性的业务和应用访问逻辑规则;</p> <p>能够对网络通信行为进行还原和记录, 以供安全人员进行取证分析, 还原内容包括: TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。</p>			
7	监测管理平台	<p>1、硬件特性</p> <p>硬盘容量≥16TB, 可用容量≥14.4TB;</p> <p>内存≥64G;</p> <p>设备接口≥4 个千兆电口, 1 个串口;</p> <p>2、功能要求</p> <p>支持自动识别资产, 在不影响内部网络的前提下, 通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息, 如: 操作系统、开放的端口号等; 能够与 CNCERT、VIRUSTOTAL 等国内外权威机构共享威胁情报, 具备僵尸网络识别能力, 行为规则 35 万条以上; 结合情报以及各种行为检测引擎, 支持各种流行、新型僵尸网络以及蠕虫病毒检测;</p> <p>支持“脆弱性识别”, 具有检测 HTTP、FTP、LDAP、VMWARE、ORACLE、VNC 等协议弱密码的功能, 检测列表包含账号、密码、服务器、所属分支和业务、最近发生时间、弱密码类型等信息(提供工信部关于“脆弱性识别”功</p>	1	台	SIP-1000-F60 0

		<p>能的相关检测报告证明)</p> <p>支持“文件威胁分析”，支持展示文件审计进度，包括恶意文件数、未知恶意文件数、待分析文件数、安全文件数；支持在页面展示文件分析过程、检测趋势图、发现次数最多的恶意文件 TOP5；支持展示恶意文件详情，包括支持记录恶意文件感染的主机、所属分支、文件名、病毒名称、传输协议等；支持导出文件威胁分析结果。</p> <p>(提供工信部关于“文件威胁分析”功能的相关检测报告证明)</p> <p>支持通过 SNMP 协议，获取待监测设备机器名、CPU 负载、内存使用和流量情况，同时也支持 OID 定制；</p> <p>支持与单位现网内使用的防火墙设备进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击 IP；</p> <p>支持检索接入设备传输过来的所有安全日志，可基于时间、攻击类型、严重等级等选择项进行组合查询，可基于具体设备、来源/目的所属、IP 地址、特征 ID、URL 进行具体条件搜索。</p>			
十二	全管理平台及配套设备升级				
1	统一身份认证网关	<p>千兆电口≥4 个；配置不低于 5 个核心应用接入授权。</p> <p>支持可信 CA 导入/导出管理，支持 PEM/DER/PCKS7 证书格式导入支持双向证书认证机制</p> <p>提供证书过滤、用户/组织关系、用户名+证书多重认证开启功能 支持地址、端口、超时、PAP/CHAP/MS-CHAPv1/MS-CHAPv2 协议支持 NAS 配置管理，支持每个 NAS 配置不同密钥</p> <p>支持 RADIUS 验证多种模式：密码+动态口令、前缀模式、Challenge 模式认证支持 LDAP 认证，支持 Client BaseDN 设置及认证</p> <p>支持 LDAP 协议的查询、认证指令</p> <p>支持 POP3、SMTP、IMAP 三种邮件协议、服务器设置，支持邮件帐号密码认证支持 HTTP 认证：IP、端口、URL、</p>	1	台	LXR-TESS10000-S

		<p>用户、密码及 HTTP Response 检测认证</p> <p>支持短信认证：短信网关设置、单次短信有效时间、发送超时、短信提示模板、验证失败次数配置</p> <p>提供单点登录令牌认证服务</p> <p>提供 SSO 共享、不共享配置及策略控制支持密码代填、Token 验证两类 SSO 机制</p> <p>支持单点登出、登出过程自定义流程控制功能</p>			
2	控制中心	<p>配置≥500 并发用户授权；千兆电口≥6 个，≥千兆光口 2 个。</p> <p>支持 TCP 单包授权机制</p> <p>支持 UDP+TCP 单包授权机制，为了保障安全，需根据设备清单库来鉴权识别提供用户、分组统一管理功能，包括用户信息增删改查，用户信息备份导出、状态管理</p> <p>单个、批量添加，导入/导出用户及用户组，支持导入密码加解密支持按用户选择认证服务器</p> <p>提供名字、密码、邮箱、电话等属性设置</p> <p>支持强密码校验，首次登录强制修改密码功能</p> <p>用户/组可形成 1 比 N 归属，支持父组/子组之间继承支持用户按认证服务器自动分组</p> <p>用户状态可设置：允许，锁定、禁止状态控制，支持认证失败次数自动锁定用户状态</p> <p>支持 API 服务/API 服务组两级分类资源配置，API 组包含 API 服务列表</p> <p>支持 API 用户、API 用户组两级分类资源配置，API 用户组支持父组/子组模式支持 HTTP、HTTPS 类 WEB 应用配置</p> <p>配置管理支持密码代填、Token 传递、透传模式、代理模式四类 WEB 应用代理</p> <p>支持 GET、POST 方法设置，支持 URLEncoding、JSON、Format 格式设置登录格式，支持用户标识 URI、用</p>	2	套	LXR-TAC100 00-10M

	<p>户标识属性提取自定义设置</p> <p>统一提供 AppID、访问密钥管理配置，为各类资源提供认证、验签服务接口支持 TCP 协议的应用代理</p> <p>支持基于角色的授权策略配置，配置主体、客体角色授权</p> <p>支持基于属性的授权策略配置，可为角色授权提供属性条件过滤规则与控制</p> <p>提供可信环境风险、用户行为分析、用户环境属性多维度的授权策略统一管理功能</p> <p>提供动态策略评估引擎，动态计算用户、行为、风险、环境等安全因子，持续完成用户、设备、应用的可信状态评估</p> <p>支持信任溯源，包括按条件统计查看信任等级趋势、信任等级分布情况、风险事件等详情</p> <p>支持根据实时的可信环境风险、用户行为分析、用户环境属性等多维度感知结果，动态的对用户访问进行放行、阻断和二次认证控制</p> <p>支持根据应用安全等级配置不同的访问策略</p> <p>支持根据风险策略和风险命中次数情况，进行风险拦截，包括阻止访问、二次认证、冻结账号和设备，并支持风险命中记录查看</p> <p>支持用户主动申请应用访问权限</p> <p>引擎提供对外 RestAPI 标准接口，可完成内部、外部授权访问的动态评估支持数据库、NoSQL 库、策略、设备、用户信息外部资源信息查询</p> <p>支持 XACML 标准、JSON 格式，自定义属性、类型引擎决策支持开启、关闭业务隐藏策略。</p> <p>支持按 IP、地址段、子网设置业务隐藏策略</p>			
--	--	--	--	--

3	可信访问网关	<p>最大加密流量不低于 600Mbps; 千兆电口≥6 个, 千兆光口≥4 个</p> <p>支持 UDP 单包授权机制支持 TCP 单包授权机制</p> <p>支持 UDP+TCP 单包授权机制, 为了保障安全, 需根据设备清单库来鉴权识别 (提供产品截图)</p> <p>提供对应用名称、应用地址、应用域名、应用协议等应用系统资源的统一管理功能</p> <p>支持 Web 业务登录表单自定义填充支持 Web 业务登出状态自动检测支持 Web 业务 URL 参数自定义配置支持应用安全等级管理</p> <p>支持 TCP 协议的业务应用代理</p> <p>支持对用户发起的应用请求的字段合法性检测功能, 提供基于请求内容大小、请求速度、请求的连接数、访问时段进行流量控制</p> <p>支持请求登录/登出 URL、参数匹配检测及响应支持 URL 请求、速率、时间段控制</p> <p>支持 SYN Flood 攻击开启</p> <p>提供文件防护, 驱动级文件防篡改功能, 可以保护整个目录、网页或文件不被恶意修改。</p> <p>提供进程防护, 采用二进制白名单机制, 机器学习, 防止进程非法修改。提供 web 防护, 基于防护规则 (数字签名) 对 WEB 流量进行监控及过滤, 防止 SQL 注入、XSS、溢出攻击, 针对 CC 攻击提供独创 session 验证模式, 高效验证正常访问/机器攻击)。</p> <p>提供 rasp 防护, 基于脚本行为 (无规则) 的方式进行漏洞攻击识别及防护, 能有效防御 SQL 注入、任意命令执行、文件上传、任意文件读写、Weblogic 反序列化、Struts2 等基于传统签名方式无法有效防护的应用漏洞。</p>	2	台	LXR-TAP100 00-10M
4	数据采集器	<p>硬件配置</p> <p>2U 设备, 实时结构化应用数据采集; 千兆电口≥4 个。</p> <p>功能要求</p> <p>支持通过流量镜像的方式旁路部署在虚</p>	2	台	DS-ADSG500 0

	<p>拟化网络中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断 TCP 威胁会话连接，支持通过流量被动识别资产。</p> <p>采集过滤条件支持但不限于源地址、目的地址、服务、流量采样比、时间等；需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置；</p> <p>支持离线采集，可通过手动 Pcap 导入或 FTP 等协议批量上传导入等方式对离线流量进行采集</p> <p>支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库 3000+。</p> <p>支持 VXLAN、GRE 、VLAN 、MPLS 的流量接入与解析，日志中可提现响应标识信息。</p> <p>支持 Oracle 、MySQL 、MSSQL 、PostgreSQL、MongoDB、DB2 等数据库行为的解析；支持 WebMail、SMTP、POP3、IMAP 邮件行为解析；</p> <p>支持 ICMP、DHCP、HTTP、TELNET、DNS、SSL 等基础协议的解析</p> <p>支持如 ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp 的登录动作解析</p> <p>支持 LDAP、Kerberos、Radius 等认证解析；</p> <p>具有自定义解析流量能力，支持基于正则表达式、TLV 格式、固定长度等提取模式对应用流量解析</p> <p>支持基于 SSL 协议的 SMTPS 、POP3S、IMAPS、HTTPS 流量进行解密，可添加基于源目的地址及端口的过滤条件。</p> <p>支持解密后的明文流量镜像至下游设备。</p> <p>支持旁路 IPv4 和 IPv6 的 IP 阻断、URL 重定向、DNS 重定向。</p> <p>应用数据采集探针</p> <p>硬件配置</p> <p>2U 设备，实时结构化应用数据采集；</p> <p>千兆电口≥4 个。</p>			
--	---	--	--	--

		<p>功能要求</p> <p>可通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署或 Agent 插件方式部署。</p> <p>支持通过 Agent 审计回环地址的流量</p> <p>支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、神舟通用、Caché 等。</p> <p>支持系统语句的过滤，支持手动添加系统语句。</p> <p>支持对 HTTP、FTP、TELNET、SMTP、samba、POP3、NFS 协议的审计。</p> <p>支持对指定时间段风险数据按不同维度进行统计排行，统计维度包括：风险最多的规则类型 TOP5、触发风险最多的保护对象 TOP5、触发风险最多的 IP TOP5、触发风险最多数据库账户 TOP5、触发风险最多应用账户 TOP5、触发风险最多工具 TOP5；</p> <p>支持对统计数据进行下钻，获取更详细的风险数据</p>			
5	数据安全分析平台	<p>支持以虚拟化的方式部署在虚拟化环境中，提供 ISO 镜像进行安装。支持以软硬一体机方式进行部署。</p> <p>支持关键字方式识别敏感数据，可设置通配符，支持简繁体自动适配；</p> <p>支持正则表达式方式识别敏感数据，配置界面支持表达式校验，保障配置效率；</p> <p>支持数据标示符方式识别敏感数据，以内置字段特征识别身份证号、护照号、驾照照号、银联卡号等常见敏感字段，内置字段特征大于 80 种。</p> <p>支持自定义数据标签，并将数据标签进行分级，分级至少支持 4 级，如：内部、核心商密、普通商密、公开</p> <p>支持自定义数据类别，必须支持以模版方式批量导入数据分级清单；</p> <p>支持多层数据分类，至少支持 2 级业务分类，3 级数据分类，满足现有行业分类分级标准；</p> <p>支持扇状图展示数据分类度、分级度、等级分布、类别分布，支持按部门和数据源过滤查询。</p>	1	套	DS-MAS-QA X-BASE

	<p>支持可视化展示高等级数据驻留数据源的风险情况。</p> <p>支持展示某个应用/应用接口/应用账号的详情，包括敏感数据标签、敏感数据标签的占比、敏感数据量的时间分布、应用账号访问敏感数据排行、来源 IP 访问敏感数据量排行、访问审计日志，并根据时间、时间标签等进行筛选。</p> <p>支持全局的应用审计日志列表展示，展示字段包括访问时间、账号、来源 ip、url、接口名称、应用名称、敏感数据量、数据标签；同时查看日志详情，详情中包括接口的返回的数据样例。</p> <p>支持支持主流数据库 Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、MongDB，K-DB、达梦、人大金仓、南大通用的审计解析。</p> <p>支持基线建模分析策略，可选部门基线和个人基线，可自定义基线时间粒度，有效识别呈现离群特征、偏离日常行为特征的异常访问风险。</p> <p>支持行为链分析策略，通过对不同的阶段设置不同的分析策略，进行多阶段命中检测，实现针对具有多个行为构成的数据风险能进行有效的检测；</p> <p>支持对策略设置风险权重，当用户命中策略时累计以生成用户的风险值。</p> <p>支持将单次追溯检索条件保存到溯源模版，方便结果复现，支持管理员按场景快速进行风险管理。</p> <p>支持特权账号态势大屏，对接密码保险箱时支持同一平台展示特权账号风险状况。</p>			
十三	感知网安全监测			

1	40G 安全监测设备	配置单电源； 配置 2 个 1000MBASE-T 接口（管理口、HA 口），4 个万兆接口；整机吞吐量>40Gbps，最大并发连接数>350W； 4 个万兆多模光口 SFP+模块（850nm，300m，LC）。 含 4 对多模光纤（LC-LC),3m 包含准入控制、资产感知、视频协议分析、数据上报主设备。 40G 安全监测控制设备（5 套） 配置单电源； 配置 2 个 1000MBASE-T 接口（管理口、HA 口），4 个万兆接口；整机吞吐量>40Gbps，最大并发连接数>350W； 4 个万兆多模光口 SFP+模块（850nm，300m，LC）。 含 4 对多模光纤（LC-LC),3m	3	台	ASM6000-HP V5.2
2	40G 安全监测控制设备	配置单电源； 配置 2 个 1000MBASE-T 接口（管理口、HA 口），4 个万兆接口； 整机吞吐量>40Gbps，最大并发连接数>350W； 4 个万兆多模光口 SFP+模块（850nm，300m，LC）。 含 4 对多模光纤（LC-LC),3m	5	台	ASM6000-HP V5.2
3	20G 安全监测设备	配置单电源； 配置 2 个 1000MBASE-T 接口（管理口、HA 口），2 个万兆接口； 2 个万兆多模光口 SFP+模块（850nm，300m，LC）。 含 2 对多模光纤（LC-LC),3m 包含准入控制、资产感知、视频协议分析、数据上报主设备。 20G 安全监测控制主机（5 套） 配置单电源； 配置 2 个 1000MBASE-T 接口（管理口、HA 口），2 个万兆接口； 2 个万兆多模光口 SFP+模块（850nm，300m，LC）。 含 2 对多模光纤（LC-LC),3m	18	台	ASM6000 V5.2
4	20G 安全监测控制设备	配置单电源； 配置 2 个 1000MBASE-T 接口（管理口、HA 口），2 个万兆接口； 2 个万兆多模光口 SFP+模块（850nm，	5	台	ASM6000 V5.2

		300m, LC)。 含 2 对多模光纤 (LC-LC),3m			
5	流量监测主机	<p>最大流量处理能力≥10Gbps； 最大报文存储性能≥5Gbps； 最大并发用户数 5 万；</p> <p>最大并发会话数 300 万；最大新建会话数 10 万/秒；</p> <p>支持 2000 种以上协议和应用识别；</p> <p>系统能够灵活自定义应用实现流量监测分析能力，支持通过 IP、端口组合条件自定义应用</p> <p>支持基于 HTTP URL 定义应用，</p> <p>支持基于 ASCII、HEX 特征值自定义应用，</p> <p>支持根据响应时间设置自定义应用的性能等级；</p> <p>支持对内网、互联网场景模式手动切换，内网模式下只识别常见网络协议和应用</p> <p>实时采集和解析网络流量，长期保存网络中的所有的网络总体流量统计数据，包括比特率（上下行）、数据包率（上下行）、网络中 TCP SYN 数量、TCP SYN ACK 数量、TCP RST 数量、TCP0 窗口数量；捕获数据包时能够根据条件过滤捕获，包括根据 MAC 地址、IP 地址、地址段、通讯协议、网络应用、TCP/UDP 端口、链路与虚链路等条件过滤捕获；</p> <p>CPU2*12 核、内存不小于 128G、磁盘不少于 5 块 单块容量不小于 2T</p> <p>单台设备最大可支持插拔单控制器：2；</p> <p>最大前端主机接口数（单控制器）：20；</p> <p>最大控制器数：16；后端端口类型：SAS3.0（单端口 4*12Gbps）；</p>	2	台	H3C Data、SeerAnalyzer-NPA
十四	运维系统				

1	运维系统	<p>资源运维监控管理 系统提供成熟的网络运维管理软件模块，支持用户感知网各类网络设备的运维管理和拓扑管理。</p> <p>设备台账管理 系统支持通过国标 GB/T28181 标准，从第三方视频监控平台获取视频点位资源数据，包括视频点位编码、点位名称、所属单位、设备资产等各类数据。</p> <p>运维服务流程建设 应包含故障响应与处理管理流程，设备报修维修管理，知识库管理；</p> <p>智能化运维场景建设 系统支持设备故障工单的自动化处置管理，包括设备故障工单的自动建单，故障已解决的设备的自动关单处理等操作。</p> <p>移动运维轻应用 系统具备基于移动终端的运维管理功能；运维数据需要实现跨网同步，定期推送的感知网中，实现运维数据的集中汇聚与上报。</p> <p>运维统计分析 系统能够提供对网络设备、服务器等各类资源的资产统计、运行状态和性能统计、故障统计，以及运维服务工单统计分析功能。</p> <p>运维门户与可视化展现 系统提供各类运行运维数据的集中可视化展现功能，包括运维总体视图、应用视图、资产视图、工单视图、网络监控视图、系统监控视图、机房视图等，从不同纬度展现各类运维工作的情况</p> <p>系统维护与配置管理 系统具备对运维管理模块所有模块进行管理，能够主动识别所有模块的产品版本、部署主机，能够实时监测各模块的关键进程运行状态。</p> <p>智能化运维场景建设 系统支持通过数据分析算法对设备运行指标进行智能分析和异常检测，改变传统“一刀切”的监控告警机制，把资源运行监测的异常分为告警和预警两种模式，告警注重可用性，预警注重健康性，</p>	1	套	/
---	------	--	---	---	---

		<p>异常定位更清晰，管理更精细化</p> <p>运维考核</p> <p>系统具备运维考核功能，支持从运维故障响应、故障处置及时率以及故障工单处理量等多维度为服务厂商的运维工作进行考核；同时，在项目建设时，支持通过二次开发定制符合用户管理规范要求的考核报表。</p> <p>运维轻应用</p> <p>系统提供运维应用功能，支持运维故障数据展示、工单处理、资产数据维护、报表查阅等运维工作的移动办公服务。</p> <p>IP 地址管理</p> <p>实现 IP 地址管理流程的电子化和自动化。</p>			
十五	嘉定分局视频图像能力及共享平台				
1	视频汇聚共享	<p>智能共享管理网关节点：支持国标、Onvif、RTSP、RTMP、主流厂商 SDK 的视频接入和管理；支持 1400 数据接入和管理；支持将高清流媒体实时图像转发给上下级联网系统、监控客户端、电视墙服务等；支持高标清的实时/历史视频流转发；支持图片、智能数据的多平台分发；支持按照数据类型、区域及点位编号等多种策略进行数据分发；支持用户权限精细化管理、视频资源屏蔽、资源专享和抢占；支持集群管理、云台和信令管理；支持统一调度的负载均衡；支持设备状态及数据统计信息报送；支持日志管理、安全认证和权限管理；支持集群的横向扩容；支持视频预热、拉流启停和动态及静态策略配置；支持国标、RTSP、RTMP、HLS、Http-FLV、RTP over TCP 视频输出及 web 客户端 H5 无插件播放；支持数据汇聚和上云，数据缓存和断点续传等；支持语音的接入和转发；支持高级用户允许开流超过设定上限的权限；支持快照配置点位数量，频率，图片服务器信息；支持 28181 平台互联和级联，支持多上级和多下级国标联网；支持对平台的组织机构、用户、资源等数据进行配置，提供用户的</p>	1	台	XF-Server-GV 6020

		<p>认证功能、用户的鉴权控制功能；支持面向前端设备、用户等资源的统一监测，提供可视化的运行态势展示和故障告警提醒</p> <p>处理器：两颗高性能处理器(内核数 8，线程数 16，主频率 2.10 GHz)；内存：DDR4 RECC 2400 16G*4；硬盘：600G SAS 盘*2；阵列卡：Raid 卡*1 支持 Raid 0/1；网络 I/O：集成 2 个 10/100/1000M 自适应以太网口；电源：标配输出功率 550W*2；导轨：2U 标准导轨。</p>			
2		<p>多协议视频共享转发节点：支持国标、RTSP、RTMP、HLS、Http-FLV、RTP over TCP 视频输出及 web 客户端 H5 无插件播放；单台支持 300 路 1080P 视频并发；支持负载均衡；支持视频流转、分发管理功能；支持视频预热；支持将高清流媒体实时图像转发给上下级联网系统、监控客户端、电视墙服务等；支持针对不同协议接入的流，启用独立的转发服务，单个流异常断开不影响其他流的正常转发；支持摄像机、NVR 及解码器使用 GB/T 28181 国标协议接入注册和流媒体转发；支持视频的实时播放、历史回放和云台控制</p>	4	台	XF-Sever-GV 9020
3		<p>感知设备信息采集节点：软硬一体化设备，支持建设标签和场景标签的手工标注和批量导入、并对标签数据进行存储、管理，和基础查询；支持通过设备名称、国标 ID、图像状态、行政区划进行搜索；支持通过 excel 表的方式批量导入新增设备及下载设备列表；支持设备管理包括查询、编辑、删除、详情、批量导入和导出；支持人工审核包括 OSD、时钟、人工校验标记、坐标信息及设备视频快照；支持任务管理、标签管理、标签标注、标签统计；支持地图模块管理包括设备展示、在线率、点位详情及修改；支持系统配置、日志管理、系统运维及系统概况展示；</p>	1	台	XF-Server-GV 2020

4		<p>公安城市快照管理节点：通过配置的时间周期获取设备状态信息，统一对视频资源进行轮巡检测，并给出接入单位视频开流失败列表以加快恢复，提高视频资源可用性。发布服务为上层应用提供视频设备的状态监测服务，支持获取视频点位状态信息图时间策略调整。支持国标、Onvif、RTSP、RTMP、主流厂商SDK 的视频接入和管理；支持管理、存储和转发快照图片；支持用户配置轮巡策略和存储策略；支持查询和统计视频开流的结果及开流时间；支持推送开流结果和开流时间给第三方平台。单节点可实现 10 万路视频设备的管理。可存储管理 10 万张图片。支持并发图片请求 50 路/秒。</p> <p>处理器：两颗高性能处理器，单颗处理器 8 核，主频率 2.10 GHz； 内存：DDR4 RECC 2400 16G*4； 硬盘：2T SAS 盘*2； 网络 I/O：集成 2 个 10/100/1000M 自适应以太网口； 电源：标配输出功率 550W*2 ；</p>	3	台	XF-Sever-GV 5020
5		<p>城市快照轮巡节点：实现获取视频点位场景图及存储管理，并通过发布服务为上层应用系统提供快照服务以及视频点位在线状态提示；单节点支持 3 万路视频快照服务，支持获取视频点位场景图时间策略调整。</p> <p>处理器：两颗高性能处理器，内核数 8，主频率 2.10 GHz； 内存：DDR4 RECC 2400 16G*4； 硬盘：2T SAS 盘*2； 网络 I/O：集成 2 个 10/100/1000M 自适应以太网口； 电源：标配输出功率 550W*2 ；</p>	1	台	XF-Sever-GV 5020

6	精细化场景分析节点	支持 GB/T 28181、ONVIF、RTSP 等协议的视频接入 个性化场景算法定制（包含：异常行为分析、人员拥堵检测、道路拥堵检测等算法） 单台最高支持 160 路视频实时解析 1. CPU：2 颗高性能 CPU，每颗 48 核，主频 2.6GHz（鲲鹏 920） 2. GPU：8 张高性能计算卡（atlas 300C） 3. 内存：512GB DDR4 4. 硬盘：480G SSD*2 + 1.92T SSD * 6 5. 网卡：双万兆光口 6. 电源：1+1 冗余电源，2000W 7. 机箱：2U 机架式服务	5	台	XF-Server-IS3 222
---	-----------	--	---	---	----------------------

五、运维服务要求

提供的运行保障服务，包括对服务范围内以及合同约定范围内的所有设施的日常例行养护、突发故障处置、故障或不合格设备部件及材料的更换修复以及与之相关的定期测试和检测、维护文档和系统资料更新、备品备件更新和仓储等工作，运行保障服务的所有工作所产生的全部费用均由服务提供方承担。

本项目服务团队应不少于 20 人。

（一）售后要求

投标人应建立专门的运维服务管理机构，设立专门的技术服务队伍，配备专业维护工程师。中标人应在提交给采购人的相关文件中详细描述组织机构的构成、人员配备及其各层级的职责分工。投标人应建立各项运维服务流程，按照流程要求提供高质量、响应快的服务，并在投标文件中详细描述相应的服务流程，应当包括技术支持内容，网络问题修复内容，设备修复更换内容等。

针对本项目具体运维要求，投标人需制订全方位的售后服务体系：

1、对易损、易耗品建立完善的用户档案，方便随时了解产品使用情况，以便及时准确解决系统故障。

2、所提供的维护设备在安装期、试运行期及验收后的服务期内，及时解决设备在设计、工艺、材料等技术或质量而产生的故障。服务队伍投标人需提供项目后续所需的维护工程师以及经验丰富的施工安装工程师组成的高水平的技术支持与售后维修服务队伍，随时向用户提供最新的有关先进技术。

（二）服务要求

投标人需设有专门维护服务部门，处理所有维修和技术支持服务，满足招标人的维修需要。专职人员承担，热线服务，限时反应。

投标人应设置维护服务热线电话，以便系统出现故障时在任何时候可以得到投标人的及时响应。并对用户所提出的技术问题及所要求解决的问题提供具体的实质性的维护服务措施。

接到故障报修后，投标人应在 7×24 小时电话支持、5×8 小时现场响应、故障诊断及排除，最佳使用环境建议、备件提供等多种方式为用户提供全面服务。

（三）现场维护服务要求

投标人应在本项目指定专门的人员定期查询检测，在现场保驾护航。每季度定期现场检测，现场签到，并检测记录。

（四）运维时限要求

1、维护单位应提供全天候 7*24 小时的故障维护服务和技术业务咨询服务，提供 7*24 小时热线电话，并有专业的技术人员负责及时解决系统出现的任何故障。

2、在接到故障报修后，维护单位应在 2 小时内响应，技术工程师应 8 小时到达现场，到达现场后小故障 24 小时修复；大故障 72 小时修复（遇到自然灾害等不可抗拒事故除外），对无法按时排除的故障，需与甲方协商确定故障解决时间，并与甲方书面确认。

项目运维服务人员必须与甲方签订项目保密协议。

（五）其他服务要求

鉴于本项目涉及网络、信息安全、系统架构、数据库及软件平台的运维，企业应具备相关的履约能力，例如：ISO20000 信息技术服务体系证书和 ISO27001 信息安全管理体系认证证书等并提供相关认证证书证明等。

六、考核要求

具体项目风险及控制措施采用绩效考核制度，绩效考核的目的是使科信支队能够对运维单位具有的运维能力以及能力的发挥程度进行分析，做出正确的评价，客观合理地对本分局内、基层派出所单位提供安全可靠、及时便捷的服务。

本项目绩效考核分为：例行操作、响应支持、优化改善三个部分，按照占据

本项目的重要程度比例分配如下：

整个运维项目总分：100分

例行操作：20分；响应支持：70分；优化改善：10分

本运维项目评价分为优(≥ 90 分)、良(≥ 80 分)、中(≥ 60 分)、差(< 60 分)。

优等：运维期满后交付全额合同款；

良等：扣除项目合同款0.5%；

中等：扣除项目合同款1%；

差等：扣除项目合同款2%。

(一) 例行操作部分（总分：20）

1、监督控制

共12分，每月1分，如：其中一个月有20%的设备未实施监督控制的工作，则扣除 $1 \times 20\% = 0.2$ 分。

2、定期检查

共8分，每季度2分，如：其中一个季度有20%的现场未实施现场定期检查工作，则扣除 $2 \times 20\% = 0.4$ 分。

由科信支队主管本运维项目民警评分。

(二) 响应支持部分：（总分：70）

1、事件驱动响应

共40分，若响应不及时或遭用户投诉每次扣1分

2、服务请求响应

共20分，若响应不及时或遭用户投诉每次扣1分

3、应急响应

共10分，若应急响应工作未按要求实施每次扣2分

(三) 优化改善部分：（总分：10）

按提交的优化改善方案及改善结果由科信支队成立项目评审组织进行年度讨论评审得分

(四) 违规处罚

当运维单位有任何工作人员发生违反保密规定的，或严重违反运维规范的行为，如：发生一机两用等上海市公安局明文严格规定的情况出现，将直接通知运

维单位更换违规工作人员，并追究运维单位连带责任，如有上述情况发生，一次直接扣除当年绩效考核评分 10 分。第二次直接取消运维单位运维资格。对造成泄密的个人将依法追究法律责任。

七、支付方式

签署合同后 15 个工作日内支付合同金额的 50%。项目通过验收后，由甲方审计部门或甲方委托的中介机构的审计结论作为最后结算价，审价后支付至审价金额的 100%，实际支付金额以当年度区财政实际拨付为准。如由委托的中介机构咨询、审核（审计）的，产生的费用中介机构依据相关规定向乙方收取。

第五章 评标方法与程序

一、投标无效情形

1、投标文件不符合《资格审查要求表》、《符合性要求表》所列任何情形之一的，将被认定为无效投标。

嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维 (2026年度运行维护项目) 资格审查要求包 1

序号	类型	审查要求	要求说明	项目级/包级
1	自定义	法定基本条件	1.符合《中华人民共和国政府采购法》第二十二条规定的条件：营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的，仅需提供营业执照）符合要求，提供财务状况及税收、社会保障资金缴纳情况声明函及没有重大违法记录的声明。 2.未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。	包 1
2	自定义	供应商资质	符合招标文件规定的合格供应商资质条件。	包 1
3	自定义	联合投标	不接受联合体投标。	包 1

嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维

(2026 年度运行维护项目) 符合性要求包 1

序号	审查要求	要求说明	项目级/包级
1	投标文件签署等要求	符合招标文件规定：(1) 投标文件由法定代表人或授权代表签字（或盖章）并加盖供应商公章；(2) 在投标文件由法定代表人授权代表签字（或盖章）的情况下，应按招标文件规定格式提供法定代表人授权委托书；(3) 按招标文件要求提供法定代表人和被授权人身份证。	包 1
2	投标有效期	符合招标文件规定：不少于 90 天。	包 1
3	投标报价	1.不得进行选择性报价（投标报价应是唯一的）； 2.不得进行可变的或者附有条件的投标报价； 3.投标报价不得超出招标文件标明的采购预算金额或项目最高限价； 4.经异常低价投	包 1

		标审查，应按时提供书面说明、证明材料，且提供的书面说明、证明材料能证明其报价合理性。	
4	服务期限	自合同签订之日起至2026年12月31日。	包1
5	合同转让与分包	不得转让与分包	包1
6	其他无效投标情况	不存在招标文件规定的其他无效投标情况	包1

2、单位负责人或法定代表人为同一人，或者存在控股、管理关系的不同供应商，参加同一包件或者未划分包件的同一项目投标的，相关投标均无效。

3、除上述以及法律法规所规定的投标无效情形外，投标文件有其他不符合招标文件要求的均作为评标时的考虑因素，而不导致投标无效。

二、评标方法与程序

（一）评标方法

根据《中华人民共和国政府采购法》及政府采购相关规定，结合项目特点，本项目采用“综合评分法”评标，总分为100分。

（二）评标委员会

1、本项目评标工作由评标委员会负责，评标委员会由采购人的代表和上海市政府采购评审专家组成，成员人数为五人以上单数。政府采购评审专家的人数不少于评标委员会成员总数的三分之二。招标人将按照相关规定，从上海市政府采购评审专家库中随机抽取评审专家。

2、评委应坚持公平、公正原则，依据投标文件对招标文件响应情况、投标

文件编制情况等，按照《投标评分细则》逐项进行综合、科学、客观评分。

（三）评标程序

本项目评标工作程序如下：

1、投标文件初审。初审包括资格性检查和符合性检查。首先，依据法律法规和招标文件的规定，审查、确定投标供应商是否具备投标资格。其次，依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，确定投标文件是否对招标文件的实质性要求作出了响应。

2、澄清有关问题。对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会可以书面形式要求投标人作出必要的澄清、说明或者纠正。投标人的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，并不得超出投标文件的范围或者改变投标文件的实质性内容。

3、比较与评分。按招标文件规定的《投标评分细则》，对资格性检查和符合性检查合格的投标文件进行评分。

4、推荐中标候选供应商名单。评标委员会按照评标得分的高低依次排名，推荐得分最高者为第一中标候选人，依此类推。如果供应商最终得分相同，则按报价由低到高确定排名顺序。得分且投标报价相同的，按技术指标优劣顺序排列。

（四）评分细则

本项目具体评分细则如下：

1、投标价格分按照以下方式进行计算：

（1）价格评分：报价分=价格分值×（评标基准价/评审价）

（2）评标基准价：是经初审合格（技术、商务基本符合要求，无重大缺、漏项）满足招标文件要求且投标价格最低的投标报价。

（3）评审价：无缺漏项的报价，投标报价即评审价；对于有缺漏项的报价，其投标报价也即评审价，缺漏项的费用视为已包括在其投标报价中。

（4）本项目面向所有企业采购。如果非预留份额专门面向中小企业采购的项目或包件，对小微企业报价给予10%的扣除，用扣除后的价格参与评审；如果非预留份额专门面向中小企业采购且接受联合体投标或者允许分包的项目或包件，对于联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额

30%以上的投标人，给予其报价 4%的扣除，用扣除后的价格参与评审。以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业，其中，联合体各方均为小微企业的，联合体视同小微企业。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。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。中小企业投标应提供《中小企业声明函》。

(5) 评审中出现下列情形之一的，评审委员会将启动异常低价投标审查程序：

① 投标报价低于全部通过符合性审查供应商投标报价平均值 50%的，即投标报价 $<$ 全部通过符合性审查供应商投标报价平均值 \times 50%；

② 投标报价低于通过符合性审查的次低报价供应商投标报价 50%的，即投标报价 $<$ 通过符合性审查的次低报价供应商投标报价 \times 50%；

③ 投标报价低于采购项目最高限价 45%的，即投标报价 $<$ 采购项目最高限价 \times 45%；

④ 评审委员会基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形。

评审委员会启动异常低价投标审查后，属于前述第①项至第④项情形的，将要求相关供应商在 30 分钟内对投标价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等。其中，属于第③项情形，供应商已随投标文件一并提交相关书面说明及必要的证明材料的，可不再重复提交。

评审委员会依据专业经验，参考同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。投标供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评审委员会应当将其作为无效投标处理。

2、投标文件其他评分因素及分值设置等详见《投标评分细则》。

3、最低报价不是被授予合同的保证。

投标评分细则（100分）

一、 资格审核阶段：

根据招标文件的要求，对投标方在投标文件中的资格进行审核和符合性检查，对符合要求的，进入技术和价格评议；

二、商务技术评审表：（共计 100 分）

综合评分法

嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026年度运行维护项目）包1评分规则：

评分项目	分值区间	评分办法
报价得分	0~10	报价得分=（评审基准价/评审价）*10
需求理解	0~12	<p>根据供应商对本项目需求的理解，项目运维设计是否完整，项目运维服务定位和目标是否清晰，是否能满足招标需求以及对现有系统现状的理解和分析是否准确进行综合打分。</p> <p>对本项目需求理解分析全面透彻，项目运维设计完整，对项目运维服务定位和目标清晰明确，完全满足招标需求且对现有系统现状的理解和分析准确的得 9-12 分；</p> <p>对本项目需求理解分析和项目运维设计有缺漏，对项目运维服务定位和目标清晰，基本满足招标</p>

		需求且对现有系统现状的理解和分析合理的得 5-8 分；对本项目需求理解分析不完整，项目运维设计缺漏多，对项目运维服务定位和目标模糊，难以满足招标需求且对现有系统现状的理解和分析不准确的得 1-4 分；未提供不得分。
疑难点分析及解决方案	0~6	<p>根据供应商对实施过程中各种可能存在的疑难点分析及解决方案等进行综合打分。</p> <p>对本项目疑难点分析准确，解决方案切实可行的得 5-6 分；疑难点分析具有一定的准确性，解决方案合理的得 3-4 分；疑难点分析不准确，解决方案不合理且可操作性弱的得 1-2 分；未提供不得分。</p>
运维服务方案	0~23	<p>根据供应商提供的运维服务方案（针对运维清单分别提出对应的运维服务方案、对用户方现状及个性化需求的理解、总体思路、服务体系、服务流程、管理和沟通机制等）是否科学合理完整，是否具有针对性，是否与项目需求相吻合等进行综合</p>

		<p>打分。</p> <p>实施方案科学合理完整，有针对性，完全满足项目需求的得 16-23 分；实施方案详细且基本合理，具有一定的针对性，基本满足项目需求的得 8-15 分；实施方案不全面不合理，针对性弱，难以满足项目需求的得 1-7 分；未提供不得分。</p>
故障应急处理方案	0~10	<p>根据供应商提供的应急响应方案（包括详细的应急响应过程，响应方式，响应时间，故障修复时间等），针对典型安全事件或风险是否有设计完善的应急预案进行综合打分。</p> <p>应急预案详细完整，应对措施合理的得 7-10 分；应急预案详细，应对措施有一定的合理性的得 4-6 分；应急预案有缺陷，应对措施不合理的得 1-3 分；未提供不得分。</p>
响应时间	0~5	<p>供应商须承诺按照采购需求提供 7*24 小时故障处理响应和重要活动应急保障。供应商提供承诺函（格式自拟，并加盖公章）的得 5 分，未提供不</p>

		得分。
质量保证措施	0~10	<p>根据供应商针对本项目提供的质量保证措施是否具体可操作，服务质量的检查、验收是否具备明确的方法和标准进行综合打分。</p> <p>措施合理完整，可操作性强，有明确的验收标准的得 7-10 分；措施详细且基本可行，有一定的验收标准的得 4-6 分；措施笼统简单，可操作性弱，验收标准不明确的得 1-3 分；未提供不得分。</p>
维护人员配置	0~10	<p>1) 项目服务团队中有一个高级工程师的得 1 分，最高得 2 分，无证书的不得分（需提供证明材料）。 (0-2 分)</p> <p>2) 项目服务团队中有一个中级工程师的得 1 分，最高得 5 分，无证书的不得分（需提供证明材料）。 (0-5 分)</p> <p>3) 项目服务团队不少于 20 人的得 3 分，少于 20 人的不得分。(0-3 分)</p> <p>注：以上证书均需提供复印件并加盖公章。</p> <p>投标人需提供人员名单</p>

		和资质材料，人员不得重复且必须为投标人本公司人员。
企业综合能力	0~4	投标人提供有效期内的 ISO20000 信息技术服务体系证书和 ISO27001 信息安全管理体认证证书（证书复印件加盖公章），每提供一个证书得 2 分，最高得 4 分，未提供不得分。
相关业绩情况	0~10	<p>投标单位需提供近三年（近三年指从开标之日起倒推 36 个月以内）类似项目业绩，每提供一个得 2 分，最高得 10 分，没有有效的类似项目业绩的得 0 分。</p> <p>应提供类似项目的合同复印件并加盖公章，其中合同复印件中需体现合同的签约主体、项目名称及内容、合同金额、交付日期等合同要素的相关内容。</p>

第六章 投标文件有关格式

一、商务响应文件有关格式

1、投标函格式

致：（招标人名称）

根据贵方（项目名称、项目编号）采购的招标公告及招标公告，（姓名和职务）被正式授权代表投标人（投标人名称、地址），按照网上投标系统规定向贵方提交投标文件 1 份。

据此函，投标人兹宣布同意如下：

- 1.按招标文件规定，我方的投标总价为（大写）元人民币。
- 2.我方已详细研究了全部招标文件，包括招标文件的澄清和修改文件（如果有的话）、参考资料及有关附件，我们已完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。
- 3.投标有效期为自开标之日起____日。
- 4.如我方中标，投标文件将作为本项目合同的组成部分，直至合同履行完毕均保持有效，我方将按招标文件及政府采购法律、法规的规定，承担完成合同的全部责任和义务。
- 5.如果我方有招标文件规定的不予退还投标保证金的任何行为，我方的投标保证金可被贵方没收。
- 6.我方同意向贵方提供贵方可能进一步要求的与本投标有关的一切证据或资料。
- 7.我方完全理解贵方不一定要接受最低报价的投标或其他任何投标。
- 8.我方已充分考虑到投标期间网上投标会发生的故障和风险，并对可能发生任何故障和风险造成的投标内容不一致、利益受损或投标失败，承担全部责任。
- 9.我方同意开标内容以网上投标系统开标时的开标记录表内容为准。我方授

权代表将对开标记录表中与我方有关的内容进行核对并确认，授权代表未进行核对及确认的，视为我方对开标记录内容无异议。

10.为便于贵方公正、择优的确定中标人及其投标货物和相关服务，我方就本次投标有关事项郑重声明如下：

(1) 我方向贵方提交的所有投标文件、资料都是准确的和真实的。

(2) 我方最近三年内因违法行为被通报或者被处罚的情况：

(3) 以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

地址： _____

电话、传真： _____

邮政编码： _____

开户银行： _____

银行账号： _____

投标人授权代表签名： _____

投标人名称（公章）： _____

日期： 年 月 日

2、开标一览表格式

项目名称：

项目编号：

嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全运维（2026年度运行维护项目）包1

项目名称	服务期限	金额(总价、元)

说明：

（1）“金额（总价、元）”指投标总价，所有价格均系用人民币表示，单位为元，精确到个数位。

（2）投标人应按照《项目招标需求》和《投标人须知》的要求报价。

（3）开标一览表内容与投标文件其它部分内容不一致时以开标一览表内容为准。

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

3、报价分类明细表格式

(可根据实际情况修改)

项目名称:

项目编号:

序号	分类名称	单位	数量	单价(元)	总价(元)	备注
1						详见明细()
2						详见明细()
3						详见明细()
4						详见明细()
5						详见明细()
...
总报价						

说明:

- (1) 所有价格均系用人民币表示, 精确到个位数。
- (2) 投标人应根据分类报价费用情况编制明细费用表并随本表一起提供。
- (3) 各投标人拟采取的竞争措施和优惠条件应在商务报价编制说明中详细列明, 标后优惠条件一律不作考虑。
- (4) 投标人应按照《项目招标需求》和《投标人须知》的要求报价。
- (5) 分项目明细报价合计应与开标一览表报价相等。

投标人授权代表签字:

投标人(公章):

日期: 年 月 日

4、资格条件响应表

项目名称：

项目编号：

项目内容（资格条件、实质性要求）	具备的条件说明（要求）	投标检查项（响应内容说明（是/否））	详细内容所对应电子投标文件页次	备注
法定基本条件	1.符合《中华人民共和国政府采购法》第二十二条规定的条件：营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的，仅提供营业执照）符合要求，提供财务状况及税收、社会保障资金缴纳情况声明函及没有重大违法记录的声明。 2. 未被列入“信用中国”网站（ www.creditchina.gov.cn ）失信被执行人名单、重大违法案件当事人名单和中国政府采购网（ www.ccgp.gov.cn ）政府采购严重违法失信行为记录名单的供应商。			
供应商资质	符合招标文件规定的合格供应商资质条件。			
联合投标	不接受联合体投标。			

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

5、符合性要求响应表

项目名称：

项目编号：

项目内容 (资格条件、实质性要求)	具备的条件说明(要求)	投标检查项(响应内容说明(是/否))	详细内容所对应电子投标文件页次	备注
投标文件签署等要求	符合招标文件规定：(1)投标文件由法定代表人或授权代表签字(或盖章)并加盖供应商公章；(2)在投标文件由法定代表人授权代表签字(或盖章)的情况下，应按招标文件规定格式提供法定代表人授权委托书；(3)按招标文件要求提供法定代表人和被授权人身份证。			
投标有效期	符合招标文件规定：不少于 90 天。			
投标报价	1.不得进行选择性的报价(投标报价应是唯一的)； 2.不得进行可变的或者附有条件的投标报价； 3.投标报价不得超出招标文件标明的采购预算金额或项目最高限价； 4.经异常低价投标审查，应按时提供书面说明、证明材料，且提供的书面说明、证明材料能证明其报价合理性。			
服务期限	自合同签订之日起至 2026 年 12 月 31 日			
合同转让与分包	不得转让与分包			
其他无效投标情况	不存在招标文件规定的其他无效投标情况			

投标人授权代表签字：

投标人(公章)：

日期： 年 月 日

6、与评标有关的投标文件主要内容索引表

项目名称：

项目编号：

投标汇标表

项目内容	具备的条件说明	响应内容说明 (是/否)	详细内容所对应电子投标文件页次	备注
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

说明：上述具体内容要求可以参照本项目评标方法与程序及评分细则。

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

7、法定代表人授权书格式

致：

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）以我方的名义参加贵单位_____项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、投标文件澄清、签约等一切具体事务和签署相关文件。

我方对被授权人的签名事项负全部责任。

在贵单位收到我方撤销授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤销而失效。除我方书面撤销授权外，本授权书自投标截止之日起直至我方的投标有效期结束前始终有效。

被授权人无转委托权，特此委托。

法定代表人（委托人）签字或盖章：

代理人（受托人）签字或盖章：

单位名称及盖章：

地址：

日期：

法定代表人身份证
(复印件) 正面

法定代表人身份证
(复印件) 反面

被授权人身份证
(复印件) 正面

被授权人身份证
(复印件) 反面

8、投标人基本情况简介格式

（一）基本情况：

- 1、单位名称：
- 2、地址：
- 3、邮编：
- 4、电话/传真：
- 5、成立日期或注册日期：
- 6、行业类型：

（二）基本经济指标（到上年度 12 月 31 日止）：

- 1、实收资本：
- 2、资产总额：
- 3、负债总额：
- 4、营业收入：
- 5、净利润：
- 6、上交税收：
- 7、在册人数：

（三）其他情况：

- 1、专业人员分类及人数：
- 2、企业资质证书情况：
- 3、近三年内因违法违规受到行业及相关机构通报批评以上处理的情况：
- 4、其他需要说明的情况：

我方承诺上述情况是真实、准确的，我方同意根据招标人进一步要求出示有关资料予以证实。

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

9、中小企业声明函

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，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（软件和信息技术服务业）；承建（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，属于（中型企业、小型企业、微型企业）；

2. （标的名称），属于（软件和信息技术服务业）；承建（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，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）中小企业划型标准为：《关于印发中小企业划型标准规定的通知》（工业和信息化部联企业〔2011〕300号）。

（2）如投标人为联合投标的，联合体各方需分别出具上述《中小企业声明函》。

（3）投标人未按照上述格式正确填写《中小企业声明函》的，视为未提供《中小企业声明函》，不享受政府采购促进中小企业发展政策。

（4）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。

注：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。

10、财务状况及税收、社会保障资金缴纳情况声明函

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。

供应商名称（公章）：

日期：

11、无重大违法记录声明

我方在参加本次政府采购活动前三年内，在经营活动中没有重大违法记录。

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。

供应商名称（公章）：

日期：

12、类似项目业绩：投标人近三年以来承接的与本项目类似项目一览表格式

项目名称：

项目编号：

序号	年份	项目名称	项目内容	服务时间	合同金额（万元）	业主情况		
						单位名称	经办人	联系方式
1								
2								
3								
4								

说明：近三年指从开标之日起倒推 36 个月以内。

附：类似项目的合同复印件，其中合同复印件中需体现合同的签约主体、项目名称及内容、合同金额、交付日期等合同要素的相关内容。

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

13、营业执照复印件

格式自拟。

2、项目经理简历表

项目名称：

项目编号：

姓名		年龄		文化程度		毕业时间	
毕业院校和专业			从事本类项目工作年限			联系方式	
职业资格			技术职称			聘任时间	
<p>主要工作经历：</p> <p>主要管理服务项目：</p> <p>主要工作特点：</p> <p>主要工作业绩：</p>							

附：身份证、学历证书、职称及职业资格证书。

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

3、拟投入本项目的人员表

项目名称：

项目编号：

项目组成 员姓名	年龄	在项目组中 的岗位	职称及职 业资格	进入本单 位时间	相关工作 经历	联系方式
.....						

附：身份证、职称及职业资格证书复印件。

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

4、技术条款响应偏离表

项目名称：

项目编号：

序号	项目需求	投标方案	偏离（响应程度）	说明

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

5、投标人相关的资质、荣誉等证书汇总表

项目名称：

项目编号：

序号	资质、荣誉等证书名称	数量	详细内容所在投标文件页次	备注
1				
2				
3				
4				
5				
6				
7				
8				
9				
.....				

投标人授权代表签字：

投标人（公章）：

日期： 年 月 日

第七章 合同文本

包 1 合同模板：

嘉定公安分局社会治安防控体系感知节点部署区级平台及 网络安全运维（2026 年度运行维护项目）采购合同

合同通用条款及专用条款

合同统一编号：[合同中心-合同编码]

项目名称：嘉定公安分局社会治安防控体系感知节点部署区级平台及网络安全
运维（2026 年度运行维护项目）

项目编号：310114000251219161656-14302737

合同各方：

甲方：[合同中心-采购单位名称]

乙方：[合同中心-供应商名称]

法定代表人：[合同中心-供应商法人姓名]（性别：[合同中心-供应商法人性别]）

地址：[合同中心-采购单位所在地]

地址：[合同中心-供应商所在地]

邮政编码：[合同中心-采购单位邮编]

邮政编码：[合同中心-供应商单位邮编]

电话：[合同中心-采购单位联系人电话]

电话：[合同中心-供应商联系人电话]

传真：[合同中心-采购单位传真]

传真：[合同中心-供应商单位传真_1]

联系人：[合同中心-采购单位联系人]

联系人：[合同中心-供应商联系人]

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，
本项目合同当事人在平等、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法律法规和规定，服务的内

容、要求、服务质量等以满足招标文件要求为基础。详见招标文件和投标文件。

1.2 项目内容：项目运维内容包括智能分析系统、视讯通系统、嘉定分局数字化勤务系统、智能图像算力支撑和功能开发配套系统、智能图像防控能力支撑配套系统、AR 全景超融合系统和视频监控轻应用配套系统、基于全局智能视频监控的动态应用服务系统、融合承载网、防控中心配套系统、网络升级服务、感知网分控中心安全加固、安全管理平台及配套设备升级、感知网安全监测、运维系统、嘉定分局视频图像能力及共享平台，共计 15 个子系统。

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,大写金额:[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：上海市嘉定区。

2.3 服务期限：[合同中心-合同有效期]。

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，甲方应及时根据合同的约定进行服务验收。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 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 甲方对乙方所提供的基础资料及乙方向甲方所提供的服务成果，甲方拥有完整的所有权，乙方对此负有保密义务，并承担相应的法律责任。

6.2 由于甲方业务的保密性原则，乙方所有参与项目运维人员需要签订相关的安全保密协议，乙方在进行维护服务活动过程中，应遵守安全保密协议，保证维护服务安全无事故。

7. 付款

7.1 本合同以人民币付款（单位：元）。

7.2 本合同款项按照以下方式支付。

7.2.1 付款条件：签署合同后15个工作日内支付合同金额的50%。项目通过验收后，由甲方审计部门或甲方委托的中介机构的审计结论作为最后结算价，审价后支付至审价金额的100%，实际支付金额以当年度区财政实际拨付为准。如由委托的中介机构咨询、审核（审计）的，产生的费用中介机构依据相关规定向乙方收取。

7.2.2 实际付款金额及付款时间以财政资金到账为准，财政资金延期支付不属于甲方违约责任。

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服务，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要求的时间内加急提供服务，直至符合要求为止。

8.2 如果乙方到期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，甲方有权另外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 甲方在合同规定的服务期限内有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。

8.4 如果甲方因工作需要对原有服务需求进行调整，可通过有效的方式及时通知乙方协商调整。

9. 乙方的权利与义务

9.1 乙方应根据合同约定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。

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 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。

10. 补救措施和索赔

10.1 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) 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

14.1 在本合同签署之前，乙方应向甲方提交一笔金额为 0 元人民币的履约保证金。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承担。

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。

14.4 如甲方逾期退还乙方履约保证金，乙方可依法向甲方追究相应违约责任。

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后生效。

19.2 本合同一式 3 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。

22. 补充条款

[合同文档模版-其他补充事宜]。

(以下无正文)

签约各方：

甲方（盖章）：**[合同中心-采购单位名称_1]** 乙方（盖章）：**[合同中心-供应商名称_1]**

法定代表人或授权委托人：**[合同中心-采购单位联系人_1]** 法定代表人或授权委托人：**[合同中心-供应商联系人_1]**

日期：**[合同中心-签订时间]** 日期：**[合同中心-签订时间_2]**

合同签订点：网上签约

第八章 质疑、未中标结果询问受理要求及附件

一、质疑受理联系方式：

联系人：周老师

联系电话：021-69521888

联系地址：上海市嘉定区嘉罗公路 1661 弄盛创企业家园 31 号 3 层

邮政编码：201808

电子邮箱：dingjiasw@163.com

二、质疑函提交要求：

供应商提交的质疑函应当一式三份。质疑函应当包括下列主要内容：

（一）供应商的名称、地址、邮编、联系人及联系电话等；

（二）采购项目的名称、编号及分包号；

（三）质疑的具体事项、质疑请求和主张；

（四）质疑所依据的具体事实和根据（应当附有充足有效的线索和相关证据材料），所依据的有关法律、法规、规章、规范性文件名称及具体条款的内容；

（五）提出质疑的日期。

质疑函应当署名。质疑供应商为自然人的，应当由本人签字；质疑供应商为法人或者其他组织的，应当由法定代表人或者主要负责人签字并加盖公章。

供应商可以委托代理人办理质疑事务。代理人应当向采购中心提交授权委托书及代理人合法、有效的身份证明，授权委托书应当载明委托代理的具体事项、权限及有效期限。

三、质疑有下列情形之一的，代理机构将驳回质疑：

（一）质疑缺乏事实和法律依据的；

（二）质疑供应商捏造事实、提供虚假材料的；

（三）质疑已经处理并答复后，质疑供应商就同一事项又提起质疑且未提供新的有效证据的；

（四）其他根据相关法律、法规、政府采购规章应当予以驳回的情形。

四、附件：

附件 1：质疑函

附件 2：法定代表人授权书

附件 1

质疑函

质疑供应商：（名称、地址、邮政编码、联系方式等）

法定代表人：（姓名、职务、地址、联系方式等）

委托代理人：（姓名、职务、地址、联系方式等）

被质疑人：（名称、地址、邮政编码、联系方式等）

（代理机构名称）：

本供应商认为（采购项目名称、编号，第几包）的（采购文件、采购过程或中标、成交结果）使我们的权益受到损害，现向你单位提出书面质疑。

一、具体质疑事项：

1、。

2、。

.....

二、质疑请求和主张：

。

三、事实依据、理由（事实陈述及所依据的有关法律、法规、规章、规范性文件名称和具体条款）：

。

附件：相关证明材料

本人或法定代表人或主要负责人签章：

单位公章：

年 月 日

附件 2

法定代表人授权书

（采购代理机构）：

本人（姓名、职务），系注册地址位于的（公司名称）法定代表人，兹代表本公司授权（被授权人的姓名、所属单位、职务），其身份证号码：，为本公司的合法代理人，就项目（项目名称、编号）采购向贵公司提出质疑，其有权以本公司名义处理一切与之有关的事务并做出相应决定。

本授权书自签发之日起至年月日止始终有效。

法定代表人签字或盖章：

职 务：

地 址：

代理人(被授权人)签字或盖章：

职 务：

公司名称：

(公章)

日 期：

附件 3

本项目采用综合评分法评审，未中标供应商如需询问本人投标结果，可以通过发送《未中标结果询问函》至我公司邮箱（dingjiasw@163.com）询问本人未中标结果。我公司在收到邮件 3 个工作日内，对询问进行回复。回复的内容仅限于：1、未通过资格审查的原因；2、未中标人本人的评审得分与排序。

未中标结果询问函

经合法授权，本供应商特委托：_____（被授权人姓名）为（项目名称、项目编号）的代表对未中标结果进行询问。

被授权人（签名）：_____

被授权人身份证号：_____

被授权人手机：_____

供应商名称及签章：_____

日期：_____年_____月_____日