ZHENG FU CAI GOU

上海市公安局徐汇分局2022年度网络安全建设政府采购项目

招标文件

招标编号：徐采中招2022-093

招标单位：上海市徐汇区政府采购中心

二〇二二年十一月

总 目 录

第一部分 投标邀请

根据《中华人民共和国政府采购法》之规定，上海市徐汇区政府采购中心受采购人委托，就上海市公安局徐汇分局 2022 年度网络安全建设政府采购项目进行国内公开招投标采购，特邀请合格的供应商前来投标。

一、合格的投标人必须具备以下条件：

1、具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商；同时经信用信息查询未被列入失信被执行人、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；

2、本项目**不允许**联合投标。

二、项目概况：

1、项目名称：上海市徐汇区政府采购中心——上海市公安局徐汇分局 2022 年度网络安全建设政府采购项目

2、招标编号：（代理机构内部项目编号：徐采中招 2022-093）

3、预算编号：0422-04004

4、项目主要内容及要求：

上海市公安局徐汇分局 2022 年度网络安全建设项目包括：感知网安全建设、流量分析平台建设、融合承载网配套建设、安全运维服务等。具体技术要求详见招标文件第三部分。

5、服务地址：上海市公安局徐汇分局指定地点。

6、项目服务期限：按照招标文件第三部分要求

7、采购项目需要落实的政府采购政策情况：根据上海市财政局沪财库[2009]19 号“关于落实政府采购优先购买福利企业产品和服务的通知”要求，本项目在同等条件下优先采购福利企业的产品和服务。同时项目采购应当符合采购价格低于市场平均价格、采购质量优良和服务良好的要求。本项目面向所有企业采购，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。其要求标准详见《政府采购促进中小企业发展管理办法》（财库[2020]46 号）中相关规定。

三、招标文件的获取

1、合格的供应商可于 **2022-11-21** 本公告发布之日起至 **2022-11-30**，登录“上海政府采购网”（http://www.zfcg.sh.gov.cn）在网上招标系统中上传如下材料：

/招标文件下载时间 2022 年 11 月 21 日至 2022 年 11 月 30 日止

采购文件上午获取时间：00:00:00~12:00:00

采购文件下午获取时间：12:00:00~23:59:59

2、凡愿参加投标的合格供应商可在上述规定的时间内下载（获取）招标文件并按照招标文件要求参加投标。

注：投标人须保证报名及获得招标文件需提交的资料和所填写内容真实、完整、有效、一致，如因投标人递交虚假材料或填写信息错误导致的与本项目有关的任何损失由投标人承担。

四、投标截止时间及开标时间：

1、投标截止时间：2022 年 12 月 12 日 9:30，迟到或不符合规定的投标文件恕不接受。

2、开标时间：2022 年 12 月 12 日 9:30。

五、投标地点和开标地点

1、投标地点：上海市政府采购网（政府采购云平台）http://www. zfcg. sh.gov.cn；根据上海市财政局相关规定，本项目招投标相关活动在上海市政府采购云平台（网址：www.zfcg.sh.gov.cn）进行。政府采购云平台是由市财政局建设和维护。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。投标人在政府采购云平台的有关操作方法可以参照政府采购云平台中相关专栏的有关内容和操作要求办理。

2、开标地点：上海市政府采购网（政府采购云平台）http://www. zfcg. sh.gov.cn；本项目实行网上远程开标，按有关规定在开标时间内无法签到、解密的供应商将被取消投标资格，不纳入评审范围。响应投标的供应商请在开标时间开始后持投标时所使用的数字证书（CA 证书）参加远程开标。

3、开标所需携带其他材料：

本项目实行网上远程开标，按有关规定在开标时间内无法签到、解密的供应商将被取消投标资格，不纳入评审范围。响应投标的供应商请在开标时间开始后持投标时所使用的数字证书（CA 证书）参加远程开标。

六、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。

七、注意事项：

1、投标单位对招标文件有疑问的可在 2022 年 11 月 25 日上午 10 点整前以书面传真的形式向徐汇区政府采购中心提出，由采购中心负责统一解答。采购中心将于 2022 年 11 月 25 日下午 17 点前通过“上海政府采购网” （http://www. zfcg. sh.gov.cn）公开发布。

2、**本项目采购预算为 11088800 元人民币，报价超过采购预算的投标不予接受。**

3、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。

八、联系方式

采购人：区城市网格化综合管理中心（区行政 采购代理机构：上海市徐汇区政府采购中心

服务中心）

地址：徐汇区南宁路 969 号

邮编： 200235

联系人：高卉

电话：54012832

地址：南宁路 969 号

邮编： 200235

联系人：王丽佳

电话：24092222*2596

第二部分 投标人须知

一、总则

1、概述

1.1 本招标文件适用于本投标邀请中所述安全建设的招标投标。

1.2 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。

1.3 根据上海市财政局相关规定，本项目招投标相关活动在上海市政府采购云平台（网址：www.zfcg.sh.gov.cn）进行。

2、定义：

2.1“招标人”指组织本次招标的上海市徐汇区政府采购中心和采购人。

2.2“采购人”指区城市网格化综合管理中心（区行政服务中心）。

2.3**“招标项目”指本招标文件中第三部分所述相关安全建设，本项目属于软件和信息技术服务业**。

2.4“潜在投标人”指符合招标文件规定的合格供应商。

2.5“投标人”指按规定获取招标文件，并按照招标文件要求提交投标文件的供应商。

2.6“上海市政府采购云平台”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），是由市财政局建设和维护。

3、合格投标人的条件

3.1 具有本项目生产、供应或实施能力，符合、承认并承诺履行本文件各项规定的国内法人和其他组织均可参加投标。

3.2 投标人应遵守有关的国家法律、法规和条例，具备《中华人民共和国政府采购法》和本文件中规定的条件：

（1）具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商；同时经信用信息查询未被列入失信被执行人、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。

（2）本项目不允许联合投标。

3.3 只有在法律上和财务上独立运作并独立于采购中心的供应商才能参加投标。

3.4 如投标人代表不是法定代表人，须持有《法定代表人授权委托书》(统一格式)。

4. 投标费用

4.1 投标人应承担所有与准备和参加投标有关的费用，采购中心和采购人在任何情况下均无义务和责任承担这些费用。

4.2 本次招标工作由徐汇区政府采购中心自行组织实施，不收取任何中介费用。

二、招标文件

5.招标文件的构成

5.1 招标文件是阐明招标的项目范围、投标文件的编写、递交、招标投标程序、评标原则、中标条件和相关的协议条款的文件。招标文件由以下六部分内容组成：

第一部分 投标邀请（招标公告）；

第二部分 投标人须知；

第三部分 招标项目需求；

第四部分 合同参考范本；

第五部分 投标文件格式；

第六部分 评标办法

5.2 投标人应详细阅读招标文件的全部内容。如果投标人没有按照招标文件要求提交全部资料或者没有对招标文件在各方面的要求都做出实质性响应，可能导致其投标被拒绝。

6.招标文件的澄清

6.1 任何通过电子采购平台获取了招标文件的潜在投标人，均可要求对招标文件进行澄清。澄清要求应于投标邀请函所述日期前，按投标邀请书中的联系地址以书面形式（包括书面材料、信函、传真等，下同）送达采购中心，采购中心将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布相关答复。

6.2 采购中心将视情况确定是否有必要召开标前会（现场踏勘）。召开标前会（现场踏勘）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。

7.招标文件的修改

7.1 在投标截止期 15 日以前任何时候，采购中心无论出于何种原因，均可对招标文件用补充文件的方式进行修改。

7.2 对招标文件的修改，将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布。补充文件将作为招标文件的组成部分，对所有获取了招标文件的潜在投标人均具有约束力。

7.3 为使投标人有足够的时间按招标文件的修改要求考虑修正投标文件，采购中心可酌情推迟投标的截止日期和开标日期，并将具体变更情况通知上述每一投标人。

8.通知

8.1 对与本项目有关的通知，采购中心将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布。

8.2 招标文件的澄清、答复、修改或补充都应由采购中心以澄清或修改公告形式发布，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。

三、投标文件

9.投标文件的语言和计量单位

9.1 投标人提交的以及投标人与采购中心就有关投标的所有来往函电均应使用中文简化字。

9.2 投标人所提供的技术文件和资料，包括图纸中的说明，应使用中文简化字。所使用的计量单位，应使用国家法定计量单位。

10.投标文件的组成及相关要求

10.1 投标文件由商务响应文件、技术响应文件两部份构成。

10.2 商务响应文件、技术响应文件所应包含的内容如下：

10.2.1 商务响应文件：

（1）投标函

（2）投标报价明细表；

（3）法定代表人证明书和法人代表委托书；

（4）投标单位基本情况表及声明；

（5）供应商行贿犯罪记录承诺书；

（6）中小企业声明函；

（7）投标人近年来已承接的主要类似项目一览表；随表附相应的合同复印件等。（复印件加盖单位公章）

（8）资格证明文件，包括：投标单位营业执照、税务登记证（复印件加盖单位公章）；投标人信用信息查询记录，投标人应当通过“信用中国”网站（www.creditchina.gov.cn）查询投标人主体信用记录（查询截止时点为 2022 年 12 月 9 日），并对查询的信用详情截屏打印并加盖单位公章；投标单位财务状况及税收、社会保障资金缴纳情况声明函。资格证明文件不满足招标要求的，将作为无效投标处理。

（9）投标单位网络安全应急服务支撑单位证书（国家级）、信息安全服务资质证书、信息系统建设和服务能力等级证书（优秀级（CS4））、ITSS 信息技术服务运行维护标准符合性证书（复印件加盖单位公章）。

（10）投标单位书面承诺函

10.2.2 技术响应文件：

（1）产品选型及说明一览表；

（2）技术参数（功能要求）偏离表；

（3）投入项目的服务人员配备及相关工作经历、资质汇总表；

（4）投标单位安全运维服务方案，包括但不限于以下内容：整体服务方案：服务理念和目标、投标人完成各服务的具体实施计划、服务流程、方法，人力、物力、技术力量的投入，服务质量保证措施，成果提交方式、考核验收方案等；项目管理组织架构及管理制度：项目

管理机构及其工作方法与流程，项目经理的管理职责，内部管理的职责分工，日常管理制度（工作制度、岗位制度等），以及公司对于项目的监管控制和服务支持。项目人员配置，运维服务人员关键岗位的标准操作程序；拟投入本项目的主要设备与工具；运维服务的应急预案；对服务满意度的自我考核测量方案以及投标人建议的服务质量检查方法或方案、对投诉处理的控制管理方案等；按照招标文件要求提供的其他技术性资料。

（5）感知网安全建设服务方案 提供详细的感知网安全建设服务方案，包括但不限于相关产品租赁的详细设计方案、所选用产品的数量、型号、详细技术参数指标等。

（6）投标产品的说明书、产品厂家彩页性能介绍样本（catalog）等技术文件；

（7）售后服务承诺（保修期内售后服务的内容、期限、响应时间、应急保障措施等）及培训等相关伴随服务实施方案；

（8）规章制度一览表；

（9）投标人认为需要提供的其它说明和资料。

10.3 上述文件中凡招标文件提供格式文本的以及要求“加盖单位公章”的材料须上传原件彩色扫描件。

10.4 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，并且招标人将对该投标人进行调查，发现有欺诈行为的按有关规定进行处理。

10.5 本项目不接受纸质投标文件。

11.投标内容填写说明

11.1 获取了招标文件的潜在投标人应认真阅读招标文件的所有内容，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。

11.2 投标人必须保证投标文件所提供的全部资料真实可靠，并接受采购中心对其中任何资料进一步审查的要求。

11.3 开标一览表要求按格式统一填写，不得自行增减内容。

11.4 投标文件须对招标文件中的内容做出实质性和完整的响应，否则其投标将被拒绝。如果投标文件填报的内容资料不详，或没有提供招标文件中所要求的全部资料及数据，包括但不限于第 10 条（投标文件的组成及相关要求）规定的内容，将可能导致投标被拒绝。

12.投标报价

12.1 所有投标报价均以人民币元为计算单位。投标价格应该已经扣除所有同业折扣以及现金折扣，应为考虑所有优惠后的最有竞争性价格，不得再以其他形式进行标后优惠，否则视为不诚信行为记入供应商诚信记录。投标报价应已经包含了购买相关服务的费用和所需缴纳的所有税费，并包含了完成全部服务内容所需的一切费用。

12.2 投标人提供的相关安全建设，应当符合国家有关法律、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。

12.3 投标人应按照招标文件中提供的投标文件格式完整地填写开标一览表、报价明细表和报价构成表等，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

12.4 除招标文件说明并允许外，投标的每一种服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价将可能导致投标被拒绝。

12.5 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。

13.投标保证金

本项目不收取投标保证金。

14.投标文件的有效期

14.1 自开标日起 90 天内，投标文件应保持有效。有效期短于该规定期限的投标，将被拒绝。

14.2 在特殊情况下，采购中心可与投标人协商延长投标文件的有效期。这种要求和答复都应以书面形式进行。此时，按本须知规定的投标保证金的有效期也相应延长。投标人可以拒绝接受延期要求而不会被没收保证金。同意延长有效期的投标人除按照采购中心要求修改投标文件有效期外，不能修改投标文件的其他内容。

15.投标文件的签署及其他规定

15.1 组成投标文件的各项文件均应遵守本条。

15.2 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。

15.3 投标人应按招标文件和电子采购平台电子招投标系统规定的内容、格式和顺序编制投标文件。凡招标文件提供有相应格式的，投标文件均应完整的按照招标文件提供的格式打印、填写并按要求在电子采购平台电子招投标系统上传。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

15.4 用于网上招投标系统上传的扫描件等有关文件应确保清晰、可辨，投标人上传文件的电子数据量不应过大，因数据量过大导致无法正常投标、开标的，投标人将自行承担其责任后果，招标人不承担任何责任。

四、投标文件的递交和解密（开标）

16.投标文件的递交和解密

16.1 投标单位在制作投标文件后应在上传投标文件截止时间之前在上海政府采购网上将电子投标文件加密上传。

16.2 举行开标会时，各投标供应商须带好本单位的 CA 证书及可以无线上网的笔记本电脑，按照规定的开标时间和地点到场后登陆上海政府采购网集中解密。按有关规定当场无法解密的供应商将被取消投标资格，不纳入评审范围。

16.3 在投标文件解密之后，投标人不得撤回投标。投标后撤回投标文件的行为将被记录在案，投标人今后参与同类政府采购项目的机会可能会受到影响.

17.投标截止时间

17.1 投标文件须按照招标文件规定的投标时间、地点解密。

17.2 采购中心推迟投标截止时间时，将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布。在这种情况下，采购中心和投标人的权利及义务将受到新的截止期的约束。

五、评标

18.评标

18.1 采购中心根据有关法律法规和本招标文件的规定，结合本招标项目的特点组建评标委员会，对具备实质性响应的投标文件进行评估和比较。评标委员会由采购人、技术、经济、法律专家和其他有关方面的代表组成。

18.2 评标原则

（1）评标应严格按照招标文件的要求和条件进行；

（2）评标委员会只对实质上响应招标文件的投标进行评价和比较；

（3）评标委员会分别对每包进行独立评标，每包只限确定一家供应商为中标单位，但一家供应商可以中一包或多包；

（4）评标委员会在评标时除考虑投标报价因素外，同时还根据各项技术和服务因素对投标人和投标服务进行综合评价。

18.3 评标办法：本项目采用综合评分法，各评标因素所占权重见第六部分评标办法。

19.对投标文件的初审

19.1 开标后，采购中心将组织对投标文件进行资格性检查，依据法律法规和招标文件的规定，对投标文件中的资格证明、投标保证金等进行审查，以确定投标供应商是否具备投标资格。

19.2 在详细评标之前，评标委员会对通过资格性检查的投标文件进行符合性检查，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，以确定是否对招标文件的实质性要求作出响应。

（1）实质上响应的投标是指与招标文件的全部条款、条件和规格相符，没有重大偏离或保留。

（2）重大偏离或保留系指投标人货物的质量、数量和交货期限等明显不能满足招标文件的要求，或者实质上与招标文件不一致，而且限制了采购中心的权利或投标人的义务，纠正这些偏离或保留将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。

（3）重大偏离不允许在开标后修正，但采购中心将允许修正投标中不构成重大偏离的地方，这些修正不会对其他实质上响应招标文件要求的投标人的竞争地位产生不公正的影响。

（4）如果实质上没有响应招标文件的要求，评标委员会将予以拒绝，投标人不得再对投标文件进行任何修正从而使其投标成为实质上响应的投标。

19.3 初审中，投标文件中如果有下列计算或表达上的错误或矛盾，将按以下原则或方法进行修正；其他错误或矛盾将按不利于出错投标人的原则进行修正：

（1）开标一览表内容与报价明细表及投标文件其他部分内容不一致的，以开标一览表内容为准。

（2）如果以文字表示的数据与数字表示的有差别，以文字为准修正数字。如果大小写金额不一致的，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，以开标一览表的总价为准，并修改单价。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。

（4）修正后的结果应对投标人具有约束力，投标人不同意以上修正，其投标将被拒绝。

19.4 评标委员会对投标文件的判定，只依据投标文件内容本身，不依据任何外来证明。

20.投标的澄清

20.1 评标委员会有权要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容等作必要的澄清、说明或者补正。投标人必须按照评标委员会通知的澄清内容和时间做出澄清。必要时评标委员会可要求投标人就澄清的问题作书面答复，该答复经投标人的法定代表人或投标人代表的签字认可，将作为投标文件内容的一部分。澄清、说明或者补正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。

20.2 如评委会一致认为某个投标人的报价明显不合理，有降低质量、不能诚信履行的可能时，评标委员会有权通知投标人限期进行解释。若该投标人未在规定期限内做出解释，或作出的解释不合理，经评标委员会取得一致意见后，可拒绝该投标。

21.评标过程保密

21.1 开标之后，直到授予投标人合同止，凡是属于审查、澄清、评价和比较投标的有关资料以及授标意向等，均不向投标人或其他与评标无关的人员透露。

21.2 在评标期间，投标人企图影响采购中心或评标委员会的任何活动，将导致投标被拒绝，并由其承担相应的法律责任。

六、授予合同

22.合同授予标准

22.1 买方将把合同授予符合招标文件的要求，并能圆满地履行合同的，对买方最为有利的得分最高的投标方。

22.2 最低报价不是被授予合同的保证。

23. 买方接受和拒绝任何或所有投标的权利

买方保留在授标之前任何时候接受或拒绝任何投标，以及宣布招标程序无效或拒绝所有投标的权利，对于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。

24. 采购中心宣布废标的权利

24.1 出现下列情况之一时，采购中心有权宣布废标，并将理由通知所有投标人：

（1）符合专业条件的投标人或者对招标文件作实质性响应的投标人不足三家的；

（2）出现影响采购公正的违法、违规行为的；

（3）投标人的报价均超过了采购预算，采购人不能支付的；

（4）因重大变故，采购任务取消的。

24.2 有下列情况之一的投标文件，将做无效投标处理：

(1) 投标文件无法按规定解密；

(2) **不具备招标文件中规定的资格要求的；**

(3) **投标报价不按招标文件规定的计价办法投报或超过招标文件规定的预算金额或投标最高限价；**

(4) **投标文件未按招标文件要求签署、盖章的；**

(5) 未按规定格式填写,内容不全或字迹模糊,辨认不清；

(6) 经行贿犯罪档案查询，被政府采购监督管理部门禁止参加政府采购活动的；

(7) **经信用信息查询，投标供应商被列入失信被执行人、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；**

(8) 不同投标人的投标文件出现了评标委员会认为不应当雷同的情况；

(9) 投标人递交两份或多份内容不同的投标文件，按招标文件规定提交备选投标方案的除外；

(10) 投标文件未对招标文件作出完全的、实质性响应,导致投标无效；

(11) 投标文件含有采购人不能接受的附加条件的；

(12) 因不可抗力造成投标文件遗失或损坏的。

25.中标通知

25.1 评标结束后，采购中心将向中标单位签发《中标通知书》,《中标通知书》一经发出即发生法律效力。

25.2 采购中心同时通过指定网络发布评标结果公告。采购中心对未中标的投标人不作未中标原因的解释，不退还投标文件。

25.3 中标通知书是合同的组成部分。

26. 签定合同

26.1 中标人应按采购中心规定的时间、地点与采购人签定中标合同。中标人不得再与采购人签署订立背离合同实质性内容的其它协议或声明，否则按开标后撤回投标处理。

26.2 中标人应按照招标文件、投标文件及评标过程中有关的澄清文件的内容与采购人签订合同。

26.3 投标人一旦中标，签订合同后，未经监管部门书面同意不得转包，否则将被视为中标后

撤回投标处理。

27. 履约保证金

27.1 中标人在总合同签定后十五（15）天内，应按照合同条款的规定，按照招标文件中提供的履约保证金格式向买方提交履约保证金。

27.2 如果中标人没有按照投标人须知第 26 条、第 27.1 条规定执行，买方将有充分理由取消原中标决定并没收其投标保证金。在此情况下，买方可将该标授予下一个综合评标得分最好的投标人，或重新招标。

28. 腐败和欺诈

28.1“腐败行为”是指提供、给予、接受或索取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行为;“欺诈行为”是指为了影响采购过程或合同实施过程而谎报事实，损害采购人的利益，包括投标人之间串通投标（递交投标书之前或之后），人为地使投标丧失竞争性，损害采购人从自由公开竞争中所能获得的权益。

28.2 如果买方认为所建议的中标人在本合同的竞争中有腐败和/或欺诈行为，则将拒绝该授标建议。

七、中标服务费

29. 中标服务费

29.1 本次招标不收取中标服务费，请投标人在测算投标报价时充分考虑这一因素。

八、询问和质疑

30. 询问和质疑

30.1 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。

30.2 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。其中，对招标文件的质疑，应当在其收到或下载招标文件之日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。投标人提出质疑应当坚持依法依规、诚实信用原则，并应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。

30.3 质疑函应明确阐述招标文件、招标过程或中标结果中使自己合法权益受到损害的实质性内容，具体、明确的质疑事项和与质疑事项相关的请求，提供相关事实依据、必要的法律依据和证据及其来源或线索，以便于有关单位调查、答复和处理。

30.4 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。

30.5 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。

30.6 投标人提起询问和质疑，应当按照《徐汇区政府采购中心质疑答复处理规程》的规定办

理。质疑函应当由质疑供应商法定代表人签字并加盖公章。质疑函应当按照财政部制定的范本填写，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。质疑供应商委托代理人办理质疑事务的，应当向徐汇区政府采购中心提交供应商法定代表人签署的授权委托书和身份证明。质疑函的递交可以采取邮寄、快递或当面递交形式。接收质疑函的联系人：柳老师，联系电话：021-24092222*2591，通讯地址：上海市南宁路 969 号。

九、保密和披露

31. 保密和披露

31.1 投标人自领取招标文件之日起，须承诺承担本招标项目下保密义务，不得将因本次招标获得的信息向第三人外传。

31.2 采购中心有权将投标人提供的所有资料向其他政府部门或有关的非政府机构负责评审标书的人员或与评标有关的人员披露。

31.3 采购中心有权在认为适当时，或在任何第三人提出要求（书面或其他方式）时，无须事先征求中标人同意而披露关于已订立合同的资料、中标人的名称及地址、中标货物的有关信息以及合同条款等。

第三部分　招标项目需求

一、 项目概述

(一) 项目背景

随着上海“智慧公安”创新发展日益深入，新兴智能感知技术不断应用于公安实战业务中，为推进“感知泛在、研判多维、指挥扁平、处置高效”的精准警务模式提供了强大动力。作为承载“智慧公安”运行的基础设施，“神经元”感知网（以下简称感知网）已是上海公安最为重要的通信网络，是实现现代警务信息化、智能化的重要基石之一。感知网的网络安全态势关系到“智慧公安”各应用系统、终端设备、数据资源能否稳定运行，关系到全体民警能否顺利开展各项工作，也关系到城市运行管理能否始终有条不紊地进行。

近年来，随着大数据、云计算、物联网等新技术、新应用在公安信息化建设中的逐步深入开展，公安信息网所承载的业务和内容发生了翻天覆地的变化，应用查询、视频图像、加密通信、虚拟网络等网络流量呈急剧上升的势头，网络拥塞现象时有发生，带宽扩容需求日益迫切，这些变化给网络的运维和管理工作带来了巨大的挑战。为适应新形势、新变化、新任务，提供高质量的网络管理服务，需要不断提高网络管理的深度和广度。按照公安部规划要求以及公安信息网建设要求，需要切实加强网络流量分析管控工作，不断提升网络态势感知、发现分析预警、流量趋势预测和风险评估处置等能力，达到由传统运维方式向自动化、智能化、标准化、可视化运维的转变，将公安信息网网络服务保障水平提高到新的高度和层次。

上海市公安局于 2020 年 9 月下发文件《上海市公安局融合承载网建设配套任务书》，分局需要完成 “上海市公安局融合承载网”的配套任务。另外，随着大数据、云计算、物联网等新技术、新应用在公安信息化建设中的逐步深入开展，公安信息网所承载的业务和内容发生了翻天覆地的变化，应用查询、视频图像、加密通信、虚拟网络等网络流量呈急剧上升的势头，网络拥塞现象时有发生，带宽扩容需求日益迫切，这些变化给网络的运维和管理工作带来了巨大的挑战。为适应新形势、新变化、新任务，提供高质量的网络管理服务，分局需要不断提高网络管理的深度和广度。

(二) 系统现状

徐汇分局网络和应用系统包括公安信息网（公安网）、公安感知网（感知网），以及互联网安全态势感知系统、互联网管理综合平台、区域无线上网终端管控系统、公安网虚拟资源

计算平台、感知网虚拟资源计算平台、协同办公应用系统、数字警务综合应用系统（情指行）、智能感知系统等。

网络和信息安全系统主要由软件安全系统和硬件安全设备所组成，主要包括安全网络管理系统、终端防病毒系统、“一机两用”终端防护系统，以及相应硬件设备，包括防火墙、入侵检测、网络安全审计和防病毒邮件网关。

目前徐汇分局网络终端数量约 3879 台，防火墙 20 台（分局派出所部署 13 台），入侵检测、网络审计、防病毒邮件网关各 1 台。

二、建设内容

（一） 感知网安全建设

以产品租赁的形式，完成感知网安全建设，租赁时间为 2 年,具体租赁产品如下：

1、 公安感知网部署万兆防火墙 2 台（万兆防火墙 A），作为边界接入防火墙，提供边界隔离与访问控制功能。

2、 公安感知网部署万兆防火墙 4 台（万兆防火墙 B），作为服务器区防火墙，提供服务器及其承载系统和数据的通信访问控制功能。

3、 公安感知网部署入侵检测 4 台。其中 2 台部署在边界接入网络节点，另外 2 台部署在服务器区接入网络节点，分别提供边界接入、服务器等重要节点的网络入侵攻击双向检测与响应处置能力。

4、 公安感知网部署防毒墙 4 台。其中 2 台部署在边界接入网络节点，另外 2 台部署在服务器区接入网络节点，分别提供边界接入、服务器等重要节点的网络恶意代码攻击检测防御功能。

5、 公安感知网部署流量探针 1 台，旁路监听边界接入网络节点通信流量。针对通信流量进行全面深度检测，识别潜在的威胁与安全风险，实现全流量威胁监测与数据上报功能。

6、 公安感知网部署 WEB 应用防火墙 2 台，提供 WEB 应用层面的攻击行为检测与拦截，为感知网业务系统和数据安全提供保障。

7、 公安感知网部署堡垒机 1 台，作为感知网网络设备、安全设备、服务器、数据库等资产集中运维管理平台，保障日常运维安全。

8、 公安感知网部署日志审计 2 台，集中管理感知网网络设备、安全设备、服务器、数据库等资产的系统日志，数据保留周期不少于 6 个月。

9、 公安感知网部署数据库审计 1 台，对访问数据库的通信流量、内容进行全面安全审计，识别异常行为，检测针对数据库的攻击行为，保障感知网数据库以及数据的安全。

10、 公安感知网部署漏洞扫描 1 台，全面发现感知网网络与信息系统资产存在的漏洞，提供漏洞评估报告和修复建议。

11、 公安感知网部署态势感知 1 台，运用大数据分析和威胁建模等多种技术手段，对公安感知网网络与信息系统存在的安全问题进行全面发现，识别网络中潜在的安全风险。作为公安感知网网络安全风险统一监测平台，为公安感知网网络安全管理与决策提供数据支撑。

12、 公安感知网部署安全监测设备 15 台（13 台部署在徐汇各派出所，2 台设备部署在分局本部），实现准入控制、资产感知、视频协议分析。设备继承安全监测设备平台提供安全基线策略，执行安全监测设备平台阻断策略，根据安全监测设备平台的策略执行结果输出记录，并上报至安全监测设备平台。

13、 公安感知网部署防病毒客户端 2 套（2000 台终端授权），提供终端层面的恶意代码防范功能，保障分局终端办公安全。

（二） 流量分析平台建设

新增采购一套网络流量分析平台（2 台 10GB 流量采集设备，为流量分析系统提供数据支撑；新增 1 套流量分析软件，为网络智能应用提供平台支撑）。通过网络流量采集分析系统建设，初步需具备以下功能：一是实现对业务应用和协议识别。二是实现对网络异常行为识别。三是实现排障需求：对网络故障和服务质量下降进行定位和故障排除。四是实现回溯需求：对网络事件进行回放和问题追踪。五是实现预测需求：对业务流量趋势分析，提前感知网络状态变化。六是实现协作需求：分析流量特征，为其它平台提供流量以及流量指标。同时根据市局平台的规范接口，能够实时的上报本级公安网流量指标，保障市局平台调取分局数据的完整性与实时性。

（三） 融合承载网配套建设

根据“上海市公安局融合承载网项目”的徐汇分局相关配套任务，采购 1 套核心层传输设备和 1 套汇聚层传输设备，完成网络改造与业务迁移。核心层设备由市局统一规划使用于公安融合承载网核心层相关节点使用，汇聚层设备按市局规划用于公安融合承载网徐汇分局节点使用。

（四） 安全运维服务

提供网络安全服务，包括日常维护服务、安全培训服务和设备保修服务。日常维护服务时间周期为 2 年，服务内容包括配置维护、系统巡检、日志分析、安全评估、安全值守、应急响应和咨询分析。安全培训服务时间周期为 2 年，每年组织开展 1 次攻防演练技术培训。设备保修服务时间周期为 2 年，对分局现有网络安全硬件设备提供原厂保修。

三、项目采购具体需求

（一） 感知网安全建设

产品租赁包含产品使用以及规则库更新，所提供的租赁设备需为全新设备。分局不承担其他额外费用。产品性能及具体参数如下：

1、 万兆防火墙 A

指标项	参数要求
硬件配置	冗余电源，配置不少于 8 个千兆电口、2 个千兆 SFP 接口插槽、2 个万兆 SFP+接口插槽，≥2 个可插拔扩展槽；
系统性能	吞吐≥30Gbps，并发连接≥300 万；
系统要求	产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制；（提供资质证书证明）
工作模式	支持路由、交换、虚拟线、Listening、混合工作模式；
路由交换	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP、ISP 路由，内置移动、联通、电信、教育网、网通、长城宽带等 ISP 服务商地址列表，可通过 Web 界面选择不同的 ISP 服务商实现快速切换；
	支持 802.1q、QinQ 模式；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；（提供截图证明）
链路聚合	支持手动和 LACP 链路聚合，可根据源/目的 mac、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 10 种链路负载算法；
IP/MAC 绑定	支持 IPv4/v6 双栈 IP/MAC 静态和动态探测绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出；

	支持防共享接入功能，能够有效识别、报警并阻断局域网网络共享行为；（提供资质证书证明）
地址转换	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
访问控制	支持一体化安全策略配置，可以通过一条策略实现五元组信息源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT 等功能配置,简化用户管理；
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；（提供资质证书证明）
双栈模式	支持 IPv4/IPv6 双栈工作模式；
	支持 NAT64,支持静态转换和前缀转换方式。支持 NAT66 地址转换，支持源地址转换；
	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
连接控制	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
未知威胁防御	支持异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供截图证明）
DDOS 防御	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
	支持静态白名单和动态黑名单功能；
文件过滤	支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件

	等超过 50 种文档类型的文件过滤；
内容过滤	支持基于 http、ftp、telnet、smtp、pop3 等协议的内容过滤策略，可对 FTP 上传/下载的文件名进行过滤，同时支持过滤 FTP 信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；
黑名单	支持静态黑名单功能，可设置多个对象条件，如：五元组信息、源 MAC、地址范围、应用、用户，实现对特定报文进行快速过滤；
	支持动态黑名单功能，可与 URL 过滤、病毒过滤、防代理功能实现联动封锁；
产品资质	提供国家信息安全测评自主原创产品测评证书；
	提供国家信息安全测评信息技术产品安全测评证书（级别：EAL4+）；

2、 万兆防火墙 B

指标项	参数要求
硬件配置	2U 机箱，冗余电源，配置不少于 2 个千兆电口、2 个万兆 SFP+接口插槽，≥3 个可插拔扩展槽；
系统性能	吞吐≥40Gbps，并发连接≥800 万；
系统要求	产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制；（提供资质证书证明）
工作模式	支持路由、交换、虚拟线、Listening、混合工作模式；
路由交换	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP、ISP 路由，内置移动、联通、电信、教育网、网通、长城宽带等 ISP 服务商地址列表，可通过 Web 界面选择不同的 ISP 服务商实现快速切换；
	支持 802.1q、QinQ 模式；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；（提供截图证明）
链路聚合	支持手动和 LACP 链路聚合，可根据源/目的 mac、源/目的 IP、源/目

	的端口、五元组、端口轮询等条件提供不少于 10 种链路负载算法；
IP/MAC 绑定	支持 IPv4/v6 双栈 IP/MAC 静态和动态探测绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出；
	支持防共享接入功能，能够有效识别、报警并阻断局域网网络共享行为；（提供资质证书证明）
地址转换	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
访问控制	支持一体化安全策略配置，可以通过一条策略实现五元组信息源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT 等功能配置,简化用户管理；
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；（提供资质证书证明）
双栈模式	支持 IPv4/IPv6 双栈工作模式；
	支持 NAT64,支持静态转换和前缀转换方式。支持 NAT66 地址转换，支持源地址转换；
	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
连接控制	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
未知威胁防御	支持异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；
DDOS 防御	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；

	支持静态白名单和动态黑名单功能；
文件过滤	支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
内容过滤	支持基于 http、ftp、telnet、smtp、pop3 等协议的内容过滤策略，可对 FTP 上传/下载的文件名进行过滤，同时支持过滤 FTP 信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；
黑名单	支持静态黑名单功能，可设置多个对象条件，如：五元组信息、源 MAC、地址范围、应用、用户，实现对特定报文进行快速过滤；
	支持动态黑名单功能，可与 URL 过滤、病毒过滤、防代理功能实现联动封锁；
产品资质	提供国家信息安全测评自主原创产品测评证书；
	提供国家信息安全测评信息技术产品安全测评证书（级别：EAL4+）；

3、 入侵检测

指标项	参数要求
硬件配置	2U 机箱，冗余电源，配置不少于 6 个千兆电口（支持 Bypass）、4 个千兆 SFP 接口插槽、2 个万兆 SFP+接口插槽，支持另扩展万兆光口；
系统性能	入侵攻击防护吞吐≥2Gbps，并发连接≥150 万；
系统要求	设备采用自主知识产权的专用安全操作系统，采用多核平台并行处理特性；（提供资质证书证明）
流量采集	支持流量采集功能，支持在设备界面对服务器地址、端口、以及采样百分比进行设置；（提供截图证明）
	支持流量采集策略设置，对流量采集的方向、时间、源 IP 地址、目的 IP 地址、源端口、目的端口进行设置；
入侵检测	支持融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵检测；
	支持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、系统漏洞类等在内的超过 5900+种攻击事件；
	支持自定义规则，并且自定义规则库可以导入导出；
	采用 “一种建立多核运行环境的方法”技术，可以使设备具有较高的检测性能；（提供资质证书证明）
	厂商需具备强大的漏洞和攻防研究能力，为 CNNVD 一级技术支撑单位和 CNVD 技术组成员，且同时获得 CNVD 2021 年度漏洞信息报送突出贡献单位、2021 年度原创漏洞发现突出贡献单位、2021 年度漏洞处置突出贡献单位；（提供资质证书证明）
攻击取证	支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据；
流量异常检测与告警	支持对设备接口流量的阀值进行设置及报警；
	支持对网络内的 TCP、UDP、其他流量协议占比进行设置及报警；
	支持对协议组的流量阀值和连接数进行设置及报警，协议组类型包括 P2P 类、即时通讯类、标准协议类、移动应用类、http 应用类、工控互联网类等；
威胁处置	支持与本项目涉及的防火墙进行联动，及时处置网络安全攻击；（提供截图证明）
DDOS 检测	支持检测包括 land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_opTSon、teardrop、targa3、ipspoof、Synflood、Icmpflood、Udpflood、Portscan、ipsweep 等在内的 DOS/DDOS 攻击；
	支持 DDOS 机器人自学习功能，学习时间可设置；
日志管理	支持多种形式的日志存储,本地存储、发送至日志服务器、本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式；
	支持攻击检测日志中可以直观的展示攻击事件中的攻击特征编码；（提供截图证明）
报表系统	支持按照时间、源 IP、源端口、目的 IP、目的端口、网络接口、风险级别等条件生成统计分析报表，报表内容包括攻击防护、病毒过滤、应用管控、URL 过滤四大类；

	支持生成日报、周报、月报，支持报表以 word、html 格式导出，支持定时通过邮件方式自动发送报表；
系统告警	支持对管理、系统、策略、安全、流量等告警；
	支持邮件、声音、snmp 多形式的告警方式；
产品资质	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（三级）；
	提供中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（级别：EAL3+）；
	提供中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证证书》；
	提供国家信息安全漏洞库兼容性资质证书；

4、 防毒墙

指标项	参数要求
硬件配置	2U 机箱，冗余电源，配置不少于 6 个千兆电口（支持 Bypass）、4 个千兆 SFP 接口插槽、2 个万兆 SFP+接口插槽，≥2 个可扩展插槽；
系统性能	防病毒吞吐≥2.5Gbps，并发连接≥400 万；
系统要求	设备必须为专业的防病毒网关产品，非防火墙/下一代防火墙、UTM、IPS 等具有防病毒功能模块的产品；
	设备采用自主知识产权的专用安全操作系统，采用多核平台并行处理特性；（提供资质证书证明）
部署模式	支持透明部署，即插即用。支持多链路防护；
	支持多接口可旁路的病毒监听检测模式，可并行监听检测多条链路、多个网段内的病毒传输行为；
防病毒	支持双库双引擎，可选择使用不同的病毒库，可选择使用不同的扫描引擎（快速扫描引擎或深度扫描引擎）；（提供截图证明）
	病毒库总数大于 600 万，可本地化完成病毒地检测过滤与处理，无需发送到云端检测；
	能够防御病毒、木马、蠕虫、间谍软件等恶意软件，且支持对压缩数据、加壳病毒的检测与处理；

	支持对 HTTP、FTP、POP3、 SMTP、IMAP 等常用应用协议进行病毒检测与过滤；
	可实时检测日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止内部网络因遭受蠕虫攻击而陷于瘫痪；
	支持 TCP 粘合技术，提升病毒检测效率；
	病毒引擎具备自动化的数据解压缩能力，无需手动配置，且至少具备 15 层的数据解压缩能力；
	支持 IPv4 和 IPv6 双栈协议的病毒扫描与检测过滤；（提供截图证明）
	支持智能检测应用协议的病毒行为，采用自动智能方式准确识别并扫描检测常用应用协议任意端口的病毒传输行为，而非通过传统手动配置协议端口绑定形式进行病毒扫描；
	要求流行病毒检测率不低于 95%；（提供国家专业病毒检测机构的证明）
内容过滤	支持 URL 过滤方式阻止非法数据进入内部网络，并且能够针对“ActiveX”、“Java Applets”及“Script”等控件实施拦截；
	支持对邮件内容的过滤，至少具有邮件主题关键字过滤、附件名称过滤、带密码保护的附件过滤等；
	可自定义禁止传输的文件类型；
	支持基于 IP 地址黑白名单、邮件地址黑白名单的垃圾邮件过滤；
产品资质	提供公安部颁发的计算机信息系统安全专用产品销售许可证（网关防病毒产品（增强级））；
	提供国家信息安全测评信息技术产品安全测评证书（级别：EAL3+）；

5、 流量探针

指标项	参数要求
硬件配置	2U 机箱，冗余电源，配置不少于 6 个千兆电口、4 个千兆 SFP 接口插槽，≥5 个可扩展插槽；
系统性能	综合威胁吞吐≥3Gbps，并发连接≥150 万；
系统要求	设备采用自主知识产权的专用安全操作系统，采用多核平台并行处理特性；（提供资质证书证明）
攻击检测	支持独立的攻击检测引擎，支持 8800 种以上的攻击规则库；

	支持扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、URL 跳转、跨站攻击、Webshell 等多种常见攻击行为；
	支持对攻击逃逸的单向/双向/深度/智能检测，包括 IP 分片、TCP 分段、TCP 校验和攻击、TCP 标志位攻击、HTTP-Header 折叠、HTTP 请求伪造参数攻击、URL 多重编码、URL NULL 字符分割攻击等类型；
	支持暴力破解检测，包括 SMTP、FTP、SMB、TELENT、LDAP、ORACLE、MYSQL、MSSQL、MONGODB、REDIS、HTTP 等协议的口令暴力破解行为，支持对发生的暴力破解行为事件进行取证；
僵木蠕检测	采用僵尸主机与控制主机异常通信行为检测的方式，具有独立的僵尸主机特征库，能够对 10000 种以上僵尸主机行为进行监测，包括僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT 等多类型的僵尸主机行为；（提供截图证明）
	支持隐蔽通信检测，支持对 HTTP、FTP、SMTP、IMAP、POP3、TELENT 等服务的隐蔽通信检测；
	支持 DGA 域名检测，采用机器学习引擎和深度神经网络学习引擎进行检测，用户可设置敏感度；
DDoS 检测	支持独立的 DDoS 检测引擎，支持对 IP 扫描攻击、端口扫描攻击等多种扫描攻击行为检测；支持 IP FLOOD 攻击检测、IP FRAG FLOOD 攻击检测、DOS 攻击检测、ICMP FLOOD 攻击检测、TCP FLOOD 攻击检测、HTTPS 自定义端口等多种 FLOOD 攻击检测；
	支持 DDOS 自学习模式检测，可设定学习时长，根据周期内流量状态自动学习，设置流量阈值，流量状态异常触发阈值，系统自动进行告警；
恶意程序检测	支持对恶意程序实现特征检测、机器学习检测、内置虚拟沙箱检测等多种检测方式，并且多种检测方式相互独立、互不影响；
	支持使用 HTTP、FTP、SMTP、POP3、IMAP、SMB、NFS 等非加密协议以及 HTTPS、FTPS、SMTPS、IMAPS 等加密协议传输的文件检测；（提供截图证明）
APT 检测	支持通过威胁情报检测已知 APT 事件，通过恶意程序检测未知 APT 事件，通过僵尸行为规则库检测已知的 APT 组织；

威胁情报	威胁情报库数量超过 820 万，可通过手动添加、批量导入的方式自定义威胁，并且满足威胁白名单能力；
加密流量检测	支持卸载 SSL，实现对 HTTPS、SMTPS 等加密流量的分析检测；
URL 检测	支持展示日、周、自定义周期的 URL 过滤事件、联动阻断次数和告警次数。支持展示联动阻断事件 TOP10、警告事件 TOP10、联动阻断主机 TOP10、警告主机 TOP10、联动阻断网址分类统计、警告网址分类统计；
威胁处置	支持与本项目涉及的防火墙联动，支持设置联动防火墙名称、地址、共享秘钥；支持设置防火墙阻塞时间；（提供截图证明）
流量审计	支持对 TCP/UDP 协议、ICMP 协议、HTTP 协议、SMTP 协议、POP3 协议、IMAP 协议、SIP 协议等流量深入内容层解析元数据；
应用识别	支持对 HTTP 应用、IM 文件传输、P2P 视频、P2P 音频、P2P 下载、即时通讯、工控物联网、加密隧道、数据库、移动应用等类型超过 4200 种应用识别；
溯源取证	支持全流量取证，将事件发生前后的流量一起留存，支持攻击取证、僵尸主机取证、恶意程序样本、威胁情报取证，取证类型支持报文取证和样本文件取证两种形式；（提供截图证明）
日志管理	支持对攻击事件、僵尸主机事件、恶意程序传播、威胁情报、URL 过滤、DDoS 攻击、IP 黑白名单、恶意加密流量等多种事件日志记录；
产品资质	提供计算机软件著作权登记证书；
	提供国家信息安全漏洞库兼容性资质证书；

6、 WEB 应用防火墙

指标项	参数要求
硬件配置	2U 机箱，冗余电源，配置不少于 6 个千兆电口、4 个千兆 SFP 接口插槽、2 个万兆光口（含光纤模块），支持另扩展万兆光口；
系统性能	应用层吞吐≥2.5Gbps，并发连接≥200 万；
系统要求	产品为专业 Web 应用安全防护系统硬件设备，而非下一代防火墙、UTM 类设备集成的 WEB 防护功能模块；
	设备采用自主知识产权的专用安全操作系统，采用多核平台并行处理特性；（提供资质证书证明）

工作模式	支持透明模式串联部署、旁路监测模式部署、负载均衡模式部署、反向代理模式部署；
访问控制	支持网络层访问控制，支持基于源 IP 、目的 IP 及源目的区域、服务类型等条件的访问控制；
	支持应用层访问控制功能，针对 HTTP 请求字段进行过滤，包括 HTTP 协议版本，请求方法，Cookie 信息等；
WEB 攻击防护	支持恶意扫描防护：通过人机识别方式，进行恶意扫描智能检测；支持扫描防护阈值设置和扫描 IP 的阻断周期设置；
	支持多种爬虫攻击防护：包括内置爬虫对象库，自定义爬虫对象，导入或者下载后端服务器 robots.txt 等方式提供爬虫攻击防护；
	支持 API 接口防护：XML 基础校验，XML schema 校验，WSDL 校验；
DDoS 攻击防护	支持基线学习，可以自动学习用户 http 正常流量阈值模型，并给出推荐阈值配置项；DDoS 流量支持检测清洗和强制防御两种模式（提供截图证明）；
	支持 DDoS 攻击动态黑名单功能，检测到 DDoS 攻击将其攻击源自动加入黑名单；
威胁处置	支持与本项目涉及的防火墙联动，提供闭环的 web 安全解决方案；（提供截图证明）
网页防篡改	网关型网页防篡改，无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容；
	缓存型网页篡改防护；WAF 通过将缓存的网站页面返回给客户端，从而保证客户端无法看到被非法篡改的页面，来做到网页篡改防护；
WEB 漏洞扫描	支持虚拟补丁功能，支持导入 WAF 内置扫描器及 appscan、w3af 等第三方扫描器的扫描结果生成 WAF 的防护规则，对此类网站漏洞直接防护；
应用交付	支持 WEB 缓存,URL 重写，HTTP 压缩等应用交付功能；
健康检查	支持对防护的 WEB 服务器进行健康检查，可以实时监测服务器的活跃状态，并且可定期备份健康记录；
日志管理	日志支持以 syslog 和 welf 两种格式向远端日志服务器发送日志，日

	志传输可加密，且管理员可以配置加密密码； 支持日志敏感信息脱敏，记录日志时将敏感数据替换为某个特定字符；
产品资质	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》； 提供中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》； 提供 IPV6 金牌证书(专业 WAF 类) ； 提供国家信息安全漏洞库兼容性资质证书；

7、 堡垒机

指标项	参数要求
硬件配置	配置不少于 6 个千兆电口、2 个千兆 SFP 接口插槽，≥2 个可扩展插槽，≥2T 存储；
系统性能	≥200 资源授权，用户数不限制；
系统要求	设备采用专用安全操作系统，采用多核平台并行处理特性；（提供资质证书证明） 采用模块化设计，可以通过扩展卡来增减业务接口，而非软件运维安全审计系统；
工作模式	采用物理旁路部署，不改变现有网络结构； 支持双机部署，保证系统发生故障时的可用性；
认证管理	支持双因子认证； 认证方式支持 OTP 动态口令认证、短信认证、数字证书认证、USB-KEY 认证、人脸识别等双因素认证方式； 支持第三方证书用户自行上传用作校验的 CA 证书和 CRL 列表； 本地 CA 支持根证书的重新生成及替换； 支持根据根证书签发出客户端证书； 支持发布生成吊销列表； 支持国密证书认证；（提供截图证明） 支持管理员通过发布公告的形式，发送通知给所有指定用户； 支持公告有效期设置，支持定期（固定时间）和周期两种（每日/每周

	/每月）方式；
资产管理	支持资产网域化管理，按照不同局域网进行资产配置和管理；
	支持混合云资源的管理，即公有云及局域网资源，支持主机、服务器、网络设备、安全设备、数据库等的资产管理； 满足公有云、云资源池、数据中心多种运维场景； 公有云设备支持一键更新发现功能；
	支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长 TOP10、今日告警总数、今日运维指令 TOP10 等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况；
	通过 IP 网段扫描，快速发现指定 IP 地址范围内的资产，并自动识别 IP 和端口，方便管理员快速添加资产；
账号管理	支持改密结果可通过邮箱、FTP 方式外发； 密码采用密码信封加密保存，以保证安全性； 支持密钥加密和明文分段发送；
运维授权	提供授权关系查看功能，图形化直观展示用户、资产、协议、账号的授权关系；（提供截图证明）
应用管理	支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不作二次开发的情况下，可灵活扩展且实现帐号口令的代填；
审计管理	支持全文审计检索； 可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯；
	支持对目标资产性能状况进行监控告警，包括 CPU、内存、磁盘、发送流量和接收流量；
	支持图形化查看用户的运维记录，查询结果以鱼骨图按照时间倒序自上而下而下展示，每个时间点详细记录运维资产、运维用户、账号、协议、会话时长等详细信息；

	支持每个运维节点可以定位至该条会话记录； 支持图形化查看账号改密历史记录，查询结果以鱼骨图按照时间倒序自上而下展示，每个节点详细记录改密信息及结果； 支持每个改密节点可以定位、查看和下载密码信封； 内置丰富报表统计模板：协议运维排名、资产运维次数 top10、资产运维趋势 top10、用户运维趋势 top10、协议运维趋势、指令分布 top10、风险指令次数、等多种类型报表模板；
系统管理	支持对堡垒机虚拟为多台逻辑堡垒机，虚拟堡垒机之间实现独立配置、独立数据，实现 IT 资源的动态分配；
产品资质	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（运维安全管理产品（增强级））； 提供国家信息安全测评信息技术产品安全测评证书（级别：EAL3+）； 提供 IPV6 金牌证书；

8、 日志审计

指标项	参数要求
硬件配置	配置不少于 7 个千兆电口，内存≥16G；SSD 系统盘≥240G；数据盘存储容量≥12T，支持 Raid5；
系统性能	≥100 个日志源授权； 日志采集处理速度≥10000EPS； 数据存储：压缩加密存储，压缩比不低 10:1；日志存储不低于 10000 条/M ； 支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于 10s；
工作模式	支持单级部署和代理分布式部署采集日志；
数据采集	支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据； 支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志；

	支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；（提供截图证明）
	支持 IPv6/IPv4 双栈环境部署，对 IPv6/IPv4 日志源的日志进行高速采集；
数据存储	支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数；
	支持 IPv6 日志的全量存储；
数据查询	支持以全国地图展示最近 24 小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能通过首页地图快速查询指定区域的日志详细信息；
	支持为不同类型日志设置不同的查询条件和显示条件；
	支持在日志查询结果上针对源 IP、目的 IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源 IP 和目的 IP（公网地址）还支持以地图方式展示；
	支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析；
告警管理	支持首页展示当日告警情况统计；支持展示当日最新告警 TOP10、TOP30 和 TOP50；
	支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备 IP、源 IP、目的 IP 等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出；
报表管理	系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；
日志源管理	支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息；

	支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示；（提供截图证明）
	支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据；
系统管理	具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置；
	支持将常用 IP 地址或 IP 地址网段标记为自定义名称，在日志查询界面可以在 IP 列中对应悬浮显示自定义名称；
产品资质	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（增强级）；
	提供中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证证书》；
	提供 IPV6 金牌证书；
	提供信息系统建设和服务能力等级证书（优秀级（CS4））。

9、 数据库审计

指标项	参数要求
硬件配置	冗余电源，配置不少于 6 个千兆电口、4 个千兆 SFP 接口插槽和 2 个可扩展槽位，≥2T 存储空间；
系统性能	审计处理能力≥2Gbps,峰值 SQL 处理能力≥15000 条/秒，日志存储能力≥40 亿条；
部署模式	支持旁路部署，对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括以下几种：WinSer2003/2008/2012/2016、Centos、opensuse、redhat、Ubuntu、中标麒麟 SV1.2-龙芯、银河麒麟 SV1.3-飞腾、银河麒麟 server-飞腾等、AIX5/6；
IPv6	支持 IPv6 网络环境下的数据库审计，可识别 IPv6 的相关主体与客体资源；（提供资质证书证明）
数据库审计	支持 Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、

	Teradata 等数据库系统；
	支持 Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis 等国际主流数据库系统；
	支持 KingBase、DaMeng、Oscar、GBase、Inspur_KDB、Highgo、GaussDB 等国内主流数据库系统；
	支持数据库请求和返回的双向审计，特别是返回字段和结果集、返回码、SQL 错误信息、返回行数、执行时长等内容；
	支持通过返回行数控制返回结果集审计大小，降低系统开销。可配置返回行数，不低于 100 万行；
业务审计	支持 HTTP、Telnet、FTP、SMTP、IMAP、POP3 的审计；
审计粒度	系统支持详细的审计日志，审计元素包括执行人 who、执行内容 what、执行时间 when、执行地点 where、执行方式 how、影响范围 Range、执行结果 ResultSet；
数据库发现	支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息；
数据库监控	支持依据数据库实例监控各个数据的数据库类型、活跃会话数、总会话数、负载等信息；
	支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估；
弱口令检测	支持数据库服务器弱口令扫描，扫描出的弱密码支持脱敏显示；
数据库攻击行为审计	支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为，利用漏洞攻击等行为进行审计，并进行实时报警；（提供截图证明）
异常行为识别	支持基于 SQL 操作进行基线构建和基线管理，支持引用基线进行告警配置；
复杂 SQL 审计	支持超长 SQL 语句审计，至少不低于 2M；
	支持嵌套 SQL 语句的审计；
	准确审计绑定变量的 SQL 语句；

	有效分割、准确审计主流数据库协议的多 SQL 语句；
联动处置	支持与本项目防火墙联动阻断功能；（提供截图证明）
磁盘管理	支持手动、自动方式的磁盘清理，可根据剩余空间、保存时限等条件灵活设置，磁盘空间占用情况的检查频率可灵活设置：10min、30min、1h、3h、6h、24h 等时长；
会话回放	支持会话回放功能,并至少支持 0.5 倍速、1 倍速、1.5 倍速、2 倍速、4 倍速五级播放速度调节；
产品资质	提供《计算机信息系统安全专用产品销售许可证》（数据库安全审计类（增强级））；
	提供中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证》、《中国国家信息安全产品认证》证书；
	提供中国信息安全测评中心颁发的国家信息安全测评信息技术产品安全测评证书（级别：EAL3+）；

10、 漏洞扫描

指标项	参数要求
硬件配置	冗余电源，内存≥16G，硬盘≥1T，配置不少于 6 个千兆电口、4 个千兆 SFP 接口插槽和 2 个扩展槽位；
系统性能	支持无限制 IP 扫描，并发扫描≥15 个系统扫描任务； 支持不少于 200 个域名（web）扫描，并发扫描≥6 个域名（web）扫描任务； 支持不少于 500 个配置核查目标，并发扫描≥10 个配置核查任务；
系统漏洞扫描	支持扫描系统漏洞数量大于 190000 种，web 漏洞数量大于 3000 种,数据库大于 2500 种，CVE 漏洞数大于 60000；
	产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD 编号；
	支持扫描主流操作系统、web 服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞；
	支持扫描虚拟机安全漏洞，如 VMWare、EXSI、KVM、XEN、XenServer、HyperV，可扫描漏洞数量大于 1500 条；

	支持扫描大数据组件的安全漏洞，如 Spark、Splunk、Kafka、Storm、Cassandra、Ambari、Impala、Solr、Oozie、Hbase、Hadoop 等；（提供截图证明）
	支持对 DB2、MSSQL、MySQL、Oracle、GBASE、DMDB 等主流数据库进行登陆认证扫描；
Web 漏洞扫描	支持通过代理服务器扫描目标 url，代理报文可选 http、http1.0、socks4、socks4a、socks5、socks5h 等多种类型；
	支持被动扫描功能，通过代理获取审计页面；（提供截图证明）
	扫描对象支持手动输入、批量文件导入及站点组导入，支持填写排除目标；
	支持显示站点树，包括站点目录信息、文件信息；
	http 认证类型支持 auto、basic、digest、ntlm；
	支持自定义路径，对有爬取限制链接进行深度扫描；
	支持排除路径名，可自定义无需爬取的 URL 链接；
	支持自定义 http 请求，包括 UserAgent、http cookie、http header、超时时间、重试次数、表单输入；
弱口令扫描	支持 DB2、FTP、IMAP、MSSQL、MYSQL、Oracle、POP3、POSTGRES、RDP、Redis、RTSP、SMB、SMTP、SNMP、SSH、TELNET、TOMAT 等的弱口令探测；
配置核查	支持主流操作系统配置核查，包括但不限于 Windows、Linux、BClinux、Solaris、HPUnix、AIX 等操作系统，支持中标麒麟、优麒麟、中兴新支点等国产化操作系统；
	支持 FW、IPS、IDS、防毒墙、ACM 等安全设备配置核查；
	支持 Elasticsearch、ZooKeeper、Spark、HDFS、Kafka、HBase、Hive、Sqoop、Yarn-MR、Impala 等大数据组件的配置核查；（提供截图证明）
漏洞管理	支持漏洞生命周期管理，包括未修复、确定、忽略、修复、已验证五种状态；
	支持同一任务的最近两次扫描结果对比，展示漏洞状态的变更情况；
	支持在线报表，可详细展示任务综述信息、站点列表、漏洞列表、对

	比分析及参考标准，漏洞分布支持风险等级过滤查看；
联动处置	支持与本项目防火墙联动功能，防火墙能根据漏扫提供的资产信息对重要资产信息进行防护，根据漏洞信息自动生成防护规则，保护内网安全；（提供截图证明）
IPv6	支持 IPv6 协议栈地址场景漏洞扫描；（提供资质证书证明）
产品资质	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（增强级）；
	提供中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》、《中国国家信息安全产品认证证书》、《IT 产品信息安全认证证书》（EAL3 增强级）；
	提供 CVE、CNNVD 漏洞库兼容性资质证书；

11、 态势感知

指标项	参数要求
硬件配置	2U 机箱，冗余电源，配置不少于 6 个千兆电口、4 个万兆 SFP+接口插槽，存储≥48TB，内存≥256G；
系统性能	≥50 个设备数据源授权； 数据采集探针性能≥20000 条/秒； 支持≥10 亿条数据秒级检索响应；
态势展示	支持态势大屏展示，包括全网态势、资产态势、漏洞态势、攻击态势，支持大屏展示时间设置，支持态势大屏中相关信息下钻跳转到对应的详细页面；
	支持拖拽方式自定义大屏界面展示顺序，支持多种地图、拓扑展示方式，包括但不限于世界、全国、省份、拓扑等，支持 logo、标题、大屏超时设置；
	支持漏洞态势分析，包括漏洞总体情况、漏洞类型分布、漏洞级别分布、高危漏洞排行 TOP5、漏洞排行 TOP10、最新漏洞发现趋势、高危漏洞类型排行、漏洞级别对比；
	支持以全球地图实时展示网络攻击态势，支持以不同颜色攻击线展示

	攻击过程，支持攻击源和攻击目的国家名称展示，支持攻击目的进行光晕显示；
安全监测	支持日志概览，包括日志源数量、安全日志数量、审计日志数量、安全日志级别分布、安全日志类型排名、日志量趋势，支持概览时间设置；
	支持日志实时监视，支持按照设备 IP、设备类型、事件级别、过滤器等条件进行事件分类监视，支持清空日志显示列表、停止和启动刷新、刷新间隔设置；
	支持联动漏扫设备、手动导入漏扫报告两种方式实现漏洞数据采集，支持同品牌及第三方漏扫设备联动，支持 excel、zip 等类型的漏扫报告导入；
	支持资产性能监测概览，支持监测设备总数、异常数、主机异常数、网络设备异常数、安全设备异常数展示，支持监控资产性能状态占比、支持性能监控详细列表，包括 IP、资产名称、性能状态、连通状态、CPU 使用率、内存使用率等；
安全处置	支持对安全处置情况进行概览分析，包括待处置告警数、待处置漏洞数、待处置风险资产数、待处置威胁源数、待处置漏洞 TOP5、风险资产 TOP5、威胁源 TOP5；
	支持通过漏洞视角进行漏洞的查询展示及处置，展示信息包括时间、漏洞名称、漏洞编号、漏洞级别、漏洞分类、影响范围，支持按照 TXT、CSV、EXCEL 进行导出；
	支持工单管理，支持指派相关责任人进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单；
	支持按预设规则进行告警，支持按照分组进行告警规则管理，告警规则内容包括规则名称、告警名称、过滤器、应用范围、告警级别、影响范围、响应方式、工单、企业微信群等；（提供截图证明）
安全分析	支持对全网安全分析，包括外联主机数、内网威胁源、外网威胁源、失陷主机数、外联主机 TOP5、内部威胁源 TOP5、外部威胁源 TOP5；
	支持对攻击线索追踪溯源分析，攻击线索类型包括 IP、端口、日志名

	称，支持追溯结果多维度展示，包括攻击关系图、端口相关 IP 关系图、日志名称相关 IP 关系图、日志列表，攻击关系图包含攻击源、支持日志详情查看、溯源、一键封堵、加入白名单、加入关注名单、封堵申请等操作；
	支持多维度威胁源画像分析，分析维度包括威胁源基础信息、威胁资产行为、遭受威胁资产趋势、资产日常访问趋势，威胁源基础信息包括地理位置、封堵状态查询；
	支持内置至少 30 种分析模型，包括失陷状态、FTP 登录失败、敏感文件信息泄露、成功暴力破解、文件上传漏洞等；
资产管理	支持全局展示资产概况，包括全部资产数/安全域数、等保业务系统数/业务系统数、已同步主库资产数/备库资产数、安全域资产分布 TOP5、业务系统定级分布、主库资产类型分布等；
	支持多视角全网拓扑管理，包括管控设备拓扑、资产拓扑、业务拓扑，支持自定义拓扑及主动扫描探测拓扑，支持对单个节点拖拽操作；
集中管控	支持与项目涉及的安全产品无缝对接进行集中管理，无需额外接口开发工作；（提供截图证明）
	支持管控拓扑图展示，支持拓扑动态提示管理设备产生的告警，支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息；
治理中心	支持统计概览，包括但不限于安全报告、合规审计日志、应急预案、跟踪文档、待整改业务系统展示，支持待整改业务系统排名、最新安全报告排名、最新跟踪文档等信息，最新安全报告支持下载；
	支持合规审计，审计设备类型包括但不限于主机、安全设备、网络设备、业务应用、中间件、数据库；
知识情报	支持内生情报管理，包括恶意 IP 地址、恶意 URL、恶意样本、恶意域名、垃圾邮件等，支持情报进行分类自定义查询，支持自定义威胁情报信息，支持威胁情报的导入；
产品资质	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销

	售许可证》；
	提供国家版权局颁布相关软件著作权；
	提供国家信息安全漏洞库兼容性资质证书；
	提供 IPV6 金牌证书；

12、 安全监测设备

指标项目		指标要求
硬件参数		2U 机架结构；冗余电源； 配置 2 个 1000MBASE-T 接口（管理口、HA 口），2 个万兆接口； 整机吞吐量>20Gbps；最大并发连接数>300W； 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、数据上报上级设备。
基本设备要求	功能要求	安全监测设备与安全监测设备管理平台采用密码技术安全认证；采用密码技术对登录用户进行身份鉴别；
		继承安全监测设备平台提供安全基线策略，执行安全监测设备平台阻断策略，根据安全监测设备平台的策略执行结果输出记录，并上报至安全监测设备平台。
		系统具有感知网安全监测设备平台采集的数据要求进行数据分析、汇总能力，降低感知网流量压力；
		系统支持感知网安全监测设备平台对接，根据安全监测设备平台要求上报汇总数据；
		系统支持感知网安全监测设备平台对接，执行安全监测设备平台下发安全策略。
	部署模式	旁路部署
	用户管理	根据安全监测设备平台的账户权限管理，提供使用权限管理。
	审计管理	提供账户登录及操作记录，提供审计日志查询，能按照管理员账号、时间段进行查询。

13、 防病毒客户端

指标项	参数要求
产品形态	系统部署采用 C/S 架构，管理采用 B/S 架构，管理员只需通过浏览器登录控制中心，即可对系统进行管理；
病毒检测	要求对流行病毒的检测能力必须超过 98%的检出率，小于 0.1%的误报率；
客户端要求	客户端授权数量不少于 4000 点（2 套）；
	客户端支持 Windows、Linux 以及国产化操作系统；
	客户端安装后占用硬盘资源≤50M，日常内存占用≤20M；
	客户端安装支持本地安装、WEB 安装。

（二） 流量分析平台建设

流量分析平台建设包括采购流量采集设备与流量分析软件，并提供 3 年质保。产品性能及具体参数如下：

1、 流量采集设备

指标项	参数要求
流量采集设备	1. 配置冗余双电源，单电源功率支持 500W； 16 个物理核及以上；处理器主频≥2.4GHz；内存 64GB、硬盘 12TB 及以上，内置数据保护模块，支持断电后把数据写入缓存空间;配置 2 个万兆光口,4 个千兆电接口，网卡支持扩展，支持 2 个扩展槽。 2. 流量采集设备，流量处理能力≥10Gbps；报文存储性能≥5Gbps；并发用户数不少于 5 万；并发会话数不少于 300 万；新建会话数不少于 10 万/秒。 3. 应支持 2000 种以上协议和应用识别；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，支持基于 HTTP URL 定义应用，支持基于 ASCII、HEX 特征值自定义应用,支持根据响应时间设置自定义应用的性能等级;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。

	4. 系统支持集中展示流量状况，包括，设备总流量、当前用户数、当前会话数、设备流量趋势、在线用户数趋势、会话数趋势、服务器流量排名、实时用户流量排名、实时应用流量排名；支持构建用户虚拟画像，展示访问各类应用记录、虚拟账号、上网时长、各类应用日志排名等；支持全局在线会话监控，查看实时会话信息，支持查询、搜索及过滤在线会话；支持服务器的实时流量、会话统计，支持服务器会话统计，支持单个服务器下的用户流量、会话统计；支持目标 IP 所在国家、地区、运营商等展示、支持目标端口访问排名统计，基于柱状图、饼图、表格展示；支持应用的实时流量展示，可以下钻到每个应用，查看每个用户访问此应用的流量、质量统计。 5. 系统能够支持 ICMP、TCP、Tracert 网络层探测，Tracert 自动路径探测，判断故障节点；支持应用层 HTTP 探测，判断业务是否正常，以及 DNS 解析时延、TCP 三次握手时延，HTTP 下载时延等，判断整个业务各个阶段交互时延、抖动、丢包。 6. 系统支持能够基于黑白名单产生告警，支持应用的历史流量展示，支持近 1 小时、1 天、1 周、1 月的应用流量展示，可以下钻到每个应用，查看每个用户访问此应用的流量、质量统计；能够对 IP 扫描、端口扫描、Land、Smurf、Fraggle 等异常报文监测与告警，支持 SYN Flood、ICMP Flood、DNS Flood 流量监测与告警，能够对电子邮件内容践行监测，定义敏感词参数，监控邮件内容敏感信息。 7. 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；系统支持数据包支持数据包截断存储，可以设定捕获并保存数据包的长度大小，如 64bytes，只保存数据包的前 64

	个字节，须能够按照不同自定义应用分别设置数据包截断长度；支持数据包去重功能，在原始流量存在重复包的情况下能够开启去重功能，自动剔除重复的数据包，确保分析结果的准确性。
维保服务	提供三年原厂维保和保修服务。

2、 流量分析软件

指标项	参数要求
网络流量分析平台	1、本平台须按用户要求定制开发（主要开展接口对接、界面优化调整、数据展示等，相关费用已包含投标报价中），各功能应满足用户使用需求，同时须与市局科技处网络流量分析平台级联，实现分局三级网流量分析全量数据上传及开放本地数据二次开发，并通过市局科技处验收。**（投标人需提供针对本项目的承诺函，格式见附件 11）** 2、应支持通过镜像端口采集全流量数据包，预处理后进行存储。 3、应支持超过 2000 余种协议（包含 TCP、UDP、HTTP、FTP、POP3、SMTP、IMAP、DNS、IPP、MDNS、NTP、NetBios、SNMP、XDMCP、DHCP、MySQL、Hotmail、POPS、AppleJuice、DirectConnect、COAP、VMware、SMTPS、DTLS、UBNTAC2、Kontiki、FastTrack、Gnutella、BitTorrent、SMBv23、Mining、NestLogSink、WhatsAppCall、DataSaver、RTSP、IMAPS、IceCast、CPHA、Discord…等），对数据包按协议、应用进行分析处理。 4、全局展示:展示所有链路汇聚的实时统计数据，包括总流量、上行流量、下行流量、主机数、应用数、协议数。 5、图形化展示:以图形化方式展示所有链路汇聚的实时统计数据，包括总流量、上行流量、下行流量、主机数、应用数、协议数。 6、全局数据细分展示:提供自定义选择展示内容，以表格形式呈现当前 de 流量相关指标，包含字节数、包数、响应时间、响应次数、IP 会话次数、TCP 会话次数等内容。 7、单点展示:以折线图方式展示当前节点的流量数、速率、包数、丢包数、TCP/UDP 连接数。 8、设备信息展示:可以选择某个 ip 或者 mac 展示当前设备的网络信息，

	包括字节数、使用协议、网络使用量、点对点连接数等。 9、特定协议分析:系统可以指定某项协议如 HTTP、SSH、FTP 等以表格、图形化等方式展示当前协议使用情况，如数量、交易时间、交易状态、响应时间能。 10、特定应用分析:系统应支持三大类应用包括(网站、app、文件处理)，展示各应用对网络资源的使用占比及所用流量。 11、服务器分析:系统可以展示指定服务器的端口使用情况及各端口的流量使用情况 12、关键日志留存:系统应支持自定义记录各类应用的使用日志留存功能，包含 FTP、WEB、ICMP 等。 13、链路监控:针对某一特定链路，展示该链路的总流量、上行流量、下行流量、包数、会话数、各类协议数等 14、告警:系统应支持自定义告警策略、告警处理、告警日志功能，并支持告警检索。 15、报表:系统应支持自定义报表功能，包括定义字段、自定义风格等。 16、统计图:系统应支持自定义表表功能，包括定义统计字段，图标式样等。 17、系统配置:包含用户管理、密码权限管理、告警策略、链路配置、IP 配置。 18、流量筛选:系统应支持按网段进行流量检索。 19、系统展示:支持展示当前系统的环境信息，包括内存使用数、cpu 占用率、磁盘空间、操作系统版本号等信息。 20、网络测试工具:系统自带 ping 测试、ICMP 测试、telnet 测试等测试。 21、网络带宽分析:系统应支持分析当前网络的网络带宽。 22、用户行为分析:系统应对异常流量、异常访问等影响安全的主机会做响应的日志记录。 23、全网协议分析:针对全网的应用协议按趋势进行分析，包括各类协议在不同时间段的网络占比。

	24、特定用户分析:针对全网用户按趋势进行分析，如用户高频访问的主机、使用的应用、占用的网络资源等。 25、单向流量分析:针对单向流量分析给出可能的判断，如服务器宕机、服务未开启、端口恶意扫描等。 26、异常应用分析:针对可用性低、响应时间长的应用进行分析，给出可能的建议。 27、常用端口分析:针对全网的端口进行分析，给出分析建议，如建议开启哪些端口，哪些端口应该关闭等。 28、网络安全智能分析:分析网内存在的恶意流量，如 SQL 注入、端口扫描、IP 扫描等。 29、资产管理:可以按照设备所属部门、所属管理网络、设备类型、IT 资产信息等多维条件对网络 IT 资产进行统计和管理。按照标准字段登记资产信息，并对其进行统计分析和管理。 30、全网分析报告:以各种维度生成统计报告，包括网络态势、应用态势、用户态势，支持展示字段自定义、展示图标自定义。 31、支持二次开发功能；所有报表可以由用户自定义；所有图标组件式样用户可以灵活定义。
维保服务	提供三年原厂维保和保修服务。

(三) 融合承载网配套建设

融合承载网配套建设包含采购核心层传输设备和汇聚层传输设备，并提供 3 年质保。产品性能及具体参数如下：

1、 核心层传输设备

核心层传输设备技术参数要求：

指标项	参数要求
设备性能	同时支持 VC 与 ODUK 交叉
	单槽位带宽不低于 200G，总容量不低于 12.8T
	单波速率支持 100G/200G/400G
	业务槽位不少于 32 个
	光层平台支持 80 波道，可平滑升级到 120 波道
	主控、电源采用 1+1 保护模式

	内置 OTDR 能力，不需要增加额外的单板即可实现 OTDR 功能，OTDR 可实现 150km 光纤的监控
100G 线路板	波分侧支持 OTU4 接口
	支持 ITU-T G.694.1 的 DWDM 技术规格
	支持 OTN、SDH 业务混合传输
	支持波长可调光模块
	支持 SDFEC2，HFEC PLUS 纠错编码
	支持将接入业务信号转换为 4 路 OTU4 信号，OTU4 信号符合 ITU-T G.694.1 准波长
10G 线路板	支持 OTN、SDH 业务的混合传输
	波分侧支持 OTU1/OTU2/OTU2e 接口
	采用 ITU-T G.709 建议的帧格式和开销处理
	支持 DWDM 技术规格
	支持波长可调光模块
10G 支路板	支持不少于 20 路的 10G 支路业务接入
	支持 SDH/SONET、以太网、OTN、SAN、视频业务
E1 接口板	支持不少于 32 路 75Ω/120Ω 的 E1 接口、100Ω 的 T1 接口
以太网业务处理板	支持不少于 20 路的以太网业务接入
	支持 GE 电口（支持自协商、1000M 全双工、100M 全双工、10M 全双工）
	支持 GE 光口（支持自协商、1000M 全双工）
	支持 FE 光口（支持 100M 全双工）
核心设备网络管理	用于市局核心型传输设备，需能够插入市局核心型传输设备机框并正常运行，同时需要与市局核心型设备统一网管，实现业务单位、分局、市局之间业务端到端配置，故障端到端定位等功能；
自主可控	100G 光模块，ODSP，算法的自研解决方案
维保服务	提供三年原厂维保和保修服务；
设备巡检	每日至少 1 次线上巡检，每季度至少 1 次现场巡检，并提供季度巡检报告。

核心层传输设备配置要求：

序号	部件名称	部件描述及配置需求	数量要求	单位	备注
1	电子架（机框+电源）	深度≤300mm，高度≤2200mm，不少于 32 个业务槽位，机框建议采用交流供电系统、且为模块化分区设计，包括：电源接口区、风扇区、业务板区、交叉及主控板区，带盘纤盒，其中主控板区、电源区为冗余设计，电源区槽位数≥10 且满配电源模块，	1	套	核心层设备

		风扇区槽位数≥4			
2	光子架（机框+电源）	深度≤300mm，高度≤350mm，不少于 13 个业务槽位，机框建议采用交流供电系统、且为模块化分区设计，包括：电源接口区、风扇区、业务板区、交叉及主控板区，带盘纤盒，其中主控板区、电源区为冗余设计，电源区槽位数≥2 且满配电源模块	5	套	核心层设备
3	光层辅材	满足本套设备正常运行所必须的光层辅材（包含且不限于：光合波/分波单板、带 OTDR 功能的光监控单板、光纤线路接口板、光放单元、色散补偿单元、光衰、光跳纤等辅材）	1	套	核心层设备配套板卡
4	VC3/VC12 低阶通用交叉板	80G VC3/VC12 低阶通用交叉板（支持 1+1 热备份，集成交叉、业务调度等功能，实现 VC-3/VC-12 业务的低阶交叉和分组业务的交换）	2	块	核心层设备配套板卡
5	带时钟处理的系统控制与通信板	带时钟处理的系统控制与通信板（支持设备通信管理、子架级联等功能和特性）	2	块	核心层设备配套板卡
6	100G 线路板	单块板卡不少于 4 路 100G 的线路业务处理板（需支持支持 OTN、SDH 业务的混合传输），需满配 100G 波分侧光模块	3	块	核心层设备配套板卡
7	10G 线路板	单块板卡不少于 30 路 10G 的线路业务处理板(需支持 OTN、SDH 业务的混合传送，将接入的业务信号处理后转换为 30 路 OTU1/OTU2/OTU2e 信号，OTU1/OTU2/OTU2e 信号为 DWDM 标准波长)，需配置 40km DWDM 万兆光模块≥20	1	块	核心层设备配套板卡
8	10G 支路业务处理板	单块板卡不少于 30 路的 10G 支路业务处理板（需支持 SDH/SONET、以太网、OTN、SAN、视频及其他业务），需配置万兆多模光模块≥20	1	块	核心层设备配套板

					卡
9	以太业务处理板	单块板卡支持接入不少于 20 路的以太网业务，需支持 GE 电口（支持自协商、1000M 全双工、100M 全双工、10M 全双工）、GE 光口（支持自协商、1000M 全双工）、FE 光口（支持 100M 全双工），需满配 15KM GE 光模块	1	块	核心层设备配套板卡
10	STM-N 光接口板	单块板卡需支持不少于 16 路 STM- N (N=64,16,4,1),需配置 STM-64 单模 1310nm 10KM 光模块数量≥4， STM-64 单模 1550nm 40Km 光模块数量≥1，STM-16 单模 1310nm 15Km 光模块数量≥7	1	块	核心层设备配套板卡
11	任意速率业务支路处理板	单块板卡需支持不少于 10 路任意速率业务，需满配 10KM GE 光模块；	2	块	核心层设备配套板卡
12	E1 业务电接口板	单块板卡不少于 32 路 E1/T1 电接口板（支持 VC-12 级别的通道开销的处理，如 J2、V5 等字节,支持至少 32 路 75Ω的 E1 接口）	3	块	核心层设备配套板卡
13	交换式以太网处理板	单块板卡支持接入不少于 10 路的以太网业务，需支持 GE 电口（支持自协商、1000M 全双工、100M 全双工、10M 全双工）、GE 光口（支持自协商、1000M 全双工）、FE 光口（100M 全双工），需满配千兆电口模块；	4	块	核心层设备配套板卡

2、 汇聚层传输设备

汇聚层传输设备技术参数要求：

指标项	参数要求
设备性能	同时支持 VC 与 ODUK 交叉
	单槽位带宽不低于 200G，总容量不低于 4.8T
	单波速率支持 100G/200G/400G

	业务槽位不少于 24 个
	光层平台支持 80 波道，可平滑升级到 120 波道
	主控、电源采用 1+1 保护模式
	内置 OTDR 能力，不需要增加额外的单板即可实现 OTDR 功能，OTDR 可实现 150km 光纤的监控
安装	同时支持 19 英寸和 21 英寸机柜安装
	OSC、OTDR 光模块都支持可插拔，单个方向模块失效更换不影响其他方向
业务端口	支持不少于 20 个 FE/GE 端口的业务单板，单板支持不小于 128 个 VC Trunk
	支持不少于 16 个 STM-N 端口业务单板
网络管理	与核心型设备统一网管，实现业务单位、分局、市局之间业务端到端配置，故障端到端定位。
自主可控	要求 100G CFP 光模块芯片自研可控
维保服务	提供三年原厂维保和保修服务；
设备巡检	每日至少 1 次线上巡检，每季度至少 1 次现场巡检，并提供季度巡检报告。

汇聚层传输设备配置要求：

序号	部件名称	部件描述及配置需求	数量要求	单位	备注
1	电子架（机框+电源）	深度≤300mm，高度≤750mm，不少于 24 个业务槽位，机框建议采用交流供电系统、且为模块化分区设计，包括：电源接口区、风扇区、业务板区、交叉及主控板区，带盘纤盒，其中主控板区、电源区为冗余设计，电源区槽位数≥4 且满配电源模块，风扇区槽位数≥2	1	套	汇聚层设备
2	光子架（机框+电源）	深度≤300mm，高度≤350mm，不少于 13 个业务槽位，机框建议采用交流供电系统、且为模块化分区设计，包括：电源接口区、风扇区、业务板区、交叉及主控板区，带盘纤盒，其中主控板区、电源区为冗余设计，电源区槽位数≥2 且满配电源模块	2	套	汇聚层设备
3	光层辅材	满足本套设备正常运行所必须的光层辅材（包含且不限于：光合波/分波单板、带 OTDR 功能的光监控单板、光纤线路接口板、光放单元、色散补偿单元、光衰、光跳纤等辅材）	1	套	汇聚层设备配套板卡
4	通用主控及交叉时钟处理板	通用交叉及主控时钟处理板(支持 1+1 热备份，集成交叉、主控、时钟功能，支持通信控制、业务调度、时钟处理等功能，实现 ODUk(k=0，1，2，2e，flex，3，4)/VC-4/VC-3/VC-12 业务的交叉和分组业	2	块	汇聚层设备配套板卡

		务的交换)			
5	VC3/VC12 低阶通用交叉板	80G VC3/VC12 低阶通用交叉板（支持 1+1 热备份，集成交叉、业务调度等功能，实现 VC-3/VC-12 业务的低阶交叉和分组业务的交换)	2	块	汇聚层设备配套板卡
6	带时钟处理的系统控制与通信板	带时钟处理的系统控制与通信板（支持设备通信管理、子架级联等功能和特性）	4	块	汇聚层设备配套板卡
7	100G 线路板	单块板卡需支持不少于 2 路 100G 的线路业务处理板（需支持支持 OTN、SDH 业务的混合传输），且配置 100G 波分侧光模块≥1	2	块	汇聚层设备配套板卡
8	10G 支路业务处理板	单块板卡需支持不少于 30 路的 10G 支路业务处理板(需支持 SDH/SONET、以太网、OTN、SAN、视频及其他业务），需配置 1310nm 万兆单模 10KM 光模块数量≥3，配置 1550nm 万兆 80KM 光模块数量≥2，配置 1550nm 万兆 40KM 光模块≥1；	2	块	汇聚层设备配套板卡
9	以太业务处理板	单块板卡需支持接入不少于 20 路的以太业务，需支持 GE 电口（支持自协商、1000M 全双工、100M 全双工、10M 全双工）、GE 光口（支持自协商、1000M 全双工）、FE 光口（支持 100M 全双工）,需配置 GE 多模光模块≥8；	1	块	汇聚层设备配套板卡
10	STM-N 光接口板	单块板卡需支持不少于 16 路 STM- N (N=64,16,4,1)光接口板，需配置 STM-16 单模 1310nm 15KM 光模块数量≥8， STM-1 单模 1310nm 40Km 光模块数量≥4，STM-16 单模 1550nm 80Km 光模块数量≥2	2	块	汇聚层设备配套板卡
11	E1 支路板	单块板卡需支持不少于 32 路 E1/T1 电接口板（支持 VC-12 级别的通道开销的处理，如 J2、V5 等字节，支持至少 32 路 75Ω 的 E1 接口）	1	块	汇聚层设备配套板卡

（四） 安全运维服务

1、 日常维护服务

维护分局现有和本项目建设的网络安全软硬件产品，保障系统配置的安全性与合规性，保障系统和功能正常运行。评估与优化分局网络安全威胁防御机制，加强分局网络安全风险

识别能力，提升分局防范网络安全风险和应对网络安全突发事件的应急处置水平。健全优化分局网络安全管理体系，为分局网络及网络安全提供专业的咨询规划，确保网络与信息系统安全建设和信息化协调发展，提高分局网络及信息系统的安全性、可靠性和合规性。

1） 配置维护

维护网络安全软硬件产品的系统配置，包括配置的添加、修改、删除、备份等，系统策略的建立、完善和变更等，系统升级，安全特征库升级等。配置管理严格遵循用户相关的管理制度和操作流程，保留工作日志，并在服务报告中体现详细数据。

每月根据市局安全要求进行硬件设备安全策略调整，每季度进行软件系统版本升级、数据库备份、安全设备规则库更新。

具体维护要求如下：

序号	维护对象	具体维护内容
1	安全网络管理系统	查看安全网络管理系统的策略部署情况，排查未注册接入设备，根据 IP 地址与用户共同注册分类，发现违规接入或擅自修改网络属性的设备列出清单，并对以上情况出具详细报告。每月异地备份一次系统数据库，包括资产信息、策略信息、状态信息以及操作记录等，备份内容保留 6 个月。
2	防病毒客户端	更新病毒库，为新接入主机安装客户端防病毒软件，对终端查杀病毒以及统计查杀病毒数据、分析病毒安全事件产生的原因。
3	“一机两用”终端防护系统	登录“一机两用”监控平台查看数据情况，确保徐汇分局一机两用注册率、防病毒软件安装率、安全助手安装率为100%。
4	安全监测系统	检查系统配置是否非法改动，对设备配置进行备份。管理安全监测策略，包括建立、完善和变更。查看安全防护策略是否有效，向安全监测平台上报数据是否正常。
5	网络审计	管理网络审计策略，包括建立、完善和变更。分析网络行为，对异常行为进行调查处置。检查网络流量的审计信息是否正常，每月备份 1 次、清理系统磁盘等。
6	防病毒邮件网关	检查防病毒邮件网关设备的安全策略是否有效，对检测到的邮件病毒进行验证和处置等。
7	防火墙	检查防火墙安全策略设置是否合理，根据徐汇分局的策略申请表配置防火墙安全策略，查看是否存在异常连接和访问等。

8	入侵检测	查看入侵检测设备的安全防护策略是否有效，对检测到的攻击行为进行验证和处置等，对特征库进行升级维护。
9	流量探针	查看探针设备的安全防护策略是否有效，向态势感知平台上报数据是否正常，对检测到的攻击行为进行验证和处置等，对特征库库进行升级维护。
10	WEB 应用防火墙	管理WEB应用安全防护策略，包括建立、完善和变更。查看安全防护策略是否有效，完成WEB攻击事件的调查分析与处置。对 WEB 应用攻击特征库进行更新与维护。
11	防毒墙	检查防毒墙设备的恶意代码防护策略是否有效，完成恶意代码的统计分析与处置，对特征库进行升级维护。
12	堡垒机	对堡垒机设备日常运维人员的账号、口令与资源，以及运维策略进行管理，包括建立、完善和变更。响应运维人员的资源维护申请需求，负责运维信息全生命周期内的安全管理。对日常运维行为进行分析和统计，调查分析和处置异常或不合规行为。
13	日志审计	检查系统配置是否非法改动，对设备配置、日志数据进行备份，管理日志源，包括日志收集策略的建立、完善和变更。配置日志审计规则，响应日志告警并处置，对日志数据进行分析和统计，调查分析和处置异常或不合规行为。
14	数据审计	检查系统配置是否非法改动，对设备配置、审计数据进行备份。配置数据审计规则，响应事件告警并处置，对数据库访问行为、攻击行为、异常进行分析和统计，调查分析和处置异常或不合规行为。
15	漏洞扫描	通过漏洞扫描管理全网资产的脆弱性，定期更新漏洞特征库，制定漏洞评估策略。
16	态势感知平台	检查系统配置是否非法改动，对配置进行管理。 监控平台态势，完成异常行为、攻击行为的调查分析与处置，根据平台数据，调整探针的威胁检测策略，调整其它安全防护策略。关联分局现有的安全设备，对全网风险进行态势分析与威胁感知。

2) 系统巡检

每月对软硬件设备进行巡检，并向用户报告巡检结果。巡检内容包括系统资源状态(CPU、内存、硬盘、网络接口等)，系统运行情况等。要求保留每日巡检记录，以及巡检过程中发

现问题后的处理过程等相关记录，并在服务报告中体现详细数据。

具体巡检要求如下：

序号	巡检对象	具体巡检要求
1	安全网络管理系统	1.检查客户端软件安装情况； 2.服务器端策略部署情况，排查未注册接入设备。
2	防病毒客户端	1.检查终端防病毒系统客户端安装数量、脱机数量； 2.查看病毒库版本信息，是否更新病毒库。
3	“一机两用”终端防护系统	1.检查终端“一机两用”终端防护系统客户端软件安装情况； 2.检查终端安全助手安装情况； 3.检查违规联网监控服务器运行情况，并出具报告。
4	安全监测系统	1.检查平台与市局一级平台对接情况，探针与平台连接情况； 2.对平台运行状态进行检查，包含 CPU 和内存的使用量等是否异常、存储空间，探针与平台数据交互情况等。
5	网络审计	1.查看网络流量的审计信息是否正常； 2.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。
6	防病毒邮件网关	1.查看安全防护策略是否有效，对检测到的邮件病毒进行统计； 2.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连 7 通性等。
7	防火墙	1.检查系统配置是否非法改动，对设备配置进行备份； 2.审查访问控制策略是否符合安全要求，每月对全局策略梳理 1 次； 3.检查设备运行状态，包含电源硬件检查、CPU 和内存的使用量等是否异常、并发连接数、吞吐量记录、网络连通性、双机状态检测等。
8	入侵检测	1.检查系统配置是否非法改动，对设备配置进行备份； 2.查看安全防护策略是否有效，导出高危风险事件报告； 3.对入侵检测特征库进行更新与维护； 4.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。
9	流量探针	1.检查系统配置是否非法改动，对设备配置进行备份； 2.查看安全防护策略是否有效，向态势感知平台上报数据是否正常； 3.对全面威胁检测特征库进行更新与维护； 4.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量

		等是否异常、吞吐量记录、网络连通性等。
10	WEB 应用防火墙	1.检查系统配置是否非法改动，对设备配置进行备份； 2.查看安全防护策略是否有效，完成 WEB 攻击事件的调查分析与处置； 3.对 WEB 应用攻击特征库进行更新与维护； 4.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。
11	防毒墙	1.检查系统配置是否非法改动，对设备配置进行备份； 2.查看恶意代码防护策略是否有效，完成恶意代码的统计分析与处置； 3.对病毒特征库进行更新与维护； 4.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。
12	堡垒机	1.检查系统配置是否非法改动，对设备配置、运维数据进行备份； 2.对日常运维行为进行分析和统计，调查分析和处置异常或不合规行为； 3.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。
13	日志审计	1.检查系统配置是否非法改动，对设备配置、日志数据进行备份； 2.对日志数据进行分析和统计，调查分析和处置异常或不合规行为； 3.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。
14	数据审计	1.检查系统配置是否非法改动，对设备配置、审计数据进行备份； 2.对审计数据进行分析和统计，调查分析和处置异常或不合规行为； 3.检查设备运行状态检查，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。
15	态势感知平台	1.检查系统配置是否非法改动，对配置进行管理； 2.检查流量探针与平台连接情况，以及数据交互情况； 3.检查平台运行状态，包含电源硬件检查、CPU 和内存的使用量等是否异常、吞吐量记录、网络连通性等。

3) 日志分析

每月对分局现有和项目建设的网络安全软硬件产品系统日志、告警日志、安全事件等数据进行安全分析：

- 检查分局日志管理的相关措施是否到位，日志采集范围、采集参数、保留时间等是否满足法律法规要求；
- 分析日志原始数据，判断网络中是否存在网络安全威胁，发现可能存在的脆弱性；
- 评估网络安全威胁等级及可利用的脆弱性，综合分析分局网络安全风险水平，并优化当前的网络安全技术防御机制；
- 保留日志分析与评估记录，并在服务报告中体现详细数据。

4） 安全评估

- 每季度对徐汇分局信息业务系统进行漏洞扫描工作，包括主机系统、网站系统、数据库系统，提供漏洞扫描报告并完成漏洞修复工作。
- 每年度对徐汇分局信息业务系统渗透测试，包括主机系统、网站系统、数据库系统，提供渗透测试报告并完成系统漏洞加固工作。

5） 安全值守

每日 5*8 小时，对本项目提供的网络安全软硬件产品所检测到的安全事件进行监控与处理，包括但不限于恶意代码攻击事件，网络入侵攻击事件，僵尸网络，用户行为异常，网络流量异常等。

按照用户有关网络安全事件管理制度或处理流程等，及时上报网络安全事件，并落实具体的技术措施完成事件处置工作，保留事件监控与处理过程等工作记录，并在服务报告中体现详细的数据。

6） 应急响应

提供 7*24 小时应急响应服务。当突发网络安全事件（包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等），10 分钟内响应，2 小时内到达现场进行事件处理与恢复，迅速采取措施和行动，以最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。

2 小时内无法恢复的事件需要提供详细的解决方案，确保网络与业务系统安全运行。

应急响应结束后，要求分析事件发生原因，总结经验教训，根据应急处置过程整理网络安全突发事件报告，并向用户提交改进计划。

7） 咨询分析

全面梳理、了解分局网络和信息系统现状，从管理与技术两方面，对分局信息安全体系框架进行规划。将“同步规划、同步建设、同步运行”的原则贯穿网络与信息化工程项目建设全过程，确保网络与信息系统安全建设与信息化发展相协调。

具体要求包括：

- 提供分局所需的网络安全解决方案设计，针对网络安全设备稳定性、防护策略等问题提供技术支持；
- 提供分局网络规划设计，针对现场实施遇到的网络问题提供解决方案，必要时提供现场技术支撑，保障实施工作顺利进行；
- 提供等保咨询服务，完善和维护管理制度及相关工作记录，提前开展测评准备工作，协助用户的定级系统顺利通过等保测评。
- 提供项目涉及到的算法规划，负责机器学习算法、知识网络、智能研判算法设计。日常工作负责安全数据态势分析、安全事件监测、异常流量分析，关联分局现有安全设备数据，运用人工服务+支撑平台的方式，结合自动化流程，进行可管理的威胁检测与响应服务、提供态势分析、安全监测、安全处置、安全分析、资产管理、集中管控等服务。
- 提供感知网视频安全监测平台及网络流量数据分析，负责分级平台与市局一级平台对接情况，探针与平台连接情况，探针与平台数据交互情况，全网资产梳理情况，准入管理情况，非法行为监控，异常阻断拦截事件处理，针对摄像头灰白屏的故障监控、漏洞发现及处理情况跟进。

2、 安全培训服务

从实战攻防视角出发，提出信息安全建设实战化的具体工作建议，协助徐汇分局统筹协调资源并进行攻防演练技术培训。

具体要求包括：

- 制定分局红蓝对抗人员选拔和培训方案；
- 提供线上攻防实训平台，学员可在线学习和练习；
- 提供在线培训课程，包括课程视频、PPT、模拟题、模拟试卷，包含单选、多选、实操题。实操部分为 CTF 解题，题目方向包含 web，逆向，pwn，杂项，密码学等；

- 提供不少于 5 套 CTF 竞赛选拔题库，配合分局开展红蓝对抗技术人员的选拔；
- 提供线下集中培训，培训内容包括 SQL 注入专题，PHP 黑魔法与命令/代码执行专题，XXE、SSTI 和 XSS 专题，对象注入专题，密码技术专题，逆向分析专题，CTF 专题，综合类题目练习等。
- 提供红蓝对抗赛前集训，内容包括专题讲解、解题策略、解题技巧培训等。

3、 设备保修服务

针对分局现有已过保的网络安全硬件设备，提供为期 2 年的原厂保修服务，保修设备清单如下：

序号	设备名称	设备品牌	设备型号	部署位置	数量
1	防火墙	天融信	NGFW4000(TG-B2106)	分局各派出所	13 台
		天融信	NGFW4000-UF(TG-5207)	分局本部	2 台
		天融信	NGFW4000-UF(TG-62242)	分局本部	4 台
		天融信	NGFW4000-UF(NG-81642)	分局本部	1 台
2	入侵检测	天融信	TopSentry 3000(TS-51528)	分局本部	1 台
3	网络审计	天融信	TopAudit(TA-424-DB)	分局本部	1 台
4	防病毒邮件网关	天融信	TopFilter 7000(TF-7514-Virus)	分局本部	1 台

四、 项目实施清单

（一） 感知网安全建设清单

序号	产品名称	部署位置	产品具体参数	数量	备注
1	万兆防火墙 A	公安感知网	详见“建设要求（一）感知网安全建设”1	2 台	产品租赁时间期限 2 年
2	万兆防火墙 B	公安感知网	详见“建设要求（一）感知网安全建设”2	4 台	产品租赁时间期限 2 年
3	入侵检测	公安感知网	详见“建设要求（一）感知网安全建设”3	4 台	产品租赁时间期限 2 年
4	防毒墙	公安感知网	详见“建设要求（一）感知网安全建设”4	4 台	产品租赁时间期限 2 年
5	流量探针	公安感知网	详见“建设要求（一）感知网安全建设”5	1 台	产品租赁时间期限 2 年
6	WEB 应用防火墙	公安感知网	详见“建设要求（一）感知网安全建设”6	2 台	产品租赁时间期限 2 年
7	堡垒机	公安感知网	详见“建设要求（一）感知网安全建设”7	1 台	产品租赁时间期限 2 年
8	日志审计	公安感知网	详见“建设要求（一）感知网安全建设”8	2 台	产品租赁时间期限 2 年
9	数据库审计	公安感知网	详见“建设要求（一）感知网安全建设”9	1 台	产品租赁时间期限 2 年
10	漏洞扫描	公安感知网	详见“建设要求（一）感知网安全建设”10	1 台	产品租赁时间期限 2 年
11	态势感知	公安感知网	详见“建设要求（一）感知网安全建设”11	1 台	产品租赁时间期限 2 年

12	安全监测设备	公安感知网（派出所）	详见“建设要求（一）感知网安全建设”12	13 台	产品租赁时间期限 2 年
		公安感知网（分局）		2 台	
13	防病毒客户端	公安感知网	详见“建设要求（一）感知网安全建设”13	2 套（2000 台终端授权）	产品租赁时间期限 2 年

（二） 流量分析平台建设清单

序号	产品名称	部署位置	产品具体参数	数量	备注
1	流量采集设备	公安信息网	详见“建设要求（二）流量分析平台建设”	2 台	产品质保 3 年
2	流量分析软件	公安信息网	详见“建设要求（二）流量分析平台建设”	1 套	产品质保 3 年

（三） 融合承载网配套建设清单

序号	产品名称	部署位置	产品具体参数	数量	备注
1	核心层传输设备	融合承载网	详见“建设要求（三）融合承载网配套建设”1	1 套	产品质保 3 年
2	汇聚层传输设备	融合承载网	详见“建设要求（三）融合承载网配套建设”2	1 套	产品质保 3 年

（四） 安全运维服务清单

序号	服务名称	服务具体内容	服务频次	服务期限
1	日常维护服务	详见“建设要求（四）安全运维服务”1	详见“建设要求（四）安全运维服务”1 条	2 年
2	安全培训服务	详见“建设要求（四）安全运维服务”2	1 次/年	2 年
3	设备保修服务	详见“建设要求（四）安全运维服务”3	/	2 年

五、 项目实施要求

(一) 项目实施相关要求

1、 本项目要求合同签署后 3 个月内完成所有软硬件产品的安装调试和产品培训工作，项目建设方应制作详细实施周期及施工组织、网络安全详细规划设计和实施安排、质量保障、培训、验收等方案。

2、 项目建设方应有完善的项目管理机制，有完善的工程实施方案，项目的实施、维护严格按照相关质量体系标准执行。项目实施过程中，项目建设方须通过建立制度化的沟通渠道等方式，加强与招标人的沟通。

3、 产品安装、联网调试、业务割接等由原厂负责，提交用户一个可使用、稳定可靠的运行网络。并保证在不中断现有网络的情况下完成网络调整和割接，并有相应的应急或回退方案。

4、 融合承载网核心层传输设备、汇聚层传输设备的安装局点由市局统一规划，项目建设方需在设备到货后，根据市局规划负责将设备运送至相关安装地点。安装设备前需要完成设备安装机房的环境检测和电路测试，对于不满足设备安装要求的机房环境和电源、电路等，必须进行改造，以达到符合联网要求，分局不承担额外费用。在上海市公安局融合承载网组建完成后，平滑无缝的与现有上海公安各套网的网络整合完成业务割接工作。上海市公安局融合承载网组建完成后，项目建设方需免费提供业务割接服务(包括但不限于上海公安信息网、上海公安感知网、上海市公安局应急联动指挥域、现有 SDH 上承载的业务及其他新业务)

5、 项目建设方负责产品的安装调试工作，安装调试时使用的工具、设备由项目建设方提供。在设备安装调试时，涉及到现有设备地理位置调整的(具体位置由用户方指定)，项目建设方必须负责设备下架、地理位置调整和安装等工作。

6、 机房设备安装应符合国家计算机及通信机房标准，相关设备要求安装在统一的标准机柜内，各机房内的设备需统一接地。

7、 项目建设方安装前负责提供下列详细资料：

- 设备机架（柜）外型尺寸、重量、面板布置、进出线方式；
- 设备所需电源种类、功耗、电压、地线要求；
- 设备机房荷重及环境要求；
- 设备安装方式和抗震措施；

- 设备及线缆等的维护标识方式；
- 上述资料需提供电子文档。

（二） 项目实施人员要求

1、 项目经理

提供项目经理 1 名，作为本项目的总负责人，提供为期 2 年现场 5*8 小时技术支持服务，7*24 小时全天候故障响应。对项目过程实行全面的管理和协调，定期组织会议制定计划和报告项目的进展，把握项目的进度，保障项目的顺利实施。

1) 项目经理应具备十年以上网络安全从业经验，熟悉网络与数据安全方面的法律法规，熟悉网络安全架构与产品，具备丰富的项目管理与网络安全咨询经验。
2) 项目经理同时拥有 PMP、ISO 27001、CISP、CDSP、ITIL 证书者优先选用，提供简历、资质证书以及上海本地社保缴纳记录。

2、 驻场人员

提供 2 名驻场工程师，提供**为期 2 年的 5*8 小时驻场技术支持服务**，如遇国庆、春节等假期以及重大会议如两会、进博会等特殊时期，提供重保服务，重保时期驻场工程师 7x24 小时待命。**如投标单位提供的驻场服务人员数量不能满足招标文件要求的，作无效投标处理。**

1) 驻场工程师应熟悉网络安全架构，精通网络安全产品的操作与维护，具备安全日志分析工作经验，至少 1 名成员具备 3 年以上的渗透测试经验，提供《CNVD 原创漏洞证明》证书。
2) 驻场工程师团队成员具备的所有证书应包含 CISP 或 CISSP、CISP-PTE、CISAW 等。提供人员简历、资质证书以及社保缴纳记录。
3) 驻场工程师应能够在短时间内独立解决本项目租赁产品的常见系统故障，提供产品原厂商资格认证。

3、 咨询与分析人员

提供网络安全咨询及分析服务工作团队，成员不少于 3 名，至少五年的网络安全从业经验。

1) 团队成员需熟悉网络安全法律法规，精通等级保护相关标准，具备丰富的 ISMS 规划设计与安全咨询经验，能够熟练运用大数据分析技术，具备算法的规划与设计经验，具备渗透测试经验等。

2） 团队成员具备的所有证书应包含 CCIE 或 HCIE、CISP 或 CISSP、CISP-PTE、CISAW 等，提供人员简历、资质证书以及社保缴纳记录。

4、 培训讲师

提供至少 1 名专业的培训讲师，从事网络安全行业工作年限不低于 10 年。

1） 精通网络安全攻防技术，近三年向国家信息安全漏洞共享平台提交不少于 5 个原创漏洞，提供原创漏洞证明材料。

2） 培训讲师须同时具备 CISP、CISSP、ISO27001、CISA、ITIL 和 CISP-DSG 证书，提供人员简历、资质证书以及社保缴纳记录。

5、 实施人员

组建一支不少于 5 人、工作责任心强、技术水平高、业务熟练、管理经验丰富的项目团队参加本项目的建设和服务。提供项目实施团队人员清单及主要人员基本信息、能力证明与项目经验证明。要求具有类似项目实施经验的技术人员全程参与，详细列出所有参与人员的基本信息及能力证明，应附相应的技能证书。

（三） 验收要求

1、 设备到货后，用户将与项目建设方共同开箱验收。验收时发现短缺、破损，用户有权要求项目建设方立即补发和负责更换。在设备及配套软件验收时发现产品损坏、数量不全、型号规格不符等问题，项目建设方应及时解决。招标人有拒收和追究赔偿责任的权利。

2、 项目建设方在用户指定时间内完成软硬件产品的安装调试和培训工作，且产品试运行无重大故障。

3、 按标书产品技术参数要求对设备集成的质量、性能和配置进行测试检查，做出测试报告,在测试或运行中出现性能指标或功能上不符合标书和合同要求时，项目建设方应及时解决。

4、 项目建设方完成招标要求及合同规定的全部建设内容，并提供相关产品的技术资料、培训材料等。

5、 项目验收时应提供符合用户要求的全套工程竣工资料。

（四） 售后服务要求

1、 产品配置

项目建设方应按照产品技术参数要求提供相关软硬件产品，根据分局实际情况提供产品部署需要的所有配件，满足本项目安全建设要求。

2、 备品备件

项目建设方应有完善的备品备件库体系，以满足本项目中最终用户单位建设期内对备品备件的需求。项目建设方应提供备品备件库负责人、联系方式（包括手机和固定电话）和相关证明文件（照片等）。若确定是硬件损坏，现场无法修复，则需要在 24 小时内提供不低于现有设备性能的备品备件进行替换（更换的设备或部件应是来自原厂商的全新同型设备或备件，不得以其它方式替代），并确保系统继续稳定运行。

3、 系统升级

项目周期内，提供免费的系统及各项功能升级服务，当业内发生或推送重大安全攻击、重大漏洞等高风险事件时，需第一时间提供解决方案，升级特征库或配置安全规则。

4、 技术支持

提供产品售后技术支持，包括安装部署、技术培训、故障处置、设备迁移等。客户发现问题后 1 小时内进行响应和支持，远程无法解决的，2 小时内至现场进行处置。故障解决后 12 小时内，应提交故障处理报告，说明故障种类、故障原因、故障解决中使用的方法及故障损失等情况。

六、其他要求

1）投标报价要求：本项目为交钥匙工程。投标人必须对以上全部采购内容及相关服务进行报价，报价中应包含设备（产品）租赁、产品采购、安装到位、系统安装集成、运维服务提供、验收合格、相关培训等伴随服务等全部明细内容，并将与本项目有关的其他所有费用全部计入投标报价，采购人不再承担其他任何费用。

2）投标方应根据招标文件的要求、上海市公安局徐汇分局的实际情况以及自身经验能力，提供具有针对性的项目服务的计划、方案、措施、标准、质量保证等具体内容，投标文件具有可操作性。

3）投标单位应为本项目组配一支有能力的服务团队，项目经理和管理、技术、服务负责人须具有同类项目的工作、管理经验。投标单位需驻场技术人员，以满足本项目服务要求。

4）投标单位需在投标文件中提供应急预案及相关保障措施、针对性方案等各项相关服

务方案。

5）投标单位应加强内部管理控制，针对招标项目，制定相应管理、巡检、运维工作流程、服务方案、人员培训等制度，建立健全各项管理机制，确保服务工作正常，良好有效。如遇管理、巡查、责任不到位，发生各类事故，应追究相关人员责任。

6）派至上海市公安局徐汇分局的服务人员须相对固定，并提供个人相关资料，服务人员如有变动须提前一个月告知。

7）投标方在投标文件中须提供本单位背景资料，包括经营业务、规模、技术力量、相应工具和装备情况等。

8）中标单位与采购人应当在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，采购人应当按照《徐汇区政府采购货物、服务项目合同履约验收管理办法》相关规定进行验收管理和支付相应合同价款，中标单位有义务参加并协助采购人验收，提供相关技术资料、合格证明等文件或材料，并对自己生产或销售的货物质量或提供的服务负责。验收书要求见附件。

9）如中标供应商实际提供服务与投标承诺服务不一致，项目实施服务承诺无法完成，服务被使用方有效投诉，经查实中标供应商要承担相应违约责任，并将按《徐汇区政府采购供应商诚信档案管理办法》规定进行相应记载和处理，同时保留向市、区政府采购管理机构通报的权利。

七、商务响应要求

类别	要求
承诺函	投标供应商须承诺保证投标的网络流量分析平台可按分局要求定制开发（主要开展接口对接、界面优化调整、数据展示等），各功能满足分局使用需求，同时与上海市公安局网络流量分析平台级联，实现分局三级网流量分析全量数据上传及开放本地数据二次开发，承诺满足通过上海市公安局科技处验收标准，相关费用已包含在投标总价内。承诺函格式详见附件。**投标供应商须出具书面承诺函，对此作出明确承诺。**

说明：对商务要求须出具书面承诺函，作出明确承诺。否则投标文件视为非实质性响应，作为无效投标处理。

第四部分　合同参考范本

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]**　　乙方：**[合同中心-供应商名称]**

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-采购人单位邮编]**　　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]**

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》、《中华人民共和国合同法》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网络安全建设：

1．1 信息化网络安全建设

乙方所提供的信息化网络安全建设其来源应符合国家的有关规定，信息化网络安全建设的内容、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，大写[合同中心-合同总价大写]元整。

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

网络安全建设地点：

2．3 服务期限

网络安全建设的服务期限：

本服务的服务期限：[合同中心-合同有效期]。

3．质量标准和要求

3．1 乙方所提供的网络安全建设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 乙方所交付的网络安全建设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网络安全建设享有合法的权利。

4．2 乙方保证在网络安全建设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网络安全建设没有侵犯任何第三人的知识产权和商业秘密等权利。

4．4 如甲方使用该网络安全建设构成上述侵权的，则由乙方承担全部责任。

5．验收

5．1 网络安全建设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网络安全建设验收。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个工作日内，确定具体日期，由双方按照本合同的规定完成网络安全建设验收。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，直至网络安全建设完全符合验收标准。

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网络安全建设验收合格后，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 本合同以人民币付款。

7．2 本合同款项按照以下方式支付。

7．2．1 付款内容：（分期付款）

付款次序	付款编号	国库支付金额	甲方支付金额
第一笔			
第二笔			
第三笔			

7．2．2 付款条件：

（1）本合同付款按照上述付款内容和付款次序分期付款。

（2）第一笔付款预付款：在本合同签订且甲方收到乙方按本合同第 14 条规定提交的履约保证金和预付款等额的银行保函以及收款凭证后，甲方在十个工作日内支付货款；

（3）第二笔服务付款：当乙方提供服务时间达到本合同服务期限二分之一并完成合同规定的相应服务事项时，甲方收到发票后十个工作日内支付货款；

（4）第三笔付款服务最终验收付款：当乙方完成合同服务期限内规定的服务事项后，服务验收单或验收报告出具后，甲方在十个工作日内支付剩余合同款项。

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网络安全建设，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，造成设备的无法正常运行，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 由于乙方网络安全建设质量或延误服务的原因，使甲方有关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，协助乙方进行系统运维和故障解决。

8．5 当设备发生故障时，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设备进行调整，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网络安全建设，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网络安全建设，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 乙方保证在设备网络安全建设中，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 乙方在履行网络安全建设时，发现设备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，保证设备正常运行。

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 乙方保证在网络安全建设中提供更换的部件是全新的、未使用过的。如果或证实网络安全建设是有缺陷的，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 在网络安全建设期限内，如果乙方对提供网络安全建设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）根据设备网络安全建设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网络安全建设的价格。

（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网络安全建设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（周、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

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为（　　）元人民币的履约保证金。履约保证金应自出具之日起至网络安全建设按本合同规定验收合格后三十天内有效。在全部设备网络安全建设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 如果合同双方在履行本合同过程中发生争议，双方应首先采取友好协商的方式解决该争议。如从协商开始十（10）天内仍不能解决，双方应将争端提交上海市徐汇区政府采购管理办公室或有关合同管理部门调解。如果经调解不能达成协议，则在买方住所地有管辖权的人民法院提起诉讼。在诉讼期间，除了必须在诉讼过程中进行解决的那部分问题外，合同其余部分应继续履行。

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设备网络安全建设。

（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，以中文书就，签字各方各执一份，一份报上海市徐汇区政府采购管理办公室备案。

20．合同附件

20．1 本合同附件包括： 采购文件、报价文件

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。

（本页无正文）

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]

合同签订点:网上签约

第五部分 投标文件格式

投标文件格式详见网上招投标系统相关附件

附件 1 投标函

徐汇区政府采购中心：

_____（投标人全称）授权_____（投标人代表姓名）(职务、职称)为我方代表，参加贵方组织的_____(项目名称、项目编号、包号)招标的有关活动，并对此项目进行投标。为此：

1、我方同意在本项目招标文件中规定的开标日起 90 天内遵守本函中的承诺且在此期限期满之前均具有约束力。

2、我方按招标文件规定提供交付的的网络安全建设的投标总价为_____（大写）元人民币。

3、我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商应当具备的条件：

（1）具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商；同时经信用信息查询未被列入失信被执行人、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。

（2）本项目不允许联合投标。

4、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，并对发生的任何故障和风险造成投标内容不一致或利益受损或投标失败，承担全部责任。

5、我方同意网上投标内容均以网上投标系统开标时的开标记录表内容为准，投标人的授权代表将在开标记录上签名以确认开标过程和结果，如果不签字，则由我们承担全部责任。

6、保证遵守招标文件的规定，忠实地执行双方所签订的合同，并承担合同规定的责任和义务。

7、如果在开标后规定的投标有效期内撤回投标，我方的投标保证金可被贵方没收。

8、我方完全理解贵方不一定接受最低价的投标或收到的任何投标。

9、我方愿意向贵方提供任何与本项投标有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

10、我方已详细审核全部投标文件，包括投标文件修改书（如有的话）、参考资料及有关附件，确认无误。

11、我方承诺：采购中心若需追加采购本项目招标文件所列货物及相关服务的，在不改变合同其他实质性条款的前提下，按相同或更优惠的折扣保证供货。

12、我方承诺接受招标文件中《中标合同》的全部条款且无任何异议。

13、我方将严格遵守《中华人民共和国政府采购法》的有关规定，若有下列情形之一的，将被处以采购金额 5‰以上 10‰以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动；有违法所得的，并处没收违法所得；情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

（1）提供虚假材料谋取中标、成交的；

（2）采取不正当手段诋毁、排挤其他供应商的；

（3）与采购人、其它供应商或者采购中心工作人员恶意串通的；

（4）向采购人、采购中心工作人员行贿或者提供其他不正当利益的；

（5）未经监管部门同意，在采购过程中与采购人进行协商谈判的；

（6）拒绝有关部门监督检查或提供虚假情况的。

与本投标有关的一切往来通讯请寄：

地址：_____

邮编：_____

电话：_____

传真：_____

投标人代表姓名：_____

投标人代表联系电话，e-mail：_____

投标人(公章)：

投标人代表(签字)：

日　期：

开标一览表

投标人（公章）：

投标人代表(签字)：

填写日期：

上海市徐汇区政府采购中心——上海市公安局徐汇分局 2022 年度网络安全建设政府采购项目包 1

项目名称	驻场服务人员数	最终报价(总价、元)

注： （1）所有价格均系用人民币表示，单位为元，保留到整数位。

（2）投标人应按照招标文件中有关投标报价要求进行报价，一旦中标不再调整。

（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。

附件 2-1 服务项报价明细表

填报单位（公章）： 第 页 共 页

序号	分类名称	费用（元）	备注
1	产品租赁服务		详见明细（ ）
2	安全运维服务		详见明细（ ）
3			详见明细（ ）
4	……		详见明细（ ）
5	……		详见明细（ ）
6	……		详见明细（ ）
7	……		详见明细（ ）
8	……		……
报价合计			

注： （1）所有价格均系用人民币表示，单位为元，保留到整数位。

（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）分项目明细报价合计应与开标一览表报价相等。

投标人代表签字：_____

投标人（公章）：_____

日期： 年 月

附件 2-2 硬件产品及系统集成投标报价明细表

1	2	3	4	5	6	7	8	9	10	11	12
产品名称	品牌	规格型号	产地	厂家	数量	设备单价	设备合价	技术服务费	安装费	其他服务费	分项合价
投标总价：											

注： 1. 投标报价要求见招标文件的“投标人须知”相关要求。

2. 表中同一行中的第 8 栏数据＝第 6 栏数据×第 7 栏数据。

3. 表中第 9 栏、第 10 栏费用应根据招标文件的“投标人须知”相关要求列明细表。

4. 表中同一行中的第 12 数据＝第 8～第 11 栏数据之和。

5. 表中的“投标总价”＝Σ（第 12 栏的数据）。

6. 表中第 11 栏的费用如果有时，应注明具体内容。

7、投标人必须按要求填报本明细表，否则会影响对投标文件的评判。

投标人代表签字：_____

投标人（公章）：_____

日期： 年 月 日

附件 3 产品选型及说明一览表

序号	产品名称	型号规格及 主要技术参数	产地	数量	性能说明	备注

注：各产品材质、详细技术参数表（请供应商也可根据自身情况调整列表予以说明），请供应商务必详细描述，如描述不清，将会影响到对投标文件的评判，请供应商充分重视。

投标人代表签字：

投标人（公章）：

日期： 年 月 日

附件 4 技术参数（功能）偏离表（可根据实际情况自行设计表式填报）

序号	产品名称及规格型号	数量	产地	招标产品配置要求	投标产品对应配置	偏差	备注

说明：1、投标人必须根据技术需求表来填写本表，如投标产品实际技术规格与技术需求无偏差，在“偏离”一列填写“无”。

2、投标产品的规格、技术参数和性能与招标文件的要求如不完全一致，在“偏离”一列填写“有”，还需填写偏差说明，并注明是“正偏离”还是“负偏离”以及偏差的幅度（以百分比表示）。

投标人代表签字：

投标人（公章）：

日期： 年 月 日

附件 5 法定代表人证明书和法人代表委托书

_____先生/女士现担任_____职务，负责全面工作，为我单位的法定代表人。

特此证明。

投标人全称：_____

公章（盖章）：

_____年_____月_____日

法人代表委托书

兹委托_____先生/女士全权代理_____（招标项目和招标编号）政府采购招标项目的招标投标工作。

特此证明。

投标人法定代表人姓名（印刷体）：_____

投标人法定代表人签字、盖章：_____

公章（盖章）：

_____年_____月_____日

附件 6-1 项目服务团队人员情况一览表

填报单位（公章）： 第 页 共 页

序号	姓 名	出生年月	性别	学历	职称等级	相关认证资格	专业经历	成功案例	拟从事岗位

注：

1、在填写时，如本表格不适合投标单位的实际情况，可根据本表格格式自行制表。

2、我方承诺以上人员均为本单位职工，并按时交纳四金。**并提供项目组人员身份证及相关资格证书、工作履历等证明材料复印件，并加盖单位公章。**

3、此表作为中标后服务承诺书的组成部分，项目组人员应保持稳定。

投标人（公章）：

投标人代表(签字)：

填写日期：

附件 6-2 拟投入项目的驻场服务等服务人员配备及相关工作经历、资质汇总表

项目名称：

序号	姓　名	出生年月	性别	学历	职称等级	相关认证资格	专业经历	成功案例	拟从事岗位

注：1、在填写时，如本表格不适合投标单位的实际情况，可根据本表格格式自行制表。

2、**我方承诺以上人员均为本单位职工，并按时交纳四金。**并提供项目组人员身份证及相关资格证书、工作履历等证明材料复印件，并加盖单位公章。

3、此表作为中标后服务承诺书的组成部分，项目组人员应保持稳定。

投标人（公章）：

投标人代表(签字)：

填写日期：

附件 6-3 项目负责人说明表

姓名		出生年月		文化程度		毕业时间	
资格证书				技术职称			
获得证书时间				聘任时间			
从业年限				进入本公司时间			
主要工作经历：（包括起止年限、单位名称、从事的工作内容、证明人、证明人联系电话）							

2019 年以来相关项目服务情况					
序号	项目名称	参与时间	项目预算金额（万元）	参与项目的角色	所附证明材料页码
1					
2					
3					
…					

注：我方承诺以上人员均为本单位职工，并按时交纳四金。并提供以上人员身份证及相关学历、资格证书、工作履历、业绩证明等证明材料复印件，并加盖单位公章。

投标人（公章）：

投标人代表(签字)：

填写日期：

附件 6-4　项目组成员的详细情况表（每人一表）

姓名		出生年月		文化程度		毕业时间	
资格证书				技术职称			
获得证书时间				聘任时间			
从业年限				进入本公司时间			
主要工作经历：（包括起止年限、单位名称、从事的工作内容、证明人、证明人联系电话）							
2019 年以来相关项目服务情况							
序号	项目名称		参与时间	项目预算金额(万元)	参与项目的角色	所附证明材料页码	
1							
2							
3							
…							

注：我方承诺以上人员均为本单位职工，并按时交纳四金。并提供以上人员身份证及相关资格证书、工作履历、业绩证明等证明材料复印件，并加盖单位公章。

投标人（公章）：

投标人代表(签字)：

填写日期：

附件 7　规章制度一览表

序号	规章制度名称	执行起始时间	备注
1			
2			
3			
…			
…			

各规章制度的具体内容另行提供。

投标人（公章）：

投标人代表(签字)：

填写日期：

附件 8　供应商行贿犯罪记录承诺书

上海市徐汇区政府采购中心：

_____（投标供应商全称）现参与你单位组织的_____政府采购项目，并承诺本公司根据《上海市政府采购供应商登记及诚信管理办法》已申请加入上海市政府采购供应商库，且在 3 年内无行贿犯罪行为记录。

投标供应商全称：_____

公章（盖章）：

法定代表人签字、盖章：_____

附件 9 中小企业声明函（服务）

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，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，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：

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：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。

附件 10　投标人近年来已承接的主要类似项目一览表

序号	年份	项目名称	合同金额	业主情况			项目主要内容
				单位名称	经办人	联系方式	
1							
2							
3							
4							
…							

注：　1、如在本表格不能全部填写完，可按此表格格式自行制表填写。
2、提供相应采购项目合同复印件，加盖单位公章。

投标人代表签字:_____

投标人（公章）：_____

日期：　　年　　月　　日

附件 11 承诺函

承诺函

致：上海市公安局徐汇分局

针对（项目名称/招标编号）项目（投标供应商名称）承诺保证投标的网络流量分析平台可按分局要求定制开发（主要开展接口对接、界面优化调整、数据展示等），各功能满足分局使用需求，同时与上海市公安局网络流量分析平台级联，实现分局三级网流量分析全量数据上传及开放本地数据二次开发，承诺满足通过上海市公安局科技处验收标准，相关费用已包含在投标总价内。如（投标供应商名称）公司中标后无法完成的，由此产生的一切后果由（投标供应商名称）公司承担。

特此承诺！

投标人代表签字：

投标人（公章）：

日　期：

说明：本承诺函为实质性响应条款，不满足招标文件要求的投标文件视为非实质性响应，作为无效投标处理。

附件 12 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）参加（单位名称）的（项目名称）采购活动，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：

附件 13 投标单位基本情况表及声明

（一）名称及其他资料：

1、单位名称：

2、地址：

3、邮编：

4、电话/传真：

5、工商注册日期：

6、企业类型：

7、注册资本：

8、法定代表人或执行事务负责人姓名：

9、人员情况

从业人员数

专业技术人数

（二）主要财务指标（2021 年 1 月 1 日至 2021 年 12 月 31 日）**并请如实另附单位财务状况报告，依法缴纳税收和社会保障资金的相关材料**

① 业务收入：_____

② 风险基金额：_____

③ 资产净值：_____

（三）**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的声明：（请如实填写）**

上海市徐汇区政府采购中心：

按照政府采购法实施条例要求，我单位郑重声明：我单位参与_____政府采购项目，在参加本项目政府采购活动前三年内在经营活动中**（没有/有）**重大违法记录。特此声明。

就我方全部所知，兹证明上述声明是真实、准确的，并已提供了全部现有资料和数据，我方同意根据招标方要求出示文件予以证实。

投标单位（公章）：

投标人代表(签字)：

填写日期：

附件：上海市徐汇区政府采购项目验收书（服务类）

供应商：　　采购单位：

采购编号	采购项目	金额（元）
项目金额合计		
验收内容		
一、规章制度	1、人员管理	
	2、设备运维	
	3、服务管理	
	4、应急管理	
	……	
二、运行记录	1、人员上岗及培训	
	2、设备检测记录	
	3、巡更记录	
	4、内审记录	
	……	
三、现场实地检查情况		

<table>
<tr><td rowspan="3">验收意见</td><td colspan="2">验收小组意见：

结论：该服务采购项目验收合格（或不合格）。</td></tr>
<tr><td colspan="2">验收小组签字：
组长：
组员：

年　月　日</td></tr>
<tr><td>供应商盖章：</td><td>采购单位盖章：</td></tr>
</table>

备注：1、采购人须按照《徐汇区政府采购货物、服务项目合同履约验收管理办法》第三章第十条“验收的基本程序”组织验收。2、政府向社会公众提供的公共服务项目（包括：以物为对象的公共服务，如公共设施管理服务、环境服务、专业技术服务等；以人为对象的公共服务，如教育、医疗卫生和社会服务等），验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告。3、该表式仅供参考。

第六部分　评标办法

上海市公安局徐汇分局2022年度网络安全建设项目

政府采购招标评标办法

一、评标依据：

1、评标办法系本着公开、公平、公正的原则，按照《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》制定，作为本次采购招标选定中标单位的依据。本次采购招标采用“综合评分法”评标，根据评标细则规定的评分标准对所有投标单位的有效投标文件进行评议，各评标项目累计总分为100分。

2、评标委员会由专家和采购单位代表组成，对各投标单位的投标报价进行甄别并经算术修正后得出各投标报价的得分，最终结果取算术平均值。

3、评标委员会依据各项评分结果汇总后，对各投标单位的得分按由高到低的顺序依次排列，得出相应名次。得分最高者为中标单位。如出现最高得分并列情况时，则取投标报价较低者作为中标单位，如出现最高得分并列且报价相同则由评标委员会以投票表决方式，得票最多者为中标单位。采购人授权评标委员会在投标供应商中直接确定本项目中标单位。

二、评标规则：

（1）参加评标的专家为上海市政府采购咨询专家库中的专家，并在评标前按规定程序产生。

（2）任何人不得干预评标委员会成员的评审权利，评审表要保存备查。

（3）评标委员会成员必须对所有投标单位作出评审。

三、“综合评分法”评标细则

1、报价（20分）采用低价优先法计算

（1）首先确定评标基准价：经评标委员会甄别确认，满足招标文件要求且投标价格最低的投标报价为评标基准价，其报价分为满分20分。

（2）确定其他投标报价分：计算公式为投标报价得分=评标基准价/打分投标单位的投标报价×20%×100。

注：①经评标委员会评审如投标单位的服务内容不能满足招标文件要求，该投标将不列入评审范围，其报价如为最低投标报价，将不作为评标基准价。②如果评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或不能诚信履约的，将要求该投标人作书面说明并提供相关证明材料。投标人不能证明其报价合理性的，评标委员会应将其作无效投标处理。

2、产品性能及质量（15分）

根据所提供的各类租赁服务产品以及购买产品性能及质量优劣进行评分，主要对各类产品的性能、市场使用程度、成熟度、可靠性、产品的性价比、品牌知名度、市场占有率、产品选型与

匹配、品牌一致性等进行综合评价。综合评价好的得（15-13 分），较好得（13-9 分），一般得（9-6 分）。

3、安全运维服务方案（15 分）

根据对各项服务需求的理解和分析到位，相关服务流程、方法，人力、物力、技术力量的投入情况，相关的应急预案，服务质量保证措施、成果提交方式、考核验收方案等进行综合评价。综合评价好的得（15-13 分），较好得（13-9 分），一般得（9-6 分）

4、服务项目团队人员配备及管理（25 分）

（1）项目负责人情况（10 分）根据项目负责人具有相应资质证书、类似项目服务的业绩证明材料、工作经历等情况进行综合评价。综合评价好的得（10-8 分），较好得（8-5 分），一般的得（5-3 分）。

（2）项目团队人员配备情况及管理（15 分）根据投标人提供从事本项目团队驻场人员、培训讲师、咨询分析人员等服务人员的业绩证明材料、工作经历、资质证书等人员配备管理情况进行综合评价。综合评价好的得（15-13 分），较好得（13-9 分），一般得（9-6 分）。

5、信息安全服务能力（3 分）

投标单位同时具有网络安全应急服务支撑单位证书（国家级）和信息安全服务资质证书的得 3 分，其他情况不得分。

6、信息系统建设和服务能力（3 分）

投标单位同时具有信息系统建设和服务能力等级证书（优秀级（CS4））和 ITSS 信息技术服务运行维护标准符合性证书的得 3 分，其他情况不得分。

7、项目实施计划及组织管理（5 分）

根据项目实施计划、项目组织管理及技术文档的管理等进行综合评价，综合评价好的得（5-4 分），较好得（4-3 分），一般得（3-2 分）。

8、管理制度及相关服务保障（5 分）

根据投标人提供的工作流程、各类规章制度以及本项目售后服务承诺、质量保障措施等进行综合评价，综合评价好的得（5-4 分），较好得（4-3 分），一般得（3-2 分）。

9、综合服务能力及投标响应度（9 分）

根据投标人综合服务能力、相关信誉及投标响应度等进行综合评价。综合评价好的得（9-8 分），较好得（8-5 分），一般得（5-3 分）。

累计最高得分 100 分。