

# 松江区电子政务外网升级优化项目 竞争性磋商文件

采 购 人：上海市松江区科技创新服务中心(上海市松江区大数据中心)

集中采购机构：上海市松江区政府采购中心

# 目 录

- 第一章 采购邀请
- 第二章 供应商须知
- 第三章 政府采购主要政策
- 第四章 采购需求
- 第五章 竞争性磋商程序及评审方法
- 第六章 响应文件有关格式
- 第七章 合同书格式和合同条款
- 附 件 项目采购需求

## 第一章 采购邀请

根据《中华人民共和国政府采购法》及相关法律、法规之规定，上海市松江区政府采购中心受委托，对松江区电子政务外网升级优化采购项目进行国内竞争性磋商采购，特邀请合格的供应商参加磋商。

### 一、项目基本情况

项目编号：**SHXM-17-20210621-1048**（内部项目编号：SJCCS2021011）

项目名称：松江区电子政务外网升级优化

采购方式：竞争性磋商

预算金额（元）：23220200.00 元

最高限价（元）：23220200.00 元

采购需求：

包名称：松江区电子政务外网升级优化

数量：1

预算金额（元）：23220200.00 元

简要规格描述：松江区政务外网 OTN 光网租用、核心路由器、汇聚路由器、委办局接入交换机采购更换，SDN 控制器采购部署，网络集成、割接现场实施，安全管理中心部署建设，运维管理平台建设，安管平台和运管平台与市级平台对接的相关工作，及后续驻场运维服务。

合同履行期限：合同签订并生效后 100 个日历天内完工（包括安装、调试及验收）

本项目**不允许**接受联合体响应。

### 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：促进中小企业、监狱企业、残疾人福利性单位发展。
- 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](http://www.creditchina.gov.cn)）、中国政府采购网（[www.ccgp.gov.cn](http://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、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。 4、本项目不允许联合体响应。 5、本项目面向大、中、小、微型等各类供应商采购。

### 三、获取采购文件

时间：**2021-06-22 至 2021-06-30** 每天上午 **09:00:00~11:00:00**，下午 **13:00:00~16:00:00**（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（元）： 0

### 四、响应文件提交

截止时间：**2021-07-14 09:00:00**（北京时间）

地点：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（<http://www.zfcg.sh.gov.cn>）电子招投标系统提交。

### 五、响应文件开启

开启时间：**2021-07-14 09:00:00**

地点：上海市松江区乐都西路 867-871 号 2 号楼 5 楼会议室。届时请供应商代表持磋商时所使用的数字证书（CA 证书）和可以无线上网的笔记本电脑参加磋商。

#### 六、其他补充事宜

1、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：[www.zfcg.sh.gov.cn](http://www.zfcg.sh.gov.cn)）电子招投标系统进行。电子采购平台是由市财政局建设和维护。供应商应根据《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。供应商在电子采购平台的有关操作方法可以参照电子采购平台中的“在线服务”专栏的有关内容和操作要求办理。

供应商人应在响应截止时间前尽早加密上传响应文件，电话通知集中采购机构进行签收，并及时查看集中采购机构在电子采购平台上的签收情况，打印签收回执，避免因临近响应截止时间上传造成集中采购机构无法在响应截止前完成签收的情形。未签收的响应文件视为响应未完成。

2、对磋商文件中的内容如有疑问，可要求澄清。请于 2021 年 07 月 02 日上午 10:00 前以书面（传真）形式告知采购方，采购方将主动或依据投标方要求澄清的问题而修改竞争性磋商文件，并通过“上海政府采购网”以澄清或修改公告形式发布。

#### 3、磋商通知

提交响应文件时间截止后，所有通过资格审查和符合性审查的供应商均参加磋商。请各提交响应文件的供应商法定代表人或其授权代表于 **2021-07-14 09:00:00** 在上海市松江区政府采购中心会议室出席磋商会议。出席磋商会议应当携带法定代表人授权委托书、政府采购专用 CA 认证证书、可以无线上网的笔记本电脑和供应商认为必要的其他相关资料。

参加磋商的供应商，在磋商结束后还有一次最后报价的机会。最后的磋商报价是履行合同的最终价格，除《采购需求》中另有说明外，最后的磋商报价应包括响应供应商为完成采购项目而提供服务的一切费用，包括响应供应商的各种成本、费用、利润和税金等。

4、本项目无磋商保证金及其他任何费用。

5、制作电子响应文件咨询电话：4008817190。

#### 七、凡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：上海市松江区科技创新服务中心(上海市松江区大数据中心)

地址：上海市松江区园中路 1 号

联系方式：37735672

##### 2.采购代理机构信息

名称：上海市松江区政府采购中心

地址：上海市松江区乐都西路 867-871 号 2 号楼 5 楼

联系方式：57746172

##### 3.项目联系方式

项目联系人：单忆琳

电话：57746172

## 第二章 供应商须知 前附表

### 一、项目情况

项目名称: 松江区电子政务外网升级优化

项目编号: 详见采购邀请(竞争性磋商公告)

项目地址: 详见采购邀请(竞争性磋商公告)

项目内容: 详见采购邀请(竞争性磋商公告)

### 二、采购人

采购人:

名称: 上海市松江区科技创新服务中心(上海市松江区大数据中心)

地址: 上海市松江区园中路1号

联系人: 阮俊

电话: 37735672

传真: 37735672

集中采购机构:

名称: 上海市松江区政府采购中心

地址: 上海市松江区乐都西路867-871号2号楼5楼

联系人: 单忆琳

电话: 57746172

传真: 67743657

### 三、合格供应商条件

- 1、符合《中华人民共和国政府采购法》第二十二条规定的供应商;
- 2、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商;
- 3、其他资格要求:

3.1 未被列入“信用中国”网站([www.creditchina.gov.cn](http://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和中国政府采购网([www.ccgp.gov.cn](http://www.ccgp.gov.cn))政府采购严重违法失信行为记录名单的供应商;

3.2 本项目不接受联合体响应;

3.3 本项目面向大、中、小、微型等各类供应商采购。

### 四、磋商有关事项

- 1、磋商答疑会: 不组织。

- 2、踏勘现场：不组织。
- 3、磋商响应文件有效期：不少于 90 天
- 4、磋商保证金：不收取
- 5、响应文件提交截止时间：详见采购邀请（竞争性磋商公告）或延期公告（如果有的话）
- 6、递交响应文件方式和网址

响应文件提交方式：由供应商在电子采购平台电子招投标系统提交。

响应文件提交 <http://www.zfcg.sh.gov.cn>

- 7、解密时间和解密地点网址：

解密时间：同响应文件提交截止时间

解密地点网址：电子采购平台电子招投标系统(网址：<http://www.zfcg.sh.gov.cn>)

- 8、磋商时间和磋商地点：

磋商时间：详见采购邀请（竞争性磋商公告）

磋商地点：详见采购邀请（竞争性磋商公告）

- 9、磋商小组的组建与竞争性磋商要求：

评审方法：详见第五章《竞争性磋商程序及评审办法》

成交供应商推荐办法：详见第五章《竞争性磋商程序及评审办法》

## 五、其它事项

- 1、付款方式：详见第四章《采购需求》——《商务要求》
- 2、质量保证期：详见第四章《采购需求》——《商务要求》
- 3、履约保证金：详见第四章《采购需求》——《商务要求》
- 4、质量保证金：详见第四章《采购需求》——《商务要求》

## 六、说明：

根据上海市财政局《关于上海市政府采购信息管理平台电子招投标系统正式运行的通知》（沪财采[2014]27号）的规定，本项目采购相关活动在由上海市财政局建设和维护的上海市政府采购信息管理平台（简称：电子采购平台）（网址：[www.zfcg.sh.gov.cn](http://www.zfcg.sh.gov.cn)）电子招投标系统进行。供应商应根据《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。供应商在电子采购平台的有关操作方法可以参照电子采购平台中的“在线服务”专栏的有关内容和操作要求办理。

供应商应当在响应文件中预留参加磋商的法定代表人或其授权代表的手机号码。如因供应商未在响应文件中预留手机号码，导致集中采购机构无法联系供应商参加磋商的，其风险由供应商自行承担，集中采购机构不承担任何责任。

供应商应在响应截止时间前尽早加密上传响应文件，电话通知集中采购机构进行签收，并及时查看集中采购机构在电子采购平台上的签收情况，打印签收回执，以免因临近响应截止时间上

传造成集中采购机构无法在响应截止前完成签收的情形。未签收的响应文件视为响应未完成。

## 供应商须知

### 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，本采购项目已具备采购条件。

1.2 本磋商文件仅适用于《采购邀请》和《供应商须知》前附表中所述采购项目的采购。

1.3 磋商文件的解释权属于《采购邀请》和《供应商须知》前附表中所述的采购人、集中采购机构。

1.4 参与采购活动的所有各方，对在参与磋商过程中获悉的国家、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，本项目采购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](http://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《供应商须知》前附表中所述的采购项目。

2.2 “服务”系指磋商文件规定的响应人为完成采购项目所需承担的全部义务。

2.3 “采购人、集中采购机构”系指《供应商须知》前附表中所述的组织本次采购的集中采购机构和采购人。

2.4 “供应商”系指从采购人、集中采购机构处按规定获取磋商文件，并按照磋商文件向采购人、集中采购机构提交响应文件的供应商。

2.5 “成交供应商”系指成交的供应商。

2.6 “甲方”系指采购人。

2.7 “乙方”系指成交并向采购人提供服务的供应商。

**2.8 磋商文件中凡标有“★”的条款均系实质性要求条款。**

**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](http://www.zfcg.sh.gov.cn)）。是由市财政局建设和维护。**

#### 3. 合格的供应商

3.1 符合《采购邀请》和《供应商须知》前附表中规定的合格供应商所必须具备的资质条件和特定条件。

3.2 《采购邀请》和《供应商须知》前附表规定接受联合体响应的，除应符合本章第 3.1 项要求外，还应遵守以下规定：

（1）联合体各方应按磋商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、合同份额；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) 采购人、集中采购机构根据采购项目的特殊要求规定供应商特定条件的,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 供应商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 供应商提供的服务应当符合磋商文件的要求,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. 磋商费用**

不论采购的结果如何,供应商均应自行承担所有与磋商有关的全部费用,采购人、集中采购机构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,包括竞争性磋商公告、磋商文件澄清或修改公告、成交公告以及延长响应文件提交截止时间等与采购活动有关的通知,采购人、集中采购机构均将通过“上海政府采购网”( <http://www.zfcg.sh.gov.cn> )公开发布。供应商在参与本采购项目采购活动期间,请及时关注以上媒体上的相关信息,供应商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,由供应商自行承担,采购人、集中采购机构在任何情况下均不对此承担任何责任。

#### **7. 询问与质疑**

7.1 供应商对采购活动事项有疑问的,可以向采购人、集中采购机构提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对供应商的询问,采购人、集中采购机构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 供应商认为磋商文件、采购过程或成交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,以书面形式向集中采购机构提出质疑。其中,对磋商文件的质疑,应当在其下载磋商文件之日(以电子采购平台显示的报名时间为准)起七个工作日内提出;对采购过程的质疑,应当在各采购程序环节结束之日起七个工作日内提出;对成交结果的质疑,应当在成交公告期限届满之日起七个工作日内提出。

供应商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 供应商可以委托代理人进行质疑。代理人提出质疑应当提交供应商签署的授权委托书,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。供应商为自然人的，应当由本人签字；供应商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 供应商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。

供应商为自然人的，应当由本人签字；供应商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。

7.5 供应商提起询问和质疑，应当按照《政府采购质疑和投诉办法》（财政部令第94号）的规定办理。质疑函或授权委托书的内容不符合《供应商须知》第7.3条和第7.4条规定的，集中采购机构将当场一次性告知供应商需要补正的事项，供应商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。

质疑函的递交应当采取当面递交形式，质疑联系部门：上海市松江区政府采购中心，联系电话：021-57746172，地址：上海市松江区乐都西路867-871号2号楼5楼2508室。

7.6 集中采购机构将在收到供应商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供应商和其他有关供应商，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 对供应商询问或质疑的答复将导致磋商文件变更或者影响采购活动继续进行的，采购人、集中采购机构将通知提出询问或质疑的供应商，并在原竞争性磋商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 供应商在本采购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，包括供应商之间串通响应等。

8.2 如果有证据表明供应商在本采购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，采购人、集中采购机构将拒绝其提交响应文件，并将报告政府采购监管部门查处；成交后发现的，成交供应商须参照《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供应商的行政与刑事责任。

8.3 采购人、集中采购机构将在**解密后至评审前**，通过“信用中国”网站

(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关供应商信用记录，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，采购人、集中采购机构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《供应商须知》的条款如与《采购邀请》、《采购需求》和《竞争性磋商程序及评审办法》就同一内容的表述不一致的，以《采购邀请》、《采购需求》和《竞争性磋商程序及评审办法》中规定的内容为准。

## **二、磋商文件**

### **10. 磋商文件构成**

10.1 磋商文件由以下部分组成：

- (1) 采购邀请
- (2) 供应商须知
- (3) 政府采购政策功能
- (4) 采购需求
- (5) 竞争性磋商程序及评审办法
- (6) 响应文件有关格式
- (7) 合同书格式和合同条款
- (8) 本项目磋商文件的澄清、答复、修改、补充内容（如有的话）

10.2 供应商应仔细阅读磋商文件的所有内容，并按照磋商文件的要求提交响应文件。如果供应商没有按照磋商文件要求提交全部资料，或者响应文件没有对磋商文件在各方面作出实质性响应，则其响应有可能被认定为无效响应，其风险由供应商自行承担。

10.3 供应商应认真了解本次采购的具体工作要求、工作范围以及职责，了解一切可能影响响应报价的资料。一经成交，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成交供应商负责。

10.4 供应商应按照磋商文件规定的日程安排，准时参加项目采购有关活动。

### **11. 磋商文件的澄清和修改**

11.1 任何要求对磋商文件进行澄清的供应商，均应在响应文件提交截止期5天以前，按《采购邀请》中的地址以书面形式（必须加盖供应商单位公章）通知采购人、集中采购机构。

11.2 对在响应文件提交截止期5天以前收到的澄清要求，采购人、集中采购机构需要对磋

商文件进行澄清、答复的；或者在响应文件提交截止前的任何时候，采购人、集中采购机构需要对磋商文件进行补充或修改的，采购人、集中采购机构将会通过“上海政府采购网”以澄清或修改公告形式发布,并通过电子采购平台发送至已下载磋商文件的供应商工作区。如果澄清或修改的内容可能影响响应文件编制的,且澄清或修改公告发布时间距响应文件提交截止时间不足5天的,则相应延长响应文件提交截止时间。延长后的具体响应文件提交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磋商文件的组成部分。当磋商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 磋商文件的澄清、答复、修改或补充都应由集中采购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,不得作为响应的依据,否则,由此导致的风险由供应商自行承担,采购人、集中采购机构不承担任何责任。

11.5 采购人、集中采购机构召开答疑会的,所有供应商应根据磋商文件或者采购人、集中采购机构通知的要求参加答疑会。供应商如不参加,其风险由供应商自行承担,采购人、集中采购机构不承担任何责任。

## **12. 踏勘现场**

12.1 采购人、集中采购机构组织踏勘现场的,所有供应商应按《供应商须知》前附表规定的时间、地点前往参加踏勘现场活动。供应商如不参加,其风险由供应商自行承担,采购人、集中采购机构不承担任何责任。采购人、集中采购机构不组织踏勘现场的,供应商可以自行决定是否踏勘现场,供应商需要踏勘现场的,采购人、集中采购机构应为供应商踏勘现场提供一定方便,供应商进行现场踏勘时应当服从采购人、集中采购机构的安排。

12.2 供应商踏勘现场发生的费用由其自理。

12.3 采购人、集中采购机构在现场介绍情况时,应当公平、公正、客观,不带任何倾向性或误导性。

12.4 采购人、集中采购机构在踏勘现场中口头介绍的情况,除采购人、集中采购机构事后形成书面记录、并以澄清或修改公告的形式发布、构成磋商文件的组成部分以外,其他内容仅供供应商在编制响应文件时参考,采购人、集中采购机构不对供应商据此作出的判断和决策负责。

## **三、响应文件**

### **13. 响应文件的语言及计量单位**

13.1 供应商提交的响应文件以及供应商与采购人、集中采购机构就有关采购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响应文件视同未提供。

13.2 响应文件计量单位,磋商文件已有明确规定的,使用磋商文件规定的计量单位;磋商文件没有规定的,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. 磋商响应文件有效期**

14.1 响应文件应从解密之日起,在《供应商须知》前附表规定的磋商响应文件有效期内有效

效。磋商响应文件有效期比磋商文件规定短的属于非实质性响应，将被认定为无效响应。

14.2 在特殊情况下，在原磋商响应文件有效期期满之前，采购人、集中采购机构可书面征求供应商同意延长磋商响应文件有效期。供应商可拒绝接受延期要求而不会导致磋商保证金被没收。同意延长有效期的供应商需要相应延长磋商保证金的有效期，但不能修改响应文件。

14.3 成交供应商的响应文件作为项目合同的附件，其有效期至成交供应商全部合同义务履行完毕为止。

## **15. 响应文件构成**

15.1 响应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《采购需求》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) 《磋商响应函》；
- (2) 《报价一览表》（在电子采购平台填写）；
- (3) 《报价分类明细表》等相关报价表格详见第六章《响应文件有关格式》；
- (4) 《资格审查要求表》；
- (5) 《符合性要求表》
- (6) 《商务响应表》；
- (7) 《与评审有关的响应文件主要内容索引表》；
- (8) 第四章《采购需求》规定的其他内容；
- (9) 相关证明文件（供应商应按照《采购需求》所规定的内容提交相关证明文件，以证明其有资格参加响应和成交后有能力履行合同）。

## **17. 磋商响应函**

17.1 供应商应按照磋商文件中提供的格式完整地填写《磋商响应函》。

17.2 供应商不按照磋商文件中提供的格式填写《磋商响应函》，或者填写不完整的，评审时将按照第五章《竞争性磋商程序及评审办法》中的相关规定予以扣分。

17.3 响应文件中未提供《磋商响应函》的，为无效响应。

## **18. 报价一览表**

18.1 供应商应按照磋商文件的要求和电子采购平台电子招投标系统提供的响应文件格式完整地填写《报价一览表》，说明其拟提供货物和相关服务的名称、规格型号、来源地、数量、价格、交付时间、质量保证期等。

18.2 《报价一览表》是为了便于采购人、集中采购机构解密。

18.3 供应商未按照磋商文件的要求和电子采购平台电子招投标系统提供的响应文件格式完整地填写《报价一览表》、或者未提供《报价一览表》，导致其解密不成功的，其责任和风险由供应商自行承担。

## 19. 报价

19.1 供应商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。除《采购需求》中另有说明外，报价应当是供应商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、管理、税费及利润等。经通知参加磋商的供应商，在磋商结束后还有一次最终报价的机会。

### 19.2 报价依据：

- (1) 本磋商文件所要求的服务内容、服务期限、工作范围和要求。
- (2) 本磋商文件明确的服务标准及审核方式。
- (3) 其他供应商认为应考虑的因素。

19.3 供应商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。供应商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《采购需求》中说明并允许外，每一种单项服务的报价以及采购项目的总价均只允许有一个报价，响应文件中包含任何有选择的报价，采购人、集中采购机构对于其响应均将予以拒绝。

19.5 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报价，采购人、集中采购机构均将予以拒绝。

19.6 供应商应按照磋商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、交付时间、价格构成等。

19.7 应以人民币报价。

## 20. 资格审查及符合性要求表

20.1 供应商应当按照磋商文件所提供格式，逐项填写并提交《资格审查要求表》、《符合性要求表》，以证明其响应符合磋商文件规定的所有合格供应商资格审查及符合性要求。

20.2 响应文件中未提供《资格审查要求表》、《符合性要求表》的，为无效响应。

## 21. 与评审有关的响应文件主要内容索引表

21.1 供应商应按照磋商文件提供的格式完整地填写《与评审有关的响应文件主要内容索引表》。

21.2 《与评审有关的响应文件主要内容索引表》是为了便于评审。《与评审有关的响应文件主要内容索引表》与响应文件其他部分就同一内容的表述应当一致，不一致时按照《供应商须知》第30条“响应文件内容不一致的修正”规定处理。

## 22. 技术响应文件

22.1 供应商应按照《采购需求》的要求编制并提交技术响应文件，对采购人、集中采购机构的技术需求全面完整地做出响应并编制服务方案，以证明其响应的服务符合磋商文件规定。

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. 响应文件的编制和签署**

23.1 供应商应按照磋商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 响应文件中凡磋商文件要求签署、盖章之处，均应显示供应商的法定代表人或法定代表人正式授权的代表签署字样及供应商的公章。供应商名称及公章应显示全称。如果是由法定代表人授权代表签署响应文件，则应当按磋商文件提供的格式出具《法定代表人授权委托书》（如供应商自拟授权书格式，则其授权书内容应当实质性符合磋商文件提供的《法定代表人授权委托书》格式之内容）并将其附在响应文件中。响应文件若有修改错漏之处，须在修改错漏之处同样显示出供应商公章或者由法定代表人或法定代表人授权代表签署字样。响应文件因字迹潦草或表达不清所引起的后果由供应商自负。

其中对《磋商响应函》、《法定代表人授权委托书》、《资格审查要求表》、《符合性要求表》以及《依法缴纳税收和社会保障资金、没有重大违法记录的声明》，供应商未按照上述要求显示公章的，其响应无效。

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，少数供应商制作的响应文件存在编写繁琐、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，提请供应商在制作响应文件时注意下列事项：

（1）磋商小组主要是依据响应文件中技术、质量以及售后服务等指标来进行评定。因此，响应文件应根据磋商文件的要求进行制作，内容简洁明了，编排合理有序，与磋商文件内容无关或不符合磋商文件要求的资料不要编入响应文件。

（2）响应文件应规范，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、响应文件的递交**

### **24. 响应文件的递交**

24.1 供应商应按照磋商文件规定，参考第六章响应文件有关格式，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响应内容。有关事项应根据电子采购平台规定的要求办理。

24.2 响应文件中含有公章，防伪标志和彩色底纹类文件（如《磋商响应函》、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，由供应商承担相应责任。

采购人、集中采购机构认为必要时，可以要求供应商提供文件原件进行核对，供应商必须按时提供，否则供应商须接受可能对其不利的评审结果，并且采购人、集中采购机构将对该供应商进行调查，发现有弄虚作假或欺诈行为的按有关规定进行处理。

24.3 供应商应充分考虑到网上提交响应文件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、操作失误造成供应商响应内容缺漏、不一致或响应失败的，采购人、集中采购机构不承担任何责任。

## **25. 响应文件提交截止时间**

25.1 供应商必须在《采购邀请（竞争性磋商公告）》规定的网上响应文件提交截止时间前将响应文件在电子采购平台电子招投标系统中上传并正式提交。

25.2 在采购人、集中采购机构按《供应商须知》规定酌情延长响应文件提交截止期的情况下，采购人、集中采购机构和供应商受响应文件提交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 在响应文件提交截止时间后上传的任何响应文件，采购人、集中采购机构均将拒绝接收。

## **26. 响应文件的修改和撤回**

在响应文件提交截止时间之前，供应商可以对在电子采购平台电子招投标系统已提交的响应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、解密**

### **27. 解密**

27.1 采购人、集中采购机构将按《采购邀请》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解密。

27.2 解密程序在电子采购平台进行，所有上传响应文件的供应商应登录电子采购平台参加解密。解密主要流程为签到和解密，每一步骤均应按照电子采购平台的规定进行操作。

27.3 响应文件提交截止，电子采购平台显示解密后，供应商进行签到操作，供应商签到完成后，由采购人、集中采购机构解除电子采购平台对响应文件的加密。供应商应在规定时间内使用数字证书对其响应文件解密。签到和解密的操作时长分别为半小时，供应商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供应商，其响应将作无效响应处理。因系统原因导致供应商无法在上述要求时间内完成签到或解密的除外。

如电子采购平台解密程序有变化的，以最新的操作程序为准。

## **六、评审**

### **28. 磋商小组**

28.1 采购人、集中采购机构将依法组建磋商小组，磋商小组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磋商小组成员总数的三分之二。

28.2 磋商小组负责对响应文件进行评审和比较，并向采购人、集中采购机构推荐成交候选供应商。

### **29. 响应文件的初审**

29.1 解密后，采购人、集中采购机构将协助磋商小组对响应文件进行初步审查，检查响应文件内容是否完整、编排是否有序、有无计算上的错误、是否提交了磋商保证金、文件签署是否规范以及供应商资格是否符合要求等。

29.2 在详细评审之前，磋商小组要对供应商资格进行审核并审查每份响应文件是否实质性响应了磋商文件的要求。未实质性响应磋商文件的响应文件按无效响应处理。磋商小组只根据响

应文件本身的内容来判定响应文件的响应性，而不寻求外部的证据。

29.3 没有实质性响应磋商文件要求的响应文件不参加进一步的磋商及评审，供应商不得通过修正或撤销不符合要求的偏离或保留从而使其响应文件成为实质上响应的文件。

29.4 解密后采购人、集中采购机构拒绝供应商主动提交的任何澄清与补正。

29.5 采购人、集中采购机构可以接受响应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. 响应文件内容不一致的修正**

30.1 响应文件内容出现前后不一致的，按照下列规定修正：

- (1) 《报价一览表》内容与响应文件其它部分内容不一致的，以《报价一览表》内容为准；
- (2) 响应文件的大写金额和小写金额不一致的，以大写金额为准；
- (3) 总价与单价和数量的乘积不一致的，以单价计算结果为准，并修正总价；
- (4) 对响应文件中不同文字文本的解释发生异议的，以中文文本为准。

响应文件中如果同时出现两种以上不一致的，则根据以上排序，按照序号在先的方法进行修正。

30.2 响应文件中如果有其他与评审有关的因素前后不一致的，将按不利于出错供应商的原则进行处理，即对于不一致的内容，评审时按照对出错供应商不利的情形进行评分；如出错供应商成交，签订合同时按照对出错供应商不利、对采购人有利的条件签约。

30.3 上述修正或处理结果对供应商具有约束作用。

### **31. 响应文件的澄清**

31.1 为有助于对响应文件审查、评价和比较，磋商小组可分别要求供应商对其响应文件中含义不明确或者有明显文字和计算错误的内容等作出必要的澄清。供应商应按照采购人、集中采购机构通知的时间和地点委派授权代表向磋商小组作出说明或答复。

31.2 供应商对澄清问题的说明或答复，还应以书面形式提交给采购人、集中采购机构，并由供应商法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

31.3 供应商的澄清文件是其响应文件的组成部分。

31.4 供应商的澄清不得超出响应文件的范围或者改变其响应文件的实质性内容，不得通过澄清而使进行澄清的供应商在评审中更加有利。

### **32. 磋商**

磋商小组所有成员集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同

时通知所有参加磋商的供应商。

供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于 3 家，政府购买服务项目（含政府和社会资本合作项目）、市场竞争不充分的科研项目以及需要扶持的科技成果转化项目，提交最后报价的供应商可以为 2 家。

磋商文件不能详细列明采购标的的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价。

### **33. 响应文件的评价与比较**

33.1 磋商小组只对被确定为实质上响应磋商文件要求的响应文件进行评价和比较。

33.2 磋商小组根据《竞争性磋商程序及评审办法》中规定的方法进行评审，并向采购人、集中采购机构提交书面评审报告和推荐成交候选供应商。

### **34. 评审的有关要求**

34.1 磋商小组应当公平、公正、客观，不带任何倾向性，磋商小组成员及参与评审的有关工作人员不得私下与供应商接触。

34.2 评审过程严格保密。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供应商或其他无关的人员透露。

34.3 任何单位和个人都不得干扰、影响评审活动的正常进行。供应商在评审过程中所进行的试图影响评审结果的一切不符合法律或采购规定的活动，都可能导致其响应被拒绝。

34.4 采购人、集中采购机构和磋商小组均无义务向供应商做出有关评审的任何解释。

## **七、定标**

### **35. 确认成交供应商**

除了《供应商须知》第 38 条规定的采购失败情况之外，采购人将根据磋商小组推荐的成交候选供应商及排序情况，依法确认本采购项目的成交供应商。

### **36. 成交公告及成交和未成交通知**

36.1 采购人确认成交供应商后，采购人、集中采购机构将在两个工作日内通过“上海政府采购网”发布成交公告，公告期限为一个工作日。

36.2 成交公告发布后同时，采购人、集中采购机构将及时向成交供应商发出《成交通知书》通知成交，向其他未成交供应商发出《成交结果通知书》。《成交通知书》对采购人、集中采购机构和供应商均具有法律约束力。

### **37. 响应文件的处理**

所有在解密会上被接受的响应文件都将作为档案保存，不论成交与否，采购人、集中采购机构

均不退回响应文件。

### **38. 采购失败**

在响应文件提交截止后，提交响应文件的供应商不足 3 家；或者在评审时，发现符合资格条件的供应商或对磋商文件做出实质响应的供应商不足 3 家，政府购买服务项目（含政府和社会资本合作项目）符合资格条件或对磋商文件做出实质响应的供应商不足 2 家；或者在最后报价时，提交最后报价的供应商不足 3 家，政府购买服务项目（含政府和社会资本合作项目）、市场竞争不充分的科研项目以及需要扶持的科技成果转化项目提交最后报价的供应商不足 2 家，磋商小组确定为采购失败的，采购人、集中采购机构将通过“上海政府采购网”发布失败公告。

## **八、授予合同**

### **39. 合同授予**

除了成交供应商无法履行合同义务之外，采购人、集中采购机构将把合同授予根据《供应商须知》第 35 条规定所确定的成交供应商。

### **40. 签订合同**

成交供应商与采购人应当在《成交通知书》发出之日起 30 日内签订政府采购合同。

### **41.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](http://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。

列入财政部、发展改革委发布的《节能产品政府采购品目清单》中强制采购类别的产品，按照规定实行强制采购；列入财政部、发展改革委、生态环境部发布的《节能产品政府采购品目清单》和《环境标志产品政府采购品目清单》中优先采购类别的产品，按规定实行优先采购。

中小企业按照《政府采购促进中小企业发展管理办法》享受中小企业扶持政策，对预留份额项目专门面向中小企业采购，对非预留份额采购项目按照规定享受价格扣除优惠政策。中小企业应提供《中小企业声明函》。享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

在政府采购活动中，监狱企业和残疾人福利性单位视同小微企业，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》。

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。

## 第四章 采购需求

### 一、项目概述

见附件

### 二、项目内容及要求

见附件

说明：

(1) 为保证采购的合法性、公平性，供应商认为上述项目技术需求存在排他性或歧视性的，可在收到或下载采购文件之日起七个工作日内提出并附相关证据，采购人、集中采购机构将及时进行调查或组织论证，如情况属实，采购人、集中采购机构将对上述相关技术需求做相应修改；

(2) 如有设备供货，采购人、集中采购机构在附件中指出的标准以及参照的规格、型号仅起说明作用，并没有任何限制性，供应商在报价中可以选用其他替代标准、规格或型号，但这些修改和替代要实质上优于采购人、集中采购机构在附件中要求及指出的工艺、材料和设备的标准以及参照的规格、型号的要求。

### 三、项目工作范围与工作要求

#### 1.工作范围

1.1 成交供应商应按照本项目现场实际条件、采购需求及最终项目目标提供设计（或设计配合）、软件、设备以及材料供货、安装、集成、系统及设备测试、调校、试运行（系统、单机）、采购人相关人员的培训及通过有关部门的验收期间提供必要的技术支持和配合、质量保证期内免费保养维修等全部工作。

1.2 依据本项目的工作内容与范围：成交供应商应包设计（或深化设计）、包设备与材料供货、包系统集成实施、包人工、包质量、包安全的方式实施本系统集成项目总承包并确保本项目最终验收顺利通过。

1.3 成交供应商应具备上海市或有关行业管理部门规定的在上海市场实施本项目所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由成交供应商自行负责。

#### 2.工作要求（包括但不限于以下要求）：

2.1 根据采购人的需求（要求）在采购人的指导下，负责完成系统方案与施工图深化设计以及出图工作（如有）。

2.2 负责编制项目实施组织设计、质量控制和技术方案、安装工艺及技术要求、施工详图等技术文件，交采购人审核后执行。

2.3 设备安装、线缆敷设和系统调（测）试均应根据技术方案经过内控审核，项目各环节应按照方案实施并进行质量自检，保证项目质量符合国家和上海市有关技术标准与规范要求。

2.4 负责编制项目进度计划和保障措施，确保按期完成。若有变更，应及时调整进度计划。

2.5 负责实施方案向有关部门的报批工作，以及项目竣工后向有关部门、单位申报测试与验收工作，并确保可以满足主管部门的要求（如有）。

2.6 根据采购人的变更要求及实施现场的实际情况，负责完成系统方案与施工图的变更设计，并经采购人及其委托监理单位（如有）审核后实施。

2.7 负责系统全部（包括子系统）设备的供应，并按合同范围、交付期限、质量标准等，保质保量按时将设备与器材等运至项目现场、完成本项目系统（包括子系统）线缆敷设和设备安装、集成、软件开发（如有）、测试、调校、系统开通、试运行等全部工作。

2.8 负责完成各系统控制室（如有）的布局设计与实施、装饰与环境以及供电等工作，并协助采购人完成控制室（机房）项目验收工作。

2.9 协助采购人和主管部门完成项目验收工作。验收按本项目合同以及国家和上海市的有关技术标准与规范进行。

2.10 负责完成项目竣工图纸与资料的编制工作，并在项目完成并交付使用前提交项目竣工资料全套（如采购人有此项要求）。

2.11 负责采购人相关人员的技术培训，并提供使用、操作手册，保证达到独立上岗操作与日常维

护的水平。

2.12 负责项目售后服务（系统免费保修期和服务响应时间不低于招标文件要求）。

#### 四、项目管理要求

1.在项目实施期间，成交供应商应严格执行国家、地方、行业有关本项目业务管理和安全作业的法律、法规和制度并按规定承担相应的费用。成交供应商因违反规定等原因造成的一切损失和责任由成交供应商自行承担。

2. 成交供应商在报价书中承诺并经采购人、集中采购机构认定的项目负责人及专业技术人员必须是本单位职工（在本单位缴纳社会保障金）和该项目实施现场的实际操作者，应具有类似本项目的实施经验，并应常驻项目现场。未经采购人同意，成交供应商不得调换或撤离上述人员。如采购人认为有必要，可要求成交供应商对上述人员中的部分人员作出更好的调整。

3. 成交供应商在项目实施期间，应按项目实际进度与环节落实所对应项目整体及各环节管理工作，按照规范做好项目实施期间相关管理与实施记录。

4. 成交供应商应严格参照执行国家与上海市有关建设工程安全文明施工管理的法律、法规和政策，积极主动落实安全文明及环境保护施工的管理和考核等有关工作，指派专人负责施工现场的安全，建立安全用电、动用明火申请批准等制度，防止隐患和落实好作业区域内的环境和原有装饰保护要求，确保作业区域周围环境的整洁和不影响正常办公区域正常工作，安全、文明实施本项目系统集成工作。

5. 成交供应商在与采购人签订项目合同的同时要签订安全生产责任协议书、治安防火责任协议书、项目文明实施协议书和廉政责任书（如采购人有此项要求），成交供应商若违反规定违章作业等，采购人有权责令停工整改，一切损失由成交供应商自行承担。

6. 成交供应商在项目实施期间必须遵守采购人的规章制度并提供实施人员名单。

7. 各供应商在报价文件中要结合本项目的特点和采购人上述的具体要求制定相应的管理措施，并在报价中列支相应的费用清单，供应商报价中未列支上述费用清单的，上述费用视为已包含在投标人的投标总报价中。

8.本项目合同不得转让、不得分包。

9.本项目设备材料供货及安装调试将纳入监理单位（如有）、采购人的管理范围，成交供应商在此过程中须服从上述单位的管理协调。

#### 五、其他要求及申明

1.供应商在进行系统设计时要考虑各系统的实用性、安全性、可靠性、兼容性、灵活性、先进性、开放性、扩展性、便捷性、高效节能、环保等各项因素，要选用技术先进、性能优良、使用可靠的设备和产品（不得选用已经停产或即将停产淘汰的产品）。为保证系统的兼容性和利于售后服务，同一个子系统内的设备需尽可能来自同一设备生产厂家，并与原有系统实现无缝对接。

2.本次采购不接受整体由进口产品所组成的系统。

#### 六、投标报价依据与要求

除第二章《投标人须知》第 19 条“投标报价”的要求外，供应商还应综合考虑以下各项要求，审慎进行投标报价。

1.报价依据：

采购需求、采购文件其他规定与要求、现场实际条件、项目有关标准、规范、资料、图纸、验收标准、市场实际价格和其他投标人认为应考虑的因素，以及行业和物价管理部门有关收费标准（如有）等。各供应商应根据本招标项目要求，结合自身能力诚信报价。

2.报价要求：

2.1 为准确投标报价，各供应商应详细了解项目实际条件、现状与各种可能产生影响的因素后制定项目技术和实施方案。各供应商在报价时要充分考虑在项目实施期限内各项工作所必须发生的各类费用及应承担的相关责任后进行报价。

2.2 本项目报价总价应是供应商根据现场实际条件达到采购需求目标、完成项目所需的所有费用。其中包括了项目系统设计、前期工作准备、设备与材料供货、集成安装等所需的设备、劳务及材料，以及前述的安装、相关软件开发与安装、人员开支、系统集成产生垃圾处理、特殊条件施工增加费、特殊产品保护费、系统测试、调校、试运转、培训等服务、有关保险费用、与安全文明

实施相关的措施费、竣工图编制费、管理费、利润、税金等费用，以及合同明示或暗示的所有责任、义务和一般风险，无论此等义务和风险是否在合同文件中详细指出。

2.3 响应报价中若发生类似知识产权归属、软件、专利费等费用，请一并报在投标总价中。除采购文件另有规定，采购人不再承担投标总价以外的其它任何费用。

2.4 供应商报价中人工工资、社会保障、福利、社会管理、税金等各类费用计费应符合国家、地方相关管理部门的规定，并包括在总价中。

2.5 本项目所有报价应以子系统为单位，需列出每个子系统单独的报价并汇总出相应的总价。不得将几个子系统混和报价。所有子系统的测试与验收费用应包括在投标总价中。采购人、集中采购机构要求投标人按照上述要求分类报价，其目的是为了便于采购人对报价书进行比较，但并不限制采购人以上述任何条件订立合同的权利。

2.6 合同价格以成交价为基准，在项目实施过程中如有采购人原因导致的设计变更，经采购人与成交供应商协商一致，可就变更合同价格另行签订补充协议。双方协商变更合同时，工作量可按实调整，单价及费率的取定均以报价书为准。变更后合同总价不得超过中标价的 10%，且不得超过本项目预算价。供应商不得以工作量变更为理由要求增加单价及费率。

## 七、商务要求：

类别	要求
磋商响应文件有效期	自开标之日起 90 天
质保期	36 个月
交货期	合同签订并生效后 100 个日历天内完工（包括安装、调试及验收）
付款方式	1) 合同生效后，核心路由器、汇聚路由器、出口路由器设备到货后，并在收到乙方提交合同金额3%的履约保证金后，甲方向乙方支付合同总价的20% 2) 全部设备到货后，支付合同总价的20%。 3) 完成网络环境的搭建，并完成初步验收后，支付合同总价的20%。 4) 所有建设内容全部完成，完成最终验收后，支付合同总价的30%。 5) 验收合格后，乙方向甲方提供金额为合同价的 3% 的银行支票或银行保函作为质量保证金之后，甲方再向乙方支付合同的余款 10%。
转让与分包	本项目合同不得转让与分包。
履约保证金	收取金额相当于合同总价百分之三（3%）；履约保证金应在项目按合同规定验收合格前保持有效；履约保证金由成交供应商在合同签订后出具。
质量保证金	收取金额相当于合同总价百分之三（3%）；质量保证金应在货物按合同规定验收合格后等同于质保期内保持有效；质量保证金由卖方在买方最后一次付款前支付出具。

## 八、响应文件的编制要求

供应商应按照第二章《供应商须知》“三、响应文件”中的相关要求编制响应文件，响应文件的商务响应文件（包括相关证明文件）和技术响应文件应当包括（但不限于）下列内容：

1、商务响应文件由以下部分组成：

- (1) 《磋商响应函》
- (2) 《报价一览表》（在电子采购平台填写）
- (3) 《报价分类明细表》
- (4) 《资格审查要求表》

- (5) 《符合性要求表》
  - (6) 《商务响应表》
  - (7) 《与评审有关的响应文件主要内容索引表》
  - (8) 《法定代表人授权委托书》（含法定代表人身份证、被授权人身份证复印件）
  - (9) 供应商营业执照（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）
  - (10) 依法缴纳税收和社会保障资金、没有重大违法记录的声明：  
具有依法缴纳税收和社会保障资金的良好记录、参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明函，截止至解密日成立不足3年的供应商可提供自成立以来无重大违法记录的书面声明。
  - (11) 供应商基本情况简介
  - (12) 供应商财务状况报告：  
供应商为法人的，提供经审计的上年度财务状况报告或基本账户的银行资信证明；其他组织和自然人，提供银行资信证明。
  - (13) 享受政府采购优惠政策的相关证明材料，包括：中小企业声明函、监狱企业证明文件、残疾人福利性单位声明函等（成交供应商为中小企业、残疾人福利性单位的，其声明函将随成交结果同时公告）；
- 2、技术响应文件由以下部分组成：
- (1) 主要管理、技术人员配备及相关工作经历、职业资格汇总表
  - (2) 项目经理情况
  - (3) 项目组人员情况
  - (4) 综合能力自述
  - (5) 需求分析及理解
  - (6) 方案设计
  - (7) 实施方案
  - (8) 售后服务方案
  - (9) 按照本磋商文件要求提供的其他技术性资料以及供应商需要说明的其他事项。
- 3、按照《项目采购需求》要求提供的其他技术性资料以及供应商需要说明的其他事项。  
以上各类响应文件格式详见磋商文件第六章《响应文件有关格式》（格式自拟除外）。

## 第五章 竞争性磋商程序及评审办法

### 一、响应无效情形

1、磋商小组将按照《供应商须知》以及《资格审查要求表》、《符合性要求表》要求对响应文件进行初审，响应文件不符合《资格审查要求表》、《符合性要求表》所列任何情形之一的，将被认定为无效响应。

2、单位负责人或法定代表人为同一人，或者存在直接控股、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响应的，相关响应均无效。

3、除上述以及法律法规所规定的响应无效情形外，响应文件有其他不符合磋商文件要求的均作为评审时的考虑因素，而不导致响应无效。

### 二、竞争性磋商程序

1、成立磋商小组。本项目评审工作由磋商小组负责，磋商小组由7人组成，其中采购人代表一名，其余为政府采购评审专家，采购代表不参加评审的，则磋商小组均由评审专家组成。集中采购机构将按照相关规定，从上海市政府采购评审专家库中随机抽取评审专家。

2、拟定磋商提纲并上传。磋商小组依据法律法规、供应商自报企业性质，拟定磋商提纲并上传至电子招投标系统中。

3、企业性质认定。磋商小组依据《政府采购促进中小企业发展暂行办法》、《关于印发中小企业划型标准规定的通知》、供应商自报企业类型及供应商资产总额、营业收入和从业人员数量情况，对供应商的企业性质进行认定。

4、响应文件初审。初审包括资格审查和符合性审查。首先，磋商小组依据法律法规和磋商文件的规定，审查、确定提交响应文件的供应商是否具备响应资格。其次，依据磋商文件的规定，从响应文件的有效性、完整性和对磋商文件的响应程度进行审查，确定响应文件是否对磋商文件的实质性要求作出了响应。

磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

5、磋商通知。集中采购机构将通知所有通过初审的供应商参加磋商。未按通知要求参加的供应商视为放弃本项目磋商，并不再接受其最后报价。

6、磋商准备。请参加磋商的供应商事先做好时间安排和磋商准备，根据通知的安排，携带法定代表人授权委托书、政府采购专用CA认证证书和供应商认为必要的其他相关资料准时参加磋商，根据磋商小组拟定的磋商提纲进行准备。

7、磋商。磋商小组所有成员集中与单一供应商分别进行磋商。在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。

8、提交最终响应文件。磋商结束后，供应商应按照磋商文件的变动情况和磋商小组的要求在规定时间内提交最终响应文件（包括最终报价，磋商文件未发生实质性变动的，供应商仅需提供最终报价及根据磋商情况作出的相关承诺），并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

9、综合评分。所有磋商和最后报价结束后，由磋商小组按照项目《评分细则》对提交最终响应文件的供应商的响应文件和最后报价进行综合评分。磋商小组应坚持客观、公正、审慎的原则综合、科学、客观评分。

10、推荐成交候选人。各评委按照评审办法对每个供应商进行独立评分，再计算平均分，从响应文件满足磋商文件全部实质性要求的供应商中，按照评审得分由高到低的顺序推荐3名成交候选供应商。政府购买服务项目（含政府和社会资本合作项目）、市场竞争不充分的科研项目以及需要扶持的科技成果转化项目，提交最后报价的供应商只有2家的，可以推荐2家成交候选供应商。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分相同且最后报价相同的，按照方案优劣/技术指标优劣顺序推荐。根据规定,采购人按照成交候选人排名顺序确定成交供应商。

### 三、竞争性磋商评审办法

根据《中华人民共和国政府采购法》及《政府采购竞争性磋商采购方式管理暂行办法》等相关规定，本项目采用“综合评分法”评审，总分为100分。

1、价格分按照以下方式进行计算：

(1) 价格评分：磋商报价得分 = 价格分值 × (磋商基准价/最后磋商报价) × 100

(2) 磋商基准价：是经初审合格（技术、商务基本符合要求，无重大缺、漏项）满足磋商文件要求且最终报价价格最低的报价。

(3) 最后磋商报价：最终报价无缺漏项的，最终报价即最后磋商报价；最终报价有缺漏项的，按照其他供应商相同项的最高报价计算其缺漏项价格，经过计算的缺漏项价格不超过其最终报价10%的，其最终报价也即最后磋商报价，缺漏项的费用视为已包括在其最终报价中，经过计算的缺漏项价格超过其最终报价10%的，其响应无效。

(4) 非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；非专门面向中小企业采购且接受联合体响应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%以上的供应商，给予其报价 3%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。中小企业响应应提供《中小企业声明函》。

(5) 磋商小组认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在磋商现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，磋商小组应当将其作为无效响应处理。

2、响应文件其他评分因素及分值设置等详见《评分细则》。

#### 评分细则（100分）

序号	评审内容	类别	评审标准	分值 (分)
1	报价得分	客观分	报价得分=30% × (磋商基准价/最后磋商报价) ×100	30
2	需求理解	主观分	根据供应商对本区政务网络现状的描述是否详细（0-2分）；项目建设需求的理解是否清晰（0-1分）；项目重点、难点和新旧系统有差异的分析是否到位（0-2）；合理化建议是否合理（0-1分）进行综合评分。	6
3	软硬件技术偏离	客观分	按照“9.2、#项汇总表”要求，对#号重要参数逐个响应，#号重要参数每负偏离一项或未完整提供佐证材料的扣2分，本项扣完为止。	20
4	实施方案	主观分	<b>网络集成要求：</b> 根据供应商提供的总体设计方案及详细拓扑结构，包括总体设计方案是否完整（0-1分），出口设计是否合理（0-1分）、核心节点设计是否合理（0-1分）、汇聚节点设计是否合理（0-1分）、接入节点设计是否合理（0-1分）、安全环境设计是否合理（0-1分）进行综合评分。	6

主观分	<p><b>网络割接方案：</b> 根据供应商提供的符合松江区政务外网现网要求的无缝业务割接方案是否可行（0-3分）；进行工程实施和现场技术保障方案是否合理（0-3分）进行综合评分。</p>	6
主观分	<p><b>安管中心建设：</b> 安全管理中心平台的实施方案必需严格贴合《上海市电子政务外网安全监测平台技术规范（征求意见稿）》的相关标准内容及要求。根据供应商提供的实施方案是否详细（0-2分）；架构设计方案是否科学（0-1分）进行综合评分。</p>	3
主观分	<p><b>运管中心建设：</b> 运行管理平台的实施方案必需严格贴合《上海市电子政务外网运行管理系统对接规范（征求意见稿）》的相关标准内容及要求。根据供应商提供的实施方案是否详细（0-2分）；架构设计方案是否科学（0-1分）进行综合评分。</p>	3
主观分	<p><b>兼容性方案：</b> 根据供应商提供的与现有网络系统的兼容性设计方案是否具有可操作性（0-3分）；所投设备之间的兼容性方案是否合理（0-3分）进行综合评分。 （供应商需提供兼容性承诺函并加盖公章，未提供本项不得分。）</p>	6
客观分	<p><b>OTN设计：</b> 1.获得位于本区内的OTN所属运营商（OTN节点数量必须满足4个）的授权函则得3分。 2.从业务的重要性来考虑出发，OTN节点须同时具备一定的冗余性，在本区（松江区）内要求拥有4个（含）以上OTN的节点，OTN节点数量每多一个，则得1分，最多得3分。 （以上，所有提供的OTN节点归属必须为同一运营商，若为多家运营商组合提供的形式，本项不得分）</p>	6

		主观分	<b>实施团队要求：</b> 实施团队总人数是否满足采购需求。（0-1分） （上述人员须提供磋商前近半年内连续三个月的社保缴费证明材料，未提供不得分）	1
		客观分	<b>实施团队要求：</b> 1、项目经理具备信息系统项目管理师认证证书的得1分。 2、项目成员具备系统集成项目管理工程师或网络工程师或信息系统项目管理师认证证书。每提供一份证书得0.5分，最高得1分。 （上述人员须提供有效期内的证书复印件、磋商前近半年内连续三个月的社保缴费证明材料，未提供不得分）	2
5	项目承诺与自罚措施	主观分	根据供应商提供的自罚措施，包括自罚资金比例大小（0-3分）；其他自罚措施是否具有可操作性（0-3分）进行综合评分。 （供应商需根据“六、针对本项目需承诺的内容”的承诺内容进行承诺，有一项不承诺的本项不得分）	6
6	售后服务	主观分	根据供应商提供的售后服务方案是否完善（0-2分）；驻场维护团队配置是否满足采购需求（0-1分）进行综合评分。	3
6	综合实力	主观分	供应商信誉状况是否良好，履约能力是否良好，营运状况是否良好。（0-2分）	2
<b>合计</b>		<b>100</b>		

## 第六章 响应文件有关格式

### 一、商务响应文件有关格式

#### 1、磋商响应函格式

致：\_\_\_\_\_（采购人、集中采购机构名称）

根据贵方\_\_\_\_\_（项目名称、项目编号）采购的竞争性磋商公告及采购邀请，  
\_\_\_\_\_（姓名和职务）被正式授权代表供应商（供应商名称、地址），按照网上采购系统规定向贵方提交响应文件 1 份。

据此函，供应商兹宣布同意如下：

- 1.按竞争性磋商文件规定，我方的报价为\_\_\_\_\_（大写）元人民币。
- 2.我方已详细研究了全部竞争性磋商文件，包括竞争性磋商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竞争性磋商文件的各项规定和要求，对竞争性磋商文件的合理性、合法性不再有异议。
- 3.磋商响应文件有效期为自解密之日起 \_\_\_\_\_日。
- 4.如我方成交，响应文件将作为本项目合同的组成部分，直至合同履行完毕止均保持有效，我方将按竞争性磋商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.我方同意向贵方提供贵方可能进一步要求的与本磋商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响应或其他任何响应。
- 8.我方已充分考虑到响应文件提交期间网上操作可能会发生的技术故障、操作失误和相应的风险，并对因网上操作的任何技术故障、操作失误造成响应文件内容缺漏、不一致或响应文件提交失败的，承担全部责任。
9. 我方同意解密内容以电子采购平台解密时的《报价一览表》内容为准。我方授权代表将及时使用数字证书对《报价一览表》中与我方有关的内容进行签名确认，授权代表未进行确认的，视为我方对解密内容无异议。
- 10.为便于贵方公正、择优地确定成交供应商及其报价货物和相关服务，我方就本次响应有关事项郑重声明如下：

（1）我方向贵方提交的所有响应文件、资料都是准确的和真实的。

（2）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：\_\_\_\_\_

供应商授权代表签名：\_\_\_\_\_

供应商名称（公章）：\_\_\_\_\_

日期： 年 月 日

## 2、报价一览表格式

项目名称:

采购编号:

### 松江区电子政务外网升级优化包 1

项目名称	交付日期	质保期	备注	响应总价(总价、元)

说明：（1）“金额（元）”指每一包件响应报价，所有价格均系用人民币表示，单位为元，精确到个位数。

（2）交付日期是指合同生效后多少天完成送货上门、就位、安装、调试、培训直至验收合格。

（3）质量保证期是指自货物按合同规定验收合格之日起多少个月。

（4）供应商应按照《采购需求》和《供应商须知》的要求报价。

供应商授权代表签字:

供 应 商（公章）:

日 期：        年        月        日

### 3、报价汇总表格式

项目名称：

采购编号：

费用类别	报价	备注
硬件设备		
应用软件开发		
系统集成费		
租赁费		
人员培训费用		
其他		
合计		

说明：（1）所有价格均系用人民币表示，单位为元，精确到个位数。

（2）供应商应按照《采购需求》和《供应商须知》的要求报价。

（3）如果不是标准配置，应附报价说明。

供应商授权代表签字： \_\_\_\_\_

供应商（公章）： \_\_\_\_\_

日期： 年 月 日

#### 4、投标报价分类明细表格式

项目名称:

采购编号:

##### (1) 各子系统报价汇总表

序号	子系统名称	各子系统设备供货、 安装报价	各子系统软件 开发报价	投标价格(元)
1				
2				
3				
合计投标总价(元)				

##### (2) 其中：各子系统设备供货、安装报价明细表

系统1 系统2……（各系统分别列出）

系统设备名称	型号、规格、品牌	产地	设备、材料单价 (含运输、服务 保险等)	数量	投标合价(人民 币元)
设备					
小计:					
材料					
小计:					
软件					
小计:					
系统集成费					
装、调试					
安装调试费					

措施费用及其他					
小计:					
培训					
小计:					
设计					
管理费					
利润					
税金					
小计:					
总价					

供应商授权代表签字:

供 应 商 (公章):

日 期:        年        月        日

5、应用软件开发说明一览表格式

项目名称:

采购编号:

序号	模块名称	单价 (人/月)	数量	合计	备注
总价					

注:以上为基本要求, 供应商可根据实际方案自行增加模块。

供应商授权代表签字: \_\_\_\_\_

供应商 (公章): \_\_\_\_\_

日期: 年 月 日

## 6、资格审查要求表

项目名称:

采购编号:

项目内容	具备的条件说明（要求）	响应检查项（响应内容说明(是/否)）	详细内容所对应电子响应文件名称与页次	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，仅需提供营业执照）；提供依法缴纳税收和社会保障资金、没有重大违法记录的书面声明。 2. 根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。 3. 未被列入“信用中国”网站( <a href="http://www.creditchina.gov.cn">www.creditchina.gov.cn</a> )失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网( <a href="http://www.ccgp.gov.cn">www.ccgp.gov.cn</a> )政府采购严重违法失信行为记录名单的供应商。			
联合体响应	本项目不接受联合体响应。			
大中小微企业	本项目面向大、中、小、微型等各类供应商采购。			

供应商授权代表签字:

供 应 商（公章）:

日 期：        年        月        日

## 7、符合性要求表

项目名称:

采购编号:

项目内容	具备的条件说明（要求）	响应检查项(响应内容说明(是/否))	详细内容所对应电子响应文件名称与页次	备注
法定代表人授权	1、在响应文件由法定代表人授权代表签字（或盖章）的情况下，应按磋商文件规定格式提供法定代表人授权委托书； 2、按磋商文件要求提供法定代表人身份证、被授权人身份证。			
响应文件内容、密封、签署等要求	符合磋商文件规定： 1、响应文件按磋商文件要求提供《磋商响应函》、《报价一览表》、《资格审查要求表》、《符合性要求表》； 2、响应文件按磋商文件要求密封（适用于纸质采购项目），电子响应文件须经电子加密（响应文件上传成功后，系统即自动加密）。			
报价	1、不得进行选择性的报价（报价应是唯一的，磋商文件要求提供备选方案的除外）； 2、报价不得超出磋商文件标明的采购预算金额或项目最高限价； 3、不得低于成本报价； 4、报价有缺漏项的，缺漏项部分的报价按照其他供应商相同项的最高报价计算，计算出的缺漏项部分报价不得超过总报价的 10%。			
商务要求	1. 磋商响应文件有效期、交付日期、交付地址、质量保证期、付款方式满足磋商文件要求。 2. 合同不得转让与分包满足磋商文件要求。 3. 履约保证金、质量保证金满足磋商文件要求。			
“★”要求	符合技术规范、技术标准和《采购需求》质量标准，或者符合磋商文件中标“★”的技术、性能及其它要求的；			
响应文件内容	1. 不同供应商的响应文件未出现磋商小组认为不应当雷同的情况（即响应文件与其他供应商的响应文件存在内容连续 20 行（含）以上相同或者 5 处（含）以上相同差错的）。 2. 供应商接受采购方按磋商文件规定对其响应文件中错误所进行的修正的；响应文件无采购方不能接受的附加条件的。			
其它无效响应情形	响应文件无政府法律法规或规章规定的其它无效响应情形的。			
公平竞争和诚实信用	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。			

供应商授权代表签字:

供 应 商 (公 章) :

日 期:        年        月        日

### 8、商务响应表格式

项目名称:

采购编号:

类别	竞争性磋商文件要求	是否响应	供应商的承诺或说明
磋商响应文件有效期			
交付期			
质保期			
付款方式			
转让与分包			
履约保证金			
质量保证金			

供应商授权代表签字:

供 应 商 (公章):

日 期:        年        月        日

### 9、与评审有关的响应文件主要内容索引表

项目名称：

采购编号：

序号	响应项目	主要内容概述	详细内容所在响应文件页次	备注
1	需求理解			
2	软硬件技术偏离			
3	实施方案			
4	项目承诺与自罚措施			
5	售后服务			
6	综合实力			
7				

说明：上述具体内容要求可以参照本项目评审方法与程序及评分细则。

供应商授权代表签字：

供应商（公章）：

日期： 年 月 日

## 10、法定代表人授权委托书格式

致：上海市松江区政府采购中心

我\_\_\_\_\_（姓名）系注册于\_\_\_\_\_（地址）的\_\_\_\_\_（供应商名称，以下简称我方）的法定代表人，现代表我方授权委托我方在职职工\_\_\_\_\_（姓名，职务）以我方的名义参加贵中心\_\_\_\_\_项目的采购活动，由其代表我方全权办理针对上述项目的响应文件提交、解密、磋商、响应文件澄清、报价、签约等一切具体事务，并签署全部有关的文件、协议及合同。

我方对被授权人的签名事项负全部责任。

在贵中心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。

被授权人无转委托权，特此委托。

法定代表人身份证复印件  
(正面)

被授权人身份证复印件  
(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  
(反面)

供应商（公章）：

受托人（签字）：

法定代表人（签字或盖章）：

身份证号码：

电话：

电话：

传真：

传真：

日期：

日期：

## 11、供应商基本情况简介格式

### （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、从业人数：

### （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、其他需要说明的情况：

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

供应商授权代表签字：

供 应 商（公章）：

日 期：        年        月        日

## 12、中小企业声明函格式

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，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业行业；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：

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

（2）本声明函所称服务由中小企业承接，是指提供服务的人员为中小企业依照《中华人民共和国民法典》订立劳动合同的从业人员，否则不享受中小企业扶持政策。

（3）从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

（4）采购标的对应的中小企业划分标准所属行业，以磋商文件第二章《供应商须知》规定为准。

（5）成交供应商为中小企业的，本声明函将随成交结果同时公告。

（6）供应商未按照上述格式正确填写《中小企业声明函》的，不享受中小企业扶持政策。

注：行业划型标准：

（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。

### 13、残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位安置残疾人\_\_\_\_人，占本单位在职职工人数比例\_\_\_\_%，符合残疾人福利性单位条件，且本单位参加单位的项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日 期：

说明：根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

（1）安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；

（2）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

（3）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

（4）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

（5）提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

如供应商不符合残疾人福利性单位条件，无需填写本声明。

**14、依法缴纳税收和社会保障资金、没有重大违法记录的声明**

声 明

我方具有依法缴纳税收和社会保障资金的良好记录，且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（公章）：

日期：

二、技术响应文件有关表格格式

1、主要管理、技术人员配备及相关工作经历、资质汇总表

项目名称：

采购编号：

项目组成 员姓名	年龄	在项目组 中的岗位	学历和毕 业时间	职称及职 业资格	进入本单 位时间	相关工作经 历	联系方式
.....							

## 2、项目实施方案及服务承诺

- (1) 项目实施方案及供应商建议的安装、调试、验收方法或方案；
- (2) 质量保证方案、技术服务、技术培训、售后服务的内容、措施等承诺。

### 3、系统兼容性方案及承诺

- (1) 系统兼容性方案；
- (2) 兼容性承诺。

包1 合同模板:

# 松江区电子政务外网升级优化项目合同

合同统一编号: [合同中心-合同编码]

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]
传真: [合同中心-采购人单位传真]	传真: [合同中心-供应商单位传真]
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信息系统设备、应用软件和服务项目:

1.1 松江区电子政务外网升级优化项目

乙方所提供的信息系统设备、应用软件其来源应符合国家的有关规定,信息系统设备、应用软件的模块配置、功能、版本、数量、价格和交付日期等详见合同附件。

2. 合同价格、交付地点和交付日期

2.1 合同价格

本合同价格为[合同中心-合同总价]元整([合同中心-合同总价大写])。

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

2.2 交付地点

本系统设备、应用软件和服务项目交付地点: 采购人指定地点。

## 2.3 交付日期

本信息系统应用软件和服务项目的交付日期：详见供应商承诺。

## 3. 质量标准和要求

3.1 乙方所交付信息系统设备、应用软件的质量标准按照国家标准、行业标准，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 乙方所交付的信息系统应用软件还应符合国家和上海市有关软件开发规定。

## 4. 权利瑕疵担保

### 4. 权利瑕疵担保

4.1 乙方保证对其交付的信息系统应用软件享有合法的权利。

4.2 乙方保证在其交付的信息系统应用软件上不存在任何未曾向甲方透露的漏洞，后门等安全隐患。

4.3 乙方保证其所交付的信息系统应用软件没有侵犯任何第三人的知识产权和商业秘密等权利。

4.4 如甲方使用该信息系统应用软件构成上述侵权的，则由乙方承担全部责任。

## 5. 交付、领受与验收

5.1 甲方应依据信息系统项目工程的条件和性质，根据乙方的要求向乙方提供信息系统的施工、安装和调试环境。如甲方未能在该时间内提供该施工和安装环境，乙方可相应顺延交付日期。如对乙方造成经济损失，甲方还应依本合同规定承担违约责任。

5.2 乙方应在进行每项交付前，以书面方式通知甲方。甲方应当在接到通知后安排接受交付。乙方在交付前应当根据附件中的检测标准对所交付的项目进行功能和运行检测，以确认交付项目符合本合同的规定。

5.3 乙方应按照合同及其附件所约定的内容进行交付，如果本合同约定甲方可以使用或拥有某软件源代码的，乙方应同时交付软件的源代码。所交付的文档与文件应当是可供人阅读的书面和电子文档。

5.4 甲方在领受交付项目后，应当对所交付项目进行检验，向乙方出具书面文件，以确认其符合本合同所约定信息系统设备及应用软件的模块、需求和功能、使用手册、维护手册。如有缺陷，应向乙方出具书面报告，陈述需要改进的缺陷。乙方应立即改进此项缺陷，并再次进行检测和评估，甲方应当再次检验并向乙方出具书面领受文件或递交缺陷报告。甲、乙双方将重复此项程序直至甲方领受或甲方依法或依约终止本合同为止。

5.5 自系统功能检测通过之日起，甲方拥有系统试运行权利。

5.6 如果由于乙方原因，导致系统在试运行期间出现故障或问题，乙方应及时排除该故障或问题。以上行为产生的费用均由乙方承担。

5.7 如果由于甲方原因，导致系统在试运行期间出现故障或问题，乙方应及时配合排除该方面的故障或问题。以上行为产生的相关费用均由甲方承担。

5.8 系统试运行完成后，甲方应及时进行系统验收。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，确定具体日期，由双方按照本合同的规定完成系统验收。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。

5.9 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，同时延长试运行期，直至系统完全符合验收标准。

5.10 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。

5.11 甲方根据信息系统应用软件模块和功能，对信息系统设备及应用软件验收合格后，甲方收取发票并在《验收单》上签署验收意见及加盖单位印章。

## 6. 知识产权和保密

6.1 甲方委托开发软件的知识产权归甲方所有。乙方向甲方交付使用的信息系统应用软件已享有知识产权的，甲方在许可的范围内合理使用。

6.2 在本合同项下的任何权利和义务不因合同乙方发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则本合同项下的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对甲方承担连带责任。

6.3 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（单位：元）。

7.2 本合同款项按照以下方式支付。

1) 合同生效后，核心路由器、汇聚路由器、出口路由器设备到货后，并在收到乙方提交合同金额 3% 的履约保证金后，甲方向乙方支付合同总价的 20%

2) 全部设备到货后，支付合同总价的 20%。

3) 完成网络环境的搭建，并完成初步验收后，支付合同总价的 20%。

4) 所有建设内容全部完成，完成最终验收后，支付合同总价的 30%。

5) 验收合格后，乙方向甲方提供金额为合同价的 3% 的银行支票或银行保函作为质量保证金之后，甲方再向乙方支付合同的余款 10%。

## 8. 辅助服务

8.1 乙方应提交所提供信息系统应用软件包括相应的每一模块技术文件，例如：操作手册、使用说明、维护手册和服务指南。这些文件应包装好随同项目交付一起交付给甲方发运。

8.2 乙方还应提供下列服务：

(1) 现场移动、安装、调试、启动监督及技术支持；

(2) 在质量保证期内对交付的信息系统设备、应用软件实施运行监督、维护、维修；

(3) 乙方应根据项目实施的计划、进度和需要与客户的合理要求，及时安排对甲方的相关人员进行培训。培训目标为使受训者能够独立、熟练地完成操作，实现依据本合同所规定的信息化系统应用软件的目標和功能。

8.3 辅助服务的费用应包含在合同价中，甲方不再另行支付。

## 9. 系统保证和维护

9.1 在乙方所交付的信息系统设备、应用软件中，不得含有未经甲方许可的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；

9.2 乙方所提供的软件，包括受甲方委托所开发的软件，如果需要经国家有关部门登记、备案、审批或许可的，乙方应当保证所提供的软件已经完成上述手续。

9.3 乙方保证，依据本合同向甲方提供的信息系统设备、应用软件及其附属产品不存在品质或工艺上的瑕疵，能够按照本合同所规定的技术规范、要求和功能进行正常运行。乙方保证其所提供的软件系统在当前情况下是最适合本项目的版本。

9.4 乙方自各项目交付验收通过之日起供应商承诺的质保期内向甲方提供免费的保修和维护服务并对由于设计、开发的缺陷而产生的故障负责。在此期间如发生系统运作故障，或出现问题，乙方将按照售后服务的承诺（见合同附件）提供技术支持和维护服务。

9.5 在质量保证期内，如果信息系统应用软件的模块或功能与合同不符，或证实信息系统设备、应用软件是有缺陷的，包括潜在的缺陷或使用不符合要求的设计、开发等，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。

9.6 乙方在约定的时间内未能弥补缺陷，甲方可采取必要的补救措施，但其风险和费用将由乙方承担，甲方根据合同规定对乙方行使的其他权利不受影响。

9.7 在维护期内如由于乙方的责任而需要对本信息系统应用软件中的模块予以更换或升级，则该部件的保修期应相应延长。

9.8 乙方应向甲方提交一笔金额为合同总价百分之三（3%）的质量保证金，质量保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交质量保证金所需的有关费用均由其自行承担。质量保证金应在甲方最后一次付款前支付，有效期为验收合格后供应商承诺的质保期个月。质量保证金期满后 15 天内，甲方应一次性将质量保证金无息退还乙方，无正当理由逾期不退的，甲方应承担由此而造成的乙方直接损失。

## 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 在质量保证期内，如果乙方对缺陷产品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) 乙方同意退货并将货款退还给甲方，由此发生的一切费用和损失由乙方承担。

(2) 根据信息系统应用软件的功能模块状况以及甲方所遭受的损失，经过买卖双方商定降低信息系统应用软件的价格。

(3) 乙方应在接到甲方通知后七天内负责采用符合合同规定的规格、质量和性能要求的新零件、部件和设备来更换有缺陷的部分或修补缺陷部分，其费用由乙方负担。同时，乙方应在约定的质量保证期基础上相应延长修补和/或更换件的质量保证期。

10.3 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，甲方有权从应付货款中扣除索赔金额或者没收质量保证金，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、地点交货和提供服务。

11.2 如乙方无正当理由而拖延交货，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交货和提供服务的情况时，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，并确定是否同意延长交货时间或延期提供服务。

## 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交货和提供服务，甲方应从货款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）赔偿迟交货物的交货价或延期服务的服务费用的百分之零点五（0.5%）计收，直至交货或提供服务为止。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 在本合同签署后，乙方应向甲方提交一笔金额为合同总价百分之三（3%）的履约保证金。履约保证金应自出具之日起至全部信息系统应用软件按本合同规定验收合格后三十天内有效。在全部信息系统应用软件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。

## **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 调解不成则向合同签订地法院起诉。

## **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信息系统应用软件。

(2) 如果乙方未能履行合同规定的其它义务。

16.2 如果甲方根据上述 16.1 款的规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买与未交货的信息系统应用软件，乙方应对购买类似的信息系统应用软件所超出的那部分费用负责。但是，乙方应继续执行合同中未终止的部分。

16.3 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 本合同一式贰份，甲乙双方各执一份。

## 20. 合同附件

20.1 本合同附件包括：竞争性磋商文件、响应文件、供应商最终承诺

20.2 本合同附件与合同具有同等效力。

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

## 21. 合同修改

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

签约各方：

甲方（盖章）：

乙方（盖章）：

法定代表人或授权委托人（签章）：

法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]**

日期：[合同中心-签订时间]

合同签订点：网上签约

**[合同中心-合同有效期]**

## 附件：项目采购需求

### 一、项目概述

项目名称	松江区政务外网升级改造项目
采购内容	松江区政务外网 OTN 光网租用、核心路由器、汇聚路由器、委办局接入交换机采购更换，SDN 控制器采购部署，网络集成、割接现场实施，安全管理中心部署建设，运维管理平台建设，安管平台和运管平台与市级平台对接的相关工作，及后续驻场运维服务。
主要技术规格	详见技术需求
项目预算	本项目预算金额 2322.02 万元，超过预算的响应按无效响应处理

#### 1.1、项目背景

松江区电子政务外网于 2003 年由松江科委采用自行采购网络设备+租用运营商裸光纤方式组建，已运行近 18 年。经过不断的扩容和优化，已覆盖了全区委办局、街道、居委会，但随着政务信息和政务应用的发展，电子政务外网越来越难满足集约化、多业务承载和网络安全自主可控要求。为配合我区政务信息化发展的需要以及满足《上海市电子政务外网建设和运行管理指南》的建设要求，现需对松江区电子政务外网网络设备进行升级优化，为今后长期的科学、合理、高效、细致的运维管理打下坚实基础，确保区政务外网内全市“一网通办”、“一网统管”、区政务数据中心平台、区视频图像共享平台的视频访问等应用的平稳运行，为支持和推进政务改革提供管理和服务保障。

以满足未来电子政务发展需求为导向，建成一张标准统一、技术先进、管理智能、安全可靠、坚强有力的新型电子政务外网。充分利用现有资源，按照国家、上海市统一规划和标准规范，完成松江区电子政务外网骨干网升级优化、各部门专网整合联通，建立电子政务外网“运维管理体系”和“安全防护体系”支撑系统，实现电子政务外网在网络架构、技术路线、网络资源、网络运维、网络安全等方面的统一管理，着力打造松江区安全可靠的基础网络支撑平台和运行环境，建设面向未来发展的可扩展全区统一电子政务外网。

### 二、项目现状和需求

#### 2.1、现状分析

松江区电子政务外网于 2019 年进行了一轮升级改造，以 SDN 技术为核心理念进行设计，采用 H3C 的园区网 SDN 技术架构方案，安全上考虑网络准入控制。政务网核心网络通过一中心及二中心 4 台核心交换机互联，替换原有 4 台老旧核心交换机，通过虚拟化组网简化管理，核心交

交换机间通过 40G 互联,同时下联 17 个街镇汇聚由千兆升级到万兆, 街镇新汇聚交换机分别以 10G 上联到一中心及二中心核心交换机, 街镇汇聚交换机上配置防火墙插卡保障街镇接入网络安全, 同时完成了近 5000 街镇终端采购方的入网部署工作。

通过引入 SDN 技术, 院外街镇网络目前已采用 H3C 的 SDN 园区网技术架构, 逻辑上核心层交换机作为三层 VxLAN 网关, 汇聚层交换机作为三层 VxLAN 网关, 接入层交换机作为 Leaf 设备的下游仅仅完成采购方接入和简单的 VLAN 隔离能力,从而实现可以兼容第三方接入设备。通过 SDN 控制器 Director 的预先定义, 每个采购方分组都获得独一无二的 VxLAN ID 标识符, 并在汇聚层实现 VRF 的自动创建以及与 VxLAN ID 的关联。

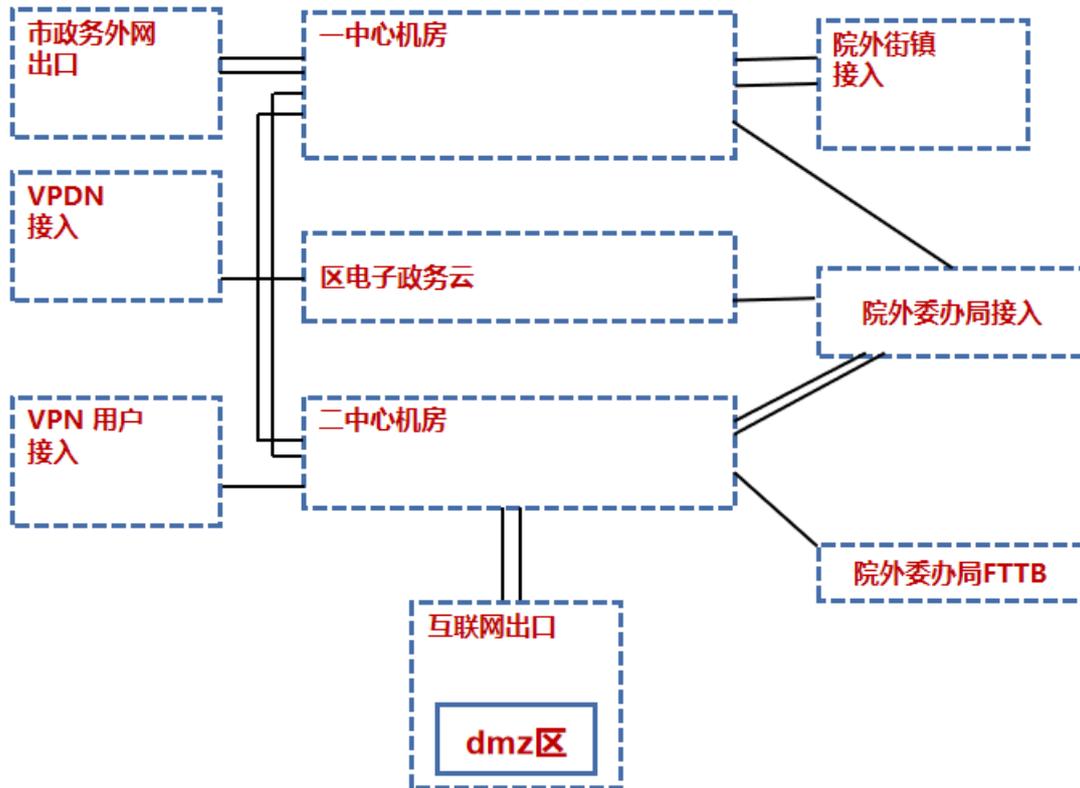
此外, 松江区电子政务外网目前涉及安全建设的部分主要有: 互联网出口区域、安全接入区域、政务网出口区域、内部服务器区和视频专网接入区域。

- 互联网出口区域由链路负载均衡、IPS、防毒墙、上网行为管理、DDOS 防护和防火墙组成, 所有设备均双机部署保证业务可靠性, 出口交换机链接 4 条互联网链路, 带宽总计 2G。
- 安全接入区域内部署 VPN 设备及防火墙, 主要负责采购方远程办公和其他机构业务专网接入。
- 政务网出口区域由两台防火墙双机部署组成作为防护边界。
- 内部服务器区域部署了两台防火墙和一台 IDS 设备保证业务可靠性。
- 视频专网接入区域也新增两台防火墙设备作为边界网关。

根据上海市大数据中心于 2020 年依据政务云化、专网整合、等保 2.0、建立统一管理体系等上海市政务信息化的发展趋势和目标, 结合实际情况编制了《上海市电子政务外网建设和运行管理指南(试行)》, 指南中对上海市级、区级电子政务外网的整体网络安全建设提出了全新的规范要求。松江区电子政务外网虽于 2019 年完成了改造升级建设, 但仍无法完全满足指南中的相关规范要求, 因此急需在现网的基础上进行优化和升级。

## 2.2、现网网络拓扑

松江区电子政务外网于 2003 年由松江区科委开始建设, 经过多年的改造和优化, 目前呈现如下架构。整体网络设备部署在两个中心, 整网采用交换机组网方式。上行连接至上海市电子政务外网, 下行连接至全区委办局、街道、居委会, 现状网络拓扑架构图如下:



### 2.3 总体建设需求

根据上海市大数据中心发布的《上海市电子政务外网建设和运行管理指南（试行）》为指导方针，现有如下总体需求：

- 租用一张采用 OTN 技术组网的光传输网络做为底层网络，并要求充分考虑 OTN 节点的冗余性。
- 业务网络采用核心、汇聚、接入的三层架构设计；核心、汇聚节点采用路由器组网方式。
- 业务网络采用“一网双平面”的架构设计。数据平面承载网络数据流量，视频平面，承载网络视频流量，两个平面在政务外网上逻辑隔离、独立运行，且互为冗余备份；
- 应基于 TCP/IP 技术构建政务外网业务网络，采用支持 IPv4/IPv6 双栈技术的网络
- 政务外网应符合等保 2.0 三级规范的要求。
- 应保证不同应用在业务网络的相互独立，可选用 VLAN、VxLAN、VPN、网络切片等方式实现不同业务的隔离；
- 应采用 SDN 技术，实现业务快速部署，流量工程和智能流量调整能力；需充分考虑与现存的 H3C 园区网 SDN 之间的兼容性问题。
- 应基于大数据分析技术和智能检测技术，对网络中不同业务的运行状态、服务质量，做到实时监控、主动运维。
- 建设安全管理中心和运行管理中心，并根据市大数据中心要求完成功能对接；同时根据松江区政务外网建设和运行管理实际情况形成相关运行管理规范。
- 在松江区街镇汇聚机房将原 4 台核心交换机两两组成一组做高可用集群，且下沉为街镇和委

办局等单位的汇聚交换机。汇聚交换机分别上联对接至街镇汇聚路由器的数据业务平面和视频业务平面的两台汇聚路由器设备；下联对接至区级院内外委办局和街镇网络接入交换机（区级院内外委办局和街镇网络的所有接入交换机此次也要求一并进行升级替换）。

此外，本次项目建设供应商须严格参照《上海市电子政务外网建设和运行管理指南》、《上海市电子政务外网运行管理系统对接规范（试行）》、《上海市电子政务外网安全监测平台技术规范（试行）》中的相关标准及要求进行设计和部署。

## 2.4、项目利旧情况

由于区电子政务外网建设较早，对于部分性能已经老化、出保、网络带宽不满足现网要求的网络安全设备应根据国家网络等保三级要求，及时替换，保证政务外网后续业务的扩展。

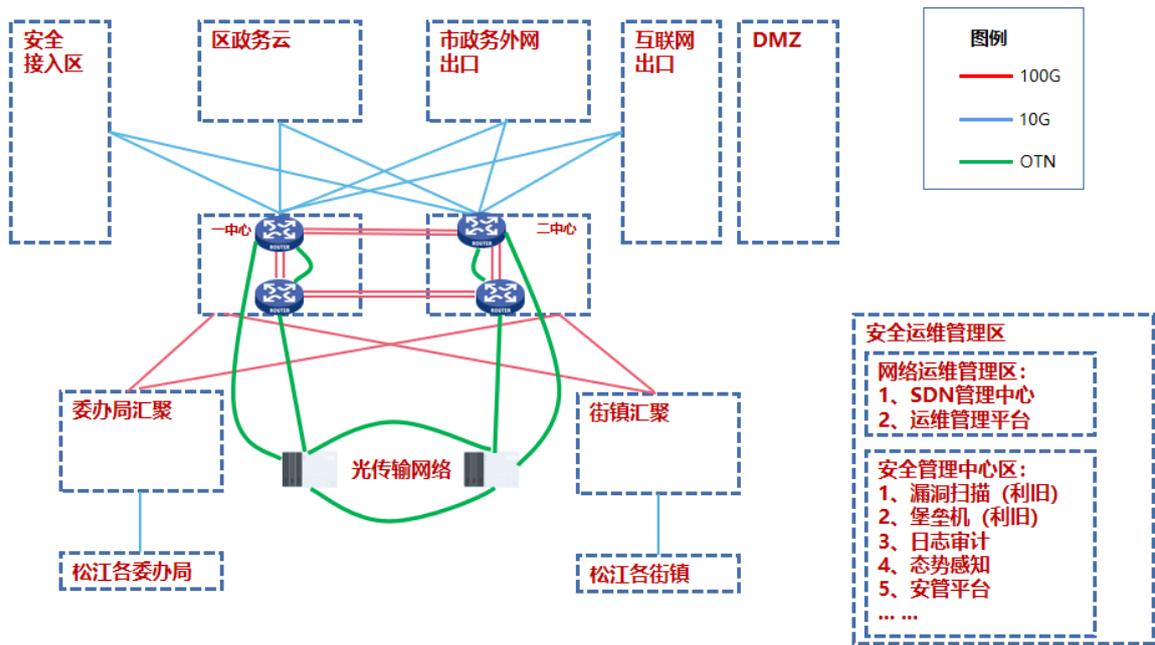
对于现网中已部署但仍可满足政务外网后续业务发展的网络、安全设备，本着节省资源，节约财政资金的原则，应继续利旧使用。例如现网中的部分防火墙、堡垒机、日志审计、负载均衡、IPS、防病毒网关等设备仍满足国家网络等级保护需求和《上海市电子政务外网建设和运行管理指南（试行）》要求，可以利旧使用。

### （利旧清单）

序号	类别	品牌	数量
1	链路负载均衡	天融信	2
2	入侵防御设备	启明星辰	2
3	防毒墙	江民	2
4	入侵检测设备	启明星辰	2
5	VPN 设备	天融信	1
6	网络审计系统	天融信	1
7	漏洞扫描系统	东软	1
8	运维审计系统（堡垒机）	东软	1
9	现网核心交换机	H3C	4
10	现网街镇汇聚交换机	H3C	17

## 2.5、总体建设目标

（总体建设目标逻辑拓扑）



为深入贯彻网络强国的战略思想，发挥信息化对经济社会发展的引领作用，高水平适应信息时代对政务网络基础设施的新要求，做强电子政务外网“全市一张网”，充分整合利用现有资源，运用先进网络技术、安全技术和理念，升级健全一张技术先进、服务优质、安全可控的电子政务外网，高效支撑松江区政务服务“一网通办”、城市运行“一网统管”现代化治理体系建设，提升城市治理现代化水平。

1、提升新型城市数字化转型应用的可持续支撑能力，提升核心骨干网络承载能力至 100G，为松江区建设新型城市数字化转型应用发展提供可持续支撑。

2、提升政务信息基础设施的集约化能力，整合部门业务专网，消除信息孤岛，提高专网整合后各部门业务的统一承载能力，实现网络集约化建设和管理。

3、提升政府社会管理和公共服务职能的保障能力，打造“事前可预防、事中可发现、事后可溯源、定责有依据”的管理、维护能力，形成 7\*24 小时不间断的政府社会管理能力和公共服务能力的网络保障。

4、提升政务信息的综合安全防护能力，按照国家信息安全技术网络安全等级保护基本要求，强化三级等保安全防护体系，形成对各类安全威胁的主动防御和安全态势的主动感知能力，创建市、区两级协同联动的安全监测平台，全面提升上海市政务信息服务的综合安全防护能力。

5、此次松江区电子政务外网光传输网络建设需采用 OTN 技术组网，为上层业务网络提供大带宽、低时延、高可靠的传输通道，通过光链路保护、资源可视化、光监控等功能，提升业务网络的传输安全和网络运维管理能力。

松江区电子政务外网的建设将紧紧围绕区政府、各政务部门深化电子政务应用、提高履行职责能力的迫切需要，为各部门实现政务、业务目标提供公共的技术环境和服务支撑，有效支持政

务部门灵活、快速部署应用业务，满足业务不断发展和改革的需要；满足架构稳定可靠，适应未来 5-8 年的演进需求；满足不同业务服务质量需求；满足安全自主可控需求；满足高效运维需求。

## 2.6、软硬件采购清单

序号	设备名称	数量	备注
<b>(一) 路由器</b>			
1	核心路由器	4	详见 3.1.1
2	汇聚路由器	4	详见 3.1.2
3	市政务外网出口路由器	2	详见 3.1.3
<b>(二) 交换机</b>			
1	汇聚交换机	1	详见 3.2.1
2	院外委办局接入交换机	35	详见 3.2.2
3	一、二中心接入交换机	50	详见 3.2.3
4	区政务云接入交换机	2	详见 3.2.4
5	互联网出口接入交换机	2	详见 3.2.5
6	市政务外网出口接入交换机	2	详见 3.2.6
7	安全接入区出口接入交换机	2	详见 3.2.7
8	管理区接入交换机	2	详见 3.2.8
<b>(三) 广域网 SDN 控制平台</b>			
1	SDN 控制平台	1	详见 3.3.1
<b>(四) 防火墙</b>			
1	互联网出口防火墙	2	详见 3.4.1
2	市政务外网出口防火墙	2	详见 3.4.2
3	安全接入区出口防火墙	2	详见 3.4.3
4	边界防火墙	4	详见 3.4.4
<b>(五) 上网行为管理</b>			
1	上网行为管理一体机	2	详见 3.5.1

(六) 日志审计			
1	日志审计一体机	1	详见 3.6.1
(七) 态势感知			
1	态势感知一体机	1	详见 3.7.1
(八) 安全管理中心			
1	安全管理平台	1	详见 3.8.1
(九) 运维管理中心			
1	运维管理平台	1	详见 3.9.1
以上所有软硬件设备自项目终验合格之日起提供 3 年原厂维保，并出具原厂商相关授权书（盖章）			

注：具体设备性能要求及技术功能参数请见下文。

## 2.7、服务采购清单

序号	项目	描述
1	OTN 租用服务	OTN 资源租用服务 1 年
2	实施服务	安装实施服务团队
3	驻场服务	3 年驻场服务

## 三、软硬件技术功能要求

### (一) 路由器

#### 3.1.1、核心路由器

功能及技术指标	详细技术参数
体系架构	支持主控板、交换网板、业务板完全物理分离，主控板、交换网板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板、交换网板和业务板槽位
	为保证设备可靠性，设备的转发全部由交换网板完成，主控板不集成转发芯片
	#为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，母卡和子卡均支持热插拔，需提供产品图片证明。
	要求响应产品为成熟产品，提供工信部入网许可证复印件
实配要求	路由器主机*4，单台主控 $\geq 2$ ，2500W 交流电源单台 $\geq 2$ ，1 端口 100G 以太网光接口子卡(QSFP28)单台 $\geq 4$ 个，共计 $\geq 16$ 个

	<p>5 端口万兆以太网光接口子卡(SFP+,LC)单台<math>\geq 2</math> 个， 共计<math>\geq 8</math> 个</p> <p>100G QSFP28 光模块(850nm,100m OM4,SR4,MPO)单台<math>\geq 3</math> 个， 共计<math>\geq 12</math> 个</p> <p>100G QSFP28 光模块(1310nm,2km,LR4L,CWDM4,LC)单台<math>\geq 2</math> 个， 共计<math>\geq 8</math> 个</p> <p>SFP+ 万兆模块(850nm,300m,LC)单台<math>\geq 10</math> 个， 共计<math>\geq 40</math> 个</p> <p>实配 3 年原厂维保及安装服务。</p>
性能要求	交换容量 $\geq 158T$ ， 包转发率 $\geq 24000M$ ， 以官网最小数值为准， 提供官方网站截图
	设备支持单槽单向最大带宽 $\geq 2Tbps$ ， 提供官方网站截图
硬件要求	整机框业务槽位数 $\geq 32$ ， 不含主控、交换机网板， 提供官方网站截图
	支持独立的交换网板 $\geq 4$ 个， 提供官方网站截图
基本功能	支持 PPP、MP、HDLC、ETHERNET 等链路层协议； 链路聚合（Link aggregation）， 支持动态聚合、手工聚合、跨板聚合、不同带宽的链路捆绑功能
	支持多路径负责分担功能（UCMP）， 支持非等速链路的负载分担， 实现不同路径按带宽比例负载分担
	支持 L2VPN、L3VPN、OptionA、B、C 类跨域， 支持 4M VPN 路由
SR 技术	支持 SR-TE、SR-TE 负载分担， SR-TE 流量调度、SR Policy， SR 跨域， BFD for SR； 支持 L3 层 MPLS SR 标签
	设备支持 SRv6 BE、SRv6 TE、SRv6 policy 支持 EVPN L2VPN/L3VPN/E-TREE/VPLS over SRv6/SRv6
	<b>★要求支持 SRv6 TE 功能， 实现 L2VPN， L3VPN 的业务流量调度； 要求支持 SRv6 TI-LFA， 实现网络快速倒换， 要求提供国家认可的第三方检测机构提供的有效的检测报告。</b>
IPv6	所投机柜需提供 IPv6 Ready II 证书
	支持 IPv6 邻居发现， PMTU 发现， TCP6， ping IPv6， traceroute IPv6， socket IPv6， 静态 IPv6 DNS， 指定 IPv6 DNS 服务器， TFTP IPv6 client。
	支持 IPv4 和 IPv6 双协议栈、IPv4 向 IPv6 的过渡技术、ICMPv6 MIB、UDP6 MIB、TCP6 MIB、IPv6 MIB 等
虚拟化	支持将两台物理设备虚拟化为一台逻辑设备， 虚拟组内可以实现一致的转发表项， 统一的管理， 跨物理设备的链路聚合
QOS	支持优先级 Mark/Remark、CAR、GTS 等功能
	为简化 ACL 配置， 设备需支持全局 ACL 功能
	支持 FIFO、PQ、WFQ、LLQ 等各种队列调度机制， 支持拥塞避免算法：Tail-Drop、RED、WRED， 支持层次化 Qos（H-Qos）
SDN	设备支持通过 Netconf（RFC 6241）协议下发配置、YANG 功能（RFC 6020）、Segment Routing 协议
	为实现设备间链路状态等信息共享， 设备需支持 BGP Link-State 功能； 为实现单节点上安全策略同步功能， 设备需支持 BGP FlowSpec 功能
	设备支持 Openflow 协议， 报文可依据流表进行转发； 为保证业务调度的精细化控制， 设备需要支持 13 层标签
	设备支持 EVPN/VxLAN（RFC 7348）功能， 能够完成 MAC 地址远端学习， 实现基于 VxLAN 的二三层 VPN
可靠性	为减小设备或线路故障对业务的影响、提高网络的可用性， 需支持 BFD

	for BGP/IS-IS/OSPF/LDP/VRRP/Static Route
	为在线进行补丁升级，支持热补丁功能；为提高设备软硬件稳定性及可靠性，主备倒换时业务不中断，交换网板、板卡、子卡均支持热插拔功能。
	为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持 NQA 检测网络网络质量
网络安全	设备支持防攻击能力，包括：ARP 攻击、IPv6 报文攻击、超大 Trace 报文攻击、TCP SYN flood、Ping flood、DHCP DDOS、PADI DDOS 的防御等
	支持 OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的 MD5 认证功能，支持 Keychain 功能，可以支持基于时间段的生效的密钥
一体化定制	支持与路由器一体化的防火墙、IPS 等安全业务插卡，提供官方网站截图，并提供板卡信息
维护特性	为方便设备运维管理，设备需内置 TCL 语言功能，能够解析执行 TCL 语言脚本；需内置 Python 语言功能，能够解析执行 Python 语言脚本、需支持配置回滚功能
	为实现精细化管理，实现不同进程动态部署到不同的 CPU 上，设备需支持进程分布式优化功能、支持 RBAC（基于角色的访问控制）功能
以上需提供所投设备的白皮书或产品文档	

### 3.1.2、汇聚路由器

功能及技术指标	详细技术参数
体系架构	支持主控板、业务板完全物理分离，主控板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板、业务板槽位 #为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，母卡和子卡均支持热插拔，需提供产品图片证明。
实配要求	路由器主机*4，双主控，2500W 交流电源单台≥2 个 1 端口 100G 以太网光接口子卡(QSFP28)单台≥3 个，共计≥12 个 1 端口 40G 以太网光接口子卡(QSFP+,LC)单台≥1 个，共计≥4 个 QSFP+ 40G 光模块(850nm,100m,SR4)单台≥2 个，共计≥8 个 100G QSFP28 光模块(850nm,100m OM4,SR4,MPO)单台≥2 个，共计≥10 个 100G QSFP28 光模块(1310nm,2km,LR4L,CWDM4,LC)单台≥2 个，共计≥8 个 实配 3 年原厂维保及安装服务。
性能要求	交换容量≥133Tbps，包转发率≥18000Mpps，以官网最小数值为准，提供官方网站截图
业务槽位	整机框业务槽位数≥24，不含主控、交换网板槽位，提供官方网站截图
电源系统	支持内置交流电源，不能配置外置交流电源，提供产品图片证明 电源系统支持 N+M 冗余，支持一体化供电方式，支持单电源供电
基本功能	支持 PPP、MP、HDLC、ETHERNET 等链路层协议；链路聚合（Link aggregation），支持动态聚合、手工聚合、跨板聚合、不同带宽的链路捆

	<p>绑功能</p> <p>支持多路径负责分担功能（UCMP），支持非等速链路的负载分担，实现不同路径按带宽比例负载分担</p> <p>支持 IPV4 静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略；IPV6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+</p> <p>支持 L2VPN、L3VPN、OptionA、B、C 类跨域，支持 4M VPN 路由</p>
SR 技术	<p>设备支持 L3 层 MPLS SR 标签</p> <p>支持 SR-TE, SR-TE 负载分担, SR-TE 流量调度、SR Policy、SR 跨域、BFD for SR、SRv6、SRv6 承载 VPN 业务</p>
IPv6	<p>支持 IPv4 和 IPv6 双协议栈、IPv4 向 IPv6 的过渡技术、ICMPv6 MIB、UDP6 MIB、TCP6 MIB、IPv6 MIB 等</p> <p>支持 IPv6 邻居发现, PMTU 发现, TCP6, ping IPv6, traceroute IPv6, socket IPv6, 静态 IPv6 DNS, 指定 IPv6 DNS 服务器, TFTP IPv6 client</p>
接口类型	<p>要求设备支持 FE、GE、10GE（LAN/WAN）、40GE、100GE、155M POS、622M POS、2.5G POS、10G POS、CPOS 接口、155M ATM、622M ATM、E1 等接口，提供官方网站截图</p> <p>支持 155M POS/622M POS/Ge 端口灵活切换，支持 ATM/POS 端口灵活切换，支持 155M ATM/622M ATM 端口灵活切换</p>
虚拟化	支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合
一体化定制	支持与路由器一体化的防火墙板卡、入侵防御板卡、LB 板卡等安全业务插卡，需提供官网截图证明
QOS	<p>支持优先级 Mark/Remark、CAR（Committed Access Rate）、GTS 等功能；支持全局 ACL 功能，为简化 ACL 配置</p> <p>支持 FIFO、PQ、WFQ、LLQ 等各种队列调度机制，支持拥塞避免算法：Tail-Drop、RED、WRED，支持层次化 Qos（H-Qos）</p>
SDN	<p>设备支持通过 Netconf(RFC 6241)协议下发配置、YANG 功能(RFC 6020)为实现设备间链路状态等信息共享，设备需支持 BGP Link-State 功能（RFC 7752）；为实现单节点上安全策略同步功能，设备需支持 BGP FlowSpec 功能（RFC 5575）；为实现按业务优先级选择隧道路径，设备需支持 CBTS 功能（YD/T 1391.1）</p> <p>设备支持 EVPN/VxLAN（RFC 7348）功能，能够完成 MAC 地址远端学习，实现基于 VxLAN 的二三层 VPN</p> <p>为减小设备或线路故障对业务的影响、提高网络的可用性，需支持 BFD for BGP/IS-IS/OSPF/LDP/VRRP/Static Route</p> <p>为在线进行补丁升级，支持热补丁功能；为提高设备软硬件稳定性及可靠性，主备切换时业务不中断，交换网板、板卡、子卡均支持热插拔功能。</p> <p>为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持 NQA 检测网络质量</p>
网络安全	<p>设备支持防攻击能力，包括：ARP 攻击、IPv6 报文攻击、超大 Trace 报文攻击、TCP SYN flood、Ping flood、DHCP DDOS、PADI DDOS 的防御等</p> <p>支持 OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的 MD5 认证功能，支持 Keychain 功能，可以支持基于时间段的生效的密钥</p>

维护特性	为方便设备运维管理，设备需内置 TCL 语言功能，能够解析执行 TCL 语言脚本；需内置 Python 语言功能，能够解析执行 Python 语言脚本、需支持配置回滚功能
	为实现精细化管理，实现不同进程动态部署到不同的 CPU 上，设备需支持进程分布式优化功能、支持 RBAC（基于角色的访问控制）功能
产品要求	要求响应产品为成熟产品，提供工信部入网许可证复印件
	所投机柜需提供 IPv6 Ready II 证书
以上需提供所投设备的白皮书或产品文档	

### 3.1.3、出口路由器

功能及技术指标	详细技术参数
体系架构	支持主控板、业务板完全物理分离，主控板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板、业务板槽位
	<b>#为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，母卡和子卡均支持热插拔，需提供产品图片证明。</b>
	要求支持主控冗余
实配要求	路由器主机*2，双主控，650W 交流电源单台≥2 个 4 端口万兆以太网光接口子卡(SFP+,LC)单台≥2 个，共计≥4 个 SFP+ 万兆模块(850nm,300m,LC)单台≥8 个，共计≥16 个 实配 3 年原厂维保及安装服务
性能要求	交换容量≥70Tbps，整机包转发率≥6000Mpps，以官网最小数值为准，提供官方网站截图
单槽位最大处理能力	≥240 Gbps
设备形态	整机框业务槽位数≥8，不含主控、交换网板槽位
电源系统	支持内置交流电源，且不需要占用业务槽位。
接口类型	要求设备支持 FE、GE、10GE（LAN/WAN）、40GE、100GE、155M POS、622M POS、2.5G POS、10G POS、CPOS 接口、155M ATM、622M ATM、E1 等接口，提供官方网站截图
广域网优化	支持 DRE、LZ、TFO 等多种 WAN 优化手段
	支持 WEB CACHE
SR 技术	支持单域及跨 BGP 域的 Segment Routing 技术，Segment Routing 与 LDP 混合组网
	支持对业务进行流量工程，支持基于按需下一跳及自动引流，并与 SR 灵活算法联动
	支持多种方法创建 SR Policy（NETCONF/CLI/BGP）、SRv6、SRv6 承载 VPN 业务
NAT	支持随板分布式 NAT 功能、NPTv6-RFC6296 功能
	支持 IPv6 邻居发现，PMTU 发现，TCP6，ping IPv6，traceroute IPv6，socket IPv6，静态 IPv6 DNS，指定 IPv6 DNS 服务器，TFTP IPv6 client
	支持 IPv4 和 IPv6 双协议栈、IPv4 向 IPv6 的过渡技术、ICMPv6 MIB、UDP6 MIB、TCP6 MIB、IPv6 MIB 等

组播 VPN	支持分布式 NG-MVPN 功能，不需要额外 License
虚拟化	支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合
产品要求	提供工信部入网许可证复印件
	所投机柜需提供 IPv6 Ready II 证书
以上需提供所投设备的白皮书或产品文档	

## (二) 交换机

### 3.2.1、汇聚交换机

功能及技术指标	参数要求
性能要求	交换容量 $\geq 76\text{Tbps}$ ，转发能力 $\geq 8640\text{Mpps}$ ，以官网最小数值为准
关键部件热插拔	主控交换卡、电源、接口模块、风扇等关键部件可热插拔
硬件要求	主控引擎模块 $\geq 2$ ，满足 1+1 冗余，业务插槽数 $\geq 6$ ，电源 $\geq 2$
实配	交换机主机*1，单台主控 $\geq 2$ ，650W 交流电源单台 $\geq 2$ 业务插槽数 $\geq 6$ 个 24 端口万兆以太网光接口(SFP+,LC)+2 端口 40G/1 端口 100G 以太网光接口模块 $\geq 1$ 套 48 端口千兆以太网电接口模块(RJ45) $\geq 1$ 套 实配 3 年原厂维保及安装服务
接口要求	以太网支持千兆电口，千兆光口，万兆光口、40G 端口、100G 端口 单槽位万兆线速端口密度 $\geq 48$ ，40G 端口密度 $\geq 24$ 、100G 端口密度 $\geq 4$ ，单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数 $\geq 48$ ，提高槽位利用率和业务可靠性
	支持 40G 跟 100G 端口切换，切换后流量正常转发，无丢包，提供工信部或提供中国合格评定国家认可委员会（CNAS）认证的第三方权威机构测试报告。
链路聚合	聚合组数 $\geq 1000$ 组，每组成员 $\geq 32$ 个 支持跨设备链路聚合
ACL	支持双向 ACL、支持端口 ACL、VLAN ACL
QOS	每端口支持 8 个优先级队列，3 个丢弃优先级，支持 SP、WRR、SP+WRR 三种队列调度算法；支持精细化的流量监管，粒度可达 8K
	支持流量整形 Shapping、WRED 拥塞避免、802.1p、TOS、DSCP、EXP 优先级映射
可靠性	双引擎快速倒换，主备切换时候板内转发无丢包；支持热补丁功能，可在线进行补丁升级
	支持 NSF/GR for OSPF/BGP/IS-IS
	支持 BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由
MAC	MAC 表 $\geq 1\text{M}$ ，学习速率 $\geq 130\text{K/S}$
路由表	IPv4 FIB 表项 $\geq 3\text{M}$ ，IPv6 FIB 表项 $\geq 1\text{M}$

	ND 表项 $\geq 256K$
IPv6	支持RIPng、OSPFv3、BGP4+、IS-ISv6协议
	支持IPv6策略路由、IPv6的VXLAN二三层互通、IPv6的VRRP功能；
	支持DHCPv6功能、IPv6 portal功能、IPv6管理功能；
ARP	ARP 表 $\geq 256K$
虚拟化	支持多虚一技术(N:1)，支持 $\geq 4$ 框虚拟化技术
	支持多虚一技术和一虚多技术的配合使用
多业务融合化	支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署 SDN 控制器
终端管理及网络安全	支持融合业务板卡，实现对摄像头等物联终端统一识别、认证和管理
MPLS	支持 L3 VPN
	支持 VLL、VLPS、MCE
VxLAN	支持 VXLAN，能够实现 VXLAN 二三层互通
管理特性	支持 Console/AUX/Telnet/SSH2.0
	支持风扇管理、电源管理、在线诊断
	支持 SNMPv1/v2、SNMPv3、RMON(RFC2819)
	支持端口镜像、VLAN 镜像、流镜像
以上需提供所投设备的白皮书或产品文档	

### 3.2.2、院外委办局接入交换机

功能及技术指标	详细技术参数
性能	交换容量 $\geq 4.32Tbps$ ，以官网最小值为准
	转发能力 $\geq 140Mpps$ ，以官网最小响应值为准
实配要求	交换机主机*35 支持 48 个 10/100/1000BASE-T 电口,4 个 1G/10G BASE-X SFP+端口 SFP+ 万兆模块(1310nm,10km,LC)单台 $\geq 4$ 个，共计 $\geq 140$ 个 实配 3 年原厂维保及安装服务
CPU 防护	实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作
VLAN 特性	支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN；
	最大 VLAN 数(不是 VLAN ID) $\geq 4094$
堆叠	最大堆叠台数 $\geq 9$ 台、堆叠带宽 $\geq 40G$ （万兆上行主机）
	支持跨设备链路聚合，单一 IP 管理，分布式弹性路由
	支持通过标准以太端口堆叠（万兆或千兆均支持）、支持远程堆叠
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预

功能及技术指标	详细技术参数
链路聚合	支持最多 8 个端口聚合；支持最多 128 个聚合组；支持 LACP
镜像功能	支持本地端口镜像和远程端口镜像 RSPAN、支持流镜像
	同时支持 N：M 的端口镜像（M 大于 1）
自动化	由于需要对区级院外委办局网络接入交换机进行替换升级，而院外委办局数量较多，因此所投交换机需支持被现园区网 SDN 控制器纳管，且能实现设备自动上线（提供原厂承诺书）
组播协议	支持 IGMP v1/v2/v3，MLD v1/v2、IGMP Snooping v1/v2/v3、MLD Snooping v1/v2
	支持组播 VLAN
	支持 PIM Snooping、MLD Proxy、PIM-DM，PIM-SM，PIM-SSM
	支持 MSDP，MSDP for IPv6 和 MBGP，MBGP for Ipv6
访问控制策略	支持基于第二层、第三层和第四层的 ACL；支持基于端口和 VLAN 的 ACL；支持 IPv6 ACL；
	支持出方向 ACL，以便于灵活实现数据包过滤；整机提供 ACL 条目数不小于 4K 条；
	支持 802.1x 认证，支持集中式 MAC 地址认证；
智能管理平台	内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级。提供官网截图
SDN/OPENFLOW	支持 OPENFLOW，支持普通模式和 Openflow 模式切换 支持多控制器（EQUAL 模式、主备模式），支持多表流水线 支持 Group table，支持 Meter
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
	支持 OAM(802.1AG, 802.3AH)以太网运行、维护和管理标准
以上需提供所投设备的白皮书或产品文档	

### 3.2.3、一、二办公中心接入交换机

功能及技术指标	详细技术参数
性能	交换容量 $\geq 4.32\text{Tbps}$ ，以官网最小值为准
	转发能力 $\geq 85\text{Mpps}$ ，以官网最小响应值为准
实配要求	交换机主机*50 支持 $\geq 48$ 个 10/100/1000BASE-T 电口,支持 $\geq 4$ 个 1000BASE-X SFP 端口 SFP-GE-单模模块-(1310nm,10km,LC)单台 $\geq 4$ 个，共计 $\geq 200$ 个 实配 3 年原厂维保及安装服务

功能及技术指标	详细技术参数
CPU 防护	实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作
VLAN 特性	支持基于端口的 VLAN，支持基于协议的 VLAN；、基于 MAC 的 VLAN。 最大 VLAN 数(不是 VLAN ID)≥4094
堆叠	最大堆叠台数≥9 台、堆叠带宽≥40G（万兆上行主机） 支持跨设备链路聚合，单一 IP 管理，分布式弹性路由 支持通过标准以太端口进行堆叠（万兆或千兆均支持）、支持远程堆叠 支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预
链路聚合	支持最多 8 个端口聚合；支持最多 128 个聚合组；支持 LACP
ERPS	实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms
镜像功能	支持本地端口镜像和远程端口镜像 RSPAN；支持流镜像 同时支持 N: M 的端口镜像（M 大于 1）
组播协议	支持 IGMP v1/v2/v3，MLD v1/v2；IGMP Snooping v1/v2/v3，MLD Snooping v1/v2；支持组播 VLAN 支持 PIM Snooping、MLD Proxy、PIM-DM，PIM-SM，PIM-SSM 支持 MSDP，MSDP for IPv6、MBGP，MBGP for Ipv6
访问控制策略	支持基于第二层、第三层和第四层的 ACL、支持基于端口和 VLAN 的 ACL； 支持出方向 ACL，以便于灵活实现数据包过滤；支持 IPv6 ACL 整机提供 ACL 条目数不小于 4K 条； 支持 802.1x 认证，支持集中式 MAC 地址认证；
SDN/OPENFLOW	支持 OPENFLOW，支持普通模式和 Openflow 模式切换 支持多控制器（EQUAL 模式、主备模式），支持多表流水线 支持 Group table，支持 Meter
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2 支持 OAM(802.1AG, 802.3AH)以太网运行、维护和管理标准
以上需提供所投设备的白皮书或产品文档	

### 3.2.4、政务云接入交换机

功能及技术指标	详细技术参数
性能	交换容量≥2.56Tbps，以官网最小值为准

功能及技术指标	详细技术参数
	转发能力 $\geq 1080\text{Mpps}$ ，，以官网最小响应值为准
实配	交换机主机*2，250W 交流电源单台 $\geq 2$ 个 支持 $\geq 48\text{SFP Plus}+2\text{QSFP Plus}+2\text{Slot}$ 40G QSFP+ 3m 电缆单台提供 1 根，共计 $\geq 2$ 根 2 端口 40G QSFP 接口板单台 $\geq 2$ 个，共计 $\geq 4$ 个 SFP+ 万兆模块(850nm,300m,LC)单台 $\geq 4$ 个，共计 $\geq 8$ 个 实配 3 年原厂维保及安装服务
VLAN 特性	支持基于端口的 VLAN，支持基于协议的 VLAN；
	支持基于 MAC 的 VLAN；
	最大 VLAN 数(不是 VLAN ID) $\geq 4094$
堆叠	最大堆叠台数 $\geq 9$ 台；最大堆叠带宽 $\geq 160\text{G}$
	支持跨设备链路聚合，单一 IP 管理，分布式弹性路由
	支持远程堆叠、通过标准以太网端口进行堆叠（万兆或 40G 均支持）
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预
链路聚合	支持最多 8 个 GE 口或 4 个 10 GE 端口聚合；支持最多 128 个聚合组； 支持 LACP
镜像功能	支持本地端口镜像和远程端口镜像 RSPAN；支持流镜像
	同时支持 N：M 的端口镜像（M 大于 1）
组播协议	支持 IGMP v1/v2/v3，MLD v1/v2；IGMP Snooping v1/v2/v3，MLD Snooping v1/v2；支持组播 VLAN
	支持 PIM Snooping、MLD Proxy、PIM-DM，PIM-SM，PIM-SSM
	支持 MSDP，MSDP for IPv6、MBGP，MBGP for Ipv6
访问控制策略	支持基于第二层、第三层和第四层的 ACL、支持基于端口和 VLAN 的 ACL；支持出方向 ACL，以便于灵活实现数据包过滤；支持 IPv6 ACL
	整机提供 ACL 条目数不小于 4K 条；
	支持 802.1x 认证，支持集中式 MAC 地址认证；
VxLAN	支持二层 VxLAN、支持三层 VxLAN、支持 EVPN
路由协议	支持 IPv4 静态路由、OSPF、BGP
	支持 IPv6 静态路由、OSPFv3、BGP4+
	支持 IPv4 和 IPv6 环境下的策略路由
	支持 IPv6 手动隧道、6to4 隧道和 ISATAP 隧道

功能及技术指标	详细技术参数
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
	支持 OAM(802.1AG, 802.3AH)以太网运行、维护和管理标准
以上需提供所投设备的白皮书或产品文档	

### 3.2.5、互联网出口交换机

功能及技术指标	详细技术参数
性能	交换容量 $\geq 2.56\text{Tbps}$ ，以官网最小值为准
	转发能力 $\geq 720\text{Mpps}$ ，以官网最小响应值为准
实配要求	交换机主机*2，250W 交流电源单台 $\geq 2$ 个 3 米 40G 堆叠线缆单台提供 1 根，共计 $\geq 2$ 根 SFP+ 万兆模块(850nm,300m,LC)单台 $\geq 2$ 个，共计 $\geq 4$ 个 实配 3 年原厂维保及安装服务
VLAN 特性	支持基于端口的 VLAN、支持基于协议的 VLAN、支持基于 MAC 的 VLAN；
	最大 VLAN 数(不是 VLAN ID) $\geq 4094$
堆叠	最大堆叠台数 $\geq 9$ 台
	最大堆叠带宽 $\geq 160\text{G}$
	支持跨设备链路聚合，单一 IP 管理，分布式弹性路由
	支持通过标准以太端口堆叠（万兆或 40G 均支持）、支持远程堆叠
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预
端口	支持 24SFP Plus+2QSFP Plus+2Slot
链路聚合	支持最多 8 个 GE 口或 4 个 10 GE 端口聚合；支持最多 128 个聚合组；支持 LACP
镜像功能	支持流镜像、支持本地端口镜像和远程端口镜像 RSPAN；
	同时支持 N: M 的端口镜像（M 大于 1）
组播协议	支持 IGMP v1/v2/v3，MLD v1/v2；IGMP Snooping v1/v2/v3，MLD Snooping v1/v2；支持组播 VLAN
	支持 PIM Snooping、MLD Proxy、PIM-DM，PIM-SM，PIM-SSM
	支持 MSDP，MSDP for IPv6、MBGP，MBGP for Ipv6
访问控制策略	支持基于第二层、第三层和第四层的 ACL、支持基于端口和 VLAN 的 ACL；支持出方向 ACL，以便于灵活实现数据包过滤；支持 IPv6 ACL

功能及技术指标	详细技术参数
	整机提供 ACI 条目数不小于 4K 条；
	支持 802.1x 认证，支持集中式 MAC 地址认证；
VxLAN	支持二层 VxLAN、支持三层 VxLAN、支持 EVPN
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
	支持 OAM(802.1AG, 802.3AH)以太网运行、维护和管理标准
以上需提供所投设备的白皮书或产品文档	

### 3.2.6、市政务外网出口交换机

功能及技术指标	详细技术参数
性能	交换容量 $\geq 2.56\text{Tbps}$ ，以官网最小值为准
	转发能力 $\geq 720\text{Mpps}$ ，以官网最小响应值为准
实配	交换机主机*2，250W 交流电源单台 $\geq 2$ 个 支持 48SFP Plus+2QSFP Plus+2Slot 40G QSFP+ 3m 电缆单台提供 1 根，共计 $\geq 2$ 根 SFP+ 万兆模块(850nm,300m,LC)单台 $\geq 4$ 个，共计 $\geq 8$ 个 实配 3 年原厂维保及安装服务
电源	支持并配置模块化双电源
端口	支持 24SFP Plus+2QSFP Plus+2Slot
VLAN 特性	支持基于端口的 VLAN，支持基于协议的 VLAN；
	支持基于 MAC 的 VLAN；
	最大 VLAN 数(不是 VLAN ID) $\geq 4094$
堆叠	最大堆叠台数 $\geq 9$ 台
	最大堆叠带宽 $\geq 160\text{G}$
	支持跨设备链路聚合，单一 IP 管理，分布式弹性路由
	支持通过标准以太端口进行堆叠（万兆或 40G 均支持）
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预
	支持远程堆叠
链路聚合	支持最多 8 个 GE 口或 4 个 10 GE 端口聚合；支持最多 128 个聚合组； 支持 LACP
镜像功能	支持本地端口镜像和远程端口镜像 RSPAN、支持流镜像
	同时支持 N: M 的端口镜像（M 大于 1）

功能及技术指标	详细技术参数
组播协议	支持 IGMP v1/v2/v3, MLD v1/v2; IGMP Snooping v1/v2/v3, MLD Snooping v1/v2; 支持组播 VLAN
	支持 PIM Snooping、MLD Proxy、PIM-DM, PIM-SM, PIM-SSM
	支持 MSDP, MSDP for IPv6、MBGP, MBGP for Ipv6
访问控制策略	支持基于第二层、第三层和第四层的 ACL、支持基于端口和 VLAN 的 ACL;
	支持出方向 ACL, 以便于灵活实现数据包过滤; 支持 IPv6 ACL
	整机提供 ACL 条目数不小于 4K 条;
	支持 802.1x 认证, 支持集中式 MAC 地址认证;
VxLAN	支持二层 VxLAN、支持三层 VxLAN、支持 EVPN
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
	支持 OAM(802.1AG, 802.3AH)以太网运行、维护和管理标准
以上需提供所投设备的白皮书或产品文档	

### 3.2.7、安全接入区出口交换机

功能及技术指标	详细技术参数
性能	交换容量 $\geq 2.56\text{Tbps}$ , 以官网最小值为准
	转发能力 $\geq 1080\text{Mpps}$ , , 以官网最小响应值为准
实配要求	交换机主机*2, 250W 交流电源单台 $\geq 2$ 个 48SFP Plus+2QSFP Plus+2Slot <b>40G</b> 电缆 3m 单台提供 1 根, 共计 $\geq 2$ 根 SFP+ 万兆模块(850nm,300m,LC)单台 $\geq 4$ 个, 共计 $\geq 8$ 个 实配 3 年原厂维保及安装服务
VLAN 特性	支持基于端口的 VLAN, 支持基于协议的 VLAN;
	支持基于 MAC 的 VLAN;
	最大 VLAN 数(不是 VLAN ID) $\geq 4094$
堆叠	最大堆叠台数 $\geq 9$ 台
	最大堆叠带宽 $\geq 160\text{G}$
	支持跨设备链路聚合, 单一 IP 管理, 分布式弹性路由
	支持通过标准以太端口进行堆叠(万兆或 40G 均支持)
	支持完善的堆叠分裂检测机制, 堆叠分裂后能自动完成 MAC 和 IP 地址的重配置, 无需手动干预

功能及技术指标	详细技术参数
	支持远程堆叠
链路聚合	支持最多 8 个 GE 口或 4 个 10 GE 端口聚合；支持最多 128 个聚合组；支持 LACP
镜像功能	支持本地端口镜像和远程端口镜像 RSPAN；支持流镜像
	同时支持 N: M 的端口镜像（M 大于 1）
组播协议	支持 IGMP v1/v2/v3, MLD v1/v2；IGMP Snooping v1/v2/v3, MLD Snooping v1/v2；支持组播 VLAN
	支持 PIM Snooping、MLD Proxy、PIM-DM, PIM-SM, PIM-SSM
	支持 MSDP, MSDP for IPv6、MBGP, MBGP for Ipv6
访问控制策略	支持基于第二层、第三层和第四层的 ACL、支持基于端口和 VLAN 的 ACL；支持出方向 ACL，以便于灵活实现数据包过滤；支持 IPv6 ACL
	整机提供 ACL 条目数不小于 4K 条；
	支持 802.1x 认证，支持集中式 MAC 地址认证；
VxLAN	支持二层 VxLAN、支持三层 VxLAN、支持 EVPN
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
	支持 OAM(802.1AG, 802.3AH)以太网运行、维护和管理标准
以上需提供所投设备的白皮书或产品文档	

### 3.2.8、管理交换机

功能及技术指标	详细技术参数
性能	交换容量 $\geq 750\text{Gbps}$ ，以官网最小值为准
	转发能力 $\geq 220\text{Mpps}$ ，以官网最小响应值为准
实配要求	交换机主机*2, 150W 交流电源单台 $\geq 2$ 个 24 个 10/100/1000BASE-T 端口, 4 个 10G/1G BASE-X SFP+端口 8 端口万兆 SFP Plus 接口板单台 $\geq 1$ 个, 共计 $\geq 2$ 个 SFP+ 电缆 1.2m 单台提供 1 根, 共计 $\geq 2$ 根 SFP+ 万兆模块(850nm,300m,LC)单台 $\geq 4$ 个, 共计 $\geq 8$ 个 实配 3 年原厂维保及安装服务
VLAN 特性	支持基于 MAC 的 VLAN、端口的 VLAN, 支持基于协议的 VLAN;
	最大 VLAN 数(不是 VLAN ID) $\geq 4094$
堆叠	最大堆叠台数 $\geq 9$ 台、最大堆叠带宽 $\geq 160\text{G}$
	支持跨设备链路聚合, 单一 IP 管理, 分布式弹性路由、标准以太端口进

功能及技术指标		详细技术参数
		行堆叠（万兆或 40G 均支持） 支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预
链路聚合		支持最多 8 个 GE 口或 4 个 10 GE 端口聚合；支持最多 128 个聚合组；支持 LACP
镜像功能		支持本地端口镜像和远程端口镜像 RSPAN；支持流镜像 同时支持 N: M 的端口镜像（M 大于 1）
组播协议		支持 IGMP v1/v2/v3, MLD v1/v2、IGMP Snooping v1/v2/v3, MLD Snooping v1/v2 支持 PIM Snooping、PIM-DM, PIM-SM, PIM-SSM、MLD Proxy、组播 VLAN；支持 MSDP, MSDP for IPv6、MBGP, MBGP for Ipv6
访问控制策略		支持基于第二层、第三层和第四层的 ACL；提供 ACL 条目数不小于 4K 条； 支持基于端口和 VLAN 的 ACL、IPv6 ACL；支持出方向 ACL，以便于灵活实现数据包过滤 支持 802.1x 认证，支持集中式 MAC 地址认证；
VxLAN		支持二层 VxLAN、支持三层 VxLAN、支持 EVPN
管理和维护		支持 SNMP V1/V2/V3、RMON、SSHV2 支持 OAM(802.1AG, 802.3AH)以太网运行、维护和管理标准
以上需提供所投设备的白皮书或产品文档		

### （三）SDN

#### 3.3.1、广域网 SDN 控制平台

功能及技术指标		详细技术参数
基础能力	网络规模	支持管理不少于 2000 台路由网络设备
实配	实配要求	本次实配≥12 个承载网网元授权， 并提供承载能力一体机≥3 台（每台内存≥128G，存储空间≥12T，电源模块≥2，含自带的操作系和数据库）。 实配 3 年软硬件原厂维保服务
拓扑收集	自动拓扑收集	支持控制器通过 BGP-LS 协议自动收集实际的拓扑信息（要求提供界面截图）
	手动拓扑	支持由管理员手动在控制器添加设备、链路等拓扑信息，控制器

	收集	对导入的网络拓扑和实际运行情况进行校对，最后形成整网的实际拓扑
拓扑管理	设备管理	支持对网络设备进行管理，包括增加、删除、属性修改等操作 支持管理员手动定义网络中各设备地理位置等信息，并在地图上进行呈现
隧道管理	隧道类型	支持在 IP 与 MPLS 网络中，使用 SR 隧道来对所有需要调度的应用流量进行封装
	隧道创建	支持控制器根据调度需要自动在设备间建立 SR 隧道，承载被调度的应用流量，支持 OSPF、IS-IS 的 SR-TE 隧道
L3VPN 业务部署	L3VPN 业务下发及管理	支持 PE 对接 CE 侧，自动化对 L3VPN 业务添加、修改、删除、回滚配置、查看操作
	应用绑定	支持 L3VPN 业务与应用组关联、修改关联、删除关联操作
QoS 业务部署	QoS 业务自动化部署	支持图形化配置 LAN 口业务自定义带宽值限速 支持图形化配置 WAN 口队列调度，按比例或带宽绝对值分配带宽，应用优先级进行业务保障、图形化配置 WAN 口限速
设备可视	设备基础信息可视	设备名称、序列号等静态信息呈现 对 CPU、内存、温度等历史信息（包括过去 1 小时、过去 1 天、过去一周、过去一月）进行统计和呈现
链路可视化	链路基础信息可视	支持链路通断，拥塞，质量状况呈现；支持链路名称、两端接口 IP 等静态信息呈现
	实时	应用组粒度粒呈现实时带宽信息，应用组实例粒度呈现实时带宽信息（要求提供界面截图）
	历史	时延、抖动、丢包、带宽利用率、应用组带宽/占比（要求提供界面截图）
应用流量可视	预定义应用流量	支持应用组实时流量及历史流量分布统计呈现
	未知应用流量	支持现网未知应用的实时流量分布统计呈现
应用质量可视	应用健康度	支持应用组内各实例质量的 SLA 符合度比例
应用定义	纯 IP 业务流分类	支持 IPv6 五元组、DSCP 任意组合进行业务流分类，自动映射到不同隧道自动进行流量调优。支持定义 IPv4/IPv6 应用。

	VPN 业务流分类	支持 IPv6 五元组、DSCP、VPN 任意组合进行业务流分类，自动映射到不同隧道自动进行流量调优。支持定义 IPv4/IPv6 应用。
链路信息	自动采集	自动下发质量探测任务，秒级感知链路质量和带宽变化，提供功能截图
链路质量	可视化	链路质量（延时、抖动、丢包）详细信息的实时呈现，支持秒级呈现，对链路的历史质量信息（包括过去 1 小时、过去 1 天、过去一周、过去一月）进行统计和呈现。
流量调度	# 路径自动调整方式	支路径自动调整方式：支持链路质量（时延、抖动、丢包）不满足、链路带宽超一级或二级阈值、设备故障、链路故障等方式即时触发链路自动调优（提供国家认可的第三方检测机构提供的有效的检测报告）
	选路策略	支持永久、指定时间、周期性时生效等时间段策略 支持共享风险组策略，主备路径避免选择同风险组链路
	批量路径优化	支持对自动调度应用进行定时或周期性或手工进行全局路径优化 支持对多个自动调度应用组实例进行批量路径优化
故障自动诊断	设备故障	支持自动诊断设备连接故障，设备 CPU、内存、温度超过阈值
	链路故障	支持自动诊断链路中断，链路质量低于阈值
	应用质量故障	支持自动诊断应用质量是否满足需求
告警管理	页面呈现	支持拓扑图中直接呈现故障信息
	告警推送	支持 E-mail 推送告警信息
	告警配置	支持告警阈值设置
设备管理	南向协议	支持 BGP-LS、Netconf、SNMP、Netstream、Telemetry、PCEP
	配置管理	支持同一设备 5 个不同时间的配置比对，可显示配置不同点
采购方访问	采购方认证	支持多采购方同过采购方名、密码认证
	账户分权	支持对不同采购方分配不同管理权限
SDN 兼容性	兼容性	此次项目中所投的广域网 SDN 控制器应与现政务外网的园区网 SDN 控制器 API 接口协议具备一致性，实现广域网 SDN 与现政务外网的园区网 SDN 支持统一界面、统一门户、统一入口，统一业务编排，

	实现采购方多场景业务的联动。
--	----------------

#### (四) 防火墙

##### 3.4.1、互联网出口防火墙

功能及技术指标	参数要求
硬件架构	采用非 X86 多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块（多核架构需提供证明材料）
	支持 SSD 硬盘不小于 480G，HDD 硬盘不小于 1T；
	要求具备接口扩展能力，支持 6 个接口扩展插槽
接口类型	≥4GE combo 口，≥8GE 电口，≥8SFP+口
性能要求	吞吐量≥35G，并发连接数≥1600 万，每秒新建连接数≥50 万/s；
实配要求	防火墙主机*2，650W 交流电源模块单台≥2 单台支持固定端口 8*GE RJ45 +8* SFP+ +4*GE combo，接口模块扩展槽位≥6 SFP+ 万兆模块(850nm,300m,LC)单台≥4 个，共计≥8 个 实配 3 年原厂维保及安装服务
NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、H.323 等多种 NAT ALG 功能
	NAT 地址池支持动态探测和可用地址分配
	支持 NAT44(4)、NAT64、PCP、溯源方案
负载均衡	多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、采购方业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权 HASH 等智能选路方式
应用安全	IPS 入侵防御、AV 防病毒、SSL 代理
	支持 URL 过滤、文件过滤
虚拟化特性	所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配 CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。上述功能要求须提供提供国家认可的第三方检测机构提供的有效的检测报告。

IPsec VPN	支持手动密钥、冗余 VPN 网关、EAP 认证
	支持 PKI (X.509)、IKEv2、IKEv2 重定向
IPv6	实现 IPV6 动态路由协议、IPV6 对象及策略、IPV6 状态防火墙、IPV6 攻击防范、IPV6 GRE/IPSEC VPN、IPV6 日志审计、IPV6 会话热备等功能。
	支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。
DDoS 防护	能够防范 DOS/DDOS 攻击、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范
	针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood 等常见 DDoS 攻击，需具备检测防御的功能
防病毒	可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表；发现病毒发送的告警信息，支持采购方编辑告警内容。支持基于文件协议、邮件协议（SMTP/POP3/imap）、共享协议（NFS/SMB）的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。
URL 过滤	支持联动云端 URL 地址库进行全面实施核查。提供功能截图
VPN	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
部署模式	实现路由模式、透明（网桥）模式、混合模式。
升级服务	整机同时具备防火墙、链路负载均衡、入侵防御、防病毒、带宽控制、应用识别和 web 应用防护等功能。
产品要求	所投产品须具备公安部监制的计算机信息系统安全专用产品销售许可证；
	<b>#同时具备中国网络安全审查技术与认证中心颁发的EAL4增强级认证证书及信息产业信息安全测评中心出具的防火墙EAL4+级型式试验报告。</b>
以上需提供所投设备的白皮书或产品文档；	

### 3.4.2、市政务外网出口防火墙

功能及技术指标	参数要求
硬件架构	采用非 X86 多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块（多核架构需提供证明材料）

	支持 SSD 硬盘不小于 480G, HDD 硬盘不小于 1T;
	要求具备接口扩展能力, 支持 6 个接口扩展插槽
接口类型	≥4GE combo 口, ≥8GE 电口, ≥8SFP+口
吞吐性能要求	吞吐量≥35G, 并发连接数≥1600 万, 每秒新建连接数≥50 万/s; 应用层 (IPS 入侵防御+AV 防病毒+应用识别) 吞吐≥14G, 并发连接数≥500 万, 每秒新建连接数 20 万/s; 当开启 IPS 入侵防御、AV 防病毒功能, 且应用层吞吐量≥7G 时, 要求设备 CPU 占有率不高于 50%, 需由设备生产厂商提供对应的设备性能保证书/承诺函。
实配要求	防火墙主机*2, 650W 交流电源模块单台≥2 单台支持固定端口 8*GE RJ45 +8* SFP+ +4*GE combo, 接口模块扩展槽位≥6 SFP+ 万兆模块(850nm,300m,LC)单台≥4 个, 共计≥8 个 防病毒特征库升级授权 3 年 IPS 特征库升级授权 3 年 实配 3 年原厂维保及安装服务
NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT, 实现 DNS、FTP、H.323 等多种 NAT ALG 功能。
	NAT 地址池支持动态探测和可用地址分配
	支持 NAT44(4)、NAT64、PCP、溯源方案
负载均衡	多出口智能选路, 支持基于链路权重、带宽、配置优先级、链路质量、采购方业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权 HASH 等智能选路方式
应用安全	IPS 入侵防御、AV 防病毒、SSL 代理
	支持 URL 过滤、文件过滤
虚拟化特性	所投设备须支持虚拟防火墙功能: 支持虚拟防火墙的创建、启动、关闭、删除功能; 可独立分配 CPU/内存等计算资源; 虚拟防火墙可独立管理, 独立保存配置; 虚拟防火墙具备独立会话管理、NAT、路由等功能。上述功能要求须提供国家认可的第三方检测机构提供的有效的检测报告。
IPsec VPN	支持手动密钥、冗余 VPN 网关、EAP 认证
	支持 PKI (X.509)、IKEv2、IKEv2 重定向
IPv6	实现 IPV6 动态路由协议、IPV6 对象及策略、IPV6 状态防火墙、

	IPV6 攻击防范、IPV6 GRE/IPSEC VPN、IPV6 日志审计、IPV6 会话热备等功能。
	支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。
DDoS 防护	能够防范 DOS/DDOS 攻击、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范
	针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood 等常见 DDoS 攻击，需具备检测防御的功能
防病毒	可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表；
	支持基于文件协议、邮件协议（SMTP/POP3/imap）、共享协议（NFS/SMB）的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息，支持采购方编辑告警内容
VPN	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
部署模式	实现路由模式、透明（网桥）模式、混合模式。
升级服务	整机同时具备防火墙、链路负载均衡、入侵防御、防病毒、带宽控制、应用识别和 web 应用防护等功能。
产品要求	所投产品须具备公安部监制的计算机信息系统安全专用产品销售许可证；
以上需提供所投设备的白皮书或产品文档	

### 3.4.3、安全接入区出口防火墙

功能及技术指标	参数要求
硬件架构	采用非 X86 多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块（多核架构需提供证明材料）
	支持 SSD 硬盘不小于 480G，HDD 硬盘不小于 1T；
	要求具备接口扩展能力，支持 6 个接口扩展插槽
接口类型	≥4GE combo 口，≥8GE 电口，≥8SFP+口
吞吐性能要求	吞吐量≥35G，并发连接数≥1600 万，每秒新建连接数≥50 万/s；

	<p>应用层（IPS 入侵防御+应用识别）吞吐<math>\geq 14G</math>，并发连接数<math>\geq 500</math>万，每秒新建连接数 20 万/s;</p> <p>当开启 IPS 入侵防御、AV 防病毒功能，且应用层吞吐量<math>\geq 7G</math>时，要求设备 CPU 占有率不高于 50%，需由设备生产厂商提供对应的设备性能保证书/承诺函。</p>
实配要求	<p>防火墙主机*2，650W 交流电源模块单台<math>\geq 2</math></p> <p>单台支持固定端口 8*GE RJ4R5 +8* SFP+ +4*GE combo，支持扩展槽位<math>\geq 6</math></p> <p>SFP+ 万兆模块(850nm,300m,LC)单台<math>\geq 4</math>个，共计<math>\geq 8</math>个</p> <p>防病毒特征库升级授权 3 年</p> <p>IPS 特征库升级授权 3 年</p> <p>实配 3 年原厂维保及安装服务</p>
NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、H.323 等多种 NAT ALG 功能。
	NAT 地址池支持动态探测和可用地址分配
	支持 NAT44(4)、NAT64、PCP、溯源方案
负载均衡	多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、采购方业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权 HASH 等智能选路方式
应用安全	IPS 入侵防御、AV 防病毒、SSL 代理
	支持 URL 过滤、文件过滤
虚拟化特性	<p>所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；</p> <p>可独立分配 CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。上述功能要求须提供国家认可的第三方检测机构提供的有效的检测报告。</p>
IPsec VPN	支持手动密钥、冗余 VPN 网关、EAP 认证
	支持 PKI (X.509)、IKEv2、IKEv2 重定向
IPv6	实现 IPV6 动态路由协议、IPV6 对象及策略、IPV6 状态防火墙、IPV6 攻击防范、IPV6 GRE/IPSEC VPN、IPV6 日志审计、IPV6 会话热备等功能。
	支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。
DDoS 防护	能够防范 DOS/DDOS 攻击、IP 分片报文、ARP 欺骗、ARP 主动

	反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范
	针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood 等常见 DDoS 攻击，需具备检测防御的功能
防病毒	可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表；
	支持基于文件协议、邮件协议（SMTP/POP3/imap）、共享协议（NFS/SMB）的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息，支持采购方编辑告警内容
VPN	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
部署模式	实现路由模式、透明（网桥）模式、混合模式。
升级服务	整机同时具备防火墙、链路负载均衡、入侵防御、防病毒、带宽控制、应用识别和 web 应用防护等功能。
产品要求	所投产品须具备公安部监制的计算机信息系统安全专用产品销售许可证；
以上需提供所投设备的白皮书或产品文档	

#### 3.4.4、边界防火墙

功能及技术指标	参数要求
硬件架构	采用非 X86 多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块（多核架构需提供证明材料）
	支持 SSD 硬盘不小于 480G，HDD 硬盘不小于 1T；
	要求具备接口扩展能力，支持 5 个接口扩展插槽
接口类型	≥4GE combo 口，≥8GE 电口，≥8SFP 口，≥8SFP+口，≥2QSFP+口
吞吐性能要求	网络吞吐量≥50G，并发连接数≥4000 万，每秒新建连接数≥60 万/s； 应用层（IPS 入侵防御+AV 防病毒+应用识别）吞吐≥18G，并发连接数≥1500 万，每秒新建连接数≥20 万/s； 当开启 IPS 入侵防御、AV 防病毒功能，且应用层吞吐量≥9G 时，

	要求设备 CPU 占有率不高于 50%，需由设备生产厂商提供对应的设备性能保证书/承诺函。
实配`	<p>防火墙主机*4，650W 交流电源模块单台≥2</p> <p>单台支持固定端口 8*GE RJ45 +8* SFP+ +4*GE combo +2*40G，支持扩展槽位≥5</p> <p>QSFP+ 40G 光模块(850nm,100m,SR)单台≥2 个，共计≥8 个</p> <p>SFP+ 万兆模块(850nm,300m,LC)单台≥2 个，共计≥8 个</p> <p>防病毒特征库升级授权 3 年</p> <p>IPS 特征库升级授权 3 年</p> <p>实配 3 年原厂维保及安装服务</p>
NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、H.323 等多种 NAT ALG 功能。
	NAT 地址池支持动态探测和可用地址分配
	支持 NAT44(4)、NAT64、PCP、溯源方案
负载均衡	多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、采购方业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权 HASH 等智能选路方式
应用安全	IPS 入侵防御、AV 防病毒、SSL 代理
	支持 URL 过滤、文件过滤
#虚拟化特性	所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配 CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。上述功能要求须提供国家认可的第三方检测机构提供的有效的检测报告。
IPsec VPN	支持手动密钥、冗余 VPN 网关、EAP 认证
	支持 PKI (X.509)、IKEv2、IKEv2 重定向
IPv6	实现 IPV6 动态路由协议、IPV6 对象及策略、IPV6 状态防火墙、IPV6 攻击防范、IPV6 GRE/IPSEC VPN、IPV6 日志审计、IPV6 会话热备等功能。
	支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。
DDoS 防护	能够防范 DOS/DDOS 攻击、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范

	针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood 等常见 DDoS 攻击，需具备检测防御的功能
防病毒	可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表；
	支持基于文件协议、邮件协议（SMTP/POP3/imap）、共享协议（NFS/SMB）的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息，支持采购方编辑告警内容
VPN	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
部署模式	实现路由模式、透明（网桥）模式、混合模式。
升级服务	整机同时具备防火墙、链路负载均衡、入侵防御、防病毒、带宽控制、应用识别和 web 应用防护等功能。
产品要求	所投产品须具备公安部监制的计算机信息系统安全专用产品销售许可证；
以上需提供所投设备的白皮书或产品文档	

## （五）上网行为管理

### 3.5.1、上网行为管理一体机

功能及技术指标	参数要求
产品性能	支持 10M/100M/1000M 自适应电接口数量 $\geq 12$ ，支持千兆 SFP 光接口数量 $\geq 12$ ，万兆接口总数 $\geq 4$ ，接口无路由/交换/LAN/WAN 等固化区分，均可作为二三层接口使用。要求提供产品正面照
	网络吞吐量 $\geq 40G$ ，应用层吞吐 $\geq 15G$ ，新建连接数 $\geq 60$ 万，并发连接数 $\geq 1000$ 万
实配要求	上网行为管理一体机*2 SFP+ 万兆模块(850nm,300m,LC)单台 $\geq 4$ 个，共计 $\geq 8$ 个 特征库升级服务授权 3 年 实配 3 年软硬件原厂维保服务
部署模式	支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备

接口配置	支持以太网接口、VLAN、桥接口、聚合接口、隧道接口、4G 无线接口、安全域、IPv6 隧道接口、Ipssec 隧道接口；支持端口镜像
NAT	支持源地址转换、目的地址转换、双向地址转换、NAT44
IPv6	支持配置基于采购方和应用均为任意的 7 元组的 IPv6 策略，支持全 IPV6 能力，产品能力包含上网行为审计、上网行为控制、流量控制、认证、日志、报表等，并提供 web 配置界面截图
应用协议识别	支持主流 P2P、IM、在线视频、网络游戏、网络炒股等应用识别
	支持 BYOD 特征库，可识别 ios 版和安卓版移动互联网软件如腾讯微博、QQ 空间等特征，并提供 web 界面配置截图
	支持基于 IP、端口、正则匹配式、URL、协议等自定义协议服务
	应用特征库数量不低于 5000+
采购方行为审计	支持 http、邮件、即时通讯、基础协议、娱乐股票、网络应用六个大类维度的采购方应用审计。
	http 类审计支持网页访问、网络社区（微博、论坛）、网页搜索、http 外发文件、http 文件下载、web 网盘上传文件、web 网盘下载文件等细粒度的审计。
	基础协议类审计支持 FTP 的账号和文件名相关审计
流量管理	支持高性能的限制通道，限制通道支持基于接口、地址、采购方、采购方组、应用、服务、时间维护的条件匹配，支持每 IP 和每采购方限速配置。
	支持通道化的 QoS，支持基于源地址、采购方、服务、应用、时间进行带宽控制，并支持配置保障带宽、限制带宽、带宽借用、每 IP 带宽、流量限额、带宽优先级等 QoS 动作，时间选择支持基于日计划、周计划、单次计划等。
	支持应用、采购方流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其 Top 流量采购方
	支持本地 web 认证，针对本地 web 认证的认证服务器可以是本地 AAA，也支持外部 radius、ldap 认证服务器支持认证页面自定义，支持针对本地认证、微信认证、短信认证、免认证、二维码认证、混合认证提供管理员自定义模板
	支持本地 web 认证、短信认证、微信认证、免认证、SAM 认证、单点登录、POP3 认证、portal 认证、访客二维码认证、混合认证等多种认证方式

	设备旁路模式部署支持所有采购方认证、旁路阻断。提供 web 界面截图
数据分析	支持采购方虚拟身份画像，以时间轴的形式展示采购方上网行为轨迹，提供 web 配置界面截图
高可靠性	支持双机热备，支持主主模式、主备模式，支持同步配置、会话、运行状态、VPN 状态、特征库，支持配置抢占模式和抢占延时，支持配置 HA 监控接口
	支持地址代理、非对称路由
维护	web 管理界面支持 Ping、Traceroute、TCP Syn 诊断工具，可支持基于接口、协议、IP 地址、端口、应用进行网络抓包，并可下载导出分析，提供 web 界面配置截图
#产品要求	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。
以上需提供所投设备的白皮书或产品文档	

## (六) 日志审计

### 3.6.1、日志审计一体机

功能及技术指标	参数要求
性能需求	事件入库性能 $\geq 4000$ EPS；日志源默认 $\geq 512$ 日志源；
	单台 $\geq 8$ 个硬盘盘位，可用实际存储总空间单台需 $\geq 32$ Tb
实配要求	日志审计一体机*1 $\geq 4$ 个千兆电口， $\geq 2$ 个万兆光口， $\geq 4$ 个万兆多模光模块 实配 3 年软硬件原厂维保服务
查询	具备日志收集实时监控，可基于设备类型、日志类型、日志等级进行监控查看
	支持按照设备类型（交换机、路由器、FW/IPS/LB/WAF、数据库、中间件、主机等设备）列表查看日志范式化分析结果，支持查看日志详情；支持基于时间、日志类别进行筛选
	支持按照日志类型进行查询，支持操作日志、审计日志、流量日志、威胁日志、主机日志等 11 大类 70 子标签进行分类
分析	支持多类型、多厂商安全设备、网络设备、操作系统、应用日志适配分析；对原始日志的日志内容进行适配分析，分析结果范式化展

	示
	可对多源日志进行递归关联、时序关联、统计关联等方式关联分析，提升安全分析结果准确性
检索	支持全文检索原始日志，检索字段变色高亮；支持任意信息、任意时间进行内容查询匹配，支持可选包含/不包含匹配方式
关联规则	支持新增、删除、修改关联规则，对关联规则进行启用和停用管理
	支持按照规则名称，事件名称，使用状态，威胁等级进行检索查询
	支持查看规则详情、安全策略命中次数统计
明细追溯	列表显示安全事件明细的详细信息，主要包括发生时间、过滤类型、事件等级、事件名称、源 IP 地址、目的 IP 地址、规则名称、事件描述、原始事件数、处理状态、支持操作等信息，支持查看原始事件详情进行追溯
报表	支持自定义报表中日志统计维度、统计方式（柱状图、饼状图、折线图、表格）
	支持采购方自定义报表样式，可基于日志、关联事件结果生成 50 多种维度的自定义统计报告；支持自定义生成 docx、html、pdf 格式报表
通知	支持配置邮件服务器地址、端口、账号密码和接受邮箱
	支持配置短信网关、增删改查接收通知号码；定制化对接短信网关、邮件服务器
权限管理	展示当前系统采购方列表和采购方状态，可对采购方进行增删改查操作
	可查看系统当前在线采购方即访问时间
日志采集	支持包括 SYSLOG、HTTP、HTTPS、SNMP、NetFlow
	支持日志源增删改功能
	双网卡多区域采集；支持列表展示日志源的详细信息，包括名称、IP、设备类型、型号、厂商名称、关联采集器、上报端口（支持特定采购方绑定特定的日志源）等信息
以上需提供所投设备的白皮书或产品文档	

## (七) 态势感知平台

### 3.7.1、态势感知一体机

功能及技术指标	参数要求
实配要求	<p>采用软硬件一体化设备，一体机数量<math>\geq 4</math>，保障系统稳定性及兼容性，内存<math>\geq 256G</math>，<math>\geq 14</math>个硬盘盘位，600G SAS 硬盘<math>\geq 2</math>，4T SATA 硬盘<math>\geq 12</math>，千兆电口<math>\geq 4</math>，10GE 光口<math>\geq 2</math>，万兆多模光模块<math>\geq 4</math>，支持额外扩展 24 个 GE 千兆电口/12 个 10GE 万兆光口，电源模块<math>\geq 2</math></p> <p><b>中心流量探针规格</b>（1 台）：采用软硬件一体化设备，保障系统稳定性及兼容性，电源<math>\geq 2</math>，特征库升级许可<math>\geq 3</math> 年，内存<math>\geq 32G</math>，<math>\geq 8</math> 个硬盘盘位，标配 1*1T SATA 硬盘，千兆电口<math>\geq 4</math>，10GE 光口<math>\geq 2</math>，万兆多模光模块<math>\geq 4</math>，吞吐量<math>\geq 10Gbps</math></p> <p><b>边界流量探针规格</b>（2 台），采用软硬件一体化设备，保障系统稳定性及兼容性，内存<math>\geq 32G</math>，<math>\geq 8</math> 个硬盘盘位，特征库升级许可<math>\geq 3</math> 年，标配 1*1T SATA 硬盘，千兆电口<math>\geq 4</math>，10GE 光口<math>\geq 2</math>，万兆多模光模块<math>\geq 4</math>，电源<math>\geq 2</math> 个，吞吐量<math>\geq 10Gbps</math></p> <p>实配 3 年软硬件原厂维保服务</p>
态势展现层	<p>根据《上海市电子政务外网建设和运行管理指南》的要求态势感知需涵盖以下内容</p> <ol style="list-style-type: none"> <li>1、感知态势：网络攻击实时态势、网络攻击历史趋势、网络安全隐患感知</li> <li>2、通报预警：多维度威胁报告、威胁事件实时分析</li> <li>3、威胁情报：IP 情报、WEB 情报、漏洞情报、文件情报</li> <li>4、漏洞扫描：系统漏洞、WEB 漏洞、数据库漏洞、配置核查</li> </ol>
数据采集层	通过部署探针、接收安全设备日志、漏洞扫描设备扫描日志等方式获取原始数据
数据存储挖掘层	建立在大数据分析系统之上，对 IP 地址库、GIS 地图库、恶意 IP、恶意文件库、资产等基础数据信息进行安全和威胁的深度挖掘
#安全信息同步	能够将安全态势指标，如资产安全状况、资产安全事件信息等实时或者定时同步至运维管理系平台，丰富网络安全运维系统的资产状态信息，对资产实现更全面的状态评估。（提供产品功能截图）
威胁攻击	统应能对网站及主机漏洞、流量异常、扫描探查、弱点攻击、僵尸网络、数据泄露、APT 攻击等各类安全攻击、威胁事件进行多视角的态势感知呈现

日志采集器	分布式日志采集器一体机：采用软硬件一体化设备，保障系统稳定性及兼容性，内存 $\geq 32G$ ，硬盘盘位 $\geq 8$ 个，标配 1*1T SATA 硬盘，GE 千兆电口 $\geq 4$ ，支持额外扩展 24 个 GE 千兆电口/12 个 10GE 万兆光口，电源 $\geq 2$ ；
日志采集器功能	支持对日志被动采集器和主动采集器进行管理，展示当前采集器列表，列表内容包括采集器名称、IP、描述、状态、租户名称、注册时间、更新时间、采集方式、统计信息等；可以按照采集器 IP、采集器状态、采集方式等条件检索查询，采集器支持编辑修改。
	为满足采购方多样日志采集方式，被动采集方式支持包括 Syslog、http、https、NetFlow、sflow、snmp 等方式，主动采集方式支持包括 FTP、JDBC\ODBC、Agent 终端采集等方式。
	为了清楚现网内日志数据采集情况，支持对所有采集数据进行趋势监控，并能显示出对应日志源的总数量和平均速率。
	支持对注册的 Agent 进行管理，支持对 Agent 进行启动、停止操作；支持以列表形式展示管理的 Agent,包括 Agent 名称、主机 IP、采集器 IP、注册时间、Agent 状态、采集状态等信息；从而实时监控 agent 状态，避免日志断收，造成采购方数据丢失。（提供产品功能截图）
	需提供 Agent 工具，包含采集 windows、linux、Solaris 版本等不同类型系统的日志信息。Agent 工具支持页面直接操作下载，无需线下操作（提供产品功能截图）
	支持通过离线导入方式导入日志，导入历时日志时，可以根据日志信息进行设备厂商、对应设备型号、文件编码、日志类型进行范式化匹配（提供产品功能截图）
其他功能	实现网站安全态势感知、内网威胁态势感知、Web 站点态势感知、脆弱性态势感知等功能。

## （八）安全管理中心

### 3.8.1、安全管理中心平台

功能及技术指标		参数要求
性能要求		事件入库性能 $\geq 15000$ 条/秒 日志源接入数量 $\geq 1024$ 个
综合	风险概览	为了方便采购方清楚全网安全状态，支持全网安全风险监控展示，包括但不限于风险资产数、风险采购方数、安全事件总数、

展示		未处理、处理中、已处理和已忽略的安全事件数，支持今日新增提示； 支持安全度打分和历史趋势查看，能够进行资产和采购方安全状态分布统计，TOP5 风险资产/风险采购方，并支持更多快速聚焦安全问题点
	风险统计	首页支持以 24 小时、7 天、30 天维度展示攻击阶段分布统计和安全事件分布统计； 展示所有资产已统计的内网开放端口和互联网开放端口分布，清楚了解现网开放端口情况；综合概览首页支持定期报表（日、周、月报）查看和下载，并可操作直接跳转到报表管理模块
	页面版块自定义	支持自定义展示图表设置，根据采购方需求选择可展示内容，包括可选资产安全信息、采购方安全信息、安全事件信息、端口分布信息和综合报告展示模块设置（提供产品功能截图）
	威胁探测	支持在首页主动威胁探测搜索框查询，可使用资产 IP/资产名称/采购方名称/情报 IP/URL/域名/MD5 进行快速风险搜索查询，帮助采购方快速查找定位所关心的风险点（提供产品功能截图）
安全事件分析	安全事件详情分析	能够展示出全部安全事件，包括通过关联分析引擎、机器学习引擎、威胁情报等不同方式产生的事件；支持展示事件首次发生时间、最近发生时间、事件名称、事件描述、事件等级、事件关注点、源 IP、目的 IP、攻击阶段、失陷状态、攻击载荷等信息
	事件检索	为了从海量事件中快速查找特定事件，支持按照源 IP、目的 IP、事件等级，关注点、事件描述、情报 IOC、失陷等级、处理状态、攻击阶段、事件名称、规则名称进行检索查询
	事件详情	支持显示安全事件的详细信息，安全事件导出到 excel 文件；为了溯源分析，支持显示单一安全事件的详细分析结果，包括显示事件基本信息，数据来源、风险危害、处置建议、威胁详情
	安全事件处置	安全事件过多时，支持对安全事件进行批量处理；对于已确认的无风险的安全事件，支持进行白名单设置，解决二次误报情况；对于需要具体人为处置的，支持对安全事件已工单的方式进行处置
	流量取证	支持对安全事件通过同品牌 IPS 设备进行网络攻击报文抓包取证，取证内容包括原始报文内容并进行展示，对于安全事件分析通报可以提供强有力的数据证据；
	终端取证	通过同品牌 EDR 进行主机终端检测结果取证，取证内容包括该事件发生的终端名称、进程名称、日志类型、日志子类型、操作类型、操作结果、日志产生时间
	风险危害与原理	支持展示对应安全事件能够导致的风险危害，能够掌握事件原理，了解危害结果；并支持对风险危害自定义内容修改，便于同样安全事件周期性处置确认（提供产品功能截图）
	风险处置建议	须提供对应安全事件的建议处置方式，提供具体排查工具，具体升级补丁，防护策略等建议内容；支持自定义处置建议编辑，后续出现同样安全事件时，可自动显示编辑后的处置建议，帮助采购方完善闭环处理；并支持修改记录留存，支持默认处置建议一键还原
	#风险采购方管理	能够展示风险采购方的失陷、高危机、低危情况以及具体信息，包括采购方名称、所属采购方组、所属区域、级别、标签等，能展示影响内网、外网（目的 IP）的采购方数量以及具体信息；能导出风险采购方 (excel)表，该功能需提供国家认可的第三方检测机构提供的有效的检测报告。

攻击溯源分析	攻击链	攻击方式越来越复杂的现状下，平台支持展示攻击阶段分布情况，支持按照扫描侦察、入侵、命令控制、横向渗透、网络黑产、数据盗取、系统破坏攻击链显示整网安全事件所处的攻击阶段
		对单个风险资产/采购方统计该资产的安全事件所处的攻击阶段；支持按天周月进行安全事件统计。
安全态势分析	智能分析	深度威胁引入监督学习、强化学习等AI人工智能算法，利用知识大脑推理检测已知及未知类型的复杂攻击，增强威胁发现能力，可以帮助管理员全面掌握规模事件的感染路径，为溯源分析取证提供帮助；
威胁处置	NAT溯源	威胁被发现后，需可以定位内网真实主机，要求平台支持 NAT 溯源功能，查找内网资产，并能够查看相对应的安全风险；在此基础上支持查找相似行为主机，提前规避再次接受到类似通报；通过设置溯源时间、NAT 转换源/目的 IP、NAT 转换源/目的端口进行自动化查询，实现溯源定位，同时关联相似行为主机。（提供产品功能截图）
	告警策略	支持新增、删除、修改事件告警策略；触发条件可以设置指定资产或区域，支持设置告警发送时间间隔；支持以邮件、短信方式进行告警；可以设置预定义告警模板与自定义告警内容，并支持告警策略查询
	告警记录	支持按照时间以列表形式展示已生成的告警结果，包括发送时间、告警策略名称、告警方式、收件人；并支持告警记录查询
异常流量分析	异常流量分析	支持展示通过网络原始流量分析异常流量事件；包含展示异常流量事件总数、异常类型分布、威胁等级分布、涉及资源分布、按照资产与采购方展示 TOP10 异常流量事件排名；支持以列表形式展示异常流量事件详情，包括 IP、高危数、中危数、低危数、异常类型、异常总数；并展示异常流量事件趋势
内网流量分析	内网流量分析总览	便于了解采购方内网应用流量使用情况，支持通过时间段、统计源、统计对象、流向条件进行访问内网流量审计；展示当前区域资产上行流量、下行流量、总流量、总流量占比；展示当前区域资产内网访问流量排名
	内网流量详细分析	支持通过不同区域展示流量审计结果，并且可以展示单个资产的流量日志详情
行为分析	采购方行为审计-活跃采购方列表	支持展示选定场景下的活跃采购方列表，包括采购方名称、采购方 IP、所属采购方组、所属区域、采购方标签；支持通过采购方名称、采购方 IP、统计周期、所属采购方组、采购方标签进行过滤查询选定场景下的活跃采购方；
		支持展示单个活跃采购方行为记录，包括采购方基础信息（采购方 IP、所属采购方、所属区域、名称、部门、职位、邮箱），采购方标签，应用访问排行，应用访问趋势，应用访问时段分布（提供产品功能截图）
场景化分析	勒索感染场景分析	通过勒索感染分析引擎做细粒度场景化分析，帮助采购方快速分析勒索感染全网态势及影响。展示被勒索病毒感染的资产数、采购方数，以及未处理资产、采购方、安全事件的统计，并可下钻查看详细列表（提供产品功能截图） 可灵活定义统计周期，根据需求选择统计当天/本周/本月的勒索感染分析结果 支持通过关系图的形式展示勒索感染主机的访问关系，便于采购方了解该勒索病毒感染范围 支持通过内网、外网的方式查询勒索感染主机的访问关系，便于

		采购方定位某一内网勒索感染主机/外网远端服务器对整体网络带来的影响
	C&C 外连场景化分析	通过 C&C 外连分析引擎做细粒度场景化分析，帮助采购方快速分析现网 C&C 外连现状。能够统计 C&C 外联安全事件发生次数趋势，展示 C&C 外连事件的风险危害与处置建议 能够统计 C&C 主机，并呈现主机 IP、所属地区、内部影响主机数等详细信息，并能通过下钻查看该主机所触发的详细安全事件信息 能够统计 C&C 发起主机（源主机），并呈现主机 IP、主机类型、C&C 主机连接次数等详细信息，并能通过下钻查看该主机所触发的详细安全事件信息
	恶意文件场景化分析	通过恶意文件分析引擎做细粒度场景化分析，帮助采购方快速分析恶意文件全网态势及影响。能够统计恶意文件数量、类型、名称、感染主机数量、发现次数等信息，并能够展示恶意文件事件的风险危害与处置建议 支持通过列表形式展示恶意文件分析详情信息，包括感染主机，感染主机类型、发现的恶意文件数、感染的内网主机数、最近检测时间，并能通过下钻查看该感染主机所触发的详细安全事件信息
	热点事件分析	支持对时下关系的热点事件进行分析； 支持新增热点事件，包括创建热点事件名称、热点事件的描述、热点事件关键字（可增加多个）；事件匹配后展示热点事件名称，该热点事件关注采购方数；根据天、周、月统计并展示关注该热点事件的采购方列表与对应采购方的关注次数；
脆弱性分析	脆弱性分析	支持查看整网脆弱性分析，包含整网漏洞类型分布、脆弱性资产，并能够以资产为维度查看资产漏洞风险、配置风险、弱口令等相关数据。
	脆弱性验证	支持对漏洞风险、配置风险、弱口令等处置结果进行脆弱性风险验证，验证方式包含联动漏洞扫描自动化验证，也支持人工核验方式。支持呈现安全事件的验证状态，包含待验证、已修复、未修复。
报表管理	报表管理	支持报表任务的新增/删除/修改/启用/停用等管理，可以按照任务类型/任务状态/任务名称进行报表查询，基于区域、资源资产、资源事件类型、等级，自定义报告输出，并支持通过邮件形式，按照天周月自动发送报表
威胁情报	威胁情报管理	支持 IP/域名/MD5 威胁情报的在线升级、离线升级（导入情报）操作；支持列表展示 MD5 情报信息，包括 MD5 值、病毒家族、危害等级等信息；IP/域名的情报查询，支持列表展示 IP/域名情报的详细信息
数据总线功能		内部数据交换接口： 是安全监测平台为平台内部数据格式不同的设备或模块之间数据的规范化交换而提供的标准接口
		数据采集接口： 是安全监测平台从各种监测对象中采集网络流量、日志、资产信息、威胁情报、漏洞以及上下级平台交互数据等数据的接口
		系统级联接口： 应支持有上下级关系的系统之间进行总体态势、统计类数据、报表、告警日志、威胁情报等数据的交互
		外部接口：安全监测平台通过各种外部接口与其他应用系统之间实现集成和数据交互

服务要求	根据市大数据中心要求和采购方实际业务情况，供应商在3年内需无偿提供运行管理中心平台的定制化开发服务。（供应商需提供相应的服务承诺书）
	提供威胁情报升级服务≥3年；提供原厂安全软件技术支持和维保服务≥3年；提供原厂安装部署实施服务
其他要求	1、所有与安管平台相关的二次开发成果版权均归甲方所有。 2、具体参数详情及要求参考《上海市电子政务外网安全监测平台技术规范(试行)》中的相关内容。

### （九）运行管理中心

#### 3.9.1、运行管理中心平台

功能及技术指标	参数要求
基本能力	实现对核心路由器、汇聚路由器、接入交换机的统一监控管理、统一告警管理、统一报表管理；
	为保障架构稳定型与数据互通性，软件产品及组件为自主研发统一产品，不得采用 OEM 第三方产品或组件；
	系统支持部署到 windows、linux 平台，支持使用 MySQL、Oracle 数据库，采用 B/S 架构。必须支持系统安装，卸载，数据同步备份、数据恢复的可视化界面。
	支持代理和免代理两种模式，可根据不同的场景选择不同的监控模式，必须支持两种模式同时使用。
	支持 agent 程序远程推送安装升级、安装环境自检等。
	开放接口：提供丰富 REST API 的接口，官网网站可查（提供官网链接），可供第三方系统调用。
配置要求	提供完成松江区电子政务外网运行管理中心平台软件定制化二次开发服务 至少 400 节点网络设备管理 license 至少 400 节点智能巡检 license 至少 400 节点 IP 地址管理 license 具备流程管理平台，支持事件管理，问题管理，服务请求功能 含运管一体机≥3 台 硬件与软件一体化部署
网络管理	支持多厂商设备管理，包含了设备的基本信息、接口信息、性能数据、面板信息、存储空间，离线自动删除和告警信息等。
	可接收分析各类 SNMP trap 告警，完成基本格式的解析，并入库，系统预定义解析各类 trap 类型不小于 8000 条。
拓扑管理	支持对网络设备指标支持最小 5 秒采集周期的实时性能监控
	自动发现拓扑：自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等。 支持 IP 拓扑、自定义拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、全景拓扑等/多种拓扑类型；拓扑支持多协议，包括 Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING 等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息。
	支持批量的设备运行状态检查。支持以任务方式（周期性任务、

智能巡检	一次性任务或立即任务)批量的检查设备运行状态。支持一键式实时输出巡检报告功能,支持 Word、PDF、HTML 多种报告格式,对于检查结果,给出详实准确的问题改进建议。
	支持网络设备虚拟化状态信息收集,包括虚拟化设备状态信息、端口绑定信息、拓扑信息、链路状态信息等。
	支持设备硬件状态信息收集,包括内存和 CPU 信息、同步状态信息、单板运行状态、电源运行状态、电源在位状态、风扇状态、设备温度状态、设备电子标签、设备 CF 卡存储介质信息、设备 Flash 卡存储介质信息、可插拔模块信息等。必须提供截图。
	支持设备运行状态信息收集,包括设备运行时间、系统时钟、LogBuffer 信息、MAC 地址表项信息、ARP 协议信息、路由表汇总信息、NAT 表项汇总信息、ACL 资源信息等。必须提供截图。
IP 地址	支持 IP 地址规划,可以自定义分区域分组进行 IP 地址规划。
	通过网络设备信息可自动分析出全网的 IP 地址情况,自动生成子网结构,IP 使用情况,IP 与交换机端口及虚接口对应关系。
	支持任意子网划分,在地址分配时判断子网网段的可用性,如创建的子网下有在用的 IP,会有提示信息。
	提供 IP 地址导入服务,将客户现有 Excel 表格记录的 IP 地址导入系统,帮助客户建立 IP 地址基线,并形成基线对比,达到可使用状态。
资源管理	配置项信息支持手动修改、与变更流程协同自动修改,与监控系统集成通过同步的方式经人工确认后自动修改 3 种修改方式,无论通过何种方式修改,配置项任意属性信息的修改时间、修改前的信息和修改后的信息都会被记录在变更日志中。
	支持通过定义配置项类型与配置项类型字段匹配的方式,建立配置项类型间的关联关系,具体配置项之间的关系可批量建立。
	支持配置项信息修改的日志记录,记录每个配置项任意属性信息的变化情况,并可对日志记录进行查询和导出,实现配置项信息变化的溯源。
	支持按配置项分类设置配置项的维保到期提醒阈值,按照提前提醒配置项维保即将到期。
运维流程	支持提供运维服务管理,包括事件管理、问题管理、服务请求等。
	支持流程自定义,可采用图像化形式定制管理流程,可供采购方在无需代码或脚本编程的情况下,实现表单内容和流程的客户化设计,以便于在系统投产后能够根据管理要求灵活调整相关流程与工单内容。
	支持按照运维管理的相关规定,规划和建立相应的事件处理工作流程,提供方便易用的采购方工作界面。
	支持事件的手动分派,并提供 API 接口实现第三方集成方式录入事件工单,支持监控告警自动生成事件工单。
	支持事件的手动分派或自动分派,支持分派工单到支持组或支持人。
#智能运维	支持设备软件状态信息收集,包括设备补丁信息、系统启动文件信息、启动配置文件信息、Debug 开关状态、信息中心、以太网接口状态、三层接口状态、端口错包信息统计、链路带宽利用率、Loopback 接口地址检查,并提供截图。
报表管理	支持多种图表展示,提供周期性报表机制,提供报表设计工具,可通过报表定制工具创建、修改、发布报表。提供不少于 5 套的定制报表开发服务。
智能运维分析	智能运维分析,构建政务网络统一运维,政务外网资源管理,运维服务体系管理 3 套专题运维建设。

数据接口类型	<p>至少要求支持并满足以下 7 项数据大类：</p> <p>接入节点信息：接入节点数据</p> <p>资源类：资源配置数据、子资源数据</p> <p>拓扑数据：拓扑关系数据</p> <p>性能类：资源性能数据、端口性能数据</p> <p>告警类：资源告警事件、端口告警事件</p> <p>常规数据类：光缆皮长、网络承载能力、工单建设、网络故障、终端数量</p> <p>机房数据类：UPS 的电压、电流、输出功率、UPS 电量-剩余时间、机房温度、湿度监测、机房视频监控视频流调用</p>
服务要求	根据市大数据中心要求和采购方实际业务情况，供应商在 3 年内需无偿提供运行管理中心平台的定制化开发服务。（供应商需提供相应的服务承诺书）
其他要求	<p>1、所有与运管平台相关的二次开发成果版权均归甲方所有。</p> <p>2、具体参数详情及要求参考《上海市电子政务外网运行管理系统对接规范（征求意见稿）》中的相关内容。</p>

#### （十）OTN

##### 3.10.1、OTN

功能及技术指标	参数要求
单波速率	OTN 的单波速率需达到 100G 及以上
扩容	支持带宽平滑扩容，网络具备向 200G 及以上带宽平滑扩容的能力
架构	需采用高可用的组网架构，具备网络自愈能力，能为各类政务应用提供安全可靠的传输网络支撑
可靠性	采用保护路径和工作路径物理光纤分离的保护策略，端到端保护倒换时间小于 50ms
排障	支持光纤线路诊断功能，能快速定位光纤线路故障
光衰	应使用 G.652 或 G.655 规格的光缆，光缆的每公里线路损耗在 0.3db 以下
其他能力	具有 SDH、分组、OTN 等多种业务统一承载的能力，能提供多种业务类型接口的接入能力，具备与已建网络互联互通的能力
	宜采用结合 SDN 技术，实现对业务和链路的快速下发和调整
节点数量	OTN 节点在本区（松江区）内须满足 4 个及以上节点的数量，要求提供节点的证明材料，并提供 OTN 所属运营商的授权并加盖公章
模块要求	需提供 OTN 设备采购方侧的光模块

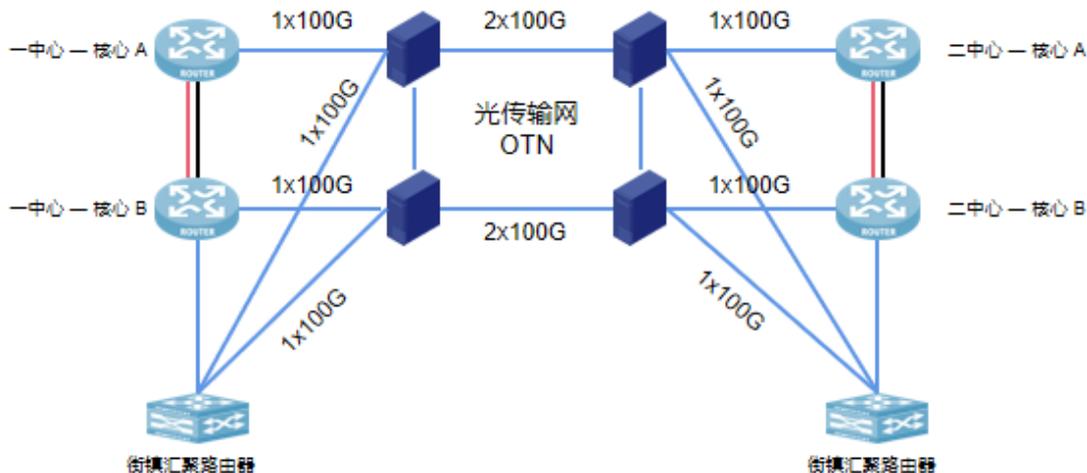
#### 四、实施要求

##### 4.1、光传输网（OTN）要求

供应商提供的方案必须体现出合理性、可行性与冗余性。

同时，供应商应在基于光传输网 OTN 拓扑的基础上，结合采购方的实际情况，并根据市大数

据中心的要求及对《上海市电子政务外网建设和运行管理指南（试行）》充分的理解，对下图光传输网 OTN 拓扑自行进行架构的优化，以期达到更合理、更安全、更可靠的目的。



#### 4.2、网络集成要求

提供针对性的详细拓扑结构，主要体现以下几方面：

- 1) 出口设计(出口冗余设计、兼容性设计、安全性设计)
- 2) 核心节点设计（可靠性设计、路由策略设计）
- 3) 汇聚节点设计（可靠性设计、网关设计、安全性设计）
- 4) 接入节点设计（可靠性设计、兼容性设计、安全性设计）
- 5) 安全环境设计（可靠性设计、兼容性设计、边界明确性、贴合等保 2.0 三级等保要求）

#### 4.3、平台设计总要求

- 1) 安管平台设计（可靠性设计、兼容性设计、突出贴合对接规范的可用性设计）
- 2) 运管平台设计（SDN 架构设计、可靠性设计、兼容性设计、突出贴合技术规范的可用性设计）

##### 4.3.1、安全管理平台设计要求

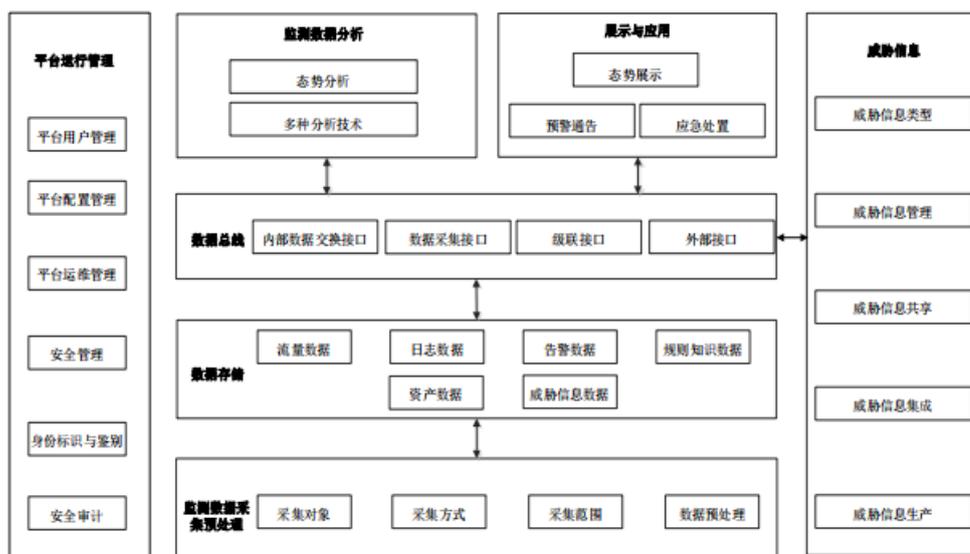
对不同的网络区域，安管平台监测的内容侧重有所不同，宜包括但不限于以下内容：

- a) 互联网出口：网络攻击、异常流量、互联网行为、资产威胁、资产脆弱性、重要系统和业务运行状态；
- b) 上级政务外网接入：跨部门/跨区域攻击、异常流量、资产威胁、资产脆弱性；
- c) 政务云接入：网络攻击、异常流量、互联网行为、资产威胁、资产脆弱性、重要系统和业务运行状态；
- d) 无线/卫星接入：网络攻击、异常流量、资产威胁、资产脆弱性、重要系统和业务运行状态；

e) 下级政务外网接入：跨部门/跨区域攻击、异常流量、资产威胁、资产脆弱性。

f) 委办局接入：跨部门横向攻击、异常流量、资产威胁、资产脆弱性。

政务外网安全监测平台是对网络安全的态势进行监测分析的安全产品，通过监视网络内的数据报文、日志、情报等数据，实时获取数据进行深度解析，监测网络中的入侵行为和异常行为，并及时告警展示的设备。该设备产品可以硬件或者软件形式实现，提供监测数据采集预处理、监测数据分析、展示与应用、数据总线、威胁情报、系统运行管理等功能，政务网络安全监测平台的技术框架如下图所示：



政

务网络安全监测平台技术框架分为总体功能和系统运行管理两部分，由六大模块组成，包括：

a) 监测数据采集预处理：依照确定的政务网络安全监测平台的采集区域、采集方式、采集的数据内容以及预处理方式进行数据采集和预处理，数据经过采集预处理后进一步进行数据分析；

b) 监测数据分析：通过机器学习、数据挖掘、关联分析等数据分析技术对网络的综合态势、攻击态势、威胁态势、资产态势、违规行为态势等进行分析，分析数据通过数据总线汇总至展示与应用模块；

c) 数据总线：实现政务网络安全监测平台中数据采集、存储、分析、展示与应用等各模块之间，以及与外部系统之间规范化数据共享和交换；

d) 展示与应用：根据决策者、管理人员和运维人员不同的需求和关注重点，进行多种态势的多维度展示，并且支持预警通告和应急处置；

e) 威胁情报：有效提升监测平台的能力，其主要能力包括：及时发现关键威胁、为事件响应提供决策需要的上下文、了解攻击者的攻击背景情报信息、提供情报运营能力以及威胁情报数据共享交换等；

f) 系统运行管理：包括系统的管理、数据存储以及自身安全防护，为系统的总体功能实现提供支撑。

### 4.3.2、运行管理平台设计要求

平台通过对政务外网网络拓扑、设备运行状态等信息的实时共享，实现政务外网服务质量监控、故障处理、业务开通等网络运行管理功能，并基于其可视化的业务呈现能力，帮助政务外网主管单位随时了解网络运行状况，以辅助做出网络调整、优化等决策。



根据《上海市电子政务外网运行管理系统对接规范（征求意见稿）》中的要求，运行管理平台总体架构至少应分为资源层、采集层、核心功能层和服务与展示层，其中：

资源层是整个网络平台需要管理的对象，包括网络设备、安全设备、机房环境等；

采集层重点采集告警数据、配置数据、性能数据等，供上层调用，以及平台对外的数据接口；

核心功能层提供统一监控、统一资源管理、集中工单管理、统一安全管理和系统内部的分级协同等模块。核心功能层向上针对展示层提供数据接口，向下整合关系/非关系型数据库提供对象关系映射服务；

服务与展示层提供系统的统一入口，并提供综合展示界面。

### 4.4、网络割接要求

供应商需要对松江区一中心和二中心的核心交换机、汇聚交换机、接入交换机及院外委办局的接入交换机等网络设备进行升级替换，并需要根据市大数据中心的需求配合采购方进行与市政务外网的对接。考虑到松江区政务外网整体业务的重要性，供应商必须提供整个网络割接的详细步骤、回退方案、并得到采购方批准后才能进行实施，且实施方案需要具体到设备配置脚本（**要求体现并结合现网配置，并非标准配置手册**）。

### 4.5、兼容性要求

为了最大限度保护采购方的现有投资、降低实施风险、加快实施效率，供应商必须提供与现有网络系统的兼容性方案及响应设备之间的兼容性方案（兼容性方案包括但不限于所投的广域网 SDN

控制器与现园区网 SDN 控制器的兼容性、所投路由器和交换机于现园区网 SDN 控制器的兼容性等内容)。兼容性方案要求设计科学合理、响应设备之间的兼容性强、响应设备与现网设备之间的兼容性强,整体兼容性程度满足采购方要求。(供应商需提供兼容性承诺函并加盖公章)

#### 4.6、实施团队要求

本次项目包含的内容极多,整个项目的交付需要团队提供项目开发、产品实施、系统迁移、运维保障等各种职责和角色的技术人员。为保障整个项目的交付和运维的顺利,需要整个团队的人员配置都具备较高的技术能力、经验和资质要求。详细的要求如下:

- (1) 供应商应成立专门的项目组织团队,明确项目团队中各成员的职责分工。
- (2) 因项目进度要求,团队成员应不少于 15 人,包含项目经理、高级技术工程师及相关工程实施人员(上述人员须提供磋商前近半年内连续三个月的社保缴费证明材料)。
- (3) 团队主要成员应具备相关的实施经验,供应商需出具相关项目组成员的工作履历。

#### 4.7 实施方案需求

为保障松江区电子政务外网顺利实施,实施方案要求切实可行、条理清晰,且实施方案必须从人员、业务、时间、突发情况等多个方面来考量,具体要求如下:

- 1) 明确各实施人员之间的分工界限和职责。
- 2) 需明确各模块之间割接时候的关联关系,合理安排各模块之间的割接顺序。
- 3) 需提供详细的割接后的拓扑及割接步骤概述。
- 4) 需提供详细的紧急预案,以防遇到紧急情况或其他不可抗力的因素导致割接无法继续进行,需要回退的情况。

#### 4.8、实施进度要求

序号	工作内容	时间计划要求
1	制定实施及割接方案	签订合同后5个日历日
2	设备到货	签订合同后15个日历日
3	完成松江政务网整网割接,并进入试运行(设备安装调试及网络试运行)	签订合同后30个日历日
4	项目初步验收	签订合同后40个日历日
5	整体系统试运行	完成初步验收后30个日历日
6	项目最终验收	试运行完成后30个日历日

7	转入运维期	提供3年驻场人员
---	-------	----------

## 五、售后服务

### 5.1、备件库

供应商设有所投硬件设备及相关配件（电源引擎、光模块等）的备件库，可向客户提供及时周到的快速备件更换服务，当设备出现影响业务的紧急故障时，应客户要求立即派遣工程技术人员用最快捷的交通工具前往现场，进行备件的现场更换与安装。

具体备件要求：

服务级别	RMA*受理及批复时间	发货/到货时间
7×24×4 小时到达	24 小时受理 30 分钟内批复	RMA 批复后 1 小时内安排备件发货，4 小时内到达

供应商为客户每季度提供一次对设备及网络进行全面检查的巡检服务，帮客户获得设备运行的第一手资料，最大可能地发现存在的隐患，并有针对性地提出预警及解决建议，使客户能够提早预防，最大限度降低运营风险，巡检可包括的内容如下（详细巡检计划及范围由服务经理与客户提前协商制定）：

编号	巡检内容		
1	硬件运行状态检查项目		
	单板状态检查	电源模块状态检查	风扇状态检查
	整机指示灯状态检查	机框防尘网检查	机房温度、湿度检查
	设备地线检查		
2	软件运行情况检查项目		
	设备运行情况检查	网络报文分析	设备对接运行状况检查
	路由运行情况检查		
3	网络整体运行情况调查		
	网络运行问题调查	网络变更情况调查	网络历史故障调查
<i>以上巡检内容根据设备具体情况会有所不同</i>			

### 5.2、供应商应急响应团队

- (1) 明确专职应急响应联系人、技术负责人；
- (2) 针对常见故障制定应急预案；
- (3) 每半年回顾、修订应急预案；
- (4) 设立 24 小时故障响应电话；
- (5) 故障发生时，如采购方要求，技术人员应在 2 小时内到达采购方现场；
- (6) 技术人员应持续处理故障，直至故障解决；
- (7) 供应商应建立无推诿机制，牵头处理所有故障；

- (8) 供应商应制定故障抢修流程并严格执行；
- (9) 供应商应建立故障等级标准以及故障升级机制；
- (10) 供应商应建立应急故障沟通机制，定期和甲方沟通应急故障抢修中的各类问题并不断提升应急抢修水平；

### 5.3、驻场服务要求

供应商应提供 3 年 5\*8 工程师（3 人）驻场服务，其中原厂（设备供应厂商）驻场工程师至少 1 人，且其中至少有 1 人必须具备相关的技术认证资质或证书，原厂（设备供应厂商）工程师需提供原厂工作证明。

### 5.4、培训要求

供应商应根据本项目的特点制定培训方案并提供培训，使采购方相关人员在培训后能够独立使用系统，而不必依赖供应商现场指导。培训课程需要重点涵盖政务网平台使用和管理培训，供应商负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表。

(1) 供应商须提供所需的培训设施和课程，以确保甲方人员能对供应商所提供的系统、设备和装置的设计、日常的运作、故障和例行维护、事故的处理和解决方面等有全面性的认识 and 了解。

(2) 培训应于指挥中心现场进行。供应商须预先编制 1 套详尽的培训计划，列出每项课程的大纲、培训导师资料及培训所需时间，提交甲方审核。

(3) 供应商须委派施工项目经理进行每项培训工作，培训需以普通话作讲授。所有导师的资历须先提交甲方作审核认可。

(4) 供应商应向受训学员提供并解释有关设计资料、文件、图纸等，以便使学员对整套系统的各个方面都能熟练掌握。

(5) 供应商经得甲方同意可以利用已安装、测试和交工试运转的装置和设备对甲方人员进行培训。供应商应提供足够的材料、设备、样本、模型、设备内部透视资料的复印本、幻灯、影片以及其它种种需要的培训教材文件，以便培训工作的进行。培训课程完成后，有关装备和教材将为甲方所有，以便日后甲方自行对其它员工进行辅助性培训之用。所有教材文件须以中文说明。

(6) 上述培训所需的费用应包括在供应商的响应报价内。

### 5.5、其他售后服务要求

(1) 为能通过监视网络内的数据、报文、日志、情报等数据，从而实时获取数据进行深度解析，监测网络中的入侵行为和异常行为，并及时通知告警信息。需根据市大数据中心的要求，**无偿**提供安全管理中心平台 3 年内所需的定制开发服务，并提供供应商的服务承诺书。

(2) 为政务外网信息管理提供统一鉴权的服务窗口，提供业务从申请、开通、运行、到后期服务

支持的全周期管理，掌握全网各类节点接入政务外网的实时情况，实现网络覆盖情况的在线化和采购方连通情况的实时化。需根据市大数据中心的要求，**无偿**提供运行管理中心平台 3 年内所需的定制开发服务，并提供供应商的服务承诺书。

## 六、针对本项目需承诺的内容

序号	承诺内容
1	承诺此次项目中所投的广域网 SDN 控制器应与现政务外网的园区网 SDN 控制器 API 接口协议具备一致性，实现广域网 SDN 与现政务外网的园区网 SDN 支持统一界面、统一门户、统一入口，统一业务编排，实现采购方多场景业务的联动。
2	承诺此次项目中所投的院外委办局网络接入交换机支持被现政务外网的园区网 SDN 控制器纳管，且能实现设备自动上线。
3	根据市大数据中心的要求，供应商承诺在 3 年内无偿提供采购人所需的安全管理中心及运行管理中心的定制化开发服务。
4	承诺当开启 IPS 入侵防御、AV 防病毒功能时，市政务外网防火墙、安全接入区防火墙的应用层吞吐性能 $\geq 7G$ 时，防火墙 CPU 占有率不得高于 50%
5	承诺当开启 IPS 入侵防御、AV 防病毒功能时，边界防火墙的应用层吞吐性能 $\geq 9G$ 时，防火墙 CPU 占有率不得高于 50%
6	供应商承诺至少购买一名所投核心网络设备的原厂技术人员进行 3 年售后驻场服务。

为确保此次采购的软硬件设备及相关服务能符合本项目建设的最终要求，供应商应针对以上承诺内容作出相应的承诺；并对违背上述承诺内容，存在偏离、弄虚作假、欺骗采购人等情况发生时，供应商将采取的自罚措施，应包括采取自罚资金（按标的总金额的百分比）及其他自罚措施，以保障采购人的相关权益。承诺及自罚措施格式自拟，须清楚标明供应商主体名称、单位地址及联系方式并加盖供应商公章。

## 七、验收要求

- 1、建设内容完成后，供应商应对相关建设内容进行完善的系统测试，并通知采购方进入系统试运行期。系统试运行为期一个月，与此同时供应商提供试运行期系统测试文档和项目验收相关文档，并且对采购方相关人员提供完善的培训。
- 2、供应商提供全套完善的项目验收资料文档，包括配置文档、使用说明书给采购方，并向采购方书面提出申请项目验收，采购方在审查验收资料无误后同意召开项目验收会。
- 3、由采购方指定时间地点并邀请相关专家参加项目验收会，就项目建设内容依据验收资料文档等进行项目验收，并出具专家验收意见书作为项目验收的结论性文件。
- 4、项目进入运营维护期，供应商持续提供磋商文件要求的针对软硬件设备的售后服务及设备保修服务。
- 5、项目终验必需具备等保测评中心出具的等保测评通过证明及网络性能测试报告。
- 6、项目初验报告内容包括但不限于：采购方对割接后的网络试运行使用报告、割接的施工实施方案、网络性能测试报告
- 7、项目终验报告内容包括但不限于：采购方对整体系统的试运行使用报告、三级等保测评通过的

证明

本项目建设内容验收标准采用政府信息化项目标准验收流程，验收内容请见下表：

序号	验收内容	描述
1	监理报告	监理方需对网络割接，设备上架等环节进行把关，并出具监理意见报告
2	采购方报告	提供采购方对整个系统的使用意见
3	建设方案	包括设计方案、施工方案、变更内容、清单、合同、磋商文件、响应文件等
4	验收报告（初验）	项目初验报告
5	验收报告（终验）	项目终验报告

## 八、其他要求

### 违约条款说明

注:以下违约条款内容需在供应商成交后合同内清晰约定，供应商需在响应文件中承诺同意以下违约条款内容。

序号	条款内容	违约措施
1	根据磋商文件项目实施进度要求，若成交供应商未按合同约定如期完成设备到货、系统集成、项目验收等内容，采购方有权采取罚款等处罚措施并向相关管理部门通报违约情况。	关键时间节点延迟1天，扣除总金额千分之一作为违约惩罚
2	所供软/硬件设备实际参数低于响应的软/硬件设备参数	采购方有权取消供应商成交资格并解除合同
3	响应文件中所提供的保证书、承诺函、授权书、公章、证书等为假冒或虚假证明的	采购方有权取消供应商成交资格并解除合同
4	未能根据合同提供采购方要求的3年原厂驻场服务人员(5*8)，或者提供虚假证明的	采购方有权取消供应商成交资格并解除合同

## 九、“★”、“#”项汇总表

### 9.1、★项汇总表

序号	项目分类	设备类型	磋商文件要求的需要实质性应答的条款	证明材料要求	是否满足	具体证明材料在响应文件中的位置	备注
1	★项	核心路由器	要求支持 SRv6 功能，实现 L2VPN, L3VPN 的业务的流量调度；要求支持 SRv6 TI-LFA，实现网络快速倒换	提供国家认可的第三方检测机构提供的有效的检测报告。			

9.2、#项汇总表

序号	项目分类	设备类型	功能项	指标要求	证明材料要求	是否满足	具体证明材料在响应文件中的位置	备注
1	#项	核心路由器	板卡	为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，母卡和子卡均支持热插拔	需提供产品图片证明			
2	#项	汇聚路由器	板卡	为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，母卡和子卡均支持热插拔	需提供产品图片证明			
3	#项	出口路由器	板卡	为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，母卡和子卡均支持热插拔	需提供产品图片证明			
4	#项	SDN	路径自动调整方式	支持链路质量（时延、抖动、丢包）不满足、链路带宽超一级或二级阈值、设备故障、链路故障等方式即时触发链路自动调优。	提供国家认可的第三方检测机构提供的有效的检测报告			
5	#项	边界防火墙	虚拟化特性	所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。	提供国家认可的第三方检测机构提供的有效的检测报告。			
6	#项	互联网防火墙	产品要求	具备中国网络安全审查技术与认证中心颁发的EAL4增强级认证证书及信息产业信息安全测评中心出具的防火墙EAL4+级型式试验报告。	提供相关证明材料			
7	#项	上网行为管理	产品要求	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复印件。	提供相关证明材料			

8	#项	态式感知	安全信息同步	能够将安全态势指标，如资产安全状况、资产安全事件信息等实时或者定时同步至运维管理系平台，丰富网络安全运维系统的资产状态信息，对资产实现更全面的状态评估。	提供产品的功能截图			
9	#项	安全管理中心平台	风险采购方管理	能够展示风险采购方的失陷、高危机、低危情况以及具体信息，包括采购方名称、所属采购方组、所属区域、级别、标签等，能展示影响内网、外网（目的IP）的采购方数量以及具体信息；能导出风险采购方 (excel)表。	提供产品的功能截图			
10	#项	运行管理中心平台	智能运维	支持设备软件状态信息收集，包括设备补丁信息、系统启动文件信息、启动配置文件信息、Debug开关状态、信息中心、以太网接口状态、三层接口状态、端口错包信息统计、链路带宽利用率、Loopback接口地址检查。	提供产品的功能供截图			

注：

- 磋商文件中凡标有“★”的条款均系实质性要求条款。供应商必须根据上述汇总表如实应答，并提供充分证明材料，否则视为无效响应。
- 磋商文件中凡标有“#”的条款均系核心技术指标，需根据上述汇总表如实响应并提供证明材料，否则在评标中将扣除相应分数。

十、附件 1：上海市电子政务外网建设和运行管理指南（试行）

十一、附件 2：上海市电子政务外网运维管理系统对接规范(试行)

十二、附件 3：上海市电子政务外网安全监测平台技术规范(试行)

上述附件以电子光盘形式发放，请供应商在指定日期前往领取，过时不候。

领取时间：2021 年 7 月 1 日上午 9：00-11：00，下午 13：00-16：00。

领取地点：上海市松江区乐都西路 867 号 2 号楼 5 楼 2508 室。