上海杨浦

招标文件

项目名称：上海市杨浦区大数据中心杨浦区电子政务外网基础设施租赁及安全、运维服务采购

项目编号：SHXM-10-20240110-1072

采购人：上海市杨浦区大数据中心（上海市杨浦区行政服务事务中心）

集中采购机构：上海市杨浦区政府采购中心

目　　录

第一章　　投标邀请

项目概况

上海市杨浦区大数据中心杨浦区电子政务外网基础设施租赁及安全、运维服务采购招标项目的潜在投标人应在上海市政府采购网（www.zfcg.sh.gov.cn）获取招标文件，并于2024-02-02 09:30:00（北京时间）前递交投标文件。

一、项目基本情况

项目编号：SHXM-10-20240110-1072

项目名称：**上海市杨浦区大数据中心杨浦区电子政务外网基础设施租赁及安全、运维服务采购**

采购方式：公开招标

预算金额：18878600.00 元

最高限价：包 1-18878600.00 元

采购需求：**本次项目采用设备租赁+服务采购的模式进行，即，所有政务外网网络升级改造的设备、链路资源、机房资源、计算资源等，均采用租赁的方式进行，并向中标人采购配套的安全、运维技术服务。**

设备租赁应包含所有升级改造设备的供货、安装、调试等，及项目范围内变更的配置服务等，以确保用户向中标人所租赁的内容是满足招标文件技术要求，并可直接使用的设备、机房、链路等。

安全、运维技术服务包含：通过建立专业高效的安全和运维服务体系，对升级后的杨浦区电子政务外网进行整体系统维护，保障网络系统的正常运行。

合同履行期限：　2024 年 4 月 1 日——2025 年 3 月 31 日

本项目（**不允许**）接受联合体投标。

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：**本采购项目执行政府采购有关鼓励支持节能产品、环境认证产品、支持中小企业、残疾人福利性单位、监狱企业等的政策规定。**

3.本项目的特定资格要求：

1、符合《中华人民共和国政府采购法》第二十二条的规定。

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

3、在中华人民共和国境内注册并取得营业执照的合格供应商，提供营业执照副本、税

务登记证、组织结构代码证（或三证或五证合一）；

4、本项目不接受联合体投标；

5、本项目面向大、中、小、微型企业采购；

6、本项目合同不得转让、不得分包。

三、获取招标文件

时间：2024-01-12 至 2024-01-21 （提供期限自本公告发布之日起不得少于 5 个工作日），每天上午 00:00:00~12:00:00，下午 12:00:00~23:59:59（北京时间，法定节假日除外）

地点：上海政府采购网（www.zfcg.sh.gov.cn）

方式：网上获取

售价（元）：0

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2024-02-02 09:30:00（北京时间）

投标地点：上海政府采购网（www.zfcg.sh.gov.cn）

开标时间：2024-02-02 09:30:00

开标地点：上海政府采购网（www.zfcg.sh.gov.cn）

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，本项目采购相关活动在由市财政局建设和维护的上海市政府采购云平台（简称：采购云平台，门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）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。供应商在采购云平台的有关操作方法可以参照采购云平台中的“操作须知”专栏的有关内容和操作要求办理。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在采购云平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

七、对本次招标提出询问，请按以下方式联系。

1.采购人信息

名 称：**上海市杨浦区大数据中心(上海市杨浦区行政服务事务中心)**

地址： **怀德路 600 号**

2.采购代理机构信息

名 称：上海市杨浦区政府采购中心

地 址：宁国路 129 号 16 楼

联系方式：65550185

3.项目联系方式

项目联系人：章笑吟

电 话：65550185

第二章　　投标人须知

前附（置）表

一、项目情况

项目名称:**上海市杨浦区大数据中心杨浦区电子政务外网基础设施租赁及安全、运维服务采购**

项目编号:**SHXM-10-20240110-1072**

项目地址：招标人指定地点。

服务期限：2024 年 4 月 1 日——2025 年 3 月 31 日

采购标的对应的中小企业划分标准所属行业：软件和信息技术服务业

二、招标人

采购人

名称：上海市杨浦区大数据中心(上海市杨浦区行政服务事务中心)

地址：惠民路 800 号 3 号楼 3 层

邮编：200082

联系人：孔锐锋

电话：25031082、18964505975

传真：25032474

集中采购机构

名称：上海市杨浦区政府采购中心

地址：宁国路 129 号 16 楼

联系人：章笑吟

电话：65550185

传真：65636267

三、合格供应商条件

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求:本采购项目执行政府采购有关鼓励支持节能产品、环境认证产品、支持中小企业、残疾人福利性单位、监狱企业等的政策规定。

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》第二十二条规定条件，未被列入“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和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商；

2)　在中华人民共和国境内注册并取得营业执照的合格供应商，提供营业执照副本、税务登

记证、组织结构代码证（或三证或五证合一）；

3） 本项目不接受联合体投标；

4） 本项目面向大、中小微型企业采购；

5） 本项目合同不得转让、不得分包。

四、招标有关事项

招标答疑时间：对招标文件有疑问，投标方应于 2024 年 1 月 22 日上午 10:00 时前以书面形式（加盖公章）传真至上海市杨浦区政府采购中心（同时发送邮箱：43871757@qq.com）。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

踏勘现场：不安排。

投标有效期：90 天

投标保证金：不收取

投标截止时间：详见投标邀请（招标公告）或延期公告（如果有的话）

递交响应文件方式和网址：

响应文件提交方式：由投标人在上海市政府采购云平台（门户网站：上海政府采购网）提交。

响应文件提交网址：http://www.zfcg.sh.gov.cn

开标时间和开标地点网址：

开标时间：同投标截止时间

开标地点网址：上海市政府采购云平台（门户网站：上海政府采购网，网址：http://www.zfcg.sh.gov.cn）

评标委员会的组建：详见第五章

评标方法：详见第五章

中标人推荐办法：详见第五章

中小企业政策：详见第三章

五、其它事项

付款方法：按季度分 4 次支付，每次绩效考核后支付 25%项目款。

履约保证金：无

六、说明

根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，

本项目采购相关活动在由市财政局建设和维护的上海市政府采购云平台（简称：采购云平台，门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）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。供应商在采购云平台的有关操作方法可以参照采购云平台中的“操作须知”专栏的有关内容和操作要求办理。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在采购云平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

投标人须知

一、总则

1．概述

1．1 根据《中华人民共和国政府采购法》、《中华人民共和国招标投标法》等有关法律、法规和规章的规定，本采购项目已具备招标条件。

1．2 本招标文件仅适用于《投标邀请》和《投标人须知》前附表中所述采购项目的招标采购。

1．3 招标文件的解释权属于《投标邀请》和《投标人须知》前附表中所述的采购人。

1．4 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其它依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

1.5 根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，本项目招投标相关活动在上海市政府采购云平台（门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。

2. 定义

2．1 “采购项目”系指《投标人须知》前附表中所述的采购项目。

2．2 “服务”系指招标文件规定的投标人为完成采购项目所需承担的全部义务。

2．3 “招标人”系指《投标人须知》前附表中所述的组织本次招标的采购人。

2．4 “集中采购机构”系指上海市杨浦区政府采购中心。

2．5 “招标咨询服务机构”系指为采购人提供本项目专业招标咨询的服务单位。

2．6 “投标人”系指从招标人处按规定获取招标文件，并按照招标文件向招标人提交投标文件的供应商。

2．7 “中标人”系指中标的投标人。

2．8“买方”系指采购人。

2．9“卖方”系指中标并向采购人提供服务的投标人。

2．10 招标文件中凡标有“★”的条款均系实质性要求条款。

2.11 “采购云平台”系指上海市政府采购云平台，门户网站为上海政府采购网（www.zfcg.sh.gov.cn），是由市财政局建设和维护。

3. 合格的投标人

3.1 符合《投标邀请》和《投标人须知》前附表中规定的合格投标人所必须具备的资格条件和特定条件。

3.2 《投标邀请》和《投标人须知》前附表规定接受联合体投标的，除应符合本章第3.1项要求外，还应遵守以下规定：

（1）联合体各方应按招标文件提供的格式签订联合体协议书，明确联合体各方权利义

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

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

4. 合格的服务

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

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

4. 3 《项目招标需求》要求提供有关产品的，投标人应当说明投标产品的来源地，并按照《项目招标需求》的要求提供其从合法途径获得该货物的相关证明。

5. 投标费用

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

6. 信息发布

本采购项目需要公开的有关信息，包括招标公告、招标文件澄清或修改公告、中标公告以及延长投标截止时间等与招标活动有关的通知，招标人均将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布。投标人在参与本采购项目招投标活动期间，请及时关注以上媒体上的相关信息，投标人因没有及时关注而未能如期获取相关信息，及因此所产生的一切后果和责任，由投标人自行承担，招标人在任何情况下均不对此承担任何责任。

7. 询问与质疑

7.1 投标人对招标活动事项有疑问的，可以向招标咨询服务机构（联系方式：谢林言18964505975）提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.2 投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。其中，对招标文件的质疑，应当在其收到招标文件之日（以采购云平台显示的报名时间为准）起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。

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

同提出。

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

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

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

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

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

质疑函的递交应当采取书面递交形式，否则视为未递交。质疑联系部门：上海市杨浦区政府采购中心章笑吟，联系电话：65550185 ，地址：上海市杨浦区宁国路 129 号 16 楼。

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

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

8. 公平竞争和诚实信用

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

8.2 如果有证据表明投标人在本招标项目的竞争中存在腐败、欺诈或其他严重违背公平

竞争和诚实信用原则、扰乱政府采购正常秩序的行为，招标人将拒绝其投标，并将报告政府采购监管部门查处；中标后发现的，中标人须参照《中华人民共和国消费者权益保护法》第55条之条文描述方式双倍赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。

8.3 招标人将在**开标后至评标前**，通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动。

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

9. 其他

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

二、招标文件

10. 招标文件构成

10.1 招标文件由以下部分组成：

（1）投标邀请（招标公告）；

（2）投标人须知；

（3）政府采购主要政策；

（4）项目招标需求；

（5）评标方法；

（6）投标文件有关格式；

（7）合同书格式；

（8）本项目招标文件的澄清、答复、修改、补充内容（如有的话）。

10.2 投标人应仔细阅读招标文件的所有内容，并按照招标文件的要求提交投标文件。如果投标人没有按照招标文件要求提交全部资料，或者投标文件没有对招标文件在各方面作出实质性响应，则投标有可能被认定为无效标，其风险由投标人自行承担。

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

10.4 投标人应按照招标文件规定的日程安排，准时参加项目招投标有关活动。

11. 招标文件的澄清和修改

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

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

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

11.4 招标文件的澄清、答复、修改或补充都应由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，不得作为投标的依据，否则，由此导致的风险由投标人自行承担，招标人不承担任何责任。

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

12. 踏勘现场

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

12.2 投标人踏勘现场发生的费用由其自理。

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

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

三、投标文件

13. 投标文件构成

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

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

14. 投标的语言及计量单位

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

件视同未提供。

14．2　投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，一律采用中华人民共和国法定计量单位（货币单位：人民币元）。

15. 投标有效期

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

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

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

16. 商务响应文件

16.1 商务响应文件由以下部分组成：

（1）《投标函》；

（2）《开标一览表》；

（3）《投标报价分类明细表》等相关报价表格详见第六章《投标文件有关格式》；

（4）资格条件及实质性要求响应表；

（5）与评标有关的投标文件主要内容索引表；

（6）投标人关于报价等的其他说明（如有的话）。

（7）第四章《招标需求》规定的其他内容；

（8）相关证明文件（投标人应按照《项目招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同）。

17. 投标函

17.1 投标人应按照招标文件中提供的格式完整地填写《投标函》。

17.2 投标人不按照招标文件中提供的格式填写《投标函》，或者填写不完整的，评标时将按照第五章《评标方法》中的相关规定予以扣分。

17.3 投标文件中未提供《投标函》的，为无效投标。

18. 开标一览表

18.1 投标人应按照招标文件的要求和采购云平台提供的投标文件格式完整地填写《开标一览表》、报价明细表和报价构成表等，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

18.2 《开标一览表》是为了便于招标人开标，《开标一览表》内容在开标时将当众公布。开标一览表的内容应与投标报价明细表内容一致，不一致时以开标一览表内容为准。

18.3 投标人未按照招标文件的要求和采购云平台提供的投标文件格式完整地填写《开

标一览表》、或者未提供《开标一览表》，导致其开标不成功的，其责任和风险由投标人自行承担。

19. 投标报价

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

19.2 报价依据：

（1）本招标文件所要求的服务内容、服务期限、工作范围和要求；

（2）本招标文件明确的服务标准及考核方式；

（3）其他投标人认为应考虑的因素。

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

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

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

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

19.7 投标应以人民币报价。

20. 资格条件响应表及实质性要求响应表

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

20.2 投标文件中未提供《资格条件及实质性要求响应表》的，为无效投标。

21．与评标有关的投标文件主要内容索引表

21．1　投标人应按照招标文件提供的格式完整地填写与评标有关的投标文件主要内容索引表。

21．2　与评标有关的投标文件主要内容索引表是为了便于评标。与评标有关的投标文件主要内容索引表与投标文件其他部分就同一内容的表述应当一致，不一致时按照《投标人须知》第 32 条“投标文件内容不一致的修正”规定处理。

22. 技术响应文件=

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

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

23．相关证明文件

23.1 投标人应按照《项目招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同。

24． 投标保证金

不收取。

25. 投标文件的编制和签署

25.1 投标人应按照招标文件和采购云平台要求的格式填写相关内容。

25.2 投标文件中凡招标文件要求签署、盖章之处，均应显示投标人的法定代表人或法定代表人正式授权的代表签署字样及投标人的公章。投标人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投标文件，则应当按招标文件提供的格式出具《法定代表人授权委托书》（如投标人自拟授权书格式，则其授权书内容应当实质性符合招标文件提供的《法定代表人授权委托书》格式之内容）并将其附在投标文件中。投标文件若有修改错漏之处，须在修改错漏之处同样显示出投标人公章或者由法定代表人或法定代表人授权代表签署字样。投标文件因字迹潦草或表达不清所引起的后果由投标人自负。

其中对《投标函》《法定代表人授权委托书》《资格条件及实质性要求响应表》《投标诚信承诺书》以及《财务状况及税收、社会保障资金缴纳情况声明函》，投标人未按照上述要求签字和显示公章的，其投标无效。

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

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

（1）评标委员会主要是依据投标文件中技术、质量以及售后服务等指标来进行评定。因此，投标文件应根据招标文件的要求进行制作，内容简洁明了，编排合理有序，与招标文件内容无关或不符合招标文件要求的资料不要编入投标文件。

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

四、投标文件的递交

26. 投标文件的递交

26.1 投标人应按照招标文件规定，参考第六章投标文件有关格式，在采购云平台中按照要求填写和上传所有投标内容。投标的有关事项应根据采购云平台规定的要求办理。

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

招标人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供，否则投标人须接受可能对其不利的评标结果，并且招标人将对该投标人进行调查，发现有弄虚作假或欺诈行为的按有关规定进行处理。

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

27. 投标截止时间

27.1 投标人必须在《投标邀请（招标公告）》规定的网上投标截止时间前将投标文件在采购云平台中上传并正式投标。

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

27.3 在投标截止时间后上传的任何投标文件，招标人均将拒绝接收。

28. 投标文件的修改和撤回

在投标截止时间之前，投标人可以对在采购云平台已提交的投标文件进行修改和撤回。有关事项应根据采购云平台规定的要求办理。

五、开标

29. 开标

29.1 招标人将按《投标邀请》或《延期公告》（如果有的话）中规定的时间在采购云平台上组织公开开标。

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

29.3 投标截止，采购云平台显示开标后，投标人进行签到操作，投标人签到完成后，由招标人解除采购云平台对投标文件的加密。投标人应在规定时间内使用数字证书对其投标

文件解密。签到和解密的操作时长分别为半小时，投标人应在规定时间内完成上述签到或解密操作，逾期未完成签到或解密的投标人，其投标将作无效标处理。有证据能证实是因系统原因导致投标人无法在上述要求时间内完成签到或解密的除外。

如采购云平台开标程序有变化的，以最新的操作程序为准。

29.4 投标文件解密后，政采云平台根据各投标人填写的《开标一览表》的内容自动汇总生成《开标记录表》。

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

六、评标

30. 评标委员会

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

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

31. 投标文件的资格审查及符合性审查

31.1 开标后，招标人将依据法律法规和招标文件的《投标人须知》、《资格条件及实质性要求响应表》，对投标人进行资格审查。确定符合资格的投标人不少于 3 家的，将组织评标委员会进行评标。

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

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

31.4 开标后招标人拒绝投标人主动提交的任何澄清与补正。

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

32. 投标文件内容不一致的修正

32.1 投标文件报价出现前后不一致的，按照下列规定修正：

（1）《开标记录表》报价与投标文件中报价不一致的，以《开标记录表》为准；

（2）大写金额和小写金额不一致的，以大写金额为准；

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

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照上述规定的顺序修正。修正后的报价经投标人确认

后产生约束力，投标人不确认的，其投标无效。

32.2 《开标记录表》内容与投标文件中相应内容不一致的，以《开标记录表》为准。

32.3 投标文件中如果有其他与评审有关的因素前后不一致的，将按不利于出错投标人的原则进行处理，即对于不一致的内容，评标时按照对出错投标人不利的情形进行评分；如出错投标人中标，签订合同时按照对出错投标人不利、对采购人有利的条件签约。

33. 投标文件的澄清

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

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

33.3 投标人的澄清文件是其投标文件的组成部分。

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

34. 投标文件的评价与比较

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

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

35. 评标的有关要求

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

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

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

35.4 招标人和评标委员会均无义务向投标人做出有关评标的任何解释。

七、定标

36. 确认中标人

除了《投标人须知》第 36 条规定的招标失败情况之外，采购人将根据评标委员会推荐的中标候选人及排序情况，依法确认本采购项目的中标人。

37. 中标公告及中标和未中标通知

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

37.2 中标公告发布同时，招标人将向中标人发出《中标通知书》通知中标，向其他未

中标人发出《中标结果通知书》。《中标通知书》对招标人和投标人均具有法律约束力。

38. 投标文件的处理

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

39. 招标失败

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

八、授予合同

40. 合同授予

除了中标人无法履行合同义务之外，招标人将把合同授予根据《投标人须知》第 33 条规定所确定的中标人。

41. 签订合同

中标人与采购人应当在《中标通知书》发出之日起 30 日内签订政府采购合同。

41．2　中标人应根据合同条款的规定，按照招标文件中提供的履约保证金格式向采购人提交履约保证金。

42. 招标咨询服单位

本项目采购方委托的招标咨询服务单位为上海申权招标咨询有限公司。

43. 其他

采购云平台有关操作方法可以参考采购云平台（网址：www.zfcg.sh.gov.cn）中的**“操作须知”**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 20 %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。对于专门面向中小企业采购，则不再执行价格评审优惠的扶持政策。

非预留份额专门面向中小企业采购的项目或包件，对小微企业报价给予 20%的扣除，用扣除后的价格参与评审；非预留份额专门面向中小企业采购且接受联合体投标或者允许分包的项目或包件，对于联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额30%以上的投标人，给予其报价 6%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。组成联合体的大中型企业或者其他自然人、法人或其他组织，与小型、微型企业之间不得存在投资关系。

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　项目招标需求

一、项目概述

见附件

二、技术需求

见附件

说明：

为保证招标的合法性、公平性，投标人认为上述技术需求指标存在排他性或歧视性条款，可在收到或下载招标文件之日或者招标文件下载期限届满之日起七个工作日内提出并附相关证据，招标人将及时进行调查或组织论证，如情况属实，招标人将对上述相关技术需求指标做相应修改。

招标人在技术需求和图纸中指出的工艺、材料和货物的标准以及参照的品牌、型号仅起说明作用，并没有任何限制性，投标人在投标中可以选用其他替代标准、品牌或型号，但这些替代要实质上优于或相当于技术规格的要求。

三、付款要求

付款方法：按季度分 4 次支付，每次绩效考核后支付 25%项目款。

四、投标文件的商务、技术和相关证明文件要求

投标人应按照第二章《投标人须知》“三、投标文件”中的相关要求编制投标文件，投标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、投标人提交的商务标应由以下部分组成：

（1）投标函

（2）开标一览表

（3）报价分类明细表

（4）资格条件及实质性要求响应表

（5）与评标有关的投标文件主要内容索引表

（6）法定代表人（负责人）授权委托书、法人（负责人）身份证和被授权人身份证，原件彩色扫描（复印件须加盖投标人公章）；

（7）提供营业执照副本原件、税务登记证、组织机构代码证原件彩色扫描件（或三证

或五证合一）；

（8）财务状况及税收、社会保障资金缴纳情况声明函；

（9）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**（中标人为中小企业、残疾人福利性单位的，其声明函将随中标结果同时公告）**；

（10）投标人基本情况简介；

（11）同类及类似项目的业绩（列表，注明项目名称、服务时间、项目负责人等情况，并提供项目合同复印件、委托方评价作为证明，合同复印首、尾页即可）；

（12）投标人认为可以证明其能力、业绩、信誉和信用的其他相关材料；

（13）投标人债务纠纷、违法违规记录等方面的情况（如果有的话）；

（14）联合投标时，提供《联合投标协议书》。

（15）提供具有投标人公章、法定代表人和授权代表签字或盖章的《投标诚信承诺书》

（16）投标人与采购项目相关的资质证书（加盖投标人公章）

2．技术响应文件由以下部分组成：

（1）投标人对采购项目总体需求的理解以及投标的服务方案。投标人应详细描述针对本项目的服务方案等。

（2）按照本招标文件要求提供的其他技术性资料以及投标人需要说明的其他事项。

五、投标说明

投标人应根据政采云平台规定的格式和要求编制网上投标文件，并按照招标文件有关规定在政采云平台进行网上投标。网上投标文件如下：

（1）开标一览表

（2）中小企业声明函

（3）《残疾人福利企业声明函》（如有）

上传扫描文件要求：

投标人应按照招标文件规定提交彩色扫描文件，并按照规定在政采云平台上传其所有资料，文件格式参考第六章投标文件有关格式。含有公章，防伪标志和彩色底纹类文件（如投标函、营业执照、身份证、认证证书等）必须采用原件彩色扫描以清晰显示。如因上传、扫描、格式等原因导致评审时受到影响，由投标人承担相应责任。

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

第五章　评标办法

一、资格审查

招标人将依据法律法规和招标文件的《投标人须知》、《资格条件及实质性要求响应表》，对投标人进行资格审查。确定符合资格的投标人不少于 3 家的，将组织评标委员会进行评标。

二、投标无效情形

1. 投标文件不符合《资格条件及实质性要求响应表》所列任何情形之一的，将被认定为无效投标。

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投标的，相关投标均无效。

3.除上述以及政府采购法律法规、规章、《投标人须知》所规定的投标无效情形外，投标文件有其他不符合招标文件要求的均作为评标时的考虑因素，而不导致投标无效。

三、评标方法与程序

1. 评标方法

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

2. 评标委员会

2.1 本项目具体评标事务由评标委员会负责，评标委员会由采购人的代表和上海市政府采购评审专家组成。招标人将按照相关规定，从上海市政府采购评审专家库中随机抽取评审专家评标委员会。

2.2 评标委员会成员应坚持客观、公正、审慎的原则，依据投标文件对招标文件响应情况、投标文件编制情况等，按照《投标评分细则》逐项进行综合、科学、客观评分。

3. 评标程序

本项目评标工作程序如下：

3.1 符合性审查。评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。

3.2 澄清有关问题。对投标文件中含义不明确或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者纠正。投标人的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，不得超出投标文件的范围或者改变投标文件的实质性内容，也不得通过澄清而使进行澄清的投标人在评标中更加有利。

3.3 比较与评分。评标委员会按招标文件规定的《投标评分细则》，对符合性审查合格的投标文件进行评分。

3.4 推荐中标候选供应商名单。各评委按照评标办法对每个投标人进行独立评分，再计算平均分值，评标委员会按照每个投标人最终平均得分的高低依次排名，推荐得分最高者为第一中标候选人，依此类推。如果供应商最终得分相同，则按报价由低到高确定排名顺序，如果报价仍相同，则由评标委员会按照少数服从多数原则投票表决。

4.评分细则

本项目具体评分细则如下：

4.1 投标价格分按照以下方式进行计算：

（1）价格评分：报价分＝价格分值×（评标基准价/评审价）

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

（3）评审价：投标报价无缺漏项的，投标报价即评审价；投标报价有缺漏项的，按照其他投标人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投标报价10%的，其投标报价也即评审价，缺漏项的费用视为已包括在其投标报价中，经过计算的缺漏项价格超过其投标报价 10%的，其投标无效。

（4）非预留份额专门面向中小企业采购的项目或包件，对小微企业报价给予 20%的扣除，用扣除后的价格参与评审；非预留份额专门面向中小企业采购且接受联合体投标或者允许分包的项目或包件，对于联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额 30%以上的投标人，给予其报价 6%的扣除，用扣除后的价格参与评审。以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业，其中，联合体各方均为小微企业的，联合体视同小微企业。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。中小企业投标应提供《中小企业声明函》。如果本项目专门面向中小企业采购，则不再执行价格评审优惠的扶持政策。

（5）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标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；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

4.2 投标文件其他评分因素及分值设置等详见《投标评分细则》。

评分细则（100 分）

评分项目	分值区间	类型	评分办法
报价分	1-10	客观分	以满足招标文件要求的所有投标单位报价的最低价作为评标基准价，其价格分为满分。其他投标人的价格分统下列公式计算：投标报价得分=（评标基准价/投标报价）×价格权值×100
项目需求理解	1-5	专家打分	根据投标方项目需求理解的全面性、透彻性、完整性：包括需求理解的准确性，对业务流程的梳理，能做出实质性响应，且能详细描述本项目建设内容，进行综合打分。
整体技术方案架构	1-5	专家打分	整体技术方案架构包括、整体网络架构、控制面架构、数据面架构、安全架构、可靠性保障等方面。 根据投标方整体服务方案的完整性、科学性、可操作性等进行综合打分。
方案设计	1-5	专家打分	方案设计包含以下三大个方面： 一、网络架构设计，含核心网架构设计和接入网架构设计。 二、安全架构设计。 三、与各边界区安全设计，包含互联网业务区边界、市政务外网业务区边界、政务云安全区边界、安全接入业务区边界、专网接入业务区边界、核心网络与业务通讯安全。 根据方案设计的完整性、科学性、可操作性等进行综合打分。
业务迁移连续性要求	1-5	专家打分	本项目为在用全区网络基础设施，对业务迁移连续性有很高的要求，需提供相关服务方案。 服务方案如涉及系统割接，需提详尽的系统、网络割接服务方案，需对现状进行分析，体现割接的针对性、合理性、稳定性和可靠性，此外方案需要有进一步论证实施等内容。投标人应在上个合同周期（2024 年 3 月 31 日到期）到期前，确保能完成全网建设实施。 根据投标方以上方案的完整性、科学性、可操作性，满足业务连续性要求情况等方面进行综合打分。
网络资源服务	1-5	专家打分	包含业务组网、光传输设计及同步方案，根据投标方网络资源服务的完整性、科学性、可操作性等进行综合打分。
机房现状分析及机房资源服务	1-5	专家打分	根据投标方对本项目的机房现状分析和机房资源服务的针对性、合理性，可以充分体现方案稳定性和可靠性，有进一步完善建设方案等内容，进行综合打分。
项目管理与实施	1-4	专家打分	根据投标方所提供的项目组织的合理性、过程管理的规范性、质量保证措施、风险管理的有效性及技术文档和管理文档的完整性，进行综合打分。

资源和网络协议规划	1-3	专家打分	包含资源设计方案和网络协议规划，根据投标方资源设计方案和网络协议规划技术合理性，系统功能描述清楚、完善程度，进行综合打分。
网络安全服务	1-4	专家打分	包含安全时间监控与分析、漏洞管理、热点事件应急、重保服务等方面。根据网络安全服务的合理性，系统功能描述清楚、完善程度，进行综合打分。
运维保障服务	1-4	专家打分	根据本项目特点制定的项目运维服务方案，包括但不限于： 1、项目的关键节点的管理协调 2、服务性能指标（故障响应时间、服务措施、故障恢复时间等） 3、保证服务连续性(提供灾备高可用方案) 对上述内容服务保障方案等进行综合打分。
管理办法与运维制度	1-5	专家打分	根据本项目特点制定的管理办法与运维制度进行综合打分。
项目管理和组织保障	1-3	专家打分	根据投标方的项目实施计划及责任组织保障措施进行综合打分。
应急处理及业务连续性能力	1-2	专家打分	根据投标单位提供的应急处理方案及业务连续性计划详细、合理，有针对性进行综合打分。
机房网络安全要求	0-2	客观分	投标人所提供的机房需承诺满足信息系统安全等级保护三级要求。提供承诺文件得 2 分，不提供不得分。
售后服务能力	0-3	客观分	投标方具备直连基础运营商骨干网络信息枢纽的条件，提供使用场地（预提供服务场地）不低于 10 年的所有权或使用权的相关证明材料，并加盖公章。 如提供的为自有产权机房，得 3 分； 提供的为 20 年以上（含 20 年）租期使用权机房，得 2 分； 提供的为 10-20（含 10 年，不含 20 年）年租期使用权机房，得 1 分； 提供的为 10 年（不含 10 年）以下租期使用权机房，得 0.5 分； 不提供不得分。
项目经理专业性要求	0-3	客观分	项目经理具有与本项目相关的项目管理专业人士资格认证、正高级工程师职称、具备信息技术应用创新人员认证，有一项满足得 1 分，最高得 3 分。持证人需提供社保缴纳明细证明（近六个月中任意一个月，2023 年 7 月 1 日至本项目开标截止日）
网络负责人专业性要求	0-1	客观分	网络负责人具备**数据通信专家认**证或**企业基础架构专家认证**。网络负责人具备上述任一认证得 1 分。 持证人需提供社保缴纳明细证明（近六个月中任意一个月，2023 年 7 月 1 日至本项目开标截止日）。

运维驻场负责人	0-2	客观分	运维驻场负责人具有注册信息安全工程师或项目管理专业人士资格认证资质，负责现场运维、安全管理各项要求，满足一项得 1 分，最高得 2 分，不提供不得分。持证人需提供社保缴纳明细证明（近六个月中任意一个月，2023 年 7 月 1 日至本项目开标截止日）。
运维驻场工程师专业性要求	0-4	客观分	运维驻场工程师具有**注册信息安全工程师资质**，负责现场运维、安全各项操作要求，有一人满足得 0.5 分，最高得 4 分，不提供不得分。持证人需提供社保缴纳明细证明(近六个月中任意一个月，2023 年 7 月 1 日至本项目开标截止日）。
人员组织架构	1-5	专家打分	根据投标人项目团队人员的组织结构形式的合理性、可实施性，进行综合打分。
人员配备情况	1-5	专家打分	根据投标人项目团队人员配备情况（年龄、工作经历、专业等）、工作经验等情况综合打分。
业绩证明	0-5	客观分	提供 2021 年 1 月 1 日至本项目开标截止日类似业绩，附合同复印件并加盖公章，每提供一个得 1 分，最高得 5 分，不提供或提供不满足要求不得分。
企业综合实力	1-5	专家打分	根据投标方的综合服务能力、协议履行情况等综合实力进行评分。

附：上述计算结果四舍五入后保留 2 位有效小数，按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的，按技术指标优劣顺序排列。

第六章　　投标文件有关格式

一、商务响应文件有关格式

1、投标函格式

致：_____（招标人名称）

根据贵方_____（项目名称、招标编号）采购的招标公告及投标邀请，_____（姓名和职务）被正式授权代表投标人（投标人名称、地址），按照上海市政府采购云平台规定向贵方提交投标文件 1 份。

据此函，投标人兹宣布同意如下：

1.按招标文件规定，我方的投标总价为_____（大写）元人民币。

2.我方已详细研究了全部招标文件，包括招标文件的澄清和修改文件（如果有的话）、参考资料及有关附件，我们已完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

3.投标有效期为自开标之日起 _____日。

4.如我方中标，投标文件将作为本项目合同的组成部分，直至合同履行完毕止均保持有效，我方将按招标文件及政府采购法律、法规的规定，承担完成合同的全部责任和义务。

5.如果我方有招标文件规定的不予退还投标保证金的任何行为，我方的投标保证金可被贵方没收。

6.我方同意向贵方提供贵方可能进一步要求的与本投标有关的一切证据或资料。

7.我方完全理解贵方不一定要接受最低报价的投标或其他任何投标。

8.我方已充分考虑到投标期间网上投标可能会发生的技术故障、操作失误和相应的风险，并对因网上投标的任何技术故障、操作失误造成投标内容缺漏、不一致或投标失败的，承担全部责任。

9. 我方同意开标内容以上海市政府采购云平台开标时的《开标记录表》内容为准。我方授权代表将及时使用数字证书对《开标记录表》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，视为我方对开标记录内容无异议。

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

（1）我方向贵方提交的所有投标文件、资料都是准确的和真实的。

（2）我方不是采购人的附属机构或与采购存在其他利害关系。

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

地址：_____

电话、传真：_____

邮政编码：_____

开户银行：_____

银行账号：_____

投标人授权代表签名：_____

投标人名称（公章）：_____

日期：_____年___月___日

2、开标一览表格式

项目名称：

招标编号：

上海市杨浦区大数据中心杨浦区电子政务外网基础设施租赁及安全、运维服务采购包 1

包名称	服务期限	付款方式是否满足招标文件要求（是/否）	最终报价（总价、元）

说明：（1）“金额（元）”指每一包件投标报价，所有价格均系用人民币表示，单位为元，精确到分。

（2）投标人应按照《项目招标需求》和《投标人须知》的要求报价。

（3）开标一览表内容与投标文件其它部分内容不一致时以开标一览表内容为准。

3、报价分类明细表格式

项目名称：
包号：

序号	分类名称	报价费用	备注
			详见明细（ ）
			详见明细（ ）
			详见明细（ ）
			详见明细（ ）
			详见明细（ ）
			详见明细（ ）
	其他费用		详见明细（ ）
	税金		详见明细（ ）
	利润		详见明细（ ）
报价合计			

说明：（1）所有价格均系用人民币表示，单位为元/年，精确到分。

（2）投标人应按照《项目招标需求》和《投标人须知》以及行业定价要求报价。

（3）投标人应根据分类报价费用情况编制明细费用表并随本表一起提供。

（4）分项目明细报价合计应与开标一览表报价相等。

_____投标人授权代表签字：

_____投标人（公章）：

日期：　　年　　月　　日

4、资格条件及实质性要求响应表

项目名称：

包号：

项目内容（资格条件、实质性要求）	具备的条件说明（要求）	投标检查项（响应内容说明(是/否)）	详细内容所对应电子投标文件名称	备注
资格条件、实质性要求	提供营业执照副本原件、税务登记证、组织机构代码证原件彩色扫描件（或三证或五证合一）			
资格条件、实质性要求	提供财务状况及税收、社会保障资金缴纳情况声明函并加盖公章			
资格条件、实质性要求	提供信用查询截图。同时，招标人和评标委员会将通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动。			
资格条件、实质性要求	法人(负责人)授权书具有法定代表人(负责人)签字或盖章			
资格条件、实质性要求	法人(负责人)身份证和被授权人身份证，原件彩色扫描（复印件须加盖投标人公章）			
资格条件、实质性要求	提供具有投标人公章、法定代表人和授权代表签字或盖章的《投标诚信承诺书》			
资格条件、实质性要求	招标人和评标委员会审查,未发现本项目存在《政府采购货物和服务招标投标管理办法》第三十七条所列的串通投标的情况。评标过程中发现投标人有上述情形的，评标委员会应认定其投标无效，并书面报告本级财政部门。			
资格条件、实质性要求	投标有效期符合招标文件规定：不少于 90 天。			
资格条件、实质性要求	付款条件满足招标文件要求			
合同转让与分包	本项目合同不得转让、不得分包。			
★号条款	1、★满足验收要求,提供以下内容承诺函：			

	验收需满足本项目上线运营交付要求，并于 2024 年 2 月 29 日前完成整体上线，包括不限于网络核心层、汇聚层、所有接入节点以及安全设备。招标人根据中标人投标响应文件中服务方案、服务承诺等内容的实施情况对项目进行验收，验收完成后进入试运行。如中标人未通过验收，招标人有权中止合同，并且需由中标人支付招标人因中标人未能按照承诺响应完成项目造成的业务影响费用（包含但不限于因服务未能按时上线所需要支付的延续服务费，可能包含网络及安全设备租赁费、运维服务费等）			
★号条款	2、★满足业务连续性要求，提供以下内容承诺函： 在保证政务外网业务连续性，不影响原有政务外网基础设施服务的前提下，于 2024 年 3 月 31 日前，完成网络割接迁移工作，招标文件内 787 个接入节点均进入各政务外网需求单位正常使用状态，且所有网络割接迁移成本，均包含在报价之内，投标人明确政务外网网络基础设施业务连续性对招标人的重要性，能够预见未能满足承诺要求将对招标人造成巨大的损失；因此投标人同意如未满足承诺要求，招标人有权单方面解除合同且中标人承担违约责任，包括但不限于返还招标人已支付费用、承担招标人再次招标的费用、因无法割接迁移产生的所有费用等。			
★号条款	**★预算金额：**18878600 元，超过预算作废标处理。			

_____投标人授权代表签字：

_____投标人（公章）：

日期：　　年　　月　　日

5、与评标有关的投标文件主要内容索引表

项目名称：

包号：

项目内容	具备的条件说明	响应内容说明(是/否)	详细内容所对应电子投标文件名称及页码	备注
1				
2				
3				
4				
……				

说明：上述具体内容要求可以参照本项目评标方法与程序及评分细则。

_____投标人授权代表签字：

_____投标人（公章）：

日期：　　年　　月　　日

6.客观分评审因素响应情况表

序号	名称	是否响应	响应情况	响应材料对应在投标文件中的页码
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
……				

_____投标人授权代表签字：

_____投标人（公章）：

日期：　　年　　月　　日

二、技术响应文件有关表格格式

1、项目负责人情况表

项目名称：
包号：

姓名		出生年月		文化程度		毕业时间	
毕业院校和专业			从事本类项目工作年限			联系方式	
职业资格			技术职称			聘任时间	
主要工作经历： 主要管理服务项目： 主要工作特点： 主要工作业绩： 胜任本项目负责人的理由：							

_____投标人授权代表签字：

_____投标人（公章）：

日期：_____年_____月_____日

2、主要管理、技术人员配备及相关工作经历、职业资格汇总表

项目名称：

包号：

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
……							

_____投标人授权代表签字：

_____投标人（公章）：

日期：_____年_____月_____日

三、各类银行保函格式

1、预付款银行保函格式

致：_____（采购人名称）

鉴于_____（乙方名称）（以下简称“乙方”）根据___年月___日与贵方签订的_____号合同（以下简称“合同”）向贵方提供（服务描述）。

根据贵方在合同中规定，乙方要得到预付款，应向贵方提交由一家信誉良好的银行出具的、金额为_____（以大写和数字表示的保证金金额）的银行保函，以保证其正确和忠实地履行所述的合同条款。

我行_____（银行名称）根据乙方的要求，无条件地和不可撤消地同意作为主要责任人而且不仅仅作为保证人，保证在收到贵方第一次要求就支付给贵方不超过（以大写和数字表示的保证金金额），我行无权反对和不需要先向乙方索赔。

我行进而同意，要履行的合同条件或买卖双方签署的其他合同文件的改变、增加或修改，无论如何均不能免除我行在本保函下的任何责任。我行在此表示不要求接到上述改变、增加或修改的通知。

本保函自收到合同预付款起直至　　年　　月　　日前一直有效。

_____出证行名称：

_____出证行地址：

_____经正式授权代表本行的代表的姓名和职务（打印和签字）：

_____银行公章：

_____出证日期：

说明：1、本保函应由商业银行的总行、**分行或者支行出具，支行**以下机构出具的保函恕不接受。

2、本保函由中标人在合同签订后提交。

四、相关证明文件格式

1、投标人基本情况简介格式

（一）基本情况：

1、单位名称：

2、地址：

3：邮编：

4、电话/传真：

5、成立日期或注册日期：

6、行业类型：

（二）基本经济指标（到上年度 12 月 31 日止）：

1、实收资本：

2、资产总额：

3、负债总额：

4、营业收入：

5、净利润：

6、上交税收：

7、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，我方同意根据招标人进一步要求出示有关资料予以证实。

_____投标人授权代表签字：

_____投标人（公章）：

日期：_____年_____月_____日

2、法定代表人(负责人)授权书格式

致：上海市杨浦区政府采购中心

我_____（姓名）系注册于_____（地址）的_____（投标人名称，以下简称我方）的法定代表人（负责人），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_____项目的投标活动，由其代表我方全权办理针对上述项目的投标、开标、投标文件澄清、签约等一切具体事务，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。

在此粘贴 法人（负责人）身份证和被授权人身份证，原件彩色扫描 （复印件须加盖投标人公章）

投标人公章：	受托人（代理人）（签字）：
法定代表人（负责人）（签字或盖章）：	住所：
邮政编码：	身份证号码：
电话：	邮政编码：
传真：	电话：
日期：	传真：
	日期：

3、同类或类似项目业绩：投标人近年承接的与本项目类似项目一览表格式

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

_____投标人授权代表签字：

_____投标人（公章）：

日期：_____年_____月_____日

4、《联合投标协议书》格式（如有）

联合投标各方：

甲方：

法定代表人：

住所：

乙方：

法定代表人：

住所：

（如果有的话，可按甲、乙、丙、丁…序列增加）

根据《政府采购法》第二十四条之规定，为响应上海市杨浦区政府采购中心组织实施的项目（项目名称、招标编号）的招标活动，各方经协商，就联合进行投标之事宜，达成如下协议：

一、各方一致决定，以 _____ 为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或授权代理人根据招标文件规定及投标内容而对招标方和采购人所作的任何合法承诺，包括书面澄清及响应等均对联合投标各方产生约束力。如果中标并签订合同，则联合投标各方将共同履行对招标方和采购人所负有的全部义务并就采购合同约定的事项对采购人承担连带责任。

三、联合投标其余各方保证对主办人为响应本次招标而提供的服务提供全部质量保证及售后服务支持。

四、本次联合投标中，甲方承担的合同份额为　　元，乙方承担的合同份额为　　元。

甲方承担的工作和义务为：

乙方承担的工作和义务为：

五、本协议提交招标方后，联合投标各方不得以任何形式对上述实质内容进行修改或撤销。

六、本协议一式三份，甲、乙双方各持一份，另一份作为投标文件的组成部分提交杨浦区政府采购中心。

甲方（盖章）：

法定代表人（签字）：

20　年　月　日

乙方（盖章）：

法定代表人（签字）：

20　年　月　日

5、中小企业声明函（服务）

本公司（联合体）郑重声明，根据 《政府采购促进中小企业发展管理办法》 （财库〔2020〕46 号）的规定，本公司（联合体）参加 *（单位名称）*的*（项目名称）*采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. *（标的名称）*，属于*（软件和信息技术服务业）*；承接企业为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元[1]，属于*（中型企业、小型企业、微型企业）*；

2. *（标的名称）*，属于*（软件和信息技术服务业）*；承接企业为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元[1]，属于*（中型企业、小型企业、微型企业）*；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

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

（2）本声明函所称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《中华人民共和国劳动合同法》订立劳动合同的从业人员，否则不享受中小企业扶持政策。

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

（4）采购标的对应的中小企业划分标准所属行业，以**招标文件第二章《投标人须知》规定为准。**

（5）中标人为中小企业的，本声明函将随中标结果同时公告。

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

注：各行业划型标准：

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

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

上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6、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）。

中标人为残疾人福利性单位的，本声明函将随中标结果同时公告。

如投标人不符合残疾人福利性单位条件，无需填写本声明。

7、投标诚信承诺书

本公司郑重承诺:

本公司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,将遵循公开、公平、公正和诚信守信的原则，参加_____项目的投标。

一、所提供的一切材料都是真实、有效、合法的。

二、不与采购人、其他供应商或者采购机构串通投标，损害国家利益、社会利益和他人的合法权益。

三、不向采购人或评标委员会成员或相关人员行贿，以谋取中标。

四、不以他人名义投标或者其他方式弄虚作假，骗取中标。

五、不接受任何形式的挂靠，不扰乱招投标市场秩序。

六、不在投标中哄抬价格或恶意压价。

七、不在招投标活动中进行虚假、恶意的质疑和投诉。

八、保证所提供的所有货物、服务均无专利权、商标权、著作权或其他知识产权等有侵害他方的行为。

九、保证中标之后，按照投标文件承诺履约、实施项目。

十、本公司若有违反承诺内容的行为，愿意承担相应的法律责任。如已中标的，自动放弃中标资格；给采购人造成损失的，依法承担赔偿责任，

投标供应商全称：_____（盖章）

投标供应商地址：_____

法定代表人（签字或盖章）：_____手机：_____

授权代理人（签字或盖章）：_____手机：_____

年　　月　　日

8. 财务状况及税收、社会保障资金

缴纳情况声明函

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

1. 具有健全的财务会计制度；

2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

第七章　　合同条款及合同格式

包 1 合同模板：

[合同中心-合同名称]

合同统一编号：［合同中心-合同编码］

项目名称：上海市杨浦区大数据中心杨浦区电子政务外网基础设施租赁及安全、运维服务采购

合同各方：

甲方：[合同中心-采购单位名称]

地址：[合同中心-采购单位所在地]

电话：[合同中心-采购单位联系人电话]

联系人：[合同中心-采购单位联系人]

乙方：[合同中心-供应商名称]

法定代表人：[合同中心-供应商法人姓名]

（[合同中心-供应商法人性别]）

地址：[合同中心-供应商所在地]

电话：[合同中心-供应商联系人电话]

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服务：

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

2. 合同价格、服务地点和服务期限

2．1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

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

2．2 服务地点：详见招标文件

2．3 服务期限：2024 年 4 月 1 日——2025 年 3 月 31 日[合同中心-合同有效期]以投标文件为准。

3．质量标准和要求

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

3．2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4．权利瑕疵担保

4．1 乙方保证对其交付的服务享有合法的权利。

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

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

4．4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5．验收

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

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

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

5．4 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

6．保密

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

7．付款

7．1 本合同以人民币付款（单位：元）。

7．2 本合同款项按照以下方式支付。

7．2．1 付款内容：（分期付款）

7．2．2 付款条件：

[合同中心-支付方式名称]

付款方法：按季度分 4 次支付，每次绩效考核后支付 25%项目款。

8．甲方的权利义务

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

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

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

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

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

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

9．乙方的权利与义务

9．1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服

务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

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

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

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

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

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

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

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

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

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

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

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

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，

按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供服务。

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

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

12．误期赔偿

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

13．不可抗力

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

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

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

14．履约保证金

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为/元人民币的履约保证

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

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

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

15．争端的解决

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

15．2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15．3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16．违约终止合同

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

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

（2）如果乙方未能履行合同规定的其它义务。

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

17．破产终止合同

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

18．合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19．合同生效

19．1 本合同在合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19．2 本合同一式份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20. 合同附件

20. 1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20. 2 本合同附件与合同具有同等效力。

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

21．合同修改

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

[合同中心-补充条款列表]

签约各方：

甲方（盖章）：	乙方（盖章）：
法定代表人或授权委托人（签章）：	法定代表人或授权委托人（签章）：
日期：**[合同中心-签订时间]**	日期：[合同中心-签订时间_1]

合同签订点:网上签约

附件：

技术需求

项目名称：上海市杨浦区大数据中心杨浦区电子政务外网基础设施租赁及安全、运维服务采购

项目单位：杨浦区大数据中心（杨浦区行政服务事务中心）

★预算金额：18878600 元，超过预算作废标处理。

服务期限：2024 年 4 月 1 日——2025 年 3 月 31 日

一、项目的整体概况

1、项目背景

为提升杨浦区电子政务网络支撑能力，充分发挥电子政务外网在“数字政府”建设中的基础支撑作用，依据《上海市公共数据和一网通办管理办法》（上海市人民政府令 2018 年第 9 号）中 “本市加强市、区两级电子政务基础设施的统筹规划和统一管理，推进电子政务网络、电子政务云、大数据资源平台、电子政务灾难备份中心等共建共用，保障电子政务基础设施的安全可靠”的要求，需建设电子政务外网，满足“全市一张网”的要求。

根据《上海市电子政务外网建设和运行管理指南》要求，我区于 2020 年 4 月开始启动新政务外网升级改造的规划和调研工作，项目经评估后，于 2020 年 11 月进行了公开招标。因原项目期满，服务期将于 2024 年 3 月 31 日到期，需重新进行采购。

2、总体架构

本项目需按照《上海市电子政务外网建设和运行管理指南》要求提供杨浦区电子政务外网基础设施租赁及安全、运维服务。

杨浦区电子政务外网由底层光传输网络和上层业务网络组成。在政务外网的重要节点采用光传输设备组建底层光传输网络。光传输设备在一对光纤中同时传输多个波长，有效提升光纤的传输容量，并提供光纤链路的自动保护和恢复能力，解决政务外网光纤接入光纤利用率不足、自愈保护能力差、业务调度缺乏灵活性等问题。

上层业务网络基于 IP 技术，采用数据平面和视频平面构建互为备份的“一网双平面”架构。数据平面、视频平面互为备份，故障时数据平面、视频平面可实现冗余保护，确保政务外网业务的灵活调度和稳定可靠运行。

3、总体目标

杨浦区政务外网网络改造方案原则上遵循上海市人民政府《上海市公共数据和一网通办管理方法》（上海市人民政府令第 9 号）要求，参照《上海市电子政务外网建设和运行管理指南》，结合杨浦区政务信息化实际情况，以先进适用为技术功能出发点进行规划设计。目标是保障区政府及各部门开展电子政务应用、实现信息资源共享，打造一张满足未来 5 年内杨浦区电子政务发展需求、安全可靠、性能先进、可视可管可控、具有较强演进能力的电子政务外网系统。

改造后的网络系统将满足上海市人民政府《上海市公共数据和一网通办管理方法》（上海市人民政府令第 9 号）及上海市大数据中心《上海市电子政务外网建设和运行管理指南》中对区级电子政务外网系统的各项要求。

4、项目模式

本次项目采用设备租赁+服务采购的模式进行，即，所有政务外网网络升级改造的设备、链路资源、机房资源、计算资源等，均采用租赁的方式进行，并向中标人采购配套的安全、运维技术服务。

设备租赁应包含所有升级改造设备的供货、安装、调试等，及项目范围内变更的配置服务等，以确保用户向中标人所租赁的内容是满足招标文件技术要求，并可直接使用的设备、机房、链路等。

安全、运维技术服务包含：通过建立专业高效的安全和运维服务体系，对升级后的杨浦区电子政务外网进行整体系统维护，保障网络系统的正常运行。

5、项目需求

5.1 业务类型

政务外网中的业务主要分为视频业务和数据业务两大种类。

（1）视频业务

主要包括用于市区两级以及区政府同下属各部门、委办局、街道等召开视频会议的视频流量。

（2）数据业务

数据业务包括区政务各部门、委办局、街道、事业单位等利用政务外网，进行公文处理、事务审批、电子邮件、移动办公等日常在线办公应用，基于“云网一体化”架构，通过政务外网接入区政务云或本地化平台开展城市社会治理、提供公共服务、实现数据资源共享，以及通过政务外网进行 Internet 互联网访问等，产生数据流量的业务。

5.2 接入规模

本次杨浦区政务外网接入节点除现有的 787 个现有用户需要接入外，服务期内应满足杨浦电子政务外网用户节点扩容及迁移需求。

截止到 2023 年 11 月 30 日，杨浦区现有委办局、街道、办事机构、事业单位、区属企业及条线下属设点 787 个，清单如下：

1	上海市杨浦区消防支队	周家嘴路 3097 号
2	公助一村居委会	周家嘴路 4214 弄 26 号
3	定海路街道第三睦邻中心	周家嘴路 4214 弄 26 号
4	民政局救助站 1	周家嘴路 4214 弄 16 号 3#救助楼
5	司法局社区矫正中心	周家嘴路 4214 弄 16 号 2 楼机房
6	救助站 2	周家嘴路 4214 弄 16 号办公楼
7	延吉新村城管中心	周家嘴路 3889 号一楼
8	延吉新村城运中心	周家嘴路 3889 号二楼
9	延吉新村管理办	周家嘴路 3889 号二楼
10	延吉新村房办	周家嘴路 3889 号二楼
11	富阳居委会	周家嘴路 3118 弄 30 号二楼
12	控江派出所	周家嘴路 2985 号一楼户籍窗口
13	阳明居委会	周家嘴路 2360 号 2 楼
14	江浦城运中心	周家嘴路 2299 号
15	姚家桥居委会	周家嘴路 2001 弄 2 号楼一楼
16	又一村居委会	周家嘴路 1683 弄 30 号 104 室
17	大花园居委会	周家嘴路 1299 弄 40 号二楼
18	中原一村居委会	中原一村 61 号 101-103 室
19	中原路 99 弄居委会	中原路 99 弄 19 号甲
20	中原路 990 弄居委会	中原路 990 弄 1-1 号
21	民星路 600 弄居委会	中原路 60 弄 3 号
22	殷行城运 2	中原路 571 号
23	长海居委会	中原路 32 弄 26 号 102 室
24	中翔居委会	中原路 28 弄 4 号 102 室
25	杨浦区退役军人事务局（4 所）	中原路 28 弄 20 号
26	杨浦区退役军人事务局（8 所）	中原路 28 弄 11 号 105 室
27	中原路派出所	中原路 1111 号综合窗口
28	大运盛居委会	中山北二路 99 弄 57 号 105 室
29	政立二居委会	政云路 220 号 2 楼
30	建德国际居委会（街道残联）	政悦路 588 弄 32 号 2 楼
31	新江湾城街道残联	政悦路 588 弄 32 号
32	雍景苑居委会	政悦路 500 弄 2 号 2 楼
33	新江湾派出所	政悦路 333 号一楼综合窗口
34	新江湾城街道社区事务受理服务中心(居家养老)	政悦路 329 号
35	新江湾城城管中心（城运、司法所、网格办）	政悦路 318 号二楼
36	新江湾城城运中心（该点同一机柜有 2 个 pon）	政悦路 318 号 214 室
37	五角场街道办	政通路 54 号
38	五角场街道社区党群服务中心（自治办）	政通路 30 号
39	建新居委会	政通路 285 弄 12 号
40	政民居委会	政通路 240 弄 C1

41	政通路第一居委会	政通路 100 弄 24 号 101 室
42	五角场街道社区事务受理服务中心	政通路 100 弄 11 号
43	复旦居委会	政肃路 45 弄 17 号 102 室
44	消防淞沪中队	政青路 70 号
45	国权北居委会	政立路 817 弄 5 号 201 室
46	长海路派出所	政立路 65 号监控室、三楼计算机室
47	政立一居委会	政立路 637 号 3 楼
48	国定路第一居委会	政立路 580 弄 61 号甲
49	财大居委会	政立路 580 弄 38 号甲
50	长海街道办	政立路 55 号
51	就促东区分中心(外劳，培训，职介）	政立路 205 号
52	正文花苑居委会	政立路 1585 弄 40 号 2 楼
53	五角场社区事务受理分 2	政化路 279-285 号
54	五角场社区事务受理分 2	政化路 279-285 号
55	五角场街道文化中心会场	政化路 257 号 5 层
56	消防支队政和中队	政和路 519 号
57	仁恒怡庭居委（筹）	政和路 388 弄
58	新江湾城社区卫生服务中心	政和路 107 号
59	江湾国际居委会	政和路 1011 号 2 楼
60	新江湾城街道江湾国际社区睦邻中心	政和路 1011 号 203 室
61	长海街道市光社区睦邻中心	政府路 78 号 2 楼
62	五角场城运中心	政旦东路 4 号二楼
63	五角场城管中心 1	政旦东路 4 号
64	五角场城管中心 2	政旦东路 4 号
65	五角场街道司法所 1	政旦东路 10 号
66	五角场街道司法所 2	政旦东路 10 号
67	四平新村第一居委会	政本路 115 号
68	明园村居委会	长阳路 910 弄 11 号一楼
69	辽昆居委会	长阳路 539 弄 2 号
70	定海路街道办（含司法所）	长阳路 3077 号
71	定海路街道社区党群服务中心	长阳路 3066 号 4 楼
72	定海路街道社区事务受理服务中心服务办 1、2 楼	长阳路 3066 号 2 楼
73	定海路街道社区事务受理服务中心服务办 5 楼部分	长阳路 3066 号 2 楼
74	定海路街道社区事务受理服务中心网格中心 301	长阳路 3066 号 2 楼
75	定海路街道社区事务受理服务中心宣文办 2 楼部分	长阳路 3066 号 2 楼
76	卫百辛集团	长阳路 2555 号 1 号楼 12 楼
77	劳务人事争议仲裁院	长阳路 2467 号 22 号楼
78	劳动监察大队	长阳路 2467 号 11 号楼
79	西白林寺居委会	长阳路 2166 号 202 室
80	大桥派出所	长阳路 2143 号一楼综合窗口
81	宁武路居委会	长阳路 1900 弄 4 号 104 室
82	双阳路居委会	杨浦区顺平路 1260 弄 31 号
83	长阳创谷大数据点位自助服务区	长阳路 1687 号
84	疾病预防控制中心	长阳路 1565 号 1 号楼
85	妇幼保健院（所）	宁国路 241 号 31 号 宁国坊

86	大桥社区卫生服务中心	长阳路 1389 弄 75 号
87	长眉居委会	长阳路 1389 弄 17 号 101 室
88	长阳新苑居委会	长阳路 1318 弄 57 号 102 室
89	凤联居委会	长岭路凤城六村 1 号 105 室
90	教育局	长岭路 91 号 2 楼
91	凤城三村第三居委会	长岭路 60 弄 12 号
92	住房保障房屋管理局	长岭路 115 号 4 楼
93	自然资源确权登记事务中心 1	长岭路 111 号（在用）
94	自然资源确权登记事务中心 2	长岭路 111 号（备用）
95	长海城管中心 1	长海一村 42 号
96	长海街道城管中心 2（100M）	长海一村 42 号
97	长海一村居委会	长海一村 23 号二层
98	黑山新村居委会	长海四村 13 号底层
99	长海三村居委会	长海三村 35 号 102 室
100	长海路街道综治中心（多部门，含司法所，平安办，信访问办）	长海路 605 号 2 楼
101	杨浦图书馆	长海路 366 号
102	长海二村居委会	长海二村 68 号甲
103	长白三村居委会	长白三村 57 号甲
104	图们路居委会	长白路 125 号
105	盛世豪园居委会（筹）	闸殷路 889 弄 25 号 101 室
106	闸殷路 81 弄居委会	闸殷路 81 弄 48 号 102 室
107	闸殷路第二居委会	闸殷路 181 弄 22 号 103 室
108	党校（行政学院）	闸殷路 155 号 3 楼
109	党校（社会主义学院）	闸殷路 155 号 3 楼
110	党校（团校 1）	闸殷路 155 号 3 楼
111	杨浦区投资服务发展中心四分中心	源泉路 100 号
112	长海城运中心（装新地址）	原地址：长海路 508 号 211 室，新地址长海路 580 号
113	1 号楼老大楼部分重要部门	榆林路 707 号
114	怀德居委会	榆林路 620 号 101 室（新地址）
115	惠明居委会	榆林路 555 号（新地址）
116	联通大厦	榆林路 185 号 二楼展厅
117	友谊新村居委会	友谊新村 235 号-1
118	城投集团	营口路 798 号 5 楼
119	佳泰居委会	营口路 789 弄 63 号底楼
120	市东医院营口路分院	营口路 762 号 7 楼
121	长海社区卫生服务中心	营口路 760 号
122	佳龙居委会	营口路 600 弄 43 号二楼
123	公安人口办	营口路 588 号 17 楼
124	殷行养老服务中心	殷行一村 74 号甲
125	殷行街道殷行新村社区睦邻点	殷行一村 74 号
126	殷行一村居委会	殷行一村 44 号 102 室
127	新江湾城街道办	殷行路 990 号
128	东森涵碧居委会	殷行路 851 号 4 楼
129	时代花园居委会	殷行路 850 弄 53 号 2 楼
130	杨浦区投资服务发展中心六分中心 分点 1	殷行路 833 号 4 楼
131	工农二村第二居委会	殷行路 571 弄 6 号 102 室

132	殷行司法所	殷行路 485 号
133	殷行路 470 弄居委会	殷行路 470 弄 33 号 102 室
134	工农二村第一居委会	殷行路 451 弄 1 号 102 室
135	殷行社区卫生服务中心	殷行路 429 号
136	殷行路 310 弄居委会	殷行路 310 弄 64 号 101 室
137	工农新村居委会	殷行路 305 弄 94 号 105 室
138	殷行二村居委会	殷行路 301 弄 12 号 103 室
139	殷行路 250 弄居委会	殷行路 250 弄 37 号
140	杨浦区退役军人事务局（江湾服务管理中心）	殷行路 1628 弄 1 号
141	睿达路居委会（筹）	殷行路 1628 弄 15 号 3 楼
142	政务逸仙维护业务测试线路 PON	逸仙路 38 号 4 楼
143	邯郸路居委会	逸仙路 167 弄 2 号 103 室
144	城市运行管理中心	移动大楼 8 楼
145	城运中心视频物联网专线 1	移动大楼
146	城运中心视频物联网专线 2	移动大楼
147	十七棉工房第二居委会	杨树浦路 3061 弄 151 号
148	定海路街道第四睦邻点	杨树浦路 3061 弄 151 号
149	凉州路居委会	杨树浦路 2811 弄 1 号 101 室
150	滨江办	杨树浦路 2086 号 3 楼
151	滨江	杨树浦路 1500 号 1 层
152	杨浦城管滨江项目点位	杨树浦路 1426 号靠近安浦路（变更到绿之丘）
153	消防支队杨树浦消防中队	杨树浦路 1307 号 1 层
154	福宁路居委会	杨树浦路 1177 弄 16 号 102 室
155	海杨居委会	扬州路 588 弄 3 号 103 室
156	许阳居委会	扬州路 310 号甲
157	延吉新村街道办	延吉中路 77 号
158	延吉新村街道社区事务受理服务中心	延吉中路 77 号
159	延吉新村街道社区党群服务中心	延吉中路 49 号
160	紫城居委会	延吉中路 365 弄 5 号 101 室
161	杨浦区退役军人事务局（1 所）	延吉中路 320 弄 8 号
162	延吉一村居委会	延吉一村 7 号 103 室
163	凤城三村第一居委会	延吉西路 80 弄 27 号 101 室
164	控江社区卫生服务中心	延吉西路 100 号 4 楼
165	延吉五六村居委会	延吉五村 54 号底楼
166	延吉四村居委会	延吉四村 60 号
167	延吉街道延吉社区第一睦邻中心	延吉四村 60 号
168	延吉二三村居委会	延吉三村 24 号底楼
169	延吉七村居委会	延吉七村 20 号 101 室
170	松花新村居委会	延吉东路 82 弄 26 号二楼
171	松延居委会	延吉东路 5 弄 3 号 102 室
172	就促延吉东路分中心	延吉东路 325 号
173	长白路第二居委会	新地址长白路 22-24 号
174	长白新村城运中心	延吉东路 212 号二楼
175	长白二村第一居委会	延吉东路 140 弄院内
176	延东居委会	延吉东路 137 弄 8 号甲
177	长白新村派出所	延吉东路 109~111 号一楼综合窗口
178	长白新村街道社区事务受理服务中心	延吉东路 107 号

179	长白新村街道社区党群服务中心	延吉东路 105 号二楼
180	延吉养老服务中心	延吉 7 村 20 号（淞花江路）
181	三湘居委会	学府路 88 弄 35 号 201 室
182	老年护理医院（老院）	许昌路 426 号
183	纺三居委会	许昌路 356 号
184	江浦社区卫生服务中心	许昌路 1482 号
185	辽源二村第二居委会	许昌路 1471 弄 3 号 104 室
186	旧改办 1	许昌路 1296 号 6 楼、8 楼
187	旧改办 2	许昌路 1296 号 6 楼、8 楼
188	杨浦滨江 1	许昌路 1296 号 4、5 楼
189	杨浦滨江 2	许昌路 1296 号 4、5 楼
190	杨浦区投资服务发展中心一分中心	许昌路 1296 号
191	江浦路街道办	许昌路 1212 号
192	江浦路街道社区事务受理服务中心	许昌路 1150 号
193	江浦路街道社区事务受理服务中心（社区服务办）	许昌路 1150 号
194	江浦路街道社区事务受理服务中心(优化营商办)	许昌路 1150 号
195	江浦路街道社区事务受理服务中心(宣文办)	许昌路 1150 号
196	血液管理中心 1（10M）	翔殷支路 116 号
197	翔殷新村居委会	翔殷三村 41 号 104 室
198	政翔殷居委会	翔殷路 934 弄 7 号 105 室
199	杨浦区退役军人事务局（3 所）	翔殷路 871 弄 69 号
200	梅花村居委会	翔殷路 871 弄 4 号
201	消防支队翔殷路 81 号中队	翔殷路 81 号
202	长海街道黄兴社区睦邻中心	翔殷路 791 弄 3 号
203	长海路街道社区党群服务中心	翔殷路 505 弄 3 号二楼（同幢楼另有文化中心）
204	长海路街道社区党群社区文化活动中心	翔殷路 505 弄 3 号二楼（同幢楼另有文化中心）
205	莱茵居委会	翔殷路 500 弄 37 号底楼
206	翔殷路 491 弄居委会	翔殷路 491 弄 43 号底层
207	消防支队翔殷中队	翔殷路 354 号 1 层
208	洪东居委会	翔殷路 309 弄 42 号
209	梅林居委会	翔殷路 280 弄 20 号 2 楼
210	星云苑居委会	翔殷路 258 弄 55 号
211	五角场社区卫生服务中心	武东路 9 号
212	武东居委会	武川路 103 号二楼
213	市政水务管理事务中心	五角场政通路 168 号 4 楼
214	社会工作党委	未知
215	创智坊居委会（筹）	伟康路 129 号
216	长白街道图们路社区睦邻点	图们路 5 号
217	长白街道老乐汇社区睦邻中心	图们路 10 弄 8 号
218	长白养老服务中心（新地址）	图门路 10 弄 7 号第三间
219	同济新村居委会	同济新村合作楼 1 号
220	沪东工人文化宫分会场	通北路 540 弄 3 楼
221	嘉禄居委会	通北路 517 号
222	平凉路派出所	通北路 1 号一楼户籍窗口
223	铁岭路 90 弄居委会	铁岭路 90 弄 15 号 101 室
224	铁岭路 50 弄居委会	铁岭路 50 弄 51 号 101 室

225	四平社区卫生服务中心	铁岭路 39 号
226	鞍山一村第一居委会	铁岭路 28 弄 9 号 101 室
227	波阳居委会	腾越路 465 弄 11 号
228	杨浦区中心医院	腾越路 450 号
229	江浦街道大连路睦邻中心	唐山路 1099 弄 2 号楼
230	大连路居委会	唐山路 1099 弄 1 号 106 室
231	华庭香景园居委（筹）	绥中路 68 弄 4 号
232	四平路派出所	苏家屯路 9 号一楼户籍办公室
233	鞍山四村第三居委会	苏家屯路 29 弄 4 号
234	公安出入境	淞沪路 605 号办证大厅 5 号窗口
235	就促五角场分中心	淞沪路 605 号 4 楼
236	加州水郡居委会（筹）	淞沪路 1888 弄 3 号 1 楼
237	松花江路 95 弄居委会	松花江路 95 弄 9 号-7 临
238	民政局社会福利院	松花江路 55 弄 5 号
239	杨浦区房屋维修应急中心	松花江路 388 号
240	松花江路居委会	松花江路 337 号 105 室
241	长白社区卫生服务中心	松花江路 15 号
242	控江城管中心	松花江路 1150 号二楼
243	控江城运中心	松花江路 1150 号 4 楼
244	五角场街道城运中心、	四平路 2500 号京岛大厦 22 楼
245	五角场街道社区平安办	四平路 2500 号京岛大厦 22 楼
246	五角场街道社区管理办	四平路 2500 号京岛大厦 22 楼
247	四平居委会	四平路 2065 弄 18 号二楼
248	和乐苑居委会	顺平路 60 弄 4 号 303 室
249	定海路街道第一睦邻中心	顺平路 59 弄 22 号楼 4 楼
250	和润苑居委会	顺平路 59 弄 22 号 301 室
251	延吉新村派出所	水丰路 385 号一楼户籍窗口
252	延吉社区卫生服务中心	水丰路 383 号
253	环境监测站	水丰路 107 号
254	闸殷路第一居委会	水电新村 8 号
255	双阳居委会	双阳一村 36 号 101 室
256	双花居委会	松花江路 1070 号
257	老年护理医院	双阳路 488 号（控江医院内）
258	控江医院	双阳路 480 号
259	控江一村居委会	双阳路 426 号/控江路 980 弄 8 号二楼（两个地址都是）
260	纪委、监委 1、巡察办（巡查组）	双阳路 393 号 3 楼
261	巡察办（巡查组）	双阳路 393 号
262	机管局后勤负责（国安）	双阳路 357 号
263	幸福村居委会	双阳路 300 弄 29 号 101 室
264	香阁丽苑居委会	双阳北路 395 弄 54 号甲
265	黄兴花园居委会	双阳北路 288 弄 103 号(1 楼半)
266	张家浜居委会	双辽支路 65 弄 3 号 103 室
267	陈家头第三居委会	双辽支路 60 弄 23 号 107 室
268	陈家头第二居委会	双辽新村 19 号 1 楼
269	江浦街道陈家头睦邻中心	双辽新村 16-17 号
270	陈家头第一居委会	双辽路 200 弄 35 号甲
271	消保委	舒兰路 90 号 5 楼

272	舒兰路居委会	舒兰路 61 弄 10 号 101 室
273	卫生健康教学基地	舒兰路 51 号
274	市光一村第二居委会	市光一村 50 号 101 室
275	市光一村第一居委会	市光一村 3 号 103 室
276	市光一村第三居委会	市光一村 105 号
277	市光四村第二居委会	市光四村 65 号 101 室
278	殷行街道社区党群服务中心	市光四村 56 号
279	市光四村第三居委会	市光四村 3 号 102-103 室
280	市光四村第一居委会	市光四村 103 号 103 室
281	市光三村第一居委会	市光三村 50 号 101 室
282	市光三村第二居委会	市光三村 179 号 103 室
283	殷行街道社区党群服务中心	市光三村 164 号
284	市东医院	市光路 999 号 2 号楼 6 楼
285	殷行街道营商办（和开鲁一村居委同地址）	市光路 988 号
286	市光路第二居委会	市光路 60 弄 30 号甲
287	市光二村第二居委会	市光二村 23 号 103 室
288	市光二村第一居委会	市光二村 13 号
289	市光二村第三居委会	市光二村 108 号 201 室
290	市京一村居委会	世界路 91 弄 4 号 104 室
291	世界居委会	世界路 15 弄 43 号 101 室
292	消防支队国和中队	世界路 118 号 1 层
293	长海街道世界路残联	世界路 107 号
294	三门社区睦邻中心 3	上海市三门路 358 弄 36 号甲
295	三门社区睦邻中心 2	上海市三门路 358 弄 27 号甲
296	五角场街道蓝天社区睦邻中心	上海市黄兴路 2053 弄社区活动中心 3 楼
297	长海养老服务中心	三门路 88-90
298	市光路第三居委会	三门路 36 弄 4 号 101 室
299	三门路居委会	三门路 358 弄 26 号 103 室
300	五角场街道仁德社区睦邻中心	仁德路 67 弄 10 支弄 42 号
301	仁德居委会	仁德路 148 弄 4 号 101 室
302	文化花园居委会	仁德路 100 弄 10 号
303	虬江居委会	虬江码头路 1 弄 6 号 101 室
304	锦杨苑居委会	齐齐哈尔路 598 弄 38 号 101 室
305	公证处 1（总部）	平凉路 852 号 5 楼
306	司法局法律援助非诉讼中心（医疗调节办）	平凉路 852 号 1 楼机房
307	人力资源和社会保障局结算中心	平凉路 790 号（780 号也是）
308	应急局 4 个科（协调、监察、自然灾害、应对、应急办）	平凉路 700 号 5 楼
309	绿容局规划发展科	平凉路 700 号 4 楼
310	绿容局市容管理科	平凉路 700 号 4 楼
311	绿容局结算中心	平凉路 700 号 4 楼
312	人力资源和社会保障局专项办	平凉路 700 号 4 楼
313	信访办	平凉路 700 号 1、2、3、6 楼
314	牙病防治所新所	平凉路 337 号
315	平凉社区卫生服务中心	齐齐哈尔路 828 号
316	十九棉居委会	平凉路 2767 弄 8 号

317	定海路街道第五睦邻点	平凉路 2767 弄 8 号
318	民防工程管理所（抗灾救灾工作站）	平凉路 2691 号（老党校）
319	定海人口普查经济普查	平凉路 2595
320	白洋淀居委会	平凉路 2545 弄 22 号 105-107 室
321	近胜里（福禄）居委会	平凉路 245 弄 6 号 105 室
322	城管执法局	平凉路 2158 号
323	公安老大楼（档案室）	平凉路 2049 号 4 楼
324	公安老大楼（信访办）	平凉路 2049 号 4 楼
325	公安老大楼（治安）	平凉路 2049 号 4 楼
326	公安老大楼（网安）	平凉路 2049 号 4 楼
327	公安老大楼（经侦）	平凉路 2049 号 4 楼
328	公安老大楼（交警）	平凉路 2049 号 4 楼
329	公安新大楼（收发室）	平凉路 1958 号 A 楼 2 楼
330	公安新大楼（指挥大厅）	平凉路 1958 号 A 楼 2 楼
331	公安新大楼（政治处）	平凉路 1958 号 A 楼 2 楼
332	公安新大楼（法制支队）	平凉路 1958 号 A 楼 2 楼
333	公安新大楼（数据科）	平凉路 1958 号 A 楼 2 楼
334	牙病防治所总院	平凉路 1814 号
335	杨家宅居委会	平凉路 1782 弄 43 号甲
336	大桥街道居家养老服务中心	平凉路 1759 号
337	大桥街道社区事务受理服务中心、党群服务中心	平凉路 1730 路
338	大桥街道社区党群服务中心	平凉路 1730 号三楼
339	东宫 2 号楼 5 楼社保（公安外来人口、路通科研数码、社保） 杨浦公安分局人口办（下属上海路通技研数码图像有限公司）	平凉路 1398 号 5 楼 502 室
340	东宫	平凉路 1500 号
341	杨浦区投资服务发展中心二分中心	长阳路 2555 号 1 幢裙房 1 层西侧、2 层西侧
342	商贸集团	平凉路 1398 号 3 楼 302
343	平眉居委会	平凉路 1157 弄 21 号 102 室
344	杨浦区退役军人事务局（7 所）	盘山路 3 弄 3 号 101 室
345	引翔港居委会	宁武路 636 号
346	公安交警 3	宁国路 58 号车驾管窗口
347	公安交警 2	宁国路 19 号事故科首问接待窗口
348	环境发展公司（垃圾清运）	宁国路 129 号 6 楼
349	采购中心	宁国路 129 号 16 楼
350	民防办指挥信息保障中心	宁国路 129 号 15 楼
351	杨浦建筑业管理事务中心 1	宁国路 129 号 11、12、13 楼
352	杨浦区文化和旅游事务管理事务中心 2	宁国路 121 号 17 楼
353	杨浦建筑业管理事务中心 2	宁国路 129 号 11、12、13 楼
354	杨浦建筑业管理事务中心 3	宁国路 129 号 11、12、13 楼
355	规划和自然资源局（执法大队）	宁国路 121 号 14、15、16 号
356	规划和自然资源局（信息中心）	宁国路 121 号 14、15、16 号
357	规划和自然资源局（地名中心、土储中心）	宁国路 121 号 14、15、16 号
358	民星一村第一居委会	嫩江路 839 弄 5 号 104 室
359	内江新村居委会	内江一村 40 号
360	内江大楼居委会	内江路 488 号
361	内江路 384 弄居委会	内江路 384 弄 31 号二楼

362	消防支队内江中队	内江路 202 号
363	爱国二村第二居委会	内江路 168 弄 7 号 101 室
364	城市废弃物管理所	内江路 161 号
365	定海路派出所	内江路 158 号一楼综合窗口
366	生态环境局执法大队	内江二村 9 号
367	延吉街道外口办公室	内江二村 21 号 101~102 室
368	民治路居委会	民治路 12 弄 41 号二楼
369	民星二村居委会	民星二村 36 号 103 室
370	民京路第一居委会	民京路 823 号甲
371	长海街道民京路残联	民京路 823 号甲
372	民庆家园居委会	民京路 658 弄 15 号 101 室
373	杨浦区投资服务发展中心六分中心 分点 2	民府路 529 号 1 楼
374	政青路居委会	民府路 1279 号
375	市光居委会	民府路 100 号
376	金安居委会	密云路 528 弄 1 号 105 室
377	四平街道密云路社区睦邻中心	密云路 460 号
378	卫生计生委监督所	眉州支路 78 号 2 号楼 4 楼
379	卫健委	眉州支路 78 号
380	大桥街道未成年人保护工作站	眉州路 988 弄 2 号楼 102 室（东田公寓）
381	大桥城运中心	眉州路 896 号
382	中王家宅居委会	眉州路 888 弄 2 号 101 室
383	大桥街道办	眉州路 871 号
384	河间路居委会	眉州路 515 弄 60 号 102 室
385	新华里居委会	眉州路 381 号 406 室
386	永安里居委会）	眉州路 272 号 2 楼
387	中医医院	眉州路 185 号
388	大桥街道眉州路社区睦邻中心	眉州路 131-133 号
389	渭南居委会	眉州路 100 弄 10 号 101 室
390	老干部局	隆昌路 777 号
391	绿容局景观所、绿容局受理中心	隆昌路 701 号 3 号楼
392	城管机动执法中队	隆昌路 701 号
393	投促办	隆昌路 690 号 2、3 楼
394	科学技术委员会、信息委	隆昌路 690 号 1 楼
395	科学技术委员会、知识产权	隆昌路 690 号 1 楼
396	绿化管理事务中心	隆昌路 677 号
397	定海街道外来人口办	隆昌路 58 号
398	定海城运中心	隆昌路 56 号
399	东白林寺居委会	隆昌路 468 弄 5 号 101 室
400	平凉路街道社区党群服务中心	龙江路 83 号
401	兰州居委会	龙江路 317 弄 11 号 2 楼
402	平凉路街道社区第一睦邻中心	龙江路 2 号
403	大桥城管中心	临青路 66 号三楼
404	富禄里居委会	临青路 66 号 107 室
405	银河苑居委会	临青路 663 号 2 楼
406	文化执法大队	临青路 565 2 楼
407	新华医院科研（上联新华医院）	临青路 430 号园区 3 号楼 2 楼弱电间

408	锦州湾路居委会	临青路 391 号
409	临青路居委会	临青路 365 号
410	周家牌路居委会	金凤大楼 平凉路 1550 弄 2 号 101 室
411	五环	辽源一村 9 号 101-108 室（五环新地址）
412	恒阳花苑居委会	辽源西路 230 弄 17 号二楼
413	江浦街道辽源西路睦邻中心	辽源西路 190 弄 6 号
414	江浦路街道外口办	辽源四村 37 号甲
415	江浦路街道平安办	辽源四村 37 号甲
416	江浦路街道司法所	辽源四村 37 号甲
417	辽源四村居委会	辽源四村 14 号 101 室
418	辽源三村居委会	辽源三村 18 号 101-103 室
419	江浦路街道社区党群服务中心	辽阳路 520 号
420	定海街道残联（新地址）	黎平路 7 号
421	金鹏居委会	兰州路 1151 弄 1 号 101-102 室
422	医疗保障局	兰州路 1118 号 2 楼机房
423	税务局	昆明路 572 号荣广商务中心 B 区 4 楼
424	江浦路街道房屋管理办事处	昆明路 1274 号
425	控江西三村居委会	控江西三村 104 号 2-4 室
426	控江五村居委会	控江五村 106 号 101 室
427	控江四村第一居委会	控江四村 28 号临-1
428	控江四村第二居委会	控江四村 150 号甲
429	控江七村居委会	控江七村 13 号 101 室
430	杨家浜居委会	控江路 888 弄 15 号甲底楼
431	延吉平安办	控江路 650 弄 15 号
432	控江路 645 弄居委会	控江路 645 弄 19 号底楼
433	延吉街道延吉社区第二睦邻中心	控江路 600 号 B 栋
434	第一康复医院分院	控江路 25 号
435	和平花苑居委会	控江路 2202 号 E 座 205-206 室
436	四平街道残联	控江路 2026 弄 9 号
437	四平街道劳动监察	控江路 2026 弄 32 号
438	控江路 18 弄居委会	控江路 18 弄 6 号 101-103 室
439	同济绿园居委会	控江路 1888 弄 25 号 101 室
440	控江路就促中心	控江路 1777 号
441	鞍山一村第三居委会	控江路 1670 弄 26 号 101-103 室
442	新华医院本部	控江路 1665 号科技楼（25 号楼）6 楼机房
443	新华医院影像（上联新华医院）	控江路 1665 号科技楼（25 号楼）6 楼机房
444	政协	控江路 1535 号 2 号楼 1F 弱电机房
445	凤新居委会	控江路 1505 弄 45 号 103 室
446	新凤城居委会居委会	控江路 1500 弄 92 号 101 室
447	控江路 121 弄居委会	控江路 121 弄 20 号
448	控江路 1197 弄居委会	控江路 1197 弄 15 号 101 室
449	望春花居委会	控江六村 31 号一楼
450	控江路 1200 弄居委会	控江二村 65 号底楼

451	控江二村 107 弄居委会	控江二村 107 弄 34 号丙底楼
452	控江东三村居委会	控江东三村 54 号 1-3 室
453	开鲁一村居委会	开鲁一村 3 号
454	开鲁五村居委会	开鲁五村 38 号 101-102 室
455	殷行城管中心	开鲁四村 5 号
456	开鲁四村居委会	开鲁四村 26 号 104 室
457	开鲁三村居委会	开鲁三村 66 号 101-103 室
458	工农二村第三居委会	开鲁路 382 弄 52 号 101 室
459	殷行街道睦邻中心	开鲁路 333 号
460	工农二村第四居委会	开鲁路 320 弄 18 号 102 室
461	开鲁六村居委会	开鲁六村 16 号 101 室
462	开鲁二村居委会	开鲁二村 12 号 104-105 室
463	长白新村城管中心	军工路 915 号
464	精神卫生中心	军工路 585 号
465	上理居委会	军工路 516 弄 210 号-1
466	复兴岛居委会	军工路 400 弄 6 号 101 室
467	军工路居委会	军工路 339 弄周家小区 4 号 101 室
468	控江街道控江社区睦邻中心（多部门、司法所 2、居家养老）	靖宇南路 99 弄 16 号
469	控江路街道残联	靖宇南路 5 弄 5 号
470	欣辉居委会	靖宇南路 118 弄 12 号 104 室
471	安图新村居委会	靖宇东路 85 弄 6 号 102-103 室
472	长白街道靖宇东路社区睦邻中心	靖宇东路 76-80 号
473	长白街道靖宇大楼社区睦邻点	靖宇东路 75 号地下室
474	长白新城居委会	靖宇东路 58 弄 29 号一层
475	长白新村街道司法所	靖宇东路 57 号-59 号
476	长白新村街道安监站	靖宇东路 55 弄 10 号 2 楼
477	长白新村街道办	靖宇东路 27 号
478	档案	靖宇东路 269 号 3 楼
479	延吉新村街道图书馆	靖宇东路 269 号 2 楼
480	杨浦区投资服务发展中心三分中心	靖宇东路 265 号 6 楼
481	杨浦总工会职工服务中心（10M）D330-104	靖宇东路 118 号
482	新时代文明实践中心	荆州路 151 号地下一层（大连路长阳路口），东南第一间，珍宝馆边上
483	国歌展示馆	荆州路 151 号地下一层（大连路长阳路口）
484	四平路街道办	锦西路 69 号
485	四平街道居家养老服务中心	锦西路 57 号 1 层
486	尚浦名邸居委会（筹）	江湾城路 88 弄 1 号 5 楼
487	上海院子居委（筹）	江湾城路 399 弄 192 号(会所 1 楼)
488	杨浦区文化馆	江湾城路 399 弄 190 号
489	橡树湾居委会	江湾城路 1299 弄 70 号 1 楼
490	江浦路就促中心	江浦路 728 号 2 楼机房
491	退役军人服务中心	江浦路 696 号
492	万新居委会	江浦路 666 弄 16 号 101 室
493	杨浦区科技和信息化中心	江浦路 627 号 31 幢 401 室
494	杨浦区委宣传部（文明办）	江浦路 627 号 31 幢 301 室

495	杨浦区司法所（行政复议局）	江浦路 627 号 24 幢 203 室
496	信创数据中心	江浦路 549 号 6 楼
497	兰州新村居委会	江浦路 1424 弄 18 号
498	星泰居委会	江浦路 1100 弄 19 号甲
499	金上海居委会	江浦路 1057 弄 17 号 101 室
500	杨浦区退役军人事务局（服务管理中心）	佳木斯路 317 号-3
501	长海街道佳木斯路残联	佳木斯路 315 弄 7 号
502	长海街道营口社区睦邻中心	佳木斯路 315 弄 7 号
503	佳木斯路 315 弄居委会	佳木斯路 315 弄 14 号乙
504	中农新村居委会	佳木斯路 191 弄 1 号(东面)
505	佳木斯路居委会	佳木斯路 110 弄 11 号 103 室
506	平凉路街道仲裁巡回庭	济宁路 367 号
507	劳动保障事务所（工伤）、退管	济宁路 363 号
508	财政局会计中心	济宁路 252 号门面
509	红十字会事务中心	济宁路 252 号门面
510	杨浦区党建服务中心	济宁路 252 号 C 座 102 室
511	退役军人事务局	济宁路 252 号 A 座 6 楼
512	创全办	济宁路 252 号 A 座 4 楼(婚姻楼上)
513	杨浦区融媒体中心	济宁路 252 号 A 座 4 楼
514	价格认证中心	济宁路 252 号 7 幢
515	统计局普查中心	济宁路 252 号 7 幢
516	妇幼保健所婚前检查	济宁路 252 号 1 楼民政机房
517	民政局养老服务发展中心、财务结算中心、婚姻(收养）登记中心、救助中心、区居家养老服务中心	济宁路 252 号 1 楼、2 楼、3 楼、5 楼
518	秦家弄居委会	济宁路 252 号
519	机管局车队办公室	济宁路 201 号
520	五角场社区事务受理中心 分 1	纪念路 8 号 5 号楼 107 室
521	吉浦居委会	吉浦路 395 弄 16 号 101 室
522	吉浦路第一居委会	吉浦路 375 弄 37 号 202 室
523	五角场街道城运第一工作站	吉浦路 276 号(吉浦路武东路路口)
524	平凉路街道司法所	吉林路 56 号
525	平凉路街道办	吉林路 1 号
526	平凉路街道社区事务受理服务中心	吉林路 18 号
527	平凉路街道社区事务受理服务中心（残联）	霍山路 750 号 101 室
528	平凉城管中心	霍山路 1225 号
529	霍新居委会	霍山路 1191 弄 2 号
530	平凉路街道社区第二睦邻中心	霍山路 1058 号二楼
531	民防信息指挥保障中心	惠民中学一楼及地下室
532	五角场街道城综资中心第一工作站	吉浦路 276 号(吉浦路武东路路口)
533	市场监督管理局 1（含酒类）	惠民路 800 号 3 号楼 8、9、10 楼
534	市场监督管理局 2（含酒类）	惠民路 800 号 3 号楼 8、9、10 楼
535	市场监督管理局 3（含酒类）	惠民路 800 号 3 号楼 8、9、10 楼
536	国家保密局	惠民路 800 号 3 号楼 6 楼
537	纪委临时小组	惠民路 800 号 3 号楼 408 室
538	大数据中心	惠民路 800 号 3 号楼 3 楼
539	会务	惠民路 800 号 3 号楼 3 楼
540	文印	惠民路 800 号 3 号楼 3 楼

541	宣传部	惠民路 800 号 3 号楼 20 楼
542	新闻出版和电影管理办公室	惠民路 800 号 3 号楼 20 楼
543	文明办	惠民路 800 号 3 号楼 20 楼
544	政法委员会 1	惠民路 800 号 3 号楼 19 楼、5 楼
545	政法委员会 2	惠民路 800 号 3 号楼 19 楼、5 楼
546	规范和处理邪教问题领导小组办公室	惠民路 800 号 3 号楼 19 楼
547	党史研究室（区地方志办公室）	惠民路 800 号 3 号楼 18 楼
548	统计局	惠民路 800 号 3 号楼 16 楼
549	区级机关工作委员会	惠民路 800 号 3 号楼 1609 室
550	发展和改革委员会 1	惠民路 800 号 3 号楼 16、17 楼
551	发展和改革委员会 2	惠民路 800 号 3 号楼 16、17 楼
552	杨浦区总工会 1	惠民路 800 号 3 号楼 14、18 楼
553	杨浦区总工会 2	惠民路 800 号 3 号楼 14、18 楼
554	人力资源和社会保障局 1	惠民路 800 号 3 号楼 14、15 楼
555	人力资源和社会保障局 2	惠民路 800 号 3 号楼 14、15 楼
556	红十字会办公室	惠民路 800 号 3 号楼 13 楼
557	组织部 1	惠民路 800 号 3 号楼 13、21 楼、5 楼
558	组织部 2	惠民路 800 号 3 号楼 13、21 楼、5 楼
559	组织部 3	惠民路 800 号 3 号楼 13、21 楼、5 楼
560	民政局	惠民路 800 号 3 号楼 12 楼
561	绿化和市容管理局	惠民路 800 号 3 号楼 11 楼
562	团委	惠民路 800 号 3 号楼 10 楼
563	地区办 1	惠民路 800 号 3 号楼 10、13 楼
564	地区办 2	惠民路 800 号 3 号楼 10、13 楼
565	机关事务管理局	惠民路 800 号 3 号楼 7 楼
566	合作交流办（接待办）	惠民路 800 号 3 号楼 14 楼
567	政务外网区政府业务测试线路 PON1	惠民路 800 号 318 机房
568	民防办公室 1	惠民路 800 号 2 号楼 9 楼、6 楼、7 楼
569	民防办公室 2	惠民路 800 号 2 号楼 9 楼、6 楼、7 楼
570	民防办公室 3	惠民路 800 号 2 号楼 9 楼、6 楼、7 楼
571	文化和旅游局	惠民路 800 号 2 号楼 8 楼
572	妇联 1	惠民路 800 号 2 号楼 8、9 楼
573	妇联 2	惠民路 800 号 2 号楼 8、9 楼
574	应急管理局（局长、危化科）	惠民路 800 号 2 号楼 7 楼
575	区政府财政机房	惠民路 800 号 2 号楼 6 楼
576	商务委 1	惠民路 800 号 2 号楼 20、21 楼
577	商务委 2	惠民路 800 号 2 号楼 20、21 楼
578	司法局 1	惠民路 800 号 2 号楼 19、20 楼
579	司法局 2	惠民路 800 号 2 号楼 19、20 楼
580	财政局 1	惠民路 800 号 2 号楼 17、18 楼
581	财政局 2	惠民路 800 号 2 号楼 17、18 楼
582	金融办	惠民路 800 号 2 号楼 16 楼
583	重大办	惠民路 800 号 2 号楼 16 楼

584	建管委 1	惠民路 800 号 2 号楼 15、16 楼
585	建管委 2	惠民路 800 号 2 号楼 15、16 楼
586	科学技术委员会	惠民路 800 号 2 号楼 14 楼
587	审计局	惠民路 800 号 2 号楼 13 楼
588	规划和自然资源局	惠民路 800 号 2 号楼 12 楼
589	生态环境局	惠民路 800 号 2 号楼 11 楼
590	国有资产监督管理委员会 1	惠民路 800 号 2 号楼 10 楼、7 楼
591	国有资产监督管理委员会 2	惠民路 800 号 2 号楼 10 楼、7 楼
592	体育局 1	惠民路 800 号 2 号楼 10、11 楼
593	体育局 2	惠民路 800 号 2 号楼 10、11 楼
594	机关事务管理局 1	惠民路 800 号 2 号楼 1，2，3，4，5 楼
595	机关事务管理局 2	惠民路 800 号 2 号楼 1，2，3，4，5 楼
596	机关事务管理局 3	惠民路 800 号 2 号楼 1，2，3，4，5 楼
597	机关事务管理局 4	惠民路 800 号 2 号楼 1，2，3，4，5 楼
598	机关事务管理局 5	惠民路 800 号 2 号楼 1，2，3，4，5 楼
599	市场监督管理局（含酒类）	惠民路 800 号（上联区政府 OLT）
600	平凉养老服务中心	惠民路 702 号 3 楼
601	控江路街道社区事务受理服务中心	黄兴路 572 号
602	税务局	黄兴路 402 号
603	杨浦区退役军人事务局（2 所）	黄兴路 2053 弄 158 号底楼
604	杨浦区退役军人事务局（6 所）	黄兴路 2053 弄 151 号底楼
605	蓝天居委会	黄兴路 2053 弄 社区活动中心
606	司法局大桥司法所（大桥公共法律服务工作站）	黄兴路 156 号底楼
607	黄兴居委会	黄兴路 1019 弄 10 号底楼
608	浣纱四村居委会	浣沙四村 52 号甲
609	浣纱三村居委会	浣沙三村 25 号
610	消防支队江浦中队	怀德路 928 号
611	民政局福利院一分院	怀德路 802 号
612	行政服务中心(行政服务大厅/行政事务受理中心)	怀德路 549 号
613	平凉街道禁毒办	怀德路 366 弄 12 号 1 层
614	上水工房居委会	怀德路 191 号
615	世纪江湾居委会	恒耀路 66 弄 19 号楼 1 层居委会
616	西白林寺第二居委会	河间路 850 号
617	水月坊居委会	河间路 688 弄 5 号 3 楼
618	检察院	河间路 31 号
619	法院 1	河间路 29 号
620	大桥街道社区服务办	河间路 237 号 C 栋一层（碧桂园中心）
621	隆昌居委会	杭州路 899 号
622	广杭居委会	杭州路 66 弄 35 号
623	第一康复医院	杭州路 349 号 4 号楼 1 楼机房
624	东郸居委会	邯郸路 500 弄 6 号
625	中建大公馆居委（筹）	国秀路 181 弄物业楼 301

626	九龙仓玺园居委（筹）	国晓路 500 弄 28 号 101 室
627	国伟新苑居委会（筹）	国伟路 500 弄 4 号楼 204 室
628	城市庭院居委会	国伟路 138 弄 25 号
629	城市方园居委会	国伟路 100 弄 2 号 102-103 室
630	南茶园居委会	国顺路 81 弄 35 号
631	北茶园居委会	国顺路 80 弄 35 号
632	国年居委会	国顺路 389 弄 18 号甲
633	武装部	国顺东路 9 号
634	汇元坊居委会	国顺东路 900 弄 27 号 102
635	长海路街道浣纱睦邻中心	国顺东路 55 弄 5 号
636	院士风采馆	国顺东路 369 号
637	国顺东路 26 弄居委会	国顺东路 26 弄 46 号 101 室
638	浣纱六村居委会	国顺东路 243 弄 6 号
639	黄兴绿园居委会	国顺东路 179 弄 31 号 102 室
640	五角场派出所	国权路 86 号户籍窗口
641	国权路第一居委会	国权路 85 弄 6 号 102 室
642	航天居委会	国权路 336 弄 12 号 1 层
643	国顺居委会	国权路 230 弄 11 号
644	文化佳园居委会	国权东路 99 弄 20-21 号
645	长海街道文化佳园睦邻中心	国权东路 20-21 号
646	尚景园居委会（筹）	国权北路 1450 弄 37 号 2 楼
647	祥生泰宝居委（筹）	国权北路 1188 弄 85 号 101 室
648	国和一村第二居委会	国和一村 90 号 101 室
649	国和一村第三居委会	国和一村 60 号 102 室
650	国和一村第一居委会	国和一村 16 号 101 室
651	东方名城居委会	国和路 888 弄 52 号 102 室
652	国和路第一居委会	国和路 611 弄 61 号底楼
653	上海体院居委会	国和路 555 弄 5 号 101 室
654	杨浦区投资服务发展中心七分中心	国和路 465 号
655	长海街道社区事务受理服务中心	国和路 425 号
656	环岛治安派出所	国和路 40 号一楼治安接待大厅
657	公安交警 1	国和路 1047 号非机动车管理所窗口
658	殷行街道社区事务受理服务中心	国和路 1047 号
659	牙防所国和路分院	国和路 1045 号 1 层机房 U1
660	杨浦区检察院公益监察室（装修五角场街道）	国和路 100 号
661	国和二村第三居委会	国和二村 53 号 101 室
662	国和二村第一居委会	国和二村 140 号 101 室
663	国和二村第二居委会	国和二村 116 号 101 室
664	新江湾城街道社区党群服务中心	国浩路 173 号
665	五一居委会	国定路 601 弄 1 号 104 室
666	铁路新村居委会	国定路 277 弄 6 号甲
667	消防支队国定中队	国定路 146 号 1 层
668	国定路就促中心	国定东路 200 号 1 号楼 3 楼
669	国权居委会	国达路 8 号
670	国安路第一居委（筹）	国安路 791 号
671	国安路第二居委（筹）	国安路 518 号 2 楼
672	广远新村居委会	广远新村 69 号

673	军工路转型领导小组办公室	共青路 430 号 4 楼
674	工农四村第一居委会	工农四村 150 号 101 室
675	工农四村第二居委会	工农四村 103 号 104 室
676	工农三村第一居委会	工农三村 25 号 103-104 室
677	工农三村第三居委会	工农三村 156 号 101 室
678	工农三村第二居委会	工农三村 119 号 101 室
679	鞍山路 310 弄居委会	阜新路 284 弄 5 号 101 室
680	鞍山四村第二居委会	阜新路 182 弄 8 号甲
681	公交新村居委会	阜新路 169 弄 12 号 101 室
682	鞍山四村第一居委会	抚顺路 373 弄 1 号 104-105 室
683	四平街道抚顺路社区睦邻中心	抚顺路 370 弄
684	抚顺路 363 弄居委会	抚顺路 363 弄 4 号楼底楼
685	四平路街道社区党群服务中心	抚顺路 360 号一楼
686	四平路街道社区党群文化中心	抚顺路 360 号一楼
687	教育局信息中心、进修学院	抚顺路 340 号（另一个门铁岭路 109 号）
688	控江街道控江社区抚顺路睦邻点	抚顺路 161 号
689	四平城运中心（城运）	抚顺 378 号 3 楼
690	四平城运中心（平安办）	抚顺 378 号 3 楼
691	四平城运中心（司法所）	抚顺 378 号 3 楼
692	凤南居委会	凤南一村 56 号
693	抚岭居委会	凤城五村 21 号 101 室
694	凤城三村第二居委会	凤城三村 80 号底楼
695	凤城三村第四居委会	凤城三村 142 号 103 室
696	区政法委青少年禁毒	凤城六村 1 号 205、206
697	凤城二村第二居委会	凤城二村 91 号 102 室
698	凤城二村第一居委会	凤城二村 27 号 101 室
699	辽源新村居委会	飞虹路 740 号 103 室
700	江浦路派出所	飞虹路 737 号一楼户籍窗口
701	海上海居委会	飞虹路 600 弄 7 号 103 室
702	敦化路居委会	敦化路 2 弄 27 号甲
703	定海居委会	定海路 449 弄 4009 号
704	定海港路居委会	定海港路 363 号二楼
705	平凉城运中心	丹阳路 188 弄 4 号（新地址）
706	密云路居委会	大连西路 30 弄 29 号 104 室
707	吴家浜居委会	大连路 848 弄 5 号 101 室
708	江浦社区事务受理中心分点	大连路 588 号 B 座 1 楼（宝地广场）
709	消防支队大连中队	大连路 1202 号 1 层
710	辽源一村居委会	大连路 1184 号
711	江浦城管（新）	大连路 1166 号 1 楼
712	辽源二村第一居委会	打虎山路 8 号
713	控江路 2026 弄居委会	打虎山路 84 弄 2 号底楼
714	就促鞍山分中心	打虎山路 28 号
715	政务控江维护业务测试线路 PON	打虎山路 101 号 5 楼
716	科委控江 4 楼灾备机房	打虎山路 101 号 4 楼
717	电信政务云	打虎山路 101 号 4 楼
718	控江财政灾备托管（上联区政府）	打虎山路 101 号 4 楼
719	区卫健委打虎山路机房	打虎山路 101 号
720	区卫健委打虎山路数据机房	打虎山路 101 号

721	大连西路四弄居委会	赤峰路 59 弄 9 号
722	沧州路 180 弄居委会	沧州路 180 弄 31 号
723	控江路街道社区党群服务中心	沧州路 138 号一楼
724	控江路街道办（含司法所）	沧州路 138 号
725	四平路街道体育健身俱乐部	本溪路 274 号
726	东岸新里居委会（筹）	包头南路 588 弄 14 号
727	殷行街道办	包头路 781 号
728	残联	包头路 756 弄 40 号
729	殷行街道包头路社区睦邻中心	包头路 545 号
730	民星一村第二居委会	包头路 300 弄 10 号
731	城市名园居委会	包头路 1150 弄 15 号 205 室
732	长海街道社区事务受理服务中心（搬迁后点位）	白城南路 18 号
733	鞍山一村第二居委会	鞍山一村 124 号 103 室
734	鞍山五村居委会	鞍山五村 51 号
735	四平街道阜新路社区睦邻中心	鞍山五村 33 号甲
736	四平城管中心	鞍山五村 14 号
737	鞍山三村居委会	鞍山三村 4 号 4 室
738	杨浦投资（控股）集团有限公司	鞍山路 5 号 13 楼
739	四平街道五经普集中办公点(位置在四平路街道协税办内)	鞍山路 219 号（内部光缆调整为 PON，鞍山路 219 号一层）
740	四平路街道社区事务受理服务中心	鞍山路 158 号
741	鞍山六村居委会	鞍山六村 90 号
742	鞍山七村居委会	鞍山六村 39 号甲
743	鞍山八村居委会	鞍山八村 21 号底楼
744	杨浦区投资服务发展中心五分中心	安波路 998 号 3 楼
745	杨浦区退役军人事务局（5 所）	安波路 985 弄 16 号
746	兰新居委会	安波路 706 号 201-206 室
747	海上硕和城	安波路 567 弄 29 号 2 楼
748	融媒体中心	安波路 565 号 4 楼
749	教师公寓居委会	安波路 265 弄 7 号 206 室
750	定海社区卫生服务中心	爱国路 77 号
751	定海城管中心	爱国路 520 号二楼
752	定海街道管理办	爱国路 520 号
753	定海统计站	爱国路 21 号
754	定海协税	爱国路 21 号
755	定海禁毒	爱国路 21 号
756	区政府大院	3 号楼 19 家独立单位 2 号楼 17 家独立单位 1 号楼 3 个独立单位
757	四平路街道房办、营商办、城运中心	铁岭路 38 弄一层机房
758	延吉司法所	双阳路 555 号
759	殷行管理办	开鲁 4 村 5 号
760	人社局信访办	济宁路 252 号街面
761	翔殷路电信营业厅“一网通办”	翔殷路 1015 号创智汇 3 号楼 1 层营业厅
762	打虎山路电信营业厅“一网通办”	打虎山路 101 号 2 楼营业厅
763	长阳创谷驻场办公点	长阳路 1687 号东 1225 幢(A 楼)A503 室
764	城管机动执法中队	凤城四村 8 号
765	一网通办专班	龙江路 2 号
766	紫华居民委员会	双阳路 70 号

767	创安安全服务中心（大桥人口办）	顺平路 1260 号 1 层 11 室（长阳创谷内）
768	长隆居民委员会	隆昌路 611 号 2 楼
769	上海同济科技实业股份有限公司	四平路 1398 号同济联合广场 B 座 20F
770	杨浦国有资产经营有限公司	锦创路 20 号 18 楼
771	五角场街道城运中心分点(临时)	大学路 90 号
772	长阳路联通营业厅&殷行路联通营业厅“一网通办”	惠民路 318 机房
773	移动滨江营业厅“一网通办”	平凉路 897 号
774	光大安石核酸亭“一网通办”	惠民路与荆州路交叉口
775	五角场街道社区党群服务中心 分点	国定支路 24-28 号人人会客厅
776	长海路街道办事处(社区事务受理服务中心档案室)	佳木斯路 2 号
777	馨运居委（筹）	龙口路 2 号 3 楼
778	长海路街道办事处(社区事务受理中心)	闸殷路 1555 号国华广场一楼大厅
779	长阳路 1696 号联通一网通办	长阳路 1696 号，接入长阳路 1841 弄 22 号 101 室双阳路居委
780	控江路 1050 号联通一网通办	控江路 1050 号，接入控江路 888 弄 15 号甲底楼杨家浜居委
781	殷行路 1286 号 A20 商铺联通一网通办	殷行路 1286 号 A20 商铺，接入殷行路 851 号 4 楼东森涵碧居委
782	中原路 140 号联通一网通办	中原路 140 号，接入中原路 99 弄 19 号甲中原路 99 弄居委
783	平凉路街道办事处、营商办公室	惠民路 619 号
784	长阳创谷企业发展有限公司	长阳路 1687 号二期 6 号楼
785	五角场街道社区事务受理服务中心	国庠路 107 号
786	长海路街道办事处（劳动保障服务队）	翔殷路 580 号
787	电信国和路营业厅“一网通办”	国和路 952 号

5.3 服务内容

1)基础设施资源服务：包括机房资源服务、网络资源服务。

2)服务的实施：包括基础设施服务实施、运行保障服务实施。

3)运行保障服务：包括电子政务外网的资源监测、资源配置、资源优化、服务监控、事件处理、运维流程、日常巡检、备份恢复、灾备及高可用管理、应急预案管理、服务质量监督和报告等服务。

4)建立健全配套制度标准。投标企业可提供基于自身平台的相关标准、办法及建议，如：投标人可提供政务外网管理办法、运维制度、应急预案等。

5)建立健全满足政务外网监管需要的配套检测、监管手段（如：流量），及相应监测办法。

二、服务要求

1、业务网组网要求

杨浦区电子政务外网业务网络应满足各接入单位网络汇聚接入及灵活互通的需求，具体要求如下：

1) 业务网络采用核心、汇聚、接入的三层架构设计；

2) 骨干网络核心层和汇聚层采用冗余设计，且分布在不同机房内，设备之间互联线路应承载在 OTN 线路上；

3)核心层设备承担用户流量安全、高速、可靠转发的功能。设备选型应能满足面向未来业务发展平滑扩展的需要；核心节点应不少于 2 个，保证核心网络的高可靠性。每个核心节点应部署不少于两台路由器设备。

4)汇聚节点采用双归方式接入核心节点以提高网络可靠性。汇聚节点向上通过 40～100Gbps 链路连接核心节点，向下通过 N×1Gbps 链路或 N×10Gbps 链路连接区级各部门、街镇和村居。每个汇聚节点部署两台路由器设备，两台设备之间互联链路的带宽应与汇聚节点至核心节点的链路带宽相同。

5)杨浦区政务外网的接入节点通过 N×1Gbps 或 N×10Gbps 链路联接至汇聚节点。各接入单位根据实际情况选择单设备单链路、单设备双链路，或双设备双链路作为上行方式。

6)业务网络的核心、汇聚层应承载于政务外网光传输网络之上；

7)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；

8)应基于 TCP/IP 技术构建政务外网业务网络，采用支持 IPv4/IPv6 双栈技术的网络设备，能同时提供 IPv4 和 IPv6 方式接入服务；

9)业务网络应符合等保 2.0 三级规范的要求；

10)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；

11)应从多个维度考虑设备的安全自主可控，采用国产领先的网络和安全设备、系统。

12)区电子政务外网应设置互联互通安全边界区域，按照《上海市电子政务外网建设和运行管理指南》要求满足和市政务外网对接；对接应满足一网双平面设计需求，视频流量主走视频设备，数据流量主走数据设备，并且满足故障时秒级切换业务，业务采用互为主备设计，边界内网络和安全设备均通过万兆线路互联；

13)区电子政务外网应设置区政务云安全边界区域通过 2*10GE 万兆接入区级政务外网骨干网络，网络设计采用双设备、双线路冗余模式形成高可用保护；

14)区电子政务外网应设置专网接入区域，满足重要委办安全接入，通过 2*10GE 万兆接入区级政务外网骨干网络，网络设计采用双设备、双线路冗余模式形成高可用保护；

15)区电子政务外网应设置互联网出口区域，网络架构采用 2*10GE 万兆接入区级政务外网骨干网络，网络设计采用双设备、双线路冗余模式形成高可用保护；满足区政务外网接入用户访问互联网需求；

16)区电子政务外网应设置无线接入边界区域，按照《上海市电子政务外网建设和运行管理指南》要求满足进行网络设计，满足区内用户采用 5G 网络安全接入；

17)区电子政务外网应设置安全管理边界区域，边界网络需满足和政务外网骨干网络对接，需要管理所有区电子政务外网接入设备的运维管理；

18)区电子政务外网业务网络应满足业务分类，标记，优先级调度，需要通过差分 QOS 完成和市政务外网打通和传递；

19)区电子政务外网接入层应采用全光网络分层设计；在杨浦区内需均匀分布设置不少于 5 个 POP 节点，节点应满足不少于 2*10G 上联区电子政务外网汇聚层网络设备；

20)区电子政务外网管理网络流量和业务网络流量应承载在不同的通道上面，管理网络路由应和业务网络路由独立分开；

21)杨浦区电子政务外网业务网络带宽设计如下：

链路类型	速率
核心节点之间	40～100Gbps
与市电子政务外网之间	N×1Gbps 或 N×10Gbps
核心节点与下级汇聚节点之间	40～100Gbps
同一节点内主备冗余设备之间	40～100Gbps
汇聚节点与下级接入节点之间	N×1Gbps 或 N×10Gbps

2、传输网组网要求

光传输网应具备与现有网络兼容的能力，具体要求如下：

1)采用单波速率 100G 及以上的 OTN 技术；

2)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；

3)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；

4)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；

5)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；

6)支持光纤线路诊断功能，能快速定位光纤线路故障；

7)宜采用 SDN 技术，本项目政务外网的 SDN 控制器与区政务云 SDN 控制器开放 API 接口具备一致性，支持 SNMP、CORBA、RETS、Kafka 协议，接受区政务云协同器统一纳管，满足云网一体化运营需求，实现业务统一配置，对链路的快速下发和调整；

8)应使用 G.652 或 G.655 规格的光缆，光缆的每公里线路衰耗在 0.3dB 以下。

9)核心、汇聚设备出局的传输线路，必须保证 2 个以上不同物理路由。路由器上行和横联链路应避免传输同路由，下行和横联链路应避免传输同路由。

3、网络设备配置要求

网络建设应至少具备如下功能与设备，相关设备参数配置不低于如下数量与标准。

1）核心、汇聚节点设备功能要求：

序号	内容	配置要求	数量（台）
骨干汇聚区			

1	核心路由器	本期单台配置不少于 2 块 2 端口 100GE 板卡,用于核心设备间互联、核心设备和汇聚设备间的互联；配置不少于 1 块 20 口 10GE 板卡，用于各出口安全区域的互联；应满足不少于 8 个业务槽位；含设备安装、集成及维保。	4
2	汇聚路由器	本期需要配置不少于 2 块 2 端口 100GE 板卡,用于核心设备间互联、核心设备和汇聚设备间的互联；同时配置不少于 2 块 20 口 10GE 板卡，用于接入层设备接入；应满足不少于 8 个业务槽位；含设备安装、集成及维保。	4
3	边界路由器	业务板卡采用模块化设计，单板卡不少于 8*10GE 端口，满足三个业务板卡插槽，支持未来 8*10GE 端口扩容能力，支持 FlexE（50G 端口）	12
4	安全汇聚交换机	48*10GE，支持 IP、MAC、端口、VLAN 的组合绑定，支持 MAC 地址过滤、静态、动态、黑洞 MAC 表项、支持 LACP、支持 BFD、支持 VRRP、BFD FOR VRRP，支持 M-LAG、VxLAN。含设备安装、集成及维保	16
5	网管汇聚交换机	48*10GE，支持 IP、MAC、端口、VLAN 的组合绑定，支持 MAC 地址过滤、静态、动态、黑洞 MAC 表项、支持 LACP、支持 BFD、支持 VRRP、BFD FOR VRRP，支持 M-LAG、VxLAN。含设备安装、集成及维保	2
6	机架（专网互通）	19 英寸网络机架，含设备安装、集成及维保	6
7	SNMP 探头服务器	20Core/192G/2*1.2T/RAID/2*10GE+2*GE/Linux，含设备安装、集成及维保	2
8	网络质量服务器	20Core/192G/2*1.2T/RAID/2*10GE+2*GE/Linux，含设备安装、集成及维保	2
9	告警管理服务器	20Core/192G/2*1.2T/RAID/2*10GE+2*GE/Linux，含设备安装、集成及维保	2
10	接口服务器	20Core/192G/2*1.2T/RAID/2*10GE+2*GE/Linux，含设备安装、集成及维保	2
11	应用服务器	20Core/192G/2*1.2T/RAID/2*10GE+2*GE/Linux，含设备安装、集成及维保	4
12	数据库服务器	20Core/192G/2*1.2T/RAID/2*10GE+2*GE/Linux，含设备安装、集成及维保	2
13	SDN 服务器 1	96Core/192G/8*1.2T/RAID/8*GE，含设备安装、集成及维保	2
14	SDN 服务器 2	128Core/512G/12*1.2T/RAID/8*GE+8*10GE，含设备安装、集成及维保	1

15	网管软件	性能状态采集、告警监控、故障诊断、流量采集等功能，含集成及维保	1
16	SDN 软件	基于业务的编排、下发、自动配置控制能力以及网络流量识别、流向自动分析等扩展功能，实现网络资源与业务应用的融合管理，含集成及维保	1
光传输区			
1	核心节点波分设备	配置 6 块 100G 支线路合一业务板卡，配置 100G 波道；设备遵循业界统一标准，低功耗、高集成度，具备 OTN、分组、SDH 交叉功能和多种业务统一承载的能力，采用主备工作电源，选用不同物理路由，设备热备份；单波速率 100G，支持平滑扩容；支持针对业务的 SNCP 保护。含设备安装、集成及维保	2
2	汇聚节点波分设备	配置 4 块 100G 支线路合一业务板卡，扩容 100G 波道；设备遵循业界统一标准，低功耗、高集成度，具备 OTN、分组、SDH 交叉功能和多种业务统一承载的能力，采用主备工作电源，设备热备份；单波速率 100G，支持平滑扩容；汇聚节点与核心节点采用环形组网结构，具备保护能力。含设备安装、集成及维保	1
业务网接入区			
1	OLT	采用 10G EPON OLT，单个 PON 口带宽 10G bit/s 带宽，具备向 50G PON 平滑演进能力。单台 OLT 配置 8 个下联 PON 口和 2 个 10GE 上联口（板卡分隔）。含设备安装、集成及维保	5
2	分光器	等比 1 分 8,含设备安装、集成及维保	35
3	光分纤箱	含设备安装、集成及维保	828
4	接入路由器	支持最大 5*10GE 光口或 8 个 GE 光口，4 个 GE 电口。支持双电源/风扇冗余保护，支持 L2/L3VPN、MPLS TE、H-QoS、GRE、IPv6 等功能特性 ；含设备安装、集成及维保。	35
5	用户侧网关	支持 10G EPON 接入，用户侧提供 8*GE+8*POTS+2.4G&5GWIFI 接入；含设备安装、集成及维保。	787

2)核心路由器、汇聚路由器、边界路由器设备功能要求：

特性	核心路由器	汇聚路由器	边界路由器
接口类型	100GE/40GE/ 10GE	100GE/40GE/ 10GE	10GE
IPv4	IPv4 静态路由 、OSPF 、IS-IS 、BGP 等路由协议， VxLAN 、GRE 等隧道技术		
IPv6	IPv6 静态路由， BGP4+ 、OSPFv3 、IS-ISv6 等动态路由协议， IPv4 over IPv6 隧道和 6PE，NAT444、NAT64，静态 IPv6 DNS，指定 IPv6 DNS 服务器，TFTP，IPv6 client		
MPLS	L2VPN 、L3VPN 、EVPN， LDP LSP 、RSVP-TE 等 MPLS 技术， 宜支持 SR-TE		
SR	宜支持如下 SR 技术： 单域及跨 BGP 域的 Segment Routing 技术，SegmentRouting 与 LDP 混合组网，SR policy 技术，SRv6 承载 VPN 业务，SR 的 TI-LFAFRR 技术， BFD for SR 、BFD for SRv6		

可靠性	BFD 故障探测技术，误码倒换，IP/IPv6/LDP/TE/VPN/VPNv6 FRR 快速重路由， 端口聚合， ECMP 、UCMP， LDP， VRRP， NSR， 关键部件冗余备份， 组件可热拔插， 平滑重启（ GR）， 不中断转发 （NSF）， ISSU
QoS	多级 MPLS H-QoS，MPLS VPN、VLL 和 PWE3 的 QoS 调度，面向 TE 隧道的 QoS
OAM	基于 IP 五元组筛选追踪业务流， 对丢包 、误码类故障进行实时检测，精准定位到故障点； 支持 EFM 、CFM 、Y.1731 、MPLS-TP OAM 技术
其它特性	国密算法， BGP-LS 、PCEP 南向协议； 基于 Telemetry 的大数据分析

4、环境安全要求

杨浦区电子政务外网核心、汇聚机房的供配电系统、空调系统，在防静电、防雷、消防，防水等方面的建设，必须符合《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）的规范要求。

投标人需根据组网需求合理选择网络节点，同时提供汇聚层及以上节点的机房平面布置图。

●·机房选址

政务外网核心、汇聚机房地选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁。核心、汇聚采用两个或两个以上节点配置，且每个节点必须配置 2 台核心、汇聚设备。有条件的区域，宜采用物理地址不同的机房安装核心、汇聚设备。如因条件限制，核心、汇聚设备安装在同一机房，必须保证机房有 2 路（或以上）市电接入，核心、汇聚设备从不同列头柜引电，不同列头柜不使用同一开关。

杨浦区电子政务外网是承载杨浦区电子政务云的传输网络，通过政务外网为各委办局提供统一云服务，实现“云网合一”整体技术架构。投标人提供的核心节点应优先部署在靠近政务云（打虎山路 101 号）的节点，提高时延等网络性能，确保各委办局业务应用稳定可靠运行。

同时，为满足政务外网长期稳定运行的要求，投标人应优先提供自有机房或长期租赁机房作为本次政务外网的网络节点，同时应提供产权证明或相关证明材料。

●·机房管理

政务外网核心、汇聚机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；

●·机房环境

政务外网核心、汇聚机房应合理规划设备安装位置，应预留足够的空间作安装、维护及操作之用。房间装修必需使用阻燃材料，耐火等级符合国家相关标准规定。机房门大小应满足系统设备安装时运输需要。机房墙壁及天花板应进行表面处理，防止尘埃脱落，机房应安装防静电活动地板。

机房安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离；机房设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。应配备空调系统，以保持房间恒湿、恒温的工作环境；在机房供电线路上配置稳压器和过电压防护设备；提供短期的备用电力供应，UPS 应该满足在断电情况下工作 2 小时的运行要求。宜配置冗余或并行的电力电缆线路为计算机系统供电；建立备用供电系统。铺设线缆要求电源线和通信线缆隔离铺设，避免互相干扰。对关键设备和磁介质实施电磁屏蔽。

●·设备与介质管理

政务外网各级机房必须采用有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。

5、扩容服务要求

在日常运维过程中，当电子政务外网接入规模、网络出口或者链路带宽等不满足最终用户使用要求时，投标人需对现有网络进行优化扩容，机房等配套资源扩容由投标人根据实际需求而定。

6、项目实施要求

6.1 网络建设

投标人作为工程实施的主要组织者，需要对工程实施进行组织、协调。包括组织主设备、配套设备、配套材料(设备机柜、抗震机座、电力线、网线、光纤、蛇形套管、交流电源盒等)的采购；提供机房必要的装机条件(包括机房环境、电源、空调等)；负责整个项目实施的组织、协调及管理：制定详细的施工方案，安排、协调工程参与各方的工作，监督管理整个施工方案的执行。组织调测及验收。

投标人提供的电子政务外网组网架构应满足总体架构要求，同时提供详细网络拓扑图，包括节点位置、网元数量、设备配置及性能参数等信息。

6.2 网络割接要求

请投标人针对本次服务内容提供业务割接方案，并且进行工程实施。同时需要提供以下说明：

1)请说明本项目网络割接和调整以及进行相应的工程实施内容。

2)根据网络方案说明各节点的网络割接和调整步骤以及具体工程实施计划,进行相应的工程实施。

3)网络割接调整时需要考虑对在线业务的中断性影响，争取将影响控制在最小，争取平滑割接。配合招标人部署业务应用线路的 IP 地址数量满足割接要求，并能与现有政务云业务应用系统 IP 地址相匹配，不影响招标人业务连续性。

6.3 IPv6

杨浦区电子政务外网业务网络应遵循《推进互联网协议第六版（IPv6）规模部署行动计划》的标准和要求，投标人所提供设备应均支持 IPv4/IPv6 双栈技术及 IPv6 线速转发。全网部署端到端双栈技术实现互通，并启用基于 IPv6 的路由协议。

6.4 QoS

杨浦区电子政务外网的 QoS 总体设计原则如下：

1)采用轻载方式保障网络服务质量，建议链路月平均日峰值利用率不超过 50%；

2)采用 DiffServ 作为网络突发拥塞时 QoS 保证方式；

3)识别用户侧流量，调度重要业务进 PQ 队列，调度普通业务进默认队列尽力转发。

投标人应根据上述原则，结合业务提出详细的 QoS 方案。

6.5 IP 地址

1)投标人应根据网络结构和设备配置，给出本工程 IP 地址需求。

2)投标人应对本工程网络编址提出实施方案，以实现最佳的网络内地址分配及业务流量分布。

6.6 路由协议和路由策略

政务外网路由策略的总体要求为：

1)政务外网应实现业务网络路由和用户路由分离。IGP 负责承载设备之间的互联链路、Loopback、网管等的承载网路由；BGP 和 SRv6 负责承载区政务外网和接入部门网络、数据中心等的用户路由。管理上层次分明，从而避免用户路由震荡影响业务网络路由，保证局部的变动不影响上层路由配置和全局路由配置。

2)区级政务外网业务网络路由和用户路由可以由 IGP 统一承载。当具备条件时，也可以与市级政务外网保持一致，进行业务网络路由和用户路由的分离。

3)路由设计应能反映出整个网络的层次结构，并与自治域、各节点子网的 IP 地址分配相结合，做到合理的路由聚合，减少路由表的长度，减轻路由更新给设备带来的负荷，提高路由稳定性。

4)在同一 AS 内，应根据网络流量分担、分布与路由备份需要，统一规划路由 Metric 值，实现路由策略。

5)合理规划 IGP 区域。对于新建网络，在单管理域设备数量较少时，可以配置为单区域。

投标人应根据上述要求给出详细的路由策略设计。投标人对路由协议的设计要求保证网络的连通性、可达性，路由策略应实现网内流量流向的分担、备份和链路利用的均匀性，同时对于网络维护，路由策略应具备良好的可控性与可维护性。

投标人应给出域内路由协议的链路权值设置方案，并给出网络处于稳定状态时的选路结果。

根据路由组织方案，投标人应给出域间路由协议控制路由分布的实施方案。

投标人的路由策略方案应保证全网具备良好的路由稳定性和可扩展性且易于维护。

6.7 BGP 路由实施

自治域内， 所有 PE 运行 MP-BGP 承载 VPNv4 、VPNv6 和 EVPN 路由， 选取 4 台核心设备兼做路由反射器（ RR） 或设置独立 RR 。骨干层所有 PE 路由器与这四台 RR 建立 IBGP 关系。

不同的 AS 域，需要运行 EBGP 协议，互相通告路由。

6.8 网络安全

本次对杨浦区电子政务外网进行整体继续运营，还需完善配套的电子政务外网安全体系。网络安全系统依据国家《电子政务外网安全建设规范》的思路建设，并符合《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）规范的基本要求。在此基础上，结合当前电子政务外网的安全现状，从安全技术、安全运营管理、安全运维三个方面开展安全运营，打造运营平台化、管理一体化、态势可感知、事件可预警、事故可追溯、安全可闭环的电子政务外网安全体系。整体杨浦区电子政务外网需满足等级保护三级测评的要求。

本次网络安全部分的设计还需满足《上海市电子政务外网建设和运行管理指南》（上海市大数据中心）中对电子政务外网系统网络安全的要求。根据边界划分，安全部分运营服务主要包括互联网访问出口安全、市政务外网互联边界安全、政务云边界安全、其他安全接入区边界安全和专网接入区，并设立安全管理中心。

投标人需在设计中体现“一个中心、多重防护” 即安全管理中心、区域边界安全、通信网络安全等方面通盘考虑方案设计深度和广度，能够满足安全体系在防御、事中、事后三个阶段监测、防御、和追溯。

6.8.1 互联网接入区设计要求

为了保证各级政府部门的移动办公、远程访问、现场执法等业务能安全接入到电子政务外网，也为了保证相关企事业单位和个人能利用公网安全地接入到政务外网，杨浦区政务外网设置互联网访问区域（即互联网出口区）。

互联网访问出口的安全部分运营应至少具备如下功能与设备，相关设备参数配置不得低于如下数量与标准：

互联网出口区			
序号	内容	数量（台）	安全功能要求
1	Anti-DDoS	2	在出口区旁路部署抗 DDoS 攻击设备，针对互联网上的 DDoS 攻击进行有效的防护，支持 DDoS 检测和清洗。抗 DDoS 攻击支持常见的 SYN Flood、ACK Flood、FIN/RST Flood 功能，能抵抗 HTTP、HTTPS Flood 等攻击，并且支持流量自学习功能，可识别出超过防御阈值的攻击流量。
2	防火墙含防病毒	2	在互联网出口区部署防火墙带防毒模块，实现网络边界保护、病毒过滤和访问控制。防火墙只提供接入服务的必需的服务端口，对流经接入平台的网络数据进行合法性检查。所有的进出互联网的数据都将通过防毒模块的扫描，防止病毒文件进入政务外网。为了保证业务的高可用性，防火墙双机部署，支持性能的可扩容。防火墙支持 IPv6 协议栈、NAT64 转换技术。

3	入侵防御 IPS	2	在互联网出口区部署入侵检测防御系统，动态监视网络上所有流过的数据包，进行实时检测和分析，及时发现非法和异常行为，并且支持告警、阻断等功能。
4	沙箱	1	针对 APT 高级持续威胁，利用沙箱多引擎虚拟检测技术，以及传统的安全检测技术，识别网络中传输的恶意文件和 C&C 攻击。沙箱支持和防火墙联动以实现对威胁的实时阻断。
5	负载均衡设备	2	目前政务外网互联网出口分别为电信、移动、联通三家运营商，因此配备负载均衡设备以满足多运营商出口智能选路，确保资源优化使用、最大化吞吐率、最小化响应时间、避免过载。支持智能路由，根据现有 3 路运营商链路定制负载策略，支持链路拥塞控制技术，实现对链路过载保护，提升链路利用率；
6	接入认证控制	2	上网行为管理，在用户通过浏览器访问外网的时候，认证驱动重定向到 Portal 界面，当用户登录成功后数据包才会被驱动放通，实现认证控制。MAB 哑终端免认证，支持对哑终端进行放行，比如打印机，扫描仪等设备。不需要安装客户端，使用 Web 页面认证，使用方便，减少客户端的维护工作量，便于运营。可以在 Portal 页面上开展业务拓展，如责任公告、通知等。设备支持精细流量管理，确保业务正常进行。实现 P2P 智能流控，动态流控，出入站双向流控，上网行为识别，可精准识别外发数据，保障政务外网的资源合理分配使用。
7	VPN 网关	2	支持区政务外网 VPN 拨入的需求，SSL\IPSEC 协议
8	日志审计	1	在互联网出口区边界部署日志审计设备，通过专有协议将安全设备和网络设备的日志统一格式输出到日志审计服务器，自动分析并生成分析报表，支持图形化展示，审计日志保存 6 个月。
9	流量探针	1	部署探针，对网络边界流量进行提取和还原，送至大数据分析平台进行安全分析，识别潜在安全攻击风险。

1、防火墙含防病毒

技术指标	指标要求
规格要求	设备接口不少于 8 个万兆光口，8 个千兆光口，支持 40GE 口，接口拓展槽不少于 5 个；
	防火墙和防病毒系统
	含一年病毒库更新授权
	冗余电源
性能需求	防火墙吞吐量≥80G

	应用层吞吐量≥12G、全威胁吞吐量≥12G
	并发连接数≥3000 万
	HTTP 新建连接速率≥20 万/秒
功能要求	支持路由、交换、虚拟线、工作模式；
	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
	支持一体化安全策略配置，可以通过一条策略实现五元组等功能配置,简化用户管理；
	访问控制策略执行动作支持允许、禁止；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；支持策略加速技术；
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	支持 IPv4/IPv6 双栈工作模式；
	支持 RADIUS、LDAP、TACACS 等第三方外部认证；
	支持手动创建用户、批量导入导出用户、设备扫描方式创建用户；
	支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；
	支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、应用设置白名单；
	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
	支持监控功能，显示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
	支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；
	支持至少 2 种专业反病毒厂商的病毒特征库，病毒特征库规模超过 400 万；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
	支持静态白名单和动态黑名单功能；
	支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置；
	内置多种预定义报表模板，支持通信流量、上网行为、威胁统计

	报表，支持报表自定义；
	支持一次性报表及周期性报表，可自定义统计时间；支持报表本地存储、在线查看及邮件方式导出，支持 PDF、WORD 及 EXCEL 格式导出；
	支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；
	支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 月等；
	支持双机热备
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

2、入侵防御 IPS

技术指标	指标要求
规格要求	日志存储空间≥1T
	系统存储空间≥2G
	设备接口不少于 4 个万兆光口，4 个千兆电口；支持 40GE 接口，接口拓展槽不少于 5 个
	含一年入侵检测防御更新授权
	冗余电源
性能要求	吞吐量（全威胁应用层吞吐）≥16Gbps
	最大并发连接数≥1500 万
	每秒新建连接数≥20 万
功能要求	系统应具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵防御。
	要求支持丢弃报文、记录日志、禁止连接、TCP reset 结束 TCP 会话等多种响应动作
	要求支持自定义攻击检测规则。
	要求支持黑名单，将攻击源加入黑名单，一段时间内禁止访问
	系统应具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵防御。
	要求支持丢弃报文、记录日志、禁止连接、TCP reset 结束 TCP 会话等多种响应动作

	要求支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据。
	应涵盖广泛的攻击特征库、能够针对各种攻击的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。
	要求能够检测包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类的攻击事件；
	支持自定义规则，并且自定义规则库可以导入导出。
	支持对设备接口流量的阀值进行设置及报警。
	支持对网络内的 TCP、UDP、其他流量协议占比进行设置及报警。
	支持对协议组的流量阀值和连接数进行设置及报警，协议组类型包括 P2P 类、即时通讯类、标准协议类、移动应用类、http 应用类、工控互联网类等。
	系统应支持独立的 DDOS 检测、阻断及防御基线自学习的能力。
	系统支持防御包括 land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspoof、Synflood、Icmpflood、Udpflood、Portscan、ipsweep 等在内的 DOS/DDOS 攻击。
	系统支持 DNS 异常包及 DNS Flood 攻击防御。
	系统支持 DHCP 异常包及 DHCP Flood 攻击防御。
	系统支持 ARP 异常包及 ARP Flood 攻击防御。
	系统支持 CC 攻击防御。
	系统支持主机并发连接数和半连接数的限制。
	支持连接数控制，并且可以选择源目的区域及源目的地址、协议类型进行控制。
	支持双机热备
	支持多种形式的日志存储,本地存储、发送至日志服务器、本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式。
	支持提供基于告警级别、时间、IP 地址、事件类型、等条件的日志检索功能，具备日志导出备份、清除功能。
	支持生成日报、周报、月报。
	支持报表以 word、html 格式导出。
	系统应提供全方位的包含管理、系统、策略、安全、流量等告警。
	支持在应用排名中，展示该应用的主机的 IP 地址所对应的主机所属国家，以及连接数、上行流量、下行流量，并且可以对其进行排序。
	支持查看任意接口接受和发送报文字节大小分布图
	支持查看近 24 小时、一周、一个月内历史系统性能事件情况、连接数变化情况及新建会话速率情况
	系统支持 web、命令行等多形式灵活安全策略配置。
	支持系统资源监视。
	支持 web 页面的实时显示攻击事件。

	支持实时查看网络流量/攻击状况
	支持攻击统计展示，包括检测报文总数、发现攻击报文总数、以及攻击总数与检测总数百分比。
	支持实时基于主机、区域的攻击与被攻击的统计显示，在监控信息中直观显示 IP 地址所处国家。并支持自定义地址薄导入功能。
	支持查看连接排名，可以查看当前（用户访问此菜单时刻）通过入侵防御系统建立的连接排名信息。每一条连接信息包括如下内容：根据连接数排名方式的不同，显示排名、源 IP 地址、目的 IP 地址、协议、端口号、连接数量等信息。
	应支持基于协议的应用识别统计监控。
	应支持基于 web 类型分类的统计监控。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

3、日志审计

功能项	功能要求说明
规格要求	1U 或 2U 硬件一体机
	设备接口不少于 2 个万兆光口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
功能要求	支持对安全设备、边界检测等网络威胁进行采集和审计
	支持对证书系统进行审计，包括 CA 证书、RA 证书等
	支持对网络设备、安全设备的策略日志、告警日志、设备运行日志、操作日志等进行采集，支持 syslog 日志协议，支持 tcp、udp、http 等网络协议。
	支持对多元异构的日志数据进行标准化处理，并进行 ETL 处理，通过异常检测技术，识别异常行为、违规操作，威慑违规、取证定责、追根朔源
	审计日志集中存储，所有的日志记录都能够被存储在分布式数据存储服务器中，保证日志记录不被非法删除和篡改
	能够根据用户定义的审计策略，过滤无关的行为，当发生关键事件时，能够自动报警
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

4、流量探针

技术指标	指标要求

规格要求	设备接口不少于 4 个万兆光口，4 个千兆电口
性能要求	应用层吞吐≥10G
功能要求	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
	为了更好的对封装流量进行检测，具备二层协议识别能力，能够识别的协议包括但不限于 VLAN、MPLS VPN 等
	具备流量监控能力，包括基于用户的上行、下行流量速率监控，总体上行、下行流速监控等
	数据库是安全防护的重要对象，具备对数据库访问行为的审计能力，能够解析出用户对数据库的操作行为
	具备预定义规则集，可以做基本的 CGI 攻击、缓冲区溢出、木马后门等入侵检测
	支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；
	支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；具备独立的僵尸主机识别特征库；
	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则
	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
	默认包含超过 2000 条规则，如 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game 等
	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

5、沙箱

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆电口
	含威胁情报模块授权
性能要求	检测性能≥3G
	可执行文件检测能力≥6 万/天
	不可执行文件检测能力≥80 万/天
	AV 病毒检测率≥24 万/h
	WEB 沙箱文件检测率≥10 万/h
	Windows 沙箱文件检测率≥2500/h
功能要求	支持但不限于 Office 文档、WPS、PDF、HTML、JS、ZIP、7Z、RAR、

	CMD、PE、APK 等文件类型检测，且支持自定义文件类型。
	支持人工通过 web 批量提交和从网络下载样本检测，支持人工提交样本优先与自动还原样本检测；
	支持从 HTTP、FTP、POP3、SMTP、IMAP、SMB/CIFS 协议中还原出指定格式的承载文件
	具备独立的文件内容分析特征库分析引擎，支持对 Office 文件、PE 文件等文件内容进行检测，发现漏洞利用、木马、蠕虫、病毒、黑客工具等恶意代码；
	具备独立的文件 HASH 库检测引擎，支持对文件的 MD5 HASH 进行检测，发现已知的恶意文件，同时文件 HASH 库支持 100+万个以上已知恶意文件 MD5 特征；
	支持对样本文件的 PE 信息、证书信息、字符串信息的检测分析功能；
	支持通过 web 浏览器手动上传本地文件，支持加密上传
	支持常见网络威胁事件的检测，类型包括：ActiveX 攻击、Adobe 攻击、缓冲区溢出攻击、恶意代码、DNS 协议攻击、拒绝服务攻击、可疑文件传输、FTP 协议攻击、邮件服务攻击、恶意软件、NetBIOS 协议攻击、其他攻击、违规外联&非法访问、远程桌面攻击、远程过程调用、SCADA 系统攻击、扫描攻击、SMB 协议攻击、SNMP 协议攻击、数据库攻击、Telnet 协议攻击、攻击工具、木马、WEB 应用攻击、WEB 客户端攻击、WEB 服务端攻击、跨站脚本攻击、用户自定义攻击等
	支持反病毒检测功能，针对特种木马的反病毒检测技术进行检测和处理；
	支持捕获样本的文件操作、进程操作、注册表操作、网络通信、API 调用、office 宏指令、等详细行为；
	允许用户自主选择文件类型和运行环境等参数，支持 Windows XP 和 Windows 7 操作系统
	支持对样本产生的联网行为进行威胁情报检测，发现黑 IP、黑域名、黑 URL 及黑 MD5 请求行为及记录；
	输出详细的检测报告和原始报告，报告至少包含样本的进程树、样本的屏幕截图、样本的文件行为、进程行为、网络行为、注册表行为、API 调用。）
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6、链路负载均衡

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口,4 个千兆光口,6 个千兆电口

	含应用负载/链路负载/智能一年 DNS 授权
	冗余电源
性能要求	4 层吞吐量≥35Gbps
	并发连接数≥20,000,000
	四层每秒新建连接数≥500,000
	七层每秒新建连接数≥230,000
功能要求	支持串接部署、旁路部署；支持三角传输模式。
	必须独立专业负载设备，非插卡式扩展的负载均衡设备。
	支持双机热备部署、集群部署，设备之间同步会话信息。
	国产品牌，全中文界面，并且单一设备可同时支持包括链路负载均衡、全局负载均衡功能。无需额外购买相应授权。
	支持应用引流功能，能对关键应用设置固定线路，根据请求内容进行应用识别，从而保障关键应用的的最优访问体验。（需提供产品功能截图证明）
	支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、带宽比例、哈希、主备、首个可用、UDP 强行负载等算法。
	对于非 HTTP 协议的长连接应用，可通过分析议特征来识别消息的开始和截止，以消息为对象进行七层负载均衡，而非传统基于连接的四层负载均衡。
	支持基于 URL 的链路调度功能，可根据 URL 将访问国外网站的请求调度到指定线路。
	支持多种链路检测方法，能够通过 PING、TCP、HTTP 等方式监控链路的连通性。
	支持链路冗余机制，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅。
	支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。
	支持基于管理员自定义的时间计划来配置出站访问的链路调度策略。
	支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。
	IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66 等协议转换，提供 IPV6 产品检测报告。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

7、接入认证控制

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆光口，4 个千兆电口

性能要求	含一年 URL 和应用设别库授权；
	网络吞吐量≥25Gb
	最大并发连接数≥8,000,000
	支持准入终端数≥16000
	网关模式，网桥模式，旁路模式，多路桥接，多主模式
	提供设备实时 CPU、内存、磁盘占有率、在线用户数、系统时间、网络接口等信息；
	支持触发式 WEB 认证，静态用户名密码认证等；
	支持 Windows、Linux 和 MAC OS 客户端 EAD 认证。
	可以在线查看用户状态及其所连接的网络设备信息，如此用户接入的登录名称、登录设备 IP、设备端口、终端信息、在线 session 信息、接入开始时长、接入持续时长、安全状态等，对非法用户可以执行发送消息、在线检查、强制下线、关闭端口等操作。
	能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等。
	支持流量审计和用户管理系统联动，可以将 IP 地址对应到用户帐号、MAC 地址和主机名，并且支持 DHCP 环境和 NAT 环境；
	基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中
	审计用户使用 P2P、流媒体、炒股、网络游戏、FTP、Telnet 等应用行为；
	记录用户在指定时间段内的总上网时间； 记录用户在指定时间段内使用指定应用的总时长；
	支持 HTTP、FTP 等上传、下载动作基于文件类型过滤规则
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

8、VPN 网关

技术指标	指标要求
规格要求	设备接口不少于 6 个千兆电口，4 个千兆光口
	含 1000 用户授权
性能要求	吞吐量≥1.2Gbps
	最大并发用户数≥8000
	IPSEC 加密流量≥350Mbps
功能要求	实现路由模式、透明（网桥）模式、混合模式。
	实现静态路由、策略路由、RIP、OSPF、BGP 等路由协议。
	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
	支持 IPsec VPN 隧道自动建立，无需流量触发；

	支持 IPsec VPN 智能选路，根据应用和隧道质量调度流量。（提供功能截图）
	可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。
	支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置
	支持策略冗余分析，冲突策略分析以及命中率统计。
	支持策略风险调优，定期分析用户策略，结合应用状况和流量情况，给出优化建议。
	可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。
	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。
	支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

9、Anti-DDoS

技术指标	指标要求
规格要求	设备接口不少于 4 个 10G 万兆口，支持升级到 40GE
	含流量型/应用型等特征清洗授权
性能要求	设备攻击清洗能力不低于 40 G
	支持通过软件授权升级性能
功能要求	支持对欺骗与非欺骗的 SYN Flood、ACK Flood、ICMP Flood、ICMP Fragment、UDP Flood、UDP Fragment、FIN/RST Flood、TCP Misuse、TCP Connection Flood、TCP Fragment、HTTP Flood、HTTP Slow Attack、HTTPS Flood、SIP Flood、DNS Query Flood、DNS Reply Flood、DNS Amplification、SSDP Amplification、NTP Amplification、Chargen Amplification、SNMP Amplification 及混合类型攻击进行检测、告警并防护。
	支持水印防护算法自定义校验特征，满足对 CS 架构业务的精准防护需求。
	设备具备针对缓存 DNS 服务器及授权 DNS 服务器专用的 DNS 防护手段，至少 4 种。
	设备具备针对 HTTP Get Flood 攻击具备不少于 9 种专有防护手段，能够对 HTTP 进行解码。

	设备具备针对 HTTP POST Flood 攻击具备专有防护算法。
	支持导入 SSL 证书对 HTTPS 流量进行防护。
	设备具备对不同类型的 url 请求合法性进行验证，实行不同的防护策略，可防御 CC 及变种的能力。
	设备具备对连接耗尽型攻击的防御能力。
	设备支持使用智能攻击流量识别的技术进行防护，而不需要基于特定规则的方式，即当发生未知攻击，无需专门的撰写规则即可对这些攻击进行防护。
	设备支持高级模版匹配的功能，过滤策略可定义内容至少包含：目标 IP/掩码、目标端口、源 IP/掩码、源端口、协议类型、接口范围、包长范围、TOS、TTL/HopLimit、UDP 校验、ICMP 类型、ICMPv6 类型、TCP 选项、TCP 标志位、偏移量、深度、payload 字符。并支持对每条策略添加描述。
	支持自动识别 APP 访问来源，与 PC 源配置差异化防护策略进行精准过滤
	支持对 CDN、云清洗等使用代理源 IP 的流量进行防护，并对代理前真实源 IP 进行告警记录和黑名单过滤
	支持与云清洗进行联动，遭遇大流量 DDoS 攻击时自动切换上云，流量下降后自动切换回本地。
	支持配置群组运行模式，包括防护、告警、转发模式，告警模式下设备可以只检测告警攻击但不防护。
	支持静态和动态牵引方式，并且支持 BGP 路由协议和 OSPF 协议。
	支持二层回注、三层回注、GRE 回注、PBR 回注、MPLS LSP 回注、MPLS VPN 回注等多种回注方式。
	支持 portchannel 多端口绑定
	支持 OSPF、ISIS、RIP、OSPF6、LDP、ripng 等高级路由配置。
	管理界面要友好、易用性强，应支持集中管理、本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6.8.2 市政务外网接入区设计要求

杨浦区电子政务外网需接入市政务外网，设置边界政务外网安全接入区（市政务外网出口区），对进行数据交换的应用进行访问控制，对网络流量进行监测，防范网络入侵风险和恶意代码攻击，相关设备参数配置不得低于如下数量与标准：

市政务外网接入区			
序号	内容	数量（台）	参考规格功能要求
1	防火墙含防病毒	2	在市政务外网接入区部署防火墙带防毒模块，实现网络边界保护、病毒过滤和访问控

			制。防火墙只提供接入服务的必需的服务端口，对流经接入平台的网络数据进行合法性检查。所有的进出互联网的数据都将通过防毒模块的扫描，防止病毒文件穿梭于两级政务外网之间形成交叉感染。为了保证业务的高可用性，防火墙双机部署，支持性能的可扩容。防火墙支持 IPv6 协议栈、NAT64 转换技术。
2	入侵防御 IPS	2	在市政务外网安全接入区部署入侵防御系统，动态监视网络上所有流过的数据包，进行实时检测和分析，及时发现非法和异常行为，并且支持告警、阻断等功能。
3	沙箱	1	为了防御 APT 高级持续威胁，利用沙箱多引擎虚拟检测技术及其它安全检测技术，识别网络中传输的恶意文件和 C&C 攻击。沙箱支持和防火墙联动，以实现对威胁的实时阻断。
4	日志审计	1	在市政务外网接入区边界部署日志审计设备，通过专有协议将安全设备和网络设备的日志统一格式输出到日志审计服务器，自动分析生成分析报表，支持图形化展示，审计日志保存 6 个月。
5	流量探针	1	在市政务外网接入区边界部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析平台进行安全分析，识别潜在安全攻击风险。

1、防火墙含防病毒

技术指标	指标要求
规格要求	设备接口不少于 8 个万兆光口，8 个千兆光口，支持 40GE 口，接口拓展槽不少于 5 个
	防火墙和防病毒系统
	含一年病毒库更新授权
	冗余电源
性能需求	防火墙吞吐量≥80G
	应用层吞吐量≥12G、全威胁吞吐量≥12G
	并发连接数≥3000 万
	HTTP 新建连接速率≥20 万/秒
功能要求	支持路由、交换、虚拟线、工作模式；
	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；

	支持一体化安全策略配置，可以通过一条策略实现五元组等功能配置,简化用户管理；
	访问控制策略执行动作支持允许、禁止；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；支持策略加速技术；
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	支持 IPv4/IPv6 双栈工作模式；
	支持 RADIUS、LDAP、TACACS 等第三方外部认证；
	支持手动创建用户、批量导入导出用户、设备扫描方式创建用户；
	支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；
	支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、应用设置白名单；
	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
	支持监控功能，显示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
	支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；
	支持至少 2 种专业反病毒厂商的病毒特征库，病毒特征库规模超过 400 万；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
	支持静态白名单和动态黑名单功能；
	支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置；
	内置多种预定义报表模板，支持通信流量、上网行为、威胁统计报表，支持报表自定义；
	支持一次性报表及周期性报表，可自定义统计时间；支持报表本地存储、在线查看及邮件方式导出，支持 PDF、WORD 及 EXCEL 格式导出；
	支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；
	支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 月等；
	支持双机热备
	必须支持同时发送给多个 syslog 服务器

	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

2、入侵防御 IPS

技术指标	指标要求
规格要求	日志存储空间≥1T
	系统存储空间≥2G
	设备接口不少于 4 个万兆光口，4 个千兆电口；接口拓展槽不少于 5 个
	含一年入侵检测防御更新授权
	冗余电源
性能要求	吞吐量（全威胁应用层吞吐）≥16Gbps
	最大并发连接数≥1500 万
	每秒新建连接数≥20 万
功能要求	系统应具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵防御。
	要求支持丢弃报文、记录日志、禁止连接、TCP reset 结束 TCP 会话等多种响应动作
	要求支持自定义攻击检测规则。
	要求支持黑名单，将攻击源加入黑名单，一段时间内禁止访问
	系统应具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵防御。
	要求支持丢弃报文、记录日志、禁止连接、TCP reset 结束 TCP 会话等多种响应动作
	要求支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据。
	应涵盖广泛的攻击特征库、能够针对各种攻击的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。
	要求能够检测包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类的攻击事件；
	支持自定义规则，并且自定义规则库可以导入导出。
	支持对设备接口流量的阀值进行设置及报警。
	支持对网络内的 TCP、UDP、其他流量协议占比进行设置及报警。
	支持对协议组的流量阀值和连接数进行设置及报警，协议组类型包括 P2P 类、即时通讯类、标准协议类、移动应用类、http 应用类、工控互联网类等。
	系统应支持独立的 DDOS 检测、阻断及防御基线自学习的能力。

	系统支持防御包括 land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspoof、Synflood、Icmpflood、Udpflood、Portscan、ipsweep 等在内的 DOS/DDOS 攻击。
	系统支持 DNS 异常包及 DNS Flood 攻击防御。
	系统支持 DHCP 异常包及 DHCP Flood 攻击防御。
	系统支持 ARP 异常包及 ARP Flood 攻击防御。
	系统支持 CC 攻击防御。
	系统支持主机并发连接数和半连接数的限制。
	支持连接数控制，并且可以选择源目的区域及源目的地址、协议类型进行控制。
	支持双机热备
	支持多种形式的日志存储,本地存储、发送至日志服务器、本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式。
	支持提供基于告警级别、时间、IP 地址、事件类型、等条件的日志检索功能，具备日志导出备份、清除功能。
	支持生成日报、周报、月报。
	支持报表以 word、html 格式导出。
	系统应提供全方位的包含管理、系统、策略、安全、流量等告警。
	支持在应用排名中，展示该应用的主机的 IP 地址所对应的主机所属国家，以及连接数、上行流量、下行流量，并且可以对其进行排序。
	支持查看任意接口接受和发送报文字节大小分布图
	支持查看近 24 小时、一周、一个月内历史系统性能事件情况、连接数变化情况及新建会话速率情况
	系统支持 web、命令行等多形式灵活安全策略配置。
	支持系统资源监视。
	支持 web 页面的实时显示攻击事件。
	支持实时查看网络流量/攻击状况
	支持攻击统计展示，包括检测报文总数、发现攻击报文总数、以及攻击总数与检测总数百分比。
	支持实时基于主机、区域的攻击与被攻击的统计显示，在监控信息中直观显示 IP 地址所处国家。并支持自定义地址薄导入功能。
	支持查看连接排名，可以查看当前（用户访问此菜单时刻）通过入侵防御系统建立的连接排名信息。每一条连接信息包括如下内容：根据连接数排名方式的不同，显示排名、源 IP 地址、目的 IP 地址、协议、端口号、连接数量等信息。
	应支持基于协议的应用识别统计监控。
	应支持基于 web 类型分类的统计监控。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

3、沙箱

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆电口
	含一年威胁情报模块授权
性能要求	检测性能≥3G
	可执行文件检测能力≥6 万/天
	不可执行文件检测能力≥80 万/天
	AV 病毒检测率≥24 万/h
	WEB 沙箱文件检测率≥10 万/h
	Windows 沙箱文件检测率≥2500/h
功能要求	支持但不限于 Office 文档、WPS、PDF、HTML、JS、ZIP、7Z、RAR、CMD、PE、APK 等文件类型检测，且支持自定义文件类型。
	支持人工通过 web 批量提交和从网络下载样本检测，支持人工提交样本优先与自动还原样本检测；
	支持从 HTTP、FTP、POP3、SMTP、IMAP、SMB/CIFS 协议中还原出指定格式的承载文件
	具备独立的文件内容分析特征库分析引擎，支持对 Office 文件、PE 文件等文件内容进行检测，发现漏洞利用、木马、蠕虫、病毒、黑客工具等恶意代码；
	具备独立的文件 HASH 库检测引擎，支持对文件的 MD5 HASH 进行检测，发现已知的恶意文件，同时文件 HASH 库支持 100+万个以上已知恶意文件 MD5 特征；
	支持对样本文件的 PE 信息、证书信息、字符串信息的检测分析功能；
	支持通过 web 浏览器手动上传本地文件，支持加密上传
	支持常见网络威胁事件的检测，类型包括：ActiveX 攻击、Adobe 攻击、缓冲区溢出攻击、恶意代码、DNS 协议攻击、拒绝服务攻击、可疑文件传输、FTP 协议攻击、邮件服务攻击、恶意软件、NetBIOS 协议攻击、其他攻击、违规外联&非法访问、远程桌面攻击、远程过程调用、SCADA 系统攻击、扫描攻击、SMB 协议攻击、SNMP 协议攻击、数据库攻击、Telnet 协议攻击、攻击工具、木马、WEB 应用攻击、WEB 客户端攻击、WEB 服务端攻击、跨站脚本攻击、用户自定义攻击等
	支持反病毒检测功能，针对特种木马的反病毒检测技术进行检测和处理；
	支持捕获样本的文件操作、进程操作、注册表操作、网络通信、API 调用、office 宏指令、等详细行为；
	允许用户自主选择文件类型和运行环境等参数，支持 Windows XP 和 Windows 7 操作系统
	支持对样本产生的联网行为进行威胁情报检测，发现黑 IP、黑域名、黑 URL 及黑 MD5 请求行为及记录；

	输出详细的检测报告和原始报告，报告至少包含样本的进程树、样本的屏幕截图、样本的文件行为、进程行为、网络行为、注册表行为、API 调用。）
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

4、日志审计

功能项	功能要求说明
规格要求	1U 或 2U 硬件一体机
	设备接口不少于 2 个万兆光口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
功能要求	支持对安全设备、边界检测等网络威胁进行采集和审计
	支持对证书系统进行审计，包括 CA 证书、RA 证书等
	支持对网络设备、安全设备的策略日志、告警日志、设备运行日志、操作日志等进行采集，支持 syslog 日志协议，支持 tcp、udp、http 等网络协议。
	支持对多元异构的日志数据进行标准化处理，并进行 ETL 处理，通过异常检测技术，识别异常行为、违规操作，威慑违规、取证定责、追根朔源
	审计日志集中存储,所有的日志记录都能够被存储在分布式数据存储服务器中，保证日志记录不被非法删除和篡改
	能够根据用户定义的审计策略，过滤无关的行为，当发生关键事件时，能够自动报警
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

5、流量探针

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆电口
性能要求	应用层吞吐≥10G
功能要求	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
	为了更好的对封装流量进行检测，具备二层协议识别能力，能够识别的协议包括但不限于 VLAN、MPLS VPN 等
	具备流量监控能力，包括基于用户的上行、下行流量速率监控，总体上行、下行流速监控等

	数据库是安全防护的重要对象，具备对数据库访问行为的审计能力，能够解析出用户对数据库的操作行为
	具备预定义规则集，可以做基本的 CGI 攻击、缓冲区溢出、木马后门等入侵检测
	支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；
	支持对终端种植了远控木马或者病毒等恶意软件进行检测,并且能够对检测到的恶意软件行为进行深入的分析,展示和外部命令控制服务器的交互行为和其他可疑行为;具备独立的僵尸主机识别特征库；
	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则
	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
	默认包含超过 2000 条规则，如 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game 等
	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6.8.3 其他安全接入区设计要求

其他安全接入区包含无线通信接入(包括 3G、4G、5G 和卫星通信等)、企业用户接入以及物联网接入三种类型的接入，通过边界部署的防火墙进行边界防护和访问控制，并部署入侵防御系统、高级威胁防御（沙箱）、及防病毒网关，确保安全接入。采用 VPN 拨号接入区政务外网，通过部署的 VPN 网关接入，部署 AAA 认证服务器，结合交换机 AAA 配置，支持 Radius 协议、HWTACACS 协议等，用于无线通信用户和企业用户的认证、授权、收费功能并并支持日志审计和管理，以及探针的流量提取还原。相关设备参数配置不得低于如下数量与标准：

其他安全接入区			
序号	内容	数量（台）	参考规格功能要求
1	防火墙含防病毒和 IPS	2	为了简化安全接入区域的网络架构，考虑采用下一代防火墙，将多个安全功能进行集中部署且满足大量的并发和检测和过滤等需求。在安全接入区部署防火墙带防毒模块和 IPS，实现网络边界保护、病毒过滤和访问

			控制、以及入侵检测和防御。防火墙只提供接入服务的必需的服务端口，对流经接入平台的网络数据进行合法性检查。所有的进出互联网的数据都将通过防毒模块和 IPS 模块的扫描，为了保证业务的高可用性，防火墙双机部署，支持性能的可扩容。防火墙支持 IPv6 协议栈、NAT64 转换技术。
2	沙箱	1	为了持续防御 APT 高级持续威胁，利用沙箱多引擎虚拟检测技术及其它安全检测技术，识别网络中传输的恶意文件和 C&C 攻击。沙箱需要支持与防火墙联动，以实现对威胁的实时阻断。
3	日志审计	1	在安全接入区边界部署日志审计设备，通过专有协议将安全设备和网络设备的日志统一格式输出到日志审计服务器，自动分析生成分析报表，支持图形化展示，审计日志保存 6 个月。
4	流量探针	1	在安全接入区边界部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析平台进行安全分析，识别潜在安全攻击风险。
5	AAA 服务器	1	部署 AAA 认证服务器，结合交换机 AAA 配置，支持 Radius 协议、HWTACACS 协议等，用于无线通信用户的认证、授权、收费功能
6	VPN 网关	2	目前企业用户如需接入杨浦区电子政务外网，通过边界部署防火墙进行边界防护和访问控制，采用 VPN 拨号接入区政务外网，通过部署的 VPN 网关接入。

1、防火墙含防病毒和 IPS

技术指标	指标要求
规格要求	设备接口不少于 8 个万兆光口，8 个千兆光口，支持 40GE 口，接口拓展槽不少于 5 个
	防火墙和防病毒和 IPS 系统
	含一年病毒库更新授权
	含一年 IPS 特征库更新授权
	冗余电源
性能需求	防火墙吞吐量≥80G
	应用层吞吐量≥12G、全威胁吞吐量≥8G
	并发连接数≥3000 万
	HTTP 新建连接速率≥20 万/秒
功能要求	支持路由、交换、虚拟线、混合工作模式；
	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP、ISP 路由，内置移动、联通、电信、教育网、网通、长城宽带等 ISP 服务商地址列表，可通过 Web 界面选择不同的 ISP 服务商实现快速切换；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、

	用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
	支持一体化安全策略配置，可以通过一条策略实现五元组信息源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT 等功能配置,简化用户管理；
	访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；支持策略加速技术；
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	支持 IPv4/IPv6 双栈工作模式；
	内置强大的用户身份管理系统，支持本地认证、外部认证及免认证等方式，支持 RADIUS、LDAP、TACACS 等第三方外部认证；
	支持手动创建用户、批量导入导出用户、设备扫描方式创建用户；
	支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；
	支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、应用设置白名单；
	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
	支持监控功能，显示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
	支持独立的入侵防护规则特征库，特征总数在 5000 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；
	规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，防护动作包括告警、阻断、记录攻击报文；
	支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义，可对自定义规则导入导出；
	支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；
	支持至少 2 种专业反病毒厂商的病毒特征库，病毒特征库规模超过 400 万；
	内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
	支持静态白名单和动态黑名单功能；
	内置文件过滤引擎,支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检

	测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	内置防代理功能，防止网络用户通过代理主机实现攻击、避免计费等行为；
	支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置
	内置多种预定义报表模板，支持通信流量、上网行为、威胁统计报表，支持报表自定义；
	支持一次性报表及周期性报表，可自定义统计时间；支持报表本地存储、在线查看及邮件方式导出，支持 PDF、WORD 及 EXCEL 格式导出；
	支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；
	支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 月等；
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

2、沙箱

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆电口
	含一年威胁情报模块授权
性能要求	检测性能≥3G
	可执行文件检测能力≥6 万/天
	不可执行文件检测能力≥80 万/天
	AV 病毒检测率≥24 万/h
	WEB 沙箱文件检测率≥10 万/h
	Windows 沙箱文件检测率≥2500/h
功能要求	支持但不限于 Office 文档、WPS、PDF、HTML、JS、ZIP、7Z、RAR、CMD、PE、APK 等文件类型检测，且支持自定义文件类型。
	支持人工通过 web 批量提交和从网络下载样本检测，支持人工提交样本优先与自动还原样本检测；
	支持从 HTTP、FTP、POP3、SMTP、IMAP、SMB/CIFS 协议中还原出指定格式的承载文件
	具备独立的文件内容分析特征库分析引擎，支持对 Office 文件、PE 文件等文件内容进行检测，发现漏洞利用、木马、蠕虫、病毒、黑客工具等恶意代码；

	具备独立的文件 HASH 库检测引擎，支持对文件的 MD5 HASH 进行检测，发现已知的恶意文件，同时文件 HASH 库支持 100+万个以上已知恶意文件 MD5 特征；
	支持对样本文件的 PE 信息、证书信息、字符串信息的检测分析功能；
	支持通过 web 浏览器手动上传本地文件，支持加密上传
	支持常见网络威胁事件的检测，类型包括：ActiveX 攻击、Adobe 攻击、缓冲区溢出攻击、恶意代码、DNS 协议攻击、拒绝服务攻击、可疑文件传输、FTP 协议攻击、邮件服务攻击、恶意软件、NetBIOS 协议攻击、其他攻击、违规外联&非法访问、远程桌面攻击、远程过程调用、SCADA 系统攻击、扫描攻击、SMB 协议攻击、SNMP 协议攻击、数据库攻击、Telnet 协议攻击、攻击工具、木马、WEB 应用攻击、WEB 客户端攻击、WEB 服务端攻击、跨站脚本攻击、用户自定义攻击等
	支持反病毒检测功能，针对特种木马的反病毒检测技术进行检测和处理；
	支持捕获样本的文件操作、进程操作、注册表操作、网络通信、API 调用、office 宏指令、等详细行为；
	允许用户自主选择文件类型和运行环境等参数，支持 Windows XP 和 Windows 7 操作系统
	支持对样本产生的联网行为进行威胁情报检测，发现黑 IP、黑域名、黑 URL 及黑 MD5 请求行为及记录；
	输出详细的检测报告和原始报告，报告至少包含样本的进程树、样本的屏幕截图、样本的文件行为、进程行为、网络行为、注册表行为、API 调用。）
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

3、日志审计

功能项	功能要求说明
规格要求	1U 或 2U 硬件一体机
	设备接口不少于 2 个万兆光口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
功能要求	支持对安全设备、边界检测等网络威胁进行采集和审计
	支持对证书系统进行审计，包括 CA 证书、RA 证书等
	支持对网络设备、安全设备的策略日志、告警日志、设备运行日志、操作日志等进行采集，支持 syslog 日志协议，支持 tcp、udp、http 等网络协议。

	支持对多元异构的日志数据进行标准化处理，并进行 ETL 处理，通过异常检测技术，识别异常行为、违规操作，威慑违规、取证定责、追根朔源
	审计日志集中存储，所有的日志记录都能够被存储在分布式数据存储服务器中，保证日志记录不被非法删除和篡改
	能够根据用户定义的审计策略，过滤无关的行为，当发生关键事件时，能够自动报警
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

4、流量探针

技术指标	指标要求
规格要求	设备接口 4 个万兆光口，4 个千兆电口
	含探针特征库授权
性能要求	应用层吞吐≥10G
功能要求	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
	为了更好的对封装流量进行检测，具备二层协议识别能力，能够识别的协议包括但不限于 VLAN、MPLS VPN 等
	具备流量监控能力，包括基于用户的上行、下行流量速率监控，总体上行、下行流速监控等
	数据库是安全防护的重要对象，具备对数据库访问行为的审计能力，能够解析出用户对数据库的操作行为
	具备预定义规则集，可以做基本的 CGI 攻击、缓冲区溢出、木马后门等入侵检测
	支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；
	支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；具备独立的僵尸主机识别特征库；
	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则
	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
	默认包含超过 2000 条规则，如 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game 等
	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取

	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

5、AAA 服务器

技术指标	指标要求
规格要求	配置独立 Raid 阵列卡
	设备接口不少于 2 个万兆光口，4 个千兆电口
	双电源
功能要求	支持多种接入及认证方式，基于用户的权限控制策略，为不同用户定制不同网络访问权限，适合多种接入组网场景及应用场景。
	支持 Telnet、SSH、FTP 等多种设备认证接入方式，为不同的用户分组定制不同的授权策略，记录设备用户在登录过程中的操作行为，包括登录、登出行为、执行每一条命令行等行为。
	能够对于网络中的移动终端等无线设备与有线设备进行一体化集中管理。
	针对平台接入用户的帐号都可以用于 AAA（认证、授权、计费）服务。
	平台支持用户身份管理系统，支持 RADIUS、LDAP 等三方认证。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6、VPN 网关

技术指标	指标要求
规格要求	设备接口不少于 6 个千兆电口，4 个千兆光口
	含 1000 用户授权
性能要求	吞吐量≥1.2Gbps
	最大并发用户数≥8000
	IPSEC 加密流量≥350Mbps
功能要求	实现路由模式、透明（网桥）模式、混合模式。
	实现静态路由、策略路由、RIP、OSPF、BGP 等路由协议。
	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
	支持 IPsec VPN 隧道自动建立，无需流量触发；
	支持 IPsec VPN 智能选路，根据应用和隧道质量调度流量。（提供功能截图）

	可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。（提供功能截图）
	支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置
	支持策略冗余分析，冲突策略分析以及命中率统计。
	支持策略风险调优，定期分析用户策略，结合应用状况和流量情况，给出优化建议。（提供功能截图）
	可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式，支持父子带宽策略。
	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。
	支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。
	支持 U 盘零配置开局。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6.8.4 专网边界接入区设计要求

根据上海市大数据中心对政务外网升级改造工作任务分工和安排，需要对部门专网进行整合，

专用采用两套接入区域，考虑到物联感知网视频传输流量较大，固单独建立安全区域，其他专网合用一个区域，通过逻辑隔离的方式，将区域的流量进出上进行隔离。从安全管理上考虑专网两个区域属于同一个逻辑管辖，所有的安全相关的检测与分析都需要统一管理和检测。如下为专网接入区相关设备参数，配置不得低于如下数量与标准：

专网边界接入区			
序号	内容	数量（台）	参考规格功能要求
1	防火墙含防病毒和 IPS - 物联感知网	2	为了简化专网边界接入区域的网络架构，考虑采用下一代防火墙，将多个安全功能进行集中部署且满足大量的并发和检测和过滤等需求。在安全接入区部署防火墙带防毒模块和 IPS，实现网络边界保护、病毒过滤和访问控制、以及入侵检测和防御。防火墙只提供接入服务的必需的服务端口，对流经接入平台的网络数据进行合法性检查。所有的进出互联网的数据都将通过防毒模块和 IPS 模块的扫描，为了保证业务的高可用性，防火墙双机部署，支持

			性能的可扩容。防火墙支持 IPv6 协议栈、NAT64 转换技术。
2	防火墙含防病毒和 IPS - 其他五区	2	为了简化专网边界接入区域的网络架构，考虑采用下一代防火墙，将多个安全功能进行集中部署且满足大量的并发和检测和过滤等需求。在安全接入区部署防火墙带防毒模块和 IPS，实现网络边界保护、病毒过滤和访问控制、以及入侵检测和防御。防火墙只提供接入服务的必需的服务端口，对流经接入平台的网络数据进行合法性检查。所有的进出互联网的数据都将通过防毒模块和 IPS 模块的扫描，为了保证业务的高可用性，防火墙双机部署，支持性能的可扩容。防火墙支持 IPv6 协议栈、NAT64 转换技术。
3	沙箱	1	为了防御 APT 高级持续威胁，利用沙箱多引擎虚拟检测技术及其它安全检测技术，识别网络中传输的恶意文件和 C&C 攻击。沙箱支持和防火墙联动，以实现对威胁的实时阻断。
4	日志审计	1	在专网边界接入区边界部署日志审计设备，通过专有协议将安全设备和网络设备的日志统一格式输出到日志审计服务器，自动分析生成分析报表，支持图形化展示，审计日志保存 6 个月。
5	流量探针	1	在专网边界接入区边界部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析平台进行安全分析，识别潜在安全攻击风险。

1、防火墙含防病毒和 IPS - 物联感知网专用

技术指标	指标要求
规格要求	设备不少于 8 个万兆接口，4 个千兆光口，支持 40GE 口；
	防火墙和防病毒和 IPS 系统
	含一年病毒库更新授权
	含一年 IPS 特征库更新授权
	冗余电源
性能需求	防火墙吞吐量≥80G
	应用层吞吐量≥12G、全威胁吞吐量≥8G
	并发连接数≥3000 万
	HTTP 新建连接速率≥20 万/秒
功能要求	支持路由、交换、虚拟线、混合工作模式；
	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP、ISP 路由，内置移动、联通、电信、教育网、网通、长城宽带等 ISP 服务商地址列表，可通过 Web 界面选择不同的 ISP 服务商实现快速切换；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、

	用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
	支持一体化安全策略配置，可以通过一条策略实现五元组信息源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT 等功能配置，简化用户管理；
	访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；支持策略加速技术；
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	支持 IPv4/IPv6 双栈工作模式；
	内置强大的用户身份管理系统，支持本地认证、外部认证及免认证等方式，支持 RADIUS、LDAP、TACACS 等第三方外部认证；
	支持手动创建用户、批量导入导出用户、设备扫描方式创建用户；
	支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；
	支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、应用设置白名单；
	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
	支持监控功能，显示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
	支持独立的入侵防护规则特征库，特征总数在 5000 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；
	规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，防护动作包括告警、阻断、记录攻击报文；
	支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义，可对自定义规则导入导出；
	支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；
	支持至少 2 种专业反病毒厂商的病毒特征库，病毒特征库规模超过 400 万；
	内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
	支持静态白名单和动态黑名单功能；
	内置文件过滤引擎，支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、

	压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	内置防代理功能，防止网络用户通过代理主机实现攻击、避免计费等行为；
	支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置
	内置多种预定义报表模板，支持通信流量、上网行为、威胁统计报表，支持报表自定义；
	支持一次性报表及周期性报表，可自定义统计时间；支持报表本地存储、在线查看及邮件方式导出，支持 PDF、WORD 及 EXCEL 格式导出；
	支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；
	支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 月等；
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

2、防火墙含防病毒和 IPS －其他区域合用

技术指标	指标要求
规格要求	设备不少于 24 个万兆接口，4 个千兆光口，支持 40GE 口；
	防火墙和防病毒和 IPS 系统
	含一年病毒库更新授权
	含一年 IPS 特征库更新授权
	冗余电源
性能需求	防火墙吞吐量≥80G
	应用层吞吐量≥12G、全威胁吞吐量≥8G
	并发连接数≥3000 万
	HTTP 新建连接速率≥20 万/秒
功能要求	支持路由、交换、虚拟线、混合工作模式；
	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP、ISP 路由，内置移动、联通、电信、教育网、网通、长城宽带等 ISP 服务商地址列表，可通过 Web 界面选择不同的 ISP 服务商实现快速切换；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
	支持一体化安全策略配置，可以通过一条策略实现五元组信息源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防

	代理、APT 等功能配置,简化用户管理；
	访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；支持策略加速技术；
	提供策略查询功能,支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	支持 IPv4/IPv6 双栈工作模式；
	内置强大的用户身份管理系统，支持本地认证、外部认证及免认证等方式，支持 RADIUS、LDAP、TACACS 等第三方外部认证；
	支持手动创建用户、批量导入导出用户、设备扫描方式创建用户；
	支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；
	支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、应用设置白名单；
	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
	支持监控功能，显示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
	支持独立的入侵防护规则特征库，特征总数在 5000 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；
	规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，防护动作包括告警、阻断、记录攻击报文；
	支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义，可对自定义规则导入导出；
	支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；
	支持至少 2 种专业反病毒厂商的病毒特征库，病毒特征库规模超过 400 万；
	内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
	支持静态白名单和动态黑名单功能；
	内置文件过滤引擎，支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	内置防代理功能，防止网络用户通过代理主机实现攻击、避免计费等行为；
	支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置
	内置多种预定义报表模板，支持通信流量、上网行为、威胁统计报表，支持报表自定义；

	支持一次性报表及周期性报表，可自定义统计时间；支持报表本地存储、在线查看及邮件方式导出，支持 PDF、WORD 及 EXCEL 格式导出；
	支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；
	支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 月等；
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

3、沙箱

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆电口
	含一年威胁情报模块授权
性能要求	检测性能≥3G
	可执行文件检测能力≥6 万/天
	不可执行文件检测能力≥80 万/天
	AV 病毒检测率≥24 万/h
	WEB 沙箱文件检测率≥10 万/h
	Windows 沙箱文件检测率≥2500/h
功能要求	支持但不限于 Office 文档、WPS、PDF、HTML、JS、ZIP、7Z、RAR、CMD、PE、APK 等文件类型检测，且支持自定义文件类型。
	支持人工通过 web 批量提交和从网络下载样本检测，支持人工提交样本优先与自动还原样本检测；
	支持从 HTTP、FTP、POP3、SMTP、IMAP、SMB/CIFS 协议中还原出指定格式的承载文件
	具备独立的文件内容分析特征库分析引擎，支持对 Office 文件、PE 文件等文件内容进行检测，发现漏洞利用、木马、蠕虫、病毒、黑客工具等恶意代码；
	具备独立的文件 HASH 库检测引擎，支持对文件的 MD5 HASH 进行检测，发现已知的恶意文件，同时文件 HASH 库支持 100+万个以上已知恶意文件 MD5 特征；
	支持对样本文件的 PE 信息、证书信息、字符串信息的检测分析功能；
	支持通过 web 浏览器手动上传本地文件，支持加密上传
	支持常见网络威胁事件的检测，类型包括：ActiveX 攻击、Adobe 攻击、缓冲区溢出攻击、恶意代码、DNS 协议攻击、拒绝服务攻击、可疑文件传输、FTP 协议攻击、邮件服务攻击、恶意软件、NetBIOS 协议攻击、其他攻击、违规外联&非法访问、远程桌面攻击、远程过程调用、SCADA 系统攻击、扫描攻击、SMB 协议攻击、SNMP 协议攻击、数据库攻击、Telnet 协议攻击、攻击工具、木马、WEB 应用攻击、WEB 客户端攻击、WEB 服务

	端攻击、跨站脚本攻击、用户自定义攻击等
	支持反病毒检测功能，针对特种木马的反病毒检测技术进行检测和处理；
	支持捕获样本的文件操作、进程操作、注册表操作、网络通信、API 调用、office 宏指令、等详细行为；
	允许用户自主选择文件类型和运行环境等参数，支持 Windows XP 和 Windows 7 操作系统
	支持对样本产生的联网行为进行威胁情报检测，发现黑 IP、黑域名、黑 URL 及黑 MD5 请求行为及记录；
	输出详细的检测报告和原始报告，报告至少包含样本的进程树、样本的屏幕截图、样本的文件行为、进程行为、网络行为、注册表行为、API 调用。）
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

4、日志审计

功能项	功能要求说明
规格要求	1U 或 2U 硬件一体机
	设备接口不少于 2 个万兆光口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
功能要求	支持对安全设备、边界检测等网络威胁进行采集和审计
	支持对证书系统进行审计，包括 CA 证书、RA 证书等
	支持对网络设备、安全设备的策略日志、告警日志、设备运行日志、操作日志等进行采集，支持 syslog 日志协议，支持 tcp、udp、http 等网络协议。
	支持对多元异构的日志数据进行标准化处理，并进行 ETL 处理，通过异常检测技术，识别异常行为、违规操作，威慑违规、取证定责、追根朔源
	审计日志集中存储，所有的日志记录都能够被存储在分布式数据存储服务器中，保证日志记录不被非法删除和篡改
	能够根据用户定义的审计策略，过滤无关的行为，当发生关键事件时，能够自动报警
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

5、流量探针

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆电口
	含一年安全感知系统探针特征库授权
性能要求	应用层吞吐≥10G
功能要求	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
	为了更好的对封装流量进行检测，具备二层协议识别能力，能够识别的协议包括但不限于 VLAN、MPLS VPN 等
	具备流量监控能力，包括基于用户的上行、下行流量速率监控，总体上行、下行流速监控等
	数据库是安全防护的重要对象，具备对数据库访问行为的审计能力，能够解析出用户对数据库的操作行为
	具备预定义规则集，可以做基本的 CGI 攻击、缓冲区溢出、木马后门等入侵检测
	支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；
	支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；具备独立的僵尸主机识别特征库；
	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则
	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
	默认包含超过 2000 条规则，如 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game 等
	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6.8.5 核心网探针，准入控制相关参数配置不得低于如下数量与标准：

核心网安全			
序号	内容	数量（台）	参考规格功能要求
1	流量探针	2	在核心骨干网接入区边界部署探针，对政务外网内部单位和用户的互访流量进行提取和还原，送至后端大数据分析平台进行安全分析，识别潜在安全攻击风险。
2	准入控制	2	网络接入认证控制，提供多种认证方式以满足政务外网用户不同需求层面、不同控制颗粒度的准入认证需求，实现全方位的网络终端接入和边界管理。

1、流量探针

技术指标	指标要求
规格要求	设备接口少于 4 个万兆光口，4 个千兆电口
	含探针特征库授权
性能要求	应用层吞吐≥10G
功能要求	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
	为了更好的对封装流量进行检测，具备二层协议识别能力，能够识别的协议包括但不限于 VLAN、MPLS VPN 等
	具备流量监控能力，包括基于用户的上行、下行流量速率监控，总体上行、下行流速监控等
	数据库是安全防护的重要对象，具备对数据库访问行为的审计能力，能够解析出用户对数据库的操作行为
	具备预定义规则集，可以做基本的 CGI 攻击、缓冲区溢出、木马后门等入侵检测
	支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；
	支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；具备独立的僵尸主机识别特征库；
	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则
	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
	默认包含超过 2000 条规则，如 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game 等

	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

2、准入控制

技术指标	指标要求
规格要求	设备接口不少于 4 个万兆光口，4 个千兆光口，4 个千兆电口
性能要求	网络吞吐量≥5.5Gbs
	最大并发连接数≥200 万
	支持用户数≥25000
	支持准入终端数≥16000
	能基于流量分析，对终端安全检查是否合规。
	支持 802.1x、Portal、L2TIP IPSec VPN、SSL VPN、无线等多种网络环境的身份认证，支持基于端口的 802.1x 和基于 MAC 地址的 802.1x，可管理 HUB 或非智能交换机下的多个用户。
	用户的接入权限，可以在认证通过后下发给接入设备，由设备动态控制用户的访问权限，限制用户对内部敏感服务器和外部非法网站的访问。
	支持客户端的安全 ACL 和隔离 ACL，可以与网络接入设备配合实现对终端安全检查不合规的有效隔离。
	能够提供接入用户网络拓扑，在拓扑上实现在线用户查询、强制下线、下发消息等功能，便于用户的管理。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6.8.6 政务云接入设计

杨浦区政务云作为应用部署区域内，内部已经部署相关的安全设备，在与政务外网连接边界需部署日志审计设备和流量探针，将边界的设备例如交换机和路由器等设备的日志、流量输送至相关设备，作为保存分析查看使用。相关设备参数配置不得低于如下数量与标准：

政务云安全			
序号	内容	数量（台）	参考规格功能要求
1	日志审计	1	在政务云边界区边界部署日志审计设备，通过专有协议将安全设备和网络设备的日志统一格式输出到日志审计服务器，自动分析生成分析报表，支持图形化展示，审计日志

			保存 6 个月。
2	流量探针	1	在政务云边界区边界部署探针，对政务外网内部单位和用户的互访流量进行提取和还原，送至后端大数据分析平台进行安全分析，识别潜在安全攻击风险。

1、日志审计

功能项	功能要求说明
规格要求	1U 或 2U 硬件一体机
	设备接口不少于 2 个万兆光口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
功能要求	支持对安全设备、边界检测等网络威胁进行采集和审计
	支持对证书系统进行审计，包括 CA 证书、RA 证书等
	支持对网络设备、安全设备的策略日志、告警日志、设备运行日志、操作日志等进行采集，支持 syslog 日志协议，支持 tcp、udp、http 等网络协议。
	支持对多元异构的日志数据进行标准化处理，并进行 ETL 处理，通过异常检测技术，识别异常行为、违规操作，威慑违规、取证定责、追根朔源
	审计日志集中存储，所有的日志记录都能够被存储在分布式数据存储服务器中，保证日志记录不被非法删除和篡改
	能够根据用户定义的审计策略，过滤无关的行为，当发生关键事件时，能够自动报警
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

2、流量探针

技术指标	指标要求
规格要求	设备接口少于 4 个万兆光口，4 个千兆电口
	含探针特征库授权
性能要求	应用层吞吐≥10G
功能要求	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
	为了更好的对封装流量进行检测，具备二层协议识别能力，能够识别的协议包括但不限于 VLAN、MPLS VPN 等
	具备流量监控能力，包括基于用户的上行、下行流量速率监控，总体上行、下行流速监控等
	数据库是安全防护的重要对象，具备对数据库访问行为的审计能力，能够解析出用户对数据库的操作行为

	具备预定义规则集，可以做基本的 CGI 攻击、缓冲区溢出、木马后门等入侵检测
	支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测;支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；
	支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；具备独立的僵尸主机识别特征库；
	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则
	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
	默认包含超过 2000 条规则，如 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game 等
	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6.8.7 安全管理中心运营要求

根据《信息安全技术网络安全等级保护基本要求》 （GB/T 22239-2019），第三级安全要求中明确提出了安全管理中心要求，包括提供系统管理、审计管理、安全管理和集中管控等。着重强调了安全管理中心应符合如下要求：

- □应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
- □应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
- □应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
- □应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
- □应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
- □应能对网络中发生的各类安全事件进行识别、报警和分析。
- □满足等级保护三级的测评要求。
- □划分专门的安全管理区域，网络架构中设置运维管理区；
- □建立安全的信息传输路径，需要采用带外管理、VPN 通道、加密传输等方式进行管理；

•□部署统一网管系统，对链路、设备性能统一进行监控和告警；

•□部署日志审计系统，对设备审计日志集中汇总、集中分析、统一保存；

•□建立安全平台对安全策略、安全漏洞等安全事项的集中管理；

•□部署安全态势感知，对各类安全事件进行识别、报警和分析。

相关设备参数配置不得低于如下数量与标准：

安全管理中心			
序号	内容	数量（台）	参考规格功能要求
1	防火墙	2	在安全管理中心区域部署防火墙实现网络边界保护、访问控制。防火墙只提供接入服务的必需的服务端口，对流经接入平台的网络数据进行合法性检查。为了保证业务的高可用性，防火墙双机部署，支持性能的可扩容。防火墙支持 IPv6 协议栈、NAT64 转换技术。
2	态势感知平台	1	安全态势感知平台对网络安全进行监测与预警。系统功能包括数据采集、数据预处理、网络安全态势特征提取、态势评估和分析、态势预测、态势展示等。 态势感知平台包包含大数据平台软件、安全分析平台软件、可视化平台软件，大数据平台采用最新大数据分析和机器学习技术，抵御网络威胁和攻击。 通过探针采集抓起，从海量数据中提取关键信息，通过多维度风险评估，采用大数据分析方法关联单点异常行为，还原攻击链，准确识别和防御 APT 攻击，避免核心信息数据损失，通过部署的探针提取还原网络流量，送至大数据分析平台进行安全分析。 通过可视化平台使网络运维团队对网络中存在的威胁和异常清晰可见。从事前、事中、事后的角度形成一套具有战略纵深的网络安全态势感知体系，实现监管“可见、可管、可控”。
3	漏洞扫描系统	1	有效提高网络的安全性。通过对网络的扫描，网络管理员能了解网络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范。
4	安全管理控制系统	1	实现对全网安全策略集中管理和安全业务编排，快速部署安全业务。通过用户业务分区和应用的业务编排，自动完成安全策略的生成与部署，实现安全业务分钟级部署，有效降低安全运维成本。同时与态势感知系统联动，实现威胁检测结果自动转化为安全策略，并将安全策略下发到安全设备，实现安全设备的闭环联动处置。大幅提升网络的威胁防御能力，建

			全网主动防御体系。
5	日志审计	2	通过对网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保电子政务外网业务的不间断运营安全；为客户提供全维度、跨设备、细粒度的关联分析，透过事件的表象真实地还原事件背后的信息，提供真正可信赖的事件追责依据和业务运行的深度安全。同时提供集中化的统一管理平台，将所有的日志信息收集到平台中，实现信息资产的统一管理、监控资产的运行状况，协助用户全面审计信息系统整体安全状况。
6	堡垒机	1	提供操作日志审计、职权管控、安全认证和高效运维功能
7	通报预警	1	建设通报预警平台，对安全态势、威胁和漏洞情况进行汇总、分类、分级和研判处理，自动形成通报报告，及时上报上级安全管理中心，通报杨浦区大数据中心和相关电子政务外网接入单位。
8	网络综合审计	1	网络行为监控和审计系统对网络中的数据包进行分析、匹配、统计，通过特定的协议算法，从而实现入侵检测、信息还原等网络审计功能
9	运行支撑平台	1	资源层通过软件定义网络技术实现对底层基础网络资源的智能化管理，具备网络链路的自动调优、网络故障的快速定位、网络故障仿真和流量预测等智能化网络管理能力，结合并抓取网络管理系统功能； 采集层实现对外部系统和中央网络平台的基础设施软硬件及各种应用开展数据采集工作，包含告警数据，配置数据，性能数据，链路流量数据，及其他数据。 核心功能层要求部署监控管理、资源管理、流程管理及分级协同管理四大核心模块及对外系统接口。 监控管理模块：实现对信息化系统中网络、主机、存储、机房、应用、IP 地址等各个模块的管理。 服务与展现层面向各类平台使用用户提供运维相关服务 ，将运维服务门户成为进入运维管理平台的统通道。

安全管理中心-防火墙

技术指标	指标要求
规格要求	设备接口不少于 8 个万兆光口，8 个千兆光口，支持 40GE 口，接口拓展槽不少于 5 个；

	防火墙系统
	冗余电源
性能需求	防火墙吞吐量≥50G
	并发连接数≥4000 万
	HTTP 新建连接速率≥60 万/秒
功能要求	支持路由、交换、虚拟线、工作模式；
	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
	支持一体化安全策略配置，可以通过一条策略实现五元组等功能配置，简化用户管理；
	访问控制策略执行动作支持允许、禁止；
	提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；支持策略加速技术；
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	支持 IPv4/IPv6 双栈工作模式；
	支持 RADIUS、LDAP、TACACS 等三方外部认证；
	支持手动创建用户、批量导入导出用户、设备扫描方式创建用户；
	支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；
	支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、应用设置白名单；
	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
	支持监控功能，显示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
	支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；
	支持至少 2 种专业反病毒厂商的病毒特征库，病毒特征库规模超过 400 万；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
	支持静态白名单和动态黑名单功能；
	支持对 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证支持管理员分权管理，可自定

	义管理员权限模板，所有功能模块组合可由管理员自由组合配置；
	内置多种预定义报表模板，支持通信流量、上网行为、威胁统计报表，支持报表自定义；
	支持一次性报表及周期性报表，可自定义统计时间；支持报表本地存储、在线查看及邮件方式导出，支持 PDF、WORD 及 EXCEL 格式导出；
	支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；
	支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 月等；
	支持双机热备
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

安全管理中心-态势感知

技术指标	指标要求
规格要求	日志存储时长 180 天
	2U
	硬盘容量≥40T
	内存≥256G
	设备接口不低于 4 个万兆光口，4 个万兆电口
	冗余电源
性能参数	事件入库性能≥5000 条/秒
功能要求	支持以列表的形式展示规则信息，包括规则名称、规则描述、威胁等级、启用状态；并对规则参数可进行配置和启停管理
	支持与服务器安全监测系统进行告警和操作信息同步，告警信息包括暴力破解、异常登录、反弹 shell、本地提权、后门检测、WEB 后门、可疑操作等信息，操作信息包括操作审计日志和登入登出日志等
	支持基于源 IP、目的 IP、源端口、目的端口、起始时间等维度定义核查任务，支持统计每天访问频次及访问成功和失败次数
	具备挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；并支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计。
	提供对关联分析模型的基本管理功能，例如：可根据实际需要打开或关闭关联分析规则；
	支持基于元数据的检索与二次分析功能；
	支持第三方漏扫报告导入，支持查看漏洞的详细信息，主要包括

	漏洞级别、类型、名称、描述、受影响 IP 数、解决方案等
	支持同品牌漏扫设备联动，并支持平台界面融合方式直接创建主机、WEB、数据库扫描策略模板与参数模板，参数模板可配置扫描详细参数，包括最大 URL 链路限制、爬行路径深度限制、扫描倍数、脚本检测超时时间、口令破解时间、TCP 扫描时间、TCP 扫描范围、TCP 扫描方式、每秒最大发送请求数等； 支持对漏扫任务进行管理，支持直接选取资产库进行目标扫描，并支持定时任务扫描
	支持新增、删除、修改，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；并可查看规则详情
	支持与统一运维系统进行数据共享，同步资产数据信息，同时向运维系统同步输出资产安全事件和安全状态
	支持大屏定制标题、地图，支持定制系统名称，支持定制公司名称，支持定制 LOGO 图片
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

安全管理中心-漏洞扫描系统

功能指标	指标要求
规格要求	设备接口不少于 4 个千兆口
性能要求	支持添加 200 个资产
	漏洞扫描不限制 IP 数
功能要求	支持 SSL 加密对数据传输等进行处理，HTTPS 方式，采用 B/S 架构操作，支持 IPv6
	基线检查和变更检查支持远程检查、SSH、TELNET、SMB
	支持指定登录用户名和口令进行本地漏扫检查
	基线检查和变更检查支持离线检查、跳转机跳转
	基线检查支持系统类型包括主机类：Windows、Unix、Solaris、HP-Unix、AIX、Linux 等；网络设备：华为、H3C、Cisco、Juniper、中兴等；防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等；数据库：Mysql、DB2、Oracle、Sqlserver、Sybase 等；中间件：Tomcat、IIS、Webservices、Apache、Weblogic、Resin、Nginx 等；虚拟化平台：VMware ESXi、VMware Center、XenServer
	在安全基线违规列表中，选择某个违规信息，支持查看该违规的详细信息和解决方案
	变更检查支持检查重要文件、文件夹、注册表、启动项、进程等详细信息以及变更状态
	支持扫描识别出运行的服务和端口，内置漏洞库 58000 条以上。支持 CVE、CNVD、CNNVD、BugTraq 等，拥有完备的知识体系
	支持扫描主流虚拟机管理系统的安全漏洞，如：VMWare ESXi、Xen 等
	支持常见的 WEB 应用弱点检测，支持主流安全漏洞扫描，如：SQL

	注入、跨站脚本攻击、网页木马、系统命令执行漏洞、信息泄露、资源位置预测漏洞、目录遍历漏洞、配置不当漏洞、弱密码、内容欺骗漏洞、外链、暗链等类型漏洞；支持 WEB1.0，WEB2.0 扫描；支持对网站资产管理，快捷网站扫描
	支持一次性任务、立即任务、周期任务等多种调度方式；
	可自定义扫描时间段，设置禁止扫描时间段后，该时间段内的周期任务、一次执行任务将无法自动执行。可选择多个例外任务。禁扫时间段不会影响例外任务执行。
	以列表的方式展示告警，支持告警策略自定义、告警声音设置
	任务报告展示：支持五合一多维度展示任务详情，并支持导出 Word、PDF、HTML 等多种报表
	个性化配置包括报告名称、页眉、页脚及 LOGO。
	支持三权分立方式的授权，即管理员只负责完成设备的系统配置，安全管理员负责配置核查，审计员负责对系统本身的用户操作日志管理和审计
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

安全管理中心-安全管理控制系统

功能项	功能要求说明
规格要求	1U 或 2U 硬件一体机
	设备接口不少于 2 个万兆光口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
	支持设备自动搜索发现，支持根据起始 ip 范围搜索，支持 snmp 或 ping+snmp 方式搜索设备
	可视化 IT 资源管理、统一事件告警等功能，支持设备的增删改查、设备组的增删改查
	支持设备属性信息查看，包括 ip 地址、运行时长、网络接口信息、cpu 状态、进程状态等
	支持设备网络拓补展示，直观展示设备运行状态和风险预警
	支持设置对应的匹配条件，包括源/目的安全区域、源/目的地址、服务、时间段来实现政务外网的安全策略管控
	支持策略合规性检查：支持定义白名单、风险规则、混合规则等检查方式
	支持安全管理控制系统联动态势感知分析平台以实现威胁检测结果转化为安全策略，并将安全策略下发到安全设备，实现安全设备的闭环联动处置
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取

	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

安全管理中心-日志审计

功能项	功能要求说明
规格要求	1U 或 2U 硬件一体机
	设备接口不少于 4 个千兆口，支持万兆扩展
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
	支持通过标准接口要求进行应用系统数据采集，包括行为主体操作行为、主体角色、操作客体、事件时间等信息
	支持对云平台网络资源配置、软件资源配置、虚拟机管理、快照管理、角色管理、用户管理等进行审计
	支持对证书系统进行审计，包括 CA 证书、RA 证书等
	支持对多元异构的日志数据进行标准化处理，并进行 ETL 处理，通过异常检测技术，识别异常行为、违规操作，威慑违规、取证定责、追根朔源
	策略类型包括但不限于终端审计策略、数据库审计策略、网络审计策略应用审计策略
	支持 IPv4 网络，千兆以上审计能力，具备内容审计、行为审计、流量审计、数据库审计等，精确审计到发布内容、风险等级等要素，内置威胁检测规则库
	具有集中控制、分级管理、终端管理、系统运行日志管理、审计日志导入/导出、审计报表分析等功能；支持级联部署,通过一个统一的审计中心、多个分布式的审计监管分中心,对主机、网络、数据库审计监控子系统进行集中管理
	审计日志集中存储，所有的日志记录都能够被存储在分布式数据存储服务器中，保证日志记录不被非法删除和篡改
	能够根据用户定义的审计策略，过滤无关的行为，当发生关键事件时，能够自动报警
	能够记录完整的信息，包括事件源，事件发生的时间，事件操作结果，操作者的用户标识，IP 地址和主机名，以及完整的事件描述信息
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

安全管理中心-堡垒机

技术指标	指标要求
规格要求	设备接口不少于 4 个千兆光口
	内置存储≥4TB

	单电源,可扩展
性能要求	≥1000 个主机
	含多因素认证授权和短信网关
功能要求	支持双机热备，支持集群部署
	图形终端协议：RDP、VNC、X11 字符终端协议：Telnet、SSH 文件传输协议：FTP、SFTP 数据库类型： PLSQL、TOAD、SQL、SQLDEVELOPER；Informix； WEB 应用：HTTP、HTTPS KVM 类:DSR、DSVIEW、RARITAN、RARITAN_CC 等
	要求以上所有图形化应用在实际操作环境中均可以正常使用且可自由调整应用的窗口大小，做到无缝发布
	支持对应用中心状态、审计状态和端口状态是否正常工作进行一键检查。
	运维人员可以在系统 Web 界面填写授权审批流程单，填写内容至少应包括：设备资源、系统账号、协议类型、时间窗口；审批通过后，运维人员可立即取得相应访问权限
	为管理员和运维人员提供操作向导模式，方便用户进行设备管理和使用
	系统角色需按法案要求进行划分，至少有系统管理员、密码管理员、配置管理员、审计管理员、普通用户等多种角色。
	系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、Radius 认证、LDAP、AD 域、数字证书认证、动态令牌认证、USBKEY 认证、指纹认证和手机动态令牌认证。
	支持批量导入导出运维用户、目标设备、账号密码等，支持目标设备账号批量新增
	支持命令记录：字符终端命令记录、图形终端键盘操作记录、数据库运维 SQL 命令、图形标题栏识别（OCR）
	图形终端键盘操作记录：支持图形终端键盘操作记录，完整记录键盘动作
	支持 RDP 会话针对操作行为告警（针对标题栏进行告警），可进行告警内容设置。
	支持数据库应用针对操作命令进行告警，可进行告警内容设置（告警内容支持动作，表名等）。
	存储告警：日志存储超过设置的阀值进行邮件告警，支持定期删除计划，只保留设置时间段的日志。
	系统应具备在对系统制定报表任务时，可以配置时间周期，支持以图(柱、饼等)，统计、明细数据的方式表现。
	必须支持同时发送给多个 syslog 服务器
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

安全管理中心-通报预警平台

技术指标	指标要求
硬件规格	1U 或 2U 硬件一体机
	设备接口 4 个万兆光口，4 个千兆电口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户≥1000 个
功能要求	支持用户定义的报警策略，策略模板管理，支持上下级策略级联
	支持对态势感知系统的数据进行关联分析，对异常行为提前发出预警提示
	支持对安全态势实时感知，对威胁和漏洞情况进行汇总、分类、分级，自动形成通报报告
	支持上报上级安全管理中心
	支持网络环境中的主机、服务器等进行数据采集，发现网络中的异常、违规行为，并实时产生预警
	1.支持将预警信息转为内部通告； 2.支持通过安全预警自动派发工单到对应的安全管理员； 3.支持将预警信息手动定向指派工单；支持工单举证信息溯源， 4.工单处置人员可以直接定位到工单关联的原始信息进行查看； 5.支持将预警信息以邮件形式发送到相关人员或以站内消息形式实时推送。
	支持对违规行为进行责任溯源，支持人员行为轨迹追查
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

安全管理中心-网络综合审计

技术指标	指标要求
硬件规格	1U 或 2U 硬件一体机
	设备接口不少于 2 个万兆光口
性能要求	事件记录处理能力≥10000 条/每秒
	并发用户数≥1000 个
功能要求	平台支持审计策略制定，提供一种基于 ACL 规则形式，可根据内网的合规性设定要求，针对具体 IP，服务，端口，访问时间等策略，建立针对性的业务和应用访问逻辑规则。

	支持对网络流量、HTTP 协议、TELNET 协议、FTP 协议、NetBIOS 协议、DNS 协议等进行审计
	设备支持检测隧道、Tor 暗网通信、端口反弹等隐蔽通信方式
	系统应自带规则库
	能够对不同的审计事件赋予不同的安全级别
	审计事件的检索功能，支持源 IP、源端口、目的 IP、目的端口、引擎名、用户名、帐户、规则名、时间进行查询，支持组合条件查询方式
	审计统计功能，提供 TOPN 统计方式，支持组合条件方式统计
	支持 IPv4 网络，千兆以上审计能力，具备内容审计、行为审计、流量审计、数据库审计等，精确审计到发布内容、风险等级等要素，内置威胁检测规则库
	需内置 T 级别存储，可以选配各种 RAID 级别进行数据冗余和安全保障。系统需具备存储加密机制和查询机制
	必须支持第三方厂商通过 API 接口 get 或 push 方式进行日志或告警获取
	必须支持与第三方厂商完成联动或集成适配(协议接口包括:Syslog 协议/API 接口)

6.9 等级保护测评

配合第三方机构完成杨浦区电子政务外网系统的信息安全等级保护三级的测评工作，完善避免高危漏洞，优化整改中、低危漏洞，确保完成测评并通过。第三方测评机构的所有测评费用及整改所需费用均包含在报价中

7、运维保障要求

7.1 运维服务目标

通过建立专业高效的运维服务体系，对升级后的杨浦区电子政务外网进行整体系统维护，保障网络系统的正常运行。

通过现场安排常驻运维服务团队，使用电子政务外网网络管理软件及电子政务外网运行支撑平台功能，结合定义的内嵌流程管理体系，配套服务商的信息系统技术、供应链资源，形成人员-平台-流程-资源的运维要素有机结合，打造专业、高效的运维服务体系。

投标人提供热线电话、电子邮件和在线网站等技术支持方式，提供 7*24 小时电话响应服务和 7*24 小时的现场运维服务，重大节点强化保障，确保电子政务外网整体稳定正常运行。

日常监控、巡检：对电子政务外网进行日常监控、巡检，包括监控告警的处理，巡检异常的处理等；投标人需制定维护管理规定，并按照规定中的维护项目、周期和要求，制定详细的作业计划并执行。

系统扩容：投标人应承诺，在日常运维过程中，当电子政务外网接入规模、网络出口或者链路带宽等不满足最终用户使用要求时，投标人需对现有网络进行扩容。在主管部门发起扩容需求后，投标人需在 1 个工作日内响应，在 5 个工作日内完成扩容任务，同时向主管部门提交扩容后平台的资源情况报告。

电子政务外网故障处理：处理电子政务外网发生的各类软硬件、通信线路等故障，应确保业务正常稳定运行；其中故障处理流程需要电子化并规定处理时限及当前处理环节的责任部门和责任人。

迁移及升级割接：开展用户迁移割接和电子政务外网软硬件升级割接；中标人在升级前制定完善的操作实施方案，在方案中尽量降低对业务的影响；对于可能影响业务的各类操作，应全面评估操作影响，并提前通知招标人具体操作计划安排，在招标人的相关业务部门同意后方可执行操作。根据招标人要求提供业务开通报告及验收测试报告。

系统中断：投标人在中标后由于维护原因，需中断系统进行平台升级操作时，提前至少 72 小时（重大自然灾害除外）通知招标人做好相关准备工作，征得招标人同意方可实施。

应急演练与应急响应：根据电子政务外网高可用设计特性和各组件的重要性进行针对性演练，制订应急预案，每年组织至少 2 次应急演练。当发生重大应急事件时，招标人需在中标人的牵头下实施应急响应操作，并在事后制定重大事件报告。

安全加固：对电子政务外网各网元进行安全策略配置、安全扫描和系统漏洞的加固；

配置实施及管理：进行电子政务外网各软硬件设备的基础配置、IP 配置、角色用途、账号密码等的统一配置实施及配置管理；

节假日保障：重大节假日期间进行电子政务外网运行和信息安全的重点保障；

故障处理和响应：投标人需建立基于 7*24 小时不间断的 SLA 服务级别设计，故障响应及时率 100%，故障修复及时率 100%。投标人应建立完善的电子政务外网故障管理体系，管理体系涵盖故障处理的故障等级、职责分工和处理界面，每个处理流程留有电子化记录并在每个处理环节中落实到投标人的部门和相应的处理接口人。按照故障等级不同，需要有不同的处理时长和故障恢复时限。

7.2 运维服务要求

对杨浦区电子政务外网核心、汇聚、接入全部范围的所有节点，投标人应派遣运维团队进驻由投标人提供的驻场办公室（杨浦区惠民路 800 号）进行日常运维工作和服务，以满足日常运维服务的需求。提供服务响应时间 7×24 小时电话支持， 5×8 小时现场驻点运维服务及 7×24 小时机房值守服务等相关“下沉式”运维服务。

按照杨浦区大数据中心根据系统稳定、安全、可靠、有效运行所提出的要求和指标，及时制定、修改和完善系统运行维护方案，并确保系统运行维护方案有效执行。

在系统的安全性、稳定性和可靠性确保前提下，充分考虑系统运行状况优化和发展。

建立符合杨浦区电子政务外网实际情况的，具备专业和可操作性的 ITSS 信息技术服务架构，形成标准可靠可行的运维服务体系。

提供无推诿服务，即服务商应提供特殊措施，无论由于哪一方产生的问题而使系统发生不正常情况时，应全力协助各类资源和相关部门，使系统尽快恢复正常。

提供节点式管理，核心、汇聚节点重点全方位响应服务和技术支持；提供下沉式服务，服务覆盖范围到所有接入层，提供接入层的网络响应服务和技术支持。

8、培训要求

投标人应根据本项目的特点制定培训方案并提供培训，使招标人相关人员在培训后能够独立使用系统，而不必依赖投标人现场指导。培训课程涵盖电子政务外网的使用和管理培训，中标人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)培训总则

投标人至少满足本章要求的培训服务。

所提供的培训课程表随投标文件一起提交。

培训授课人是经过厂家认证的工程师。

投标人为所有被培训人员提供培训用文字资料和讲义等相关用品。所有的资料是中文书写。

培训工作应在合同生效后安排。

每年安排一次针对各委办局信息系统基于电子政务外网建设的培训，人数 200 人/天。

2)培训内容与课程要求

投标人应对项目中所有产品的基本知识、系统或参数配置、管理维护等提供相应的培训。投标人详细列明相应的培训课程内容、人数和时间安排。

3)培训费用

投标人应将所有培训费用（含培训教材费）及各项支出计入资源租赁费用中，不单独报价。

8.其他

本项目采用固定总价包干方式，投标总价中应包括本次招标具体点位基础上 5%以内的接入点位的新增、减少或变更。招标人不再支付额外费用。

三、人员要求

投标人应为杨浦区电子政务外网单独建立管理组织，配置不得少于 10 人的项目团队，需包含下列人员。

1、项目经理：

1）项目经理对服务项目过程实行全面管理，执行检查控制协调项目的各项工作。

2）项目经理需具有中级或以上工程师职称及相关从业证书、能力认证等。（提供相关相应能力证书或证明材料）。

3）应从事大型网络、机房维护等相关工作至少 5 年以上实际经验，从事项目经理或项目负责人至少 5 年以上实际经验。

4）具备强烈的责任心和认真负责的工作态度。

2、网络负责人

1）网络负责人主要负责整体网络的不间断性和安全性，确保政务外网的正常运行。

2）网络负责人需具有网络技术相关证书。（提供相关相应能力证书或证明材料）。

3）应从事大型网络、机房维护等相关工作至少 5 年以上实际经验，从事大型项目的网络管理至少 5 年以上实际经验。

4）具备强烈的责任心和认真负责的工作态度。

3、服务工程师：

1）服务工程师包含现场驻场运维工程师（不少于 8 人，其中 1 人为驻场运维负责人，需具备相关相应能力证书或证明材料）和二线支持团队，二线支持团队对一线运维进行远程技术与指导，紧急情况下处理应急事件、疑难问题和个案调查处理。并根据需要到现场进行响应、值守。

2）服务工程师需提供相关证书（或者类似证书）。

3)从事网络、机房维护等相关工作至少 3 年以上实际经验。

4)动手能力强，富有责任心。

5)遵守纪律、服从安排、吃苦耐劳。

运维服务内容：

对所有节点提供运维服务管理。包括：系统及设备的每日监控维护服务和日常服务及巡检，机房管理和日常维护，机房及配套设施的养护服务。

对所有节点提供下沉式服务，包括：对杨浦区电子政务外网核心、汇聚、接入全部节点采用下沉式管家服务的要求，提供下沉式服务，负责全区所有政务外网接入单位对应政务外网网络使用过程中的技术响应、故障响应。当接入单位出现政务外网网络故障、性能问题、使用故障等情况，提供远程技术支持和现场响应服务。

远程支持实时响应，根据响应事件的重要性，必要情况在 2-4 个小时内现场响应，并于当日解决问题。

下沉式服务范围要求：

杨浦区电子政务外网核心、汇聚、接入层，接入层的政务外网接入设备的使用故障、技术支持等；具体接入下联单位节点详见项目需求中的现有节点清单。

下沉式服务主要内容：

a. 除了网络系统核心、汇聚，投标人需专门提供并分组安排运维团队人员，对政务外网各接入节点提供日常技术支持与快速响应；

b. 积极主动配合各委办局相关信息技术负责人快速落地与政务外网服务相关的业务需求，了解各个委办局在政务外网业务需求以及数据在网络中流向。

c. 定期或不定期对各个委办局进行抽样调查政务外网服务满意度，听取各方意见和建议，收集需求后综合分析并作出改进和优化。

d. 通过工单系统通知及时处理各单位故障报修或技术支持等需求。工单处理完毕后完成用户满意度反馈。

下沉式服务响应要求：

1、建立基于 7*24 小时不间断的 SLA 服务级别设计，原则上远程实时响应，现场 2 小时内响应，故障解决时间不超过 T+1，重要故障或核心故障 T+0。

2、除故障响应和技术支持响应之外，还需提供每月接入设备的巡检，做好巡检记录，并排除隐患。

四、绩效考核要求

依据中标人投标响应文件、合同、服务承诺和国家相关规定，每季度工作完成后，由招标人对中标人进行绩效考核，考核合格后支付该季度费用，如中标人未通过绩效考核，招标人有权让中标人开展整改工作，整改合格后支付相应服务费用，并具有进一步要求赔偿的权利。

五、承诺要求：

1、★满足验收要求承诺

验收需满足本项目上线运营交付要求，并于 2024 年 2 月 29 日前完成整体上线，包括不限于网络核心层、汇聚层、所有接入节点以及安全设备。招标人根据中标人投标响应文件中服务方案、服务承诺等内容的实施情况对项目进行验收，验收完成后进入试运行。如中标人未通过验收，招标人有权中止合同，并且需由中标人支付招标人因中标人未能按照承诺响应完成项目造成的业务影响费用（包含但不限于因服务未能按时上线所需要支付的延续服务费，可能包含网络及安全设备租赁费、运维服务费等）

2、★满足业务连续性承诺

在保证政务外网业务连续性，不影响原有政务外网基础设施服务的前提下，于 2024 年 3 月 31 日前，完成网络割接迁移工作，招标文件内 787 个接入节点均进入各政务外网需求单位正常使用状态，且所有网络割接迁移成本，均包含在报价之内，投标人明确政务外网网络基础设施业务连续性对招标人的重要性，能够预见未能满足承诺要求将对招标人造成巨大的损失；因此投标人同意如未满足承诺要求，招标人有权单方面解除合同且中标人承担违约责任，包括但不限于返还招标人已支付费用、承担招标人再次招标的费用、因无法割接迁移产生的所有费用等。

六、绩效考核指标

一级指标	指标名称	权重分值	评分规则	评分	备注	
数量指标（10 分）	服务点位数量	10	服务点位全年平均数量≥787 个得 10 分，平均数量每少 10 个，扣 0.1 分，未达 500 个点位不得分。			
产出指标（80 分）	核心节点之间带宽配置要求	5	核心节点之间要求带宽 100Gbps，每下降 20Gbps 扣 1 分，扣完为止。			
	与市级电子政务外网之间带宽配置要求	5	与市级电子政务外网之间要求带宽 10Gbps，每下降 2Gbps 扣 1 分，扣完为止。			
	核心节点与下级汇聚节点之间带宽配置要求	5	核心节点与下级汇聚节点之间带宽要求 100Gbps，每下降 20Gbps 扣 1 分，扣完为止。			
	同一汇聚节点内主备冗余设备之间带宽配置要求	5	同一汇聚节点内主备冗余设备之间带宽要求 100Gbps，每下降 20Gbps 扣 1 分，扣完为止。			
	汇聚节点与下级重要接入节点之间带宽配置要求	5	汇聚节点与下级重要接入节点之间带宽配置要求 1Gbps，每下降 0.2Gbps 扣 1 分，扣完为止。			
	汇聚节点与下级一般接入节点之间带宽配置要求	5	汇聚节点与下级重要接入节点之间带宽配置要求 10Gbps，每下降 2Gbps 扣 1 分，扣完为止。			
	核心节点可用率	5	核心节点可用率是指核心节点正常可用的时间占服务总时间的占比，具体计算公式如下： 核心节点可用率=（统计周期天数×24×60 -核心节点不可用分钟数）/统计周期天数×24×60。 核心节点可用率不低于 99.995%。，每下降 0.005%，扣 1 分，扣完为止。			
	汇聚节点可用率	5	汇聚节点可用率是指汇聚节点正常可用的时间占服务总时间的占比，具体计算公式如下： 汇聚节点可用率=（统计周期天数×24×60 -汇聚节点不可用分钟数）/统计周期天数×24×60。 汇聚节点可用率不低于 99.99%。每下降 0.01%，扣 1 分，扣完为止。			
	链路可用性	5	链路可用性是指用户链路实际可用时间的占比，具体计算公式如下： 链路可用性=（60×24×统计周期天数×用户链路数-Σ （不可用分钟数））/60×24×统计周期天数× 用户链路数×100%。 其中，不可用分钟数是指发现用户链路中断或接到用户申告链路中断开始，到链路恢复的时间。			

			电子政务外网的用户链路可用性应达到99.99%。每下降0.01%，扣1分，扣完为止。 链路不可用不包括以下情况： 1）用户原因导致的链路不可用，如用户自有设备以及线路不可用； 2）进行必要的网络割接、测试导致的不可用。			
	与政务云对接连通性要求	5	与政务云对接连通性要求99.99%，每下降0.01%，扣1分，扣完为止。			
	与市政务外网对接连通性要求	5	与市政务外网对接连通性要求99.99%，每下降0.01%，扣1分，扣完为止。			
	与互联网对接连通性要求	5	与互联网对接连通性要求99.99%，每下降0.01%，扣1分，扣完为止。			
	与安全接入区对接连通性要求	5	与安全接入区对接连通性要求99.99%每下降0.01%，扣1分，扣完为止。			
	与专网接入区对接连通性要求	5	与专网接入区对接连通性要求99.99%每下降0.01%，扣1分，扣完为止。			
	网络故障响应及时率	10	通过热线电话、微信等方式向各委办局单位提供服务，一般服务请求响应时间为30分钟内，紧急服务请求为5分钟内。≥90%得10分，每降低1%，扣0.33分，未达60%不得分。			
效果目标（10分）	服务使用单位满意度	10	通过向各委办局单位发放满意度问卷调查，了解政务安全管理各类服务的满意度。≥90%得10分，每降低1%，扣0.33分，未达60%不得分。			
合计		100				
说明： 1、 依据本项目应实现的目标，对照已完成的情况，进行打分。 2、等级说明：评分合计85（含）-100分为优秀；70（含）-85分为良好；60（含）-70分为合格；0-60分为不合格。考核合格后支付项目服务费。 3、产出目标、效果目标可根据可根据数据运营实际工作情况以及上级单位考核内容同步进行增加或修改相应指标。						