项目编号：310109000250605115128-09255652

二级政务网年租费（2025-2026 年）

公开招标文件

2025年08月04日

采购单位：上海市虹口区城市运行综合管理中心

地　　址：飞虹路 500 号

2025年08月04日

目　　录

第一章　公开招标采购公告

根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》等规定，现就下列项目进行公开招标采购，欢迎提供本国货物、服务的单位或个人前来投标：

一、项目编号：3101090002506051151 28-09255652

二、公告期限：5 个工作日

三、采购项目内容、数量及预算

包号	包名称	数量	单位	预算金额（元）	简要规格描述或包基本概况介绍	最高限价（元）	备注
1	二级政务网年租费（2025-2026年）	1		8000000.00	虹口区电子政务外网的网络、安全以及日常运营维	8000000.00	

					护，本项目整体服务期为一年。详见招标文件中采购需求。		

四、合格投标人的资格要求

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

无

二级政务网年租费（2025-2026 年）资格审查要求包 1

序号	类型	审查要求	要求说明	项目级/包级
1	自定义	符合《中华人民共和国政府采购法》第二十二条规定及《中华人民共和国政府	提供有效证明材料。	项目级

		采购法实施条例》第十七条要求的供应商。		
2	自定义	根据《财库[2016]125号》之规定，企业信用报告合格的供应商。	提供有效证明材料。	项目级
3	自定义	有效提供企业自我声明——前三年内无违法记录及不诚信行为的供应商。	提供有效证明材料。	项目级
4	自定义	未列入失信被执行人、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、近三年不存在负面记录及其他不符合《中华人民共和	根据响应人提供的材料及外部查询有效内容核对判定。	项目级

		国政府采购法》第二十二条规定条件的供应商。		
5	自定义	投标有效期不足 90 天。	根据响应人的响应内容判定。	项目级
6	自定义	响应文件未按采购文件要求签署、盖章的	根据响应人的响应内容判定。	项目级
7	自定义	未满足带“*”号实质性指标的响应文件	根据响应人的响应内容判定。	项目级
8	自定义	以赠送方式响应的、对一个标项提供两个投标方案或两个报价的	根据响应人的响应内容判定。	项目级
9	自定义	响应文件含有采购人不能接受的附加条件的	根据响应人的响应内容判定。	项目级
10	自定义	不符合法律、法规和本采购文件规定的其他	根据响应人的响应内容判定。	项目级

		实质性要求的。		
11	自定义	供应商参加政府采购活动应当提交反映其财务状况、缴纳税收和社会保障资金情况的书面声明。	根据响应人的响应内容判定。	项目级

五、投标报名：

1、报名时间：2025-08-06 至 2025-08-14 上午 09:30:00~11:00:00；下午 14:30:00~16:30:00（节假日除外）。

2、报名方式：本项目实行网上报名，不接受现场报名。供应商登录上海政府采购网（http://www.zfcg.sh.gov.cn/）进行报名。

3、招标文件售价：0 元，招标文件请至公告附件处下载。

六、投标保证金：

[投标保证金收款账户（金额、开户行、户名、账号等）]

如需缴纳保证金，投标人应于 时前将投标保证金交至上海市虹口区政府采购中心，投标保证金若以网银、电汇方式交纳的，请将网银电脑打印凭证、电汇底单复印件写上所投项目名称、编号、投标联系人、联系电话，请在开标前一个工作日前到招标方服务台开收据。

七、投标截止时间和地点：

2025-08-27 10:00:00 上海政府采购网

八、开标时间及地点：

本次招标将于 2025-08-27 10:00:00 时整在上海政府采购网开标。

第二章　投标人须知

前附表

序号	内　容	要　　求
1	项目名称及数量	详见《公开招标采购公告》二
2	信用记录	根据财库[2016]125号文件，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），以开标当日网页查询记录为准。对列入失信被执行人、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的供应商，**其投标将作无效标处理**。
3	政府采购节能环保产品	投标产品若属于节能环保产品的，请提供财政部、环境保护保部发布有效期内环境标志产品政府采购清单以及财政部、发改委联合发布有效期内节能产品政府采购清单。 招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人须提供该清单内产品，**否则其投标将作为无效标处理。**
4	小微企业有关政策	1、根据财库〔2011〕181号的相关规定，在评审时对小型和微型企业的投标报价给予10%的扣除，取扣除后的价格作为最终投标报价（此最终投标报价仅作为价格分计算）。属于小型和微型企业的，投标文件中投标人必须提供的《中小企业声明函》以及本单位、制造商（如有）“国家企业信用信息公示系统——小微企业名录”页面查询结果（查询时间为投标前一周内，并加盖本单位公章），并在报价明细表中说明制造商情况。 2、根据财库[2017]141号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141号文件第一条的规定，并在投标文件中提供残疾人福利性单位声明函（见附件）。 3.根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在投标文件中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（格式自

		拟)。” **(注：未提供以上材料的，均不给予价格扣除)。**
5	答疑与澄清	投标人如对招标文件有异议，应当于公告发布之日起至公告期限满第 7 个工作日内，以书面形式向招标采购单位提出，逾期不予受理。
6	是否允许采购进口产品：	不允许进口产品具体要求详见第四章招标需求各标项的对应内容。
7	是否允许转包与分包	转包：否 分包：否
8	是否接受联合体投标	不允许 接受联合体投标的请提供联合体协议书。
9	是否现场踏勘	不组织现场踏勘 具体要求详见第四章招标需求各标项的对应内容。
10	是否提供演示	不进行演示 系统演示具体要求详见第四章招标需求各标项的对应内容。
11	是否提供样品	不要求提供样品 具体要求详见第四章招标需求各标项的对应内容。
12	投标文件组成	投标文件由资质文件、技术及商务文件、报价文件组成
13	中标结果公告	中标供应商确定之日起 2 个工作日内，将在上海市政府采购网(http://www.zfcg.sh.gov.cn/)发布中标公告，公告期限为 1 个工作日。
14	投标保证金	交纳：投标保证金应按《招标采购公告》六规定交纳。若一次投多个标项，只需交纳一个标项的投标保证金（按所需保证金最大额的标准交纳为准）。 退还：中标通知书发出之日起5个工作日内，未中标的投标人提供交入投标保证金时取得的第二联“供应商退款凭据”到招标方服务台办理，招标方以电汇或转账等方式退还投标保证金。
15	合同签订时间	中标通知书发出后 30 日内。规范政府采购合同签订行为，财政部制定了《政府采购货物买卖合同（试行）》，供采购人参考使用。
16	履约保证金	合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的10%。
17	付款方式	国库集中支付（采购人自行支付）详见各标项的商务要求表
18	投标文件有效期	90天
19	投标文件的	http://www.zfcg.sh.gov.cn接收

	接收	
20	招标方代理费用	无
21	解释权	本招标文件的解释权属于上海市虹口区政府采购中心。
22	新出台文件及要求	《关于简化政府采购供应商资格审查有关事项的通知》主要内容：不再要求供应商提供财务状况报告、依法缴纳税收和社会保障资金的证明材料。供应商参加政府采购活动应当提交反映其财务状况、缴纳税收和社会保障资金情况的书面声明。（如与本次采购过程中的内容有冲突，按照新文件执行）。超出招标文件要求的规定次数的质疑将不再受理。
23	备注	1，为方便告知投标单位后续政府采购相关事宜，投标单位需在投标文件中填写邮箱信息。2，电子投标文件在投标截止时间前上传至上海政府采购网，可不再打印纸质投标文件交至政府采购代理机构。3，虹口政府采购中心联系方式见采购公告，邮箱：hkqzfcgzx@163.com。

一、总　则

（一）适用范围

仅适用于本次招标文件中采购项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）定义

1、“招标方”系指组织本项目采购的上海市虹口区政府采购中心。

2、“投标人”系指向招标方提交投标文件的单位或个人。

3、“采购人” 系指委托招标方采购本次货物、服务项目的国家机关、事业单位和团体组织。

4、“货物”系指招标文件规定投标人须向采购人提供的一切材料、设备、机械、仪器仪表、工具及其它有关技术资料和文字材料。

5、“服务”系指招标文件规定投标人须承担的劳务以及其他类似的义务。

6、“项目”系指投标人按招标文件规定向采购人提供的需求总称。

（三）投标人及委托有关说明

1、授权代表须携带有效身份证件。如授权代表不是法定代表人，须有法定代表人出具的授权委托书（格式见附件）。

2、投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有。投标人投标所使用的采购项目实施人员必须为投标人员工（或投标人控股公司正式员工）。

3、以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

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

5、投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

（四）投标费用

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用

（招标文件有其他相反规定除外）。

（五）质疑

1、投标人认为招标过程或中标结果使自己的合法权益受到损害的，可以在中标结果公告期限届满之日起七个工作日内，以书面形式向招标方提出质疑，须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。2、质疑应当以书面形式提出，格式见《政府采购质疑和投诉办法》（财政部令第94号）附件范本，下载网址：中国政府采购网(http://www.ccgp.gov.cn/)，位置：“首页-下载专区-政府采购供应商质疑函范本”。供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

a 供应商的姓名或者名称、地址、邮编、联系人及联系电话；

b 质疑项目的名称、编号；

c 具体、明确的质疑事项和与质疑事项相关的请求；

d 事实依据；

e 必要的法律依据；

f 提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。质疑应明确阐述招标过程或中标结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理，质疑函不符合《政府采购质疑和投诉办法》相关规定的，应在规定期限内补齐的，招标方自收到补齐材料之日起受理；逾期未补齐的，按自动撤回质疑处理。

（六）招标文件的澄清与修改

1、投标人应认真阅读本招标文件，发现其中有误或有不合理要求的，投标人应当于公告发布之日起至公告期限满第7个工作日内以书面形式向招标方提出。招标方将在规定的时间内，在财政部门指定的政府采购信息发布媒体上发布更正公告。**逾期提出招标方将不予受理。**

2、招标方主动进行的澄清、修改：招标方无论出于何种原因，均可主动对招标文件中的相关事项，用补充文件等方式进行澄清和修改。

3、招标文件澄清、答复、修改、补充的内容为招标文件的组成部分。

当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

二、投标文件的编制

（一）投标文件的组成

投标文件由资质文件、技术及商务文件、投标报价文件三部份组成。

1、资质文件

（1）投标声明书（格式见附件，含无重大违法记录及不诚信行为声明）；

（2）投标单位可自查自招标公告发布之日起至投标截止日内任意时间的“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）投标人信用情况。对列入失信被执行人、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的供应商，其投标将作无效标处理。（投标单位可不用截图于投标文件，采购人、采购代理机构或由采购人委托的评标委员会以开标当日的查询结果为准）。

（3）法定代表人授权委托书(格式见附件)；

（4）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

（5）联合投标协议书（若需要）；

（6）联合投标授权委托书（若需要）；

（7）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

2、技术及商务文件

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人

力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标方认为需要的其他文件资料。

投标单位可根据采购需求内容和评审因素作技术文件响应。

3、报价文件：

（1）投标报价明细表（格式见附件）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）小微企业声明函、网页证明资料（若有，格式见附件）；

（4）残疾人福利企业声明函（若有，格式见附件）。

注：法定代表人授权委托书、投标声明书、投标报价明细表必须按招标文件格式要求正确签署并加盖投标人公章。

（二）投标文件的语言及计量

1、投标文件以及投标人与招标方就有关投标事宜的所有来往函电，均应以中文简体字书写。除签名、盖章、专用名称等特殊情形外，投标文件中以中文汉语以外的文字表述部分视同未提供。

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，应采用中华人民共和国法定计量单位（货币单位：人民币元），**否则将作无效标处理**。

（三）投标文件的有效期

1、自投标截止日起 90 天内投标文件应保持有效。**有效期不足的投标文件将作无效标处理。**

2、中标人的投标文件自开标之日起至合同履行完毕止均应保持有效。

（四）投标文件的签署和份数、包装

1、投标人应按本招标文件规定的格式和顺序编制、装订投标文件并标注页码，投标文件内容不完整、编排混乱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。

2、投标人在 http://www.zfcg.sh.gov.cn 上传投标文件。

3、投标文件须由投标人在规定位置盖章并由法定代表人或法定代表人的授权委托人签署，投标人应写全称。

4、投标文件不得涂改，若有修改错漏处，须加盖供应商公章或者法定代表人或授权委托人签名或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人负责。

（五）投标报价

1、投标文件只允许有一个报价，投标报价应按招标文件中相关附表格式填报，该投标报价应与明细报价汇总相等，且**不允许出现报价优惠等字样（明细出现“0”元，视同赠送）**。

2、投标报价**应包含项目所需全部货物、服务，不得缺漏**，是履行合同的最终价格（含货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用）。

3、投标报价总价金额到元为止，如投标报价总价出现角、分，将被抹除。

（六）投标保证金

1、投标人须按规定提交投标保证金。

2、保证金形式：网银、汇票、电汇、转帐支票。

3、招标方不接受以现金支票、现金及个人转账方式交纳的保证金。

投标保证金若以网银、电汇方式交纳的,请将网银电脑打印凭证、电汇底单复印件写上所投项目名称、编号、投标联系人、联系电话，请在开标前一个工作日前到招标方服务台开收据。

4、招标方在中标通知书发出后五个工作日内退还投标保证金，供应商办理投标保证金退还时需提供收据的第二联“供应商退款凭据”。**详见**

上海市政府采购网 http://www.zfcg.sh.gov.cn/ ，位置：“首页-在线服务”

保证金不计息。

5、投标人有下列情形之一的，投标保证金将不予退还：

（1）投标人在投标截止时间后撤回投标文件的；

（2）投标人在投标过程中弄虚作假，提供虚假材料的；

（3）中标人无正当理由不与采购人签订合同的；

（4）将中标项目转让给他人或者在投标文件中未说明且未经招标采购单位同意，将中标项目分包给他人的；

（5）其他严重扰乱招投标程序的；

（七）串通投标认定

有下列情形之一的，视为投标人串通投标，其投标无效：

1、不同投标人的投标文件由同一单位或者个人编制；

2、不同投标人委托同一单位或者个人办理投标事宜；

3、不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

4、不同投标人的投标文件异常一致或者投标报价呈规律性差异；

5、不同投标人的投标文件相互混装；

6、不同投标人的投标保证金从同一单位或者个人的账户转出。

（八）投标无效的情形

在评审时，如发现下列情形之一的，投标文件将被视为无效：

1、未按规定交纳投标保证金的；

2、投标方未能提供合格的资格文件、投标有效期不足的；

3、投标人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的；

4、投标文件未按招标文件要求签署、盖章的；

5、与招标文件有重大偏离、未满足带“*”号实质性指标的投标文件；

6、招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人未提供该清单内产品的；

7、投标报价超出招标文件中规定的预算金额或者最高限价的；

8、标项以赠送方式投标的、对一个标项提供两个投标方案或两个报价的；

9、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，且不能证明其报价合理性的；

10、投标人不接受报价文件中修正后的报价的；

11、未按本章“二、投标文件的编制”第五点投标报价要求报价的；

12、投标文件含有采购人不能接受的附加条件的；

13、投标人被视为串通投标的；

14、不符合法律、法规和本招标文件规定的其他实质性要求的。

（九）错误修正

投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

（一）《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。

（二）大写金额和小写金额不一致的，以大写金额为准；

（三）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；

（四）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，按照前款规定的顺序修正。修正后的报价按照经投标人加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，投标人不确认的，其投标无效。

注：除评标委员会按相关法律法规要求的澄清、说明或者补正情形之外，《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。

三、组织开、评标程序及评标委员会的评审程序

（一）组织开标程序

招标方将按照招标文件规定的时间、地点和程序组织开标（http://www.zfcg.sh.gov.cn/上开展）。

（二）组织评标程序

招标方将按照招标文件规定的时间、地点和程序组织评标，各评审专家及相关人员应参加评审活动并接受核验、签到，无关人员不得进入评审现场。

1、按规定统一收缴、保存评标现场相关人员通讯工具。

2、介绍评审现场的人员情况，宣布评审工作纪律，告知评审人员应当回避情形；组织推选评标委员会组长。

3、组织评标委员会各位成员签订《政府采购评审人员廉洁自律承诺书》。

4、采购人可以在评标前说明项目背景和采购需求，说明内容不得含有歧视性、倾向性意见，不得超出招标文件所述范围。说明应当提交书面材料，并随采购文件一并存档。

5、根据需要简要介绍招标文件（含补充文件）制定及质疑答复情况、按书面陈述项目基本情况及评审工作需注意事项等，让评审专家尽快知悉和了解所评审项目的采购需求、评审依据、评审标准、工作程序等；提醒评标委员会对客观评审项目应统一评审依据和评审标准，对主观评审项目应确定大致的评审要求和评审尺度；对评审人员提出的有关招标文件、投标文件的问题进行必要的说明、解释或讨论。

6、采购人代表或采购代理机构或由采购人委托的评标委员会对投标人资格文件进行审查并以开标当日为准对投标人“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）信用记录情况进行核实。

7、评标委员会组长组织评审人员独立评审。评标委员会对拟认定为投标文件无效，可组织相关投标人代表进行陈述、澄清或申辩；招标方可协助评标委员会组长对打分结果进行校对、核对并汇总统计；对明显畸高、畸低的评分，评标委员会组长应提醒相关评审人员进行复核或书面说明理

由，评审人员拒绝说明的，由现场监督员据实记录；评审人员的评审、修改记录应保留原件，随项目其他资料一并存档。

8、做好评审现场相关记录，协助评标委员会组长做好评审报告起草、有关内容电脑文字录入等工作，并要求评标委员会各成员签字确认。

9、评审结束后，招标方应对评标委员会各成员的专业水平、职业道德、遵纪守法等情况进行评价；同时按规定向评审专家发放评审费，并交还评审人员及其他现场相关人员的通讯工具。

（三）评审程序

1、在评审专家中推选评标委员会组长。

2、评标委员会组长召集成员认真阅读招标文件以及相关补充、质疑、答复文件、项目书面说明等材料，熟悉采购项目的基本概况，采购项目的质量要求、数量、主要技术标准或服务需求，采购合同主要条款，投标文件无效情形，评审方法、评审依据、评审标准等。

3、评审人员对各投标人投标文件的有效性、符合性、完整性和响应程度进行审查，确定是否对招标文件作出实质性响应。

4、评审人员按招标文件规定的评审方法和评审标准，依法独立对投标人投标文件进行评估、比较，并给予评价或打分，不受任何单位和个人的干预。

5、评审人员对各供应商投标文件非实质性内容有疑议或异议，或者审查发现明显的文字或计算错误等，及时向评标委员会组长提出。经评标委员会商议认为需要供应商作出必要澄清或说明的，应通知该投标人以书面形式作出澄清或说明。授权代表未到场或拒绝澄清说明或澄清说明的内容改变了投标文件的实质性内容的，评标委员会有权对该投标文件作出不利于投标人的评判。书面通知及澄清说明文件应作为政府采购项目档案归档留存。

6、评审人员需对招标方工作人员唱票或统计的评审结果进行确认，现场监督员应对评审结果签署监督意见。如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，

应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。

7、评标委员会根据评审汇总情况和招标文件规定确定中标候选供应商排序名单。

8、起草评审报告，所有评审人员须在评审报告上签字确认。

四、评审原则

1、评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。

2、评审专家因回避、临时缺席或健康原因等特殊情况不能继续参加评审工作的，应按规定更换评审专家,被更换的评审人员之前所作出的评审意见不再予以采纳，由更换后的评审人员重新进行评审。无法及时更换专家的，要立即停止评审工作、封存评审资料，并告知投标人择期重新评审的时间和地点。

3、评审人员对有关招标文件、投标文件、样品或现场演示（如有）的说明、解释、要求、标准存在不同意见的，持不同意见的评审人员及其意见或理由应予以完整记录,并在评审过程中按照少数服从多数的原则表决执行。对招标文件本身不明确或存在歧义、矛盾的内容，应作对投标人而非采购人有利的解释;对因招标文件中有关产品技术参数需求表述不清导致投标人实质性响应不一致时，应终止评审，重新组织采购。评审人员拒绝在评审报告中签字又不说明其不同意见或理由的,由现场监督员记录在案后，可视为同意评审结果。

4、财政部令第 87 号《政府采购货物和服务招标投标管理办法》第三十一条规定：使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机

抽取方式确定，其他同品牌投标人不作为中标候选人。

非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前款规定处理。

五、确定中标供应商的原则

1、项目由评标委员会根据第三章《评标办法与评分标准》规定提出中标候选人排序。

2、采购人应当自收到评标报告之日起 5 个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人，或者采购人委托评标委员会在评标报告确定的中标候选人名单中按顺序确定中标人。采购人在收到评标报告 5 个工作日内未按评标报告推荐的中标候选人顺序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

3、采购结果经采购人确认后，招标方将于 2 个工作日内在上海市政府采购网上发布中标公告，并向中标方签发《中标通知书》。

六、合同授予

（一）签订合同

1、采购人与中标人应当在《中标通知书》发出之日起 30 日内签订政府采购合同，招标方作为合同签订的鉴证方。

2、中标人拖延、拒签合同的，将被扣罚投标保证金并取消中标资格。

（二）履约保证金

1、合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的 10%。

2、按合同约定办理履约保证金退还手续。

七、货款的结算

货款由采购人按招标文件规定的付款方式自行支付。

第三章　评标办法及评分标准

根据《中华人民共和国政府采购法》等有关法律法规，结合本项目的实际需求，制定本办法。

一、总则

本次评标总分为 100 分。合格投标人的评标得分为各项目汇总得分，中标候选资格按评标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，按技术得分由高到低顺序排列。评分过程中采用四舍五入法，并保留小数 2 位。采购文件中未规定的评标标准不得作为评审依据。

二、分值的计算

技术、资信、商务及其他分按照评标委员会成员的独立评分结果汇总后的算术平均分计算，计算公式为：

技术、资信商务及其他分=评标委员会所有成员评分合计数/评标委员会组成人员数

投标人评标综合得分=价格分+(技术分+资信商务及其他分)

三、评标内容及标准

综合评分法

二级政务网年租费（2025-2026 年）包 1 评分规则：

评分项目	分值区间	评分办法
报价分	0~10	投标报价得分=价格分值×（最低有效投标价/有效投标报价）
业务设计分析	0~5	（1）投标人对现有网络架构与分区情况、网络与安全设备部署情况、网络流量情况、IP 地址与路由规划、网络所承载应用情况的了解，要求充分、完整、准确。（0-3 分） （2）根据以上了解情况，投标人需要从网络、安全、运营服务等三个方面对项目进行分析，要

		求分析充分，服务目标精确。（0-2 分）
业务连续性	0~9	（1）投标方案设计及实施中充分考虑业务连续性要求，对现有区级政务外网网络和用户业务的连续性运行、网络安全稳定性影响最小。可达成服务的工作时间计划周期最短，根据方案进行综合评价（0-3 分）； （2）网络服务系统在网络容灾备份设计上的先进性、可靠性和安全性情况，要求充分考虑业务连续性要求，根据方案进行综合评价（0-3 分）。 （3）投标方应

		保障现有区级政务外网网络和用户业务无中断。（0-3 分）
网络技术架构	0~5	（1）要求对现有政务外网运行技术架构的了解和分析充分、资料详实，对方案设计有深入把握。网络技术架构需要高可用、强扩展并适度超前，管理功能要求高效可实现性高，根据方案进行综合评价（0-3 分）； （2）网络技术架构满足项目服务的支撑与后续业务扩展，部署或变更实施所需时效性最强、对政务外网运行影响度最低，根据方案进行综合评价（0-2

		分）。
网络业务规划方案	0~5	（1）要求对区级政务外网业务类规划以及网络 IP 资源等业务情况了解充分、资料详实。业务规划方案对网络“一网双平面”实现、业务带宽及 QOS 流量调整、SDN 配置调整、主备保护、IP 地址规划等方面提供技术方案的实质性响应，根据方案可实施性、业务连续过渡性、可扩展性、可管理性情况综合评价（0-2 分）； （2）服务技术方案业务规划执行实现的时间计划安排，要求满足业务开

		通时间需要，对网络风险影响程度最低（0-3 分）。
与市级政务外网对接方案	0~4	（1）作为“全市一张网”的市区两级政务外网，投标人所提出的与市级政务外网对接实施方案要求完整、可行、安全。（0-2 分） （2）从对接业务类型、网络协议、IP 地址规划等方面进行方案描述。（0-2 分）
与市级政务外网管理系统承载网对接方案	0~6	（1）投标人所提出的与市级政务外网管理系统承载网对接实施方案要求完整、可行、安全。（0-3 分）（2）从对接业务类型、对接网

		络拓扑图，接入方式，对接带宽，IP 地址及路由协议规划，职责分工规划，具体实施步骤等方面进行方案描述。（0-3 分）
机房要求	0~2	投标人所提供运营商租用核心、汇聚机房距离要达到用户的基本功能实现要求，是否达到需求要求由评标委员会认定，可提供自有产权证明或机房长期租赁合同或者由投标单位承诺中标后提供符合要求的自有产权证明或机房长期租赁合同。
服务所用机房、光缆资源情况	0~6	（1）投标人需要提供本项目 2 个核

		心节点和3个汇聚节点（其中核心节点1与汇聚节点1同址）、8个街道办事处及8个社区事务服务中心共计 20 个接入点光缆接入设计图纸。（0-3 分） （2）投标所提供接入点光缆设计图纸符合要求，包括接入光缆、双路由走向、管井信息、交接箱信息、光缆芯数等内容（0-3 分）
安全方案设计	0~3	对政务外网安全威胁与风险情况有详实了解、资料充分，对全网业务安全性理解深入完善。要求在网络物理安全、传输安全、各主要区

		域对接边界安全、用户接入安全等方面有实质性的设计响应，设计详尽完善，安全方案部署对政务外网现网业务的影响和风险程度最低，实施具有可行性、时效性强（0-3分）。
安全等保防护情况	0~2	投标人所提供电子政务外网安全方案的合规性在以往政务外网服务项目中获得验证的，提供类似项目并通过安全等级保护测评报告，得 2 分。
全网业务及服务开通	0~10	（1）投标人制定的全网服务开通方案具备技术可行性和实践操作性。

		重点评估方案对现有网络设施、系统运行、业务流量、安全策略的影响程度。（0-3 分） （2）投标人承诺的服务开通所需的具体时限优于或者满足采购文件要求，且科学、合理（考虑到业务规模、技术复杂度、资源投入等）。（0-3 分） （3）投标人需要提供保障按时开通的具体计划、资源配置（人力、软硬件资源到位计划），包含应对计划外延误的应急预案或措施。（0-2 分） （4）投标人在

		服务开通实施计划中，需要明确提出对现有网络生产环境影响最小及服务连续性保障的承诺与自罚条款。（0-2 分）
运维服务方案整体设计	0~3	项目网络运营服务方案要求完整、合理，包括服务内容、服务团队、日常运维方案、应急响应方案、网络安全防护方案、文档和资料管理、培训等内容；（0-3 分）
服务运营与质量、安全保证措施	0~2	根据投标人提供的服务质量保证措施进行综合评分：服务质量保证措施完整并有自罚承诺、可操作性强，人员服务质量保障制度完

		善，提供完善的延伸服务，根据措施完整性情况评审。（0-2 分）
业务迁移方案	0~5	（1）如涉及业务割接，投标方应针对本次服务内容提供符合本区政务外网现网要求的无缝业务割接方案，须承诺所进行的网络割接等操作不影响网络正常运行，并提供网络无缝业务迁移承诺函（0-2 分） （2）投标人所提供业务迁移方案（含核心、汇聚、接入层、互联网出口、政务云应用等）要求完整、可行，割接步骤具体详实，实施保

		障措施完备（0-3 分）
服务团队组织与架构	0~2	要求运营整体团队的组织设置与功能架构方面设计周密，岗位职责、制度流程明确，具备长期可操作性。（0-2 分）
服务团队人员配置	0~13	（1）要求运维团队配置合理，团队数量和人员专业性配置齐全，提供每一位团队人员有关资质、社保证明、学历、专业、职称及主要从业经历。（0-2 分） （2）项目负责人具有本科及以上学历，且具备从事项目负责人或运维经理的经验，匹配采购需求中的岗位要求。

		（0-3 分） （3） 项目运营经理具备从事项目经理或运维经理的经验，匹配采购需求中的岗位要求。（0-2 分） （4）网络运维工程师配置合理，具有网络、机房、安全系统等实际维护经验，匹配采购需求中的岗位要求。（0-2 分） （5） 网络安全工程师配置合理，具备网络安全项目经验，匹配采购需求中的岗位要求。（0-2 分） （6）驻场工程师配置合理，提供

		7*24 小时驻场服务。要求驻场工程师均具有网络、机房、安全系统等实际维护经验，匹配采购需求中的岗位要求。（0-2分）
类似项目业绩	0~8	投标人近3年内承接的有效的类似项目业绩。是否属于有效类似业绩由评委认定。每有一个有效业绩得2分，最高得分为8分，没有有效的类似项目业绩的得0分。需提供相关业绩的合同关键页扫描件（至少包含合同双方签章页、项目名称及内容、合同金额、合同签订日期），否则将不予认

		可。

第四章　招标需求

二级政务网年租费项目（2025-2026）　采购需求

序号	事项	内容
1	采购单位（加盖公章）	上海市虹口区城市运行综合管理中心
2	项目名称	二级政务网年租费项目（2025-2026）
3	采购预算金额	800 万 元（国库资金：　　元）
4	项目属性	货物□　　服务☑
5	采购意向是否已公开	2025 年 06 月 05 日于上海政府采购网发布采购意向公示
6	采购标的所属行业(按工信部联企业(2011)3006 号和财库〔2020〕46 号文，用于中小企业声明函)	软件和信息技术服务业
7	特定资格要求	无
8	是否专门面向中小微企业	是□　　否☑
9	是否招一用三	是□　　否☑
10	合同履行期限	365 日历天
11	质保或免费维护期	无
12	是否允许联合体投标	是□　　否☑
13	是否允许采购进口产品	是□　　否☑
14	是否现场踏勘	是□　　否☑
15	是否要求提供样品	是□　　否☑
16	付款方式	分两笔支付，合同签订后每 6 个月支付 50%
17	验收方式（履约验收后将材料交由政采中心电子归档保存）	1. 验收方式： （1）自行组织☑ （2）委托第三方□（验收主体_____） 2.是否邀请本项目其他供应商参加验收：是□否☑ 3.是否邀请专家参加验收：是□　否☑

		4.是否邀请服务对象参加验收：是口　否☑ 5.是否第三方检测机构参加验收：是口　否☑ 6.是否参加抽查检测：是口　否☑ 7.是否存在破坏性检测：是口　否☑ 8.履约验收时间：（2 选 1） （1）具体验收日期：_____ （2）验收天数（自供应商提出验收之日起几日内组织验收）：__30 天__ 9.履约验收方式：一次性验收☑　分期验收口
18	本项目询问、质疑受理委托授权范围	虹口区政府采购中心
19	本项目评审办法	综合评分法☑　　最低评标价法口
20	按财政部 22 号令《政府采购需求管理办法》第十一条要求，是否已完成需求调查工作	是☑　　否口

项目概述

本项目根据《上海市推进新型基础设施建设行动方案（2020-2022 年）》（沪府[2020]27 号）总体部署，所采购的虹口区电子政务外网通信服务是为上海市虹口区政务外网全区节点的网络通信提供 1 年的城域网络通信服务。

虹口区电子政务外网与互联网逻辑隔离，并上联上海市政务外网，属非涉密网性质，是虹口区政府部门的业务专网，主要运行政务部门面向社会的专业性服务业务和不需在政务内网上运行的业务。虹口区政务外网是通过将区内区级委办局、区直属单位以及全区 8 个街道居委的业务网接入至统一的物理传输网络，以此为基础而形成的骨干网络平台。虹口区电子政务外网目前是承载全区政务服务“一网通办”、城市运行“一网统管”等重要政务业务，以及支撑城市数字化转型的关键基础网络设施。

本次项目拟采购整体虹口电子政务外网平台服务，整体平台服务须满足《上海市电子政务外网建设和运行管理指南》各项服务网络技术要求以及区政务外网实际业务扩展需求，服务内容涵盖网络升级改造扩容服务、服务基础光缆及机房设施服务、网络日常运营及安全防护服务等。本项目整体服务期为 1 年。

项目采购形式说明

本次项目采购的虹口区电子政务外网网络服务是以应用为导向，以满足业务需求为前提，以网络资源集约化使用为原则，采购的覆盖全区的、统一区级政务外网网络通信服务。通过该网络通信服务，合理配置虹口区电子政务外网网络服务资源，避免网络重复建设。本次招标的区级政务外网通信服务形式是整体网络交付服务方式，本项目不涉及设备采购，所有设备由中标方配置，付款方式：分两笔支付， 合同签订后每 6 个月支付 50%。

项目总体技术规范要求

投标人需根据本次招标文件下述所提出的具体技术要求，针对项目中的总体技术规范要求、网络服务技术要求、实施要求、服务与管理要求、验收要求及服务承诺，在投标文件中进行逐条实质性响应与应答，并根据实际投标情况进行具体的偏离度响应说明。

3.1 总体需求及目标要求

虹口区电子政务外网平台服务项目采用购买服务方式，即投标人提供虹口区电子政务外网网络服务，服务涵盖网络升级改造扩容服务、基础光缆及机房设施服务、网络日常运营及安全防护服务等。本项目整体服务期为 1 年；本次网络服务的总体要求如下:

3.2 服务总体要求

投标人按照本需求文件所要求的网络技术、实施以及服务要求，为虹口区电子政务外网提供可靠、安全、稳定的政务专用通信网络，并在服务周期内基于该专用通信网络，为区级政务外网现有在网服务用户及后续新增用户提供可扩展的专用网络通信带宽服务，满足用户在新建、搬迁、扩容、资源调整等方面的网络通信服务及运行管理需要。

投标人需按照本需求文件所要求的网络技术、实施以及服务要求，遵循国家和市级政务外网相关管理标准与规范，设计并实质性响应提供虹口区电子政务外网的整体政务专用网络服务方案，包括但不限于对虹口区电子政务外网业务发展需求的整体理解、服务周期内网络技术发展规划以及满足本次服务所需的专用政务通信网络的整体网络拓扑设计、设备选型设计、网络地址及各类业务规划设计、网络及安全功能性能指标设计，并对网络在带宽服务与扩展能力、网络通信设备保护与运行保障、网络运营及安全管理、人员保障及咨询服务等方面提供详尽可行、实质性的服务方案响应。

1、要求本项目网络服务所涉及所有网络软硬件设备皆保证为虹口区电子政务外网专网专用，不得用于其他任何用途与业务，包括但不限于光传输设备、路由器、交换机、网络安全设备。并提供专网专用承诺函。

2、要求本项目网络服务所涉及所有硬件产品要求具备较长的设备使用寿命周期，包括但不限于光传输设备、路由器、网络安全设备。

3、本项目所有软硬件必须是市场主流产品，有稳定的生命周期和发展策略;

4、投标人应对各项指标做出实质响应。性能指标需满足要求，可扩展性指标（如内存、插槽等）要说明可扩展能力。如果缺少指标参数、低于或高于需求的指标， 请在偏离表中明确说明;

5、投标人所提供的所有设备除特定的外接设备外，所有提供的软、硬件（如接口设备、缆线、软件、服务器等，包括招标书中未列出而系统实施又必须的软件、硬件）需配齐以构成一套适用系统。如果投标人在中标并签署合同后，在供货或系统集成时出现软、硬件有任何遗漏，均必须由投标人提供。

6、要求投标人承诺本项目所提供网络服务可按照《上海市电子政务外网建设和运行管理指南》要求完成与市级政务外网实现对接。要求投标人提供对接方案包括但不限于接入方式、对接带宽，IP 地址及路由协议规划，业务流程规划等。 同时要求投标人提供与市级政务外网对接承诺书;

7、要求投标人承诺本次所提供网络安全管理中心服务需与市级政务外网安全监测平台实现数据接口对接以及安全事件业务的联动协同。并提供具体接口对接方案以及联动协同方案以及承诺书;

8、本次项目实施过程应满足《网络安全等级保护基本要求》第三级标准中对设备配置、施工规范、集成文档、施工人员管理等要求。此外，在安全等级测评过程中，应配合测评单位的工作，对测评过程中有不满足的内容（需整改的）由投标人免费限期解决，如未能解决的，采购方有权向投标人进行索赔并解除合同。同时要求投标人提供相应承诺书。

3.3 服务交付及服务期限

投标人需按本招标要求中所规定的各项服务要求，自收到中标通知书的 20 个自然日内，开始向本次招标中所提出的服务对象及范围内用户提供虹口区电子政务外网网络通信服务。具体服务交付验收要求详见第 7 部分验收要求。

3.4 服务对象及范围

本次虹口区电子政务外网的网络通信服务主要服务于区级委办局、事业单位、区直属企业、街道办事处以及社区服务中心，投标人本次为虹口区电子政务外网提供的通信网络及服务支持为全区范围内的政务外网用户提供专用网络通信服务。同时，投标人承诺在服务周期内，可按开通和服务时间质量、时间要求，根据政务外网用户的实际网络应用需要，提供上述地区和范围内用户的专用网络通信服务。

按照《上海市电子政务外网建设和运行管理指南》以及虹口区电子政务应用实际网络需求，本项目网络服务包括：光传输网络服务、SDN 业务网络服务、业务网络边界安全体系服务以及网络安全管理中心服务。具体服务内容如下:

1、提供光传输网络服务。在政务外网核心层和汇聚层，采用 OTN 光传输设备组建底层光传输网络，实现核心、汇聚双 100G 带宽能力。

2、提供 SDN 业务网络服务。业务网络采用核心、汇聚、接入三层架构与“一网双平面”架构设计，在核心层、汇聚层部署支持 IPv4/IPv6 双栈技术和 SDN 技术的路由器设备，实现数据平台承载网络数据流量，视频平面承载网络视频流量，两个平面在区政务外网上逻辑隔离、独立运行，且互为冗余备份。

3、提供业务网络边界安全体系服务。根据区政务外网联接对象以及承载信息系统安全等级的不同，在互联网边界、市政务外网边界、政务云边界、灾备区及其他重要边界部署相应的网络安全防护设备和措施，从而满足等保 2.0 三级防护能力要求。

4、提供安全管理中心服务。根据等保 2.0 三级防护能力要求，部署态势感知平台、通报预警平台、威胁情报共享平台、漏洞扫描系统、安全管理控制系统、日志审计系统以满足系统管理、审计管理和安全管理的要求。

3.5 服务节点及带宽要求

1、投标人在虹口区范围内提供政务专用通信网络，并要求在收到中标通知书的 20 个自然日内完成所有本次项目招标范围所涉及的区级政务外网节点的开通及验收工作。具体区级政务外网接入服务节点明细待中标方签订合同后予以提供。

2、根据招标方业务需求要求以及上海市政务外网工作方案 1+16 体系规划，在服务期限内持续提供本次项目预算所涉及区级政务外网网络节点接入服务，满足用户带宽及网络通信要求。

业务网络各层设备互联链路配置方案如下：

核心层，同节点设备间通过 1*100GE 互联，不同节点同平面设备通过 1*100GE 互联；承载视频+数据双业务平面；

汇聚层，同节点设备间通过 1*40GE 互联；

汇聚层与接入层设备间，通过两条 10GE 链路捆绑互联；

核心层与市政务外网、区政务云、各外部网络或管理平台接入区，通过 40GE 或 N*10GE 互联。

3、在服务期限内，投标人所提供网络服务中，包含下述网络通信服务带宽方案设计，相应网络带宽需求由投标人根据服务期限内网络总体发展规划，并自行组织踏勘调研完成。

（1）区级政务外网通信服务期限中，新增及搬迁用户所需的网络带宽通信服务。

（2）包括但不限于区级政务外网与市级电子政务外网对接区、区级政务外网与互联网接入区等公共服务区域的网络带宽通信服务。

项目网络服务技术要求

服务网络整体技术要求

投标人提供的服务网络设计方案，符合招标文件技术要求的基础要求，基于对政务外网网络业务需求及发展需要，充分理解本次项目具体需求，有效满足高可用、强扩展、适度超前、管理功能优秀的虹口区电子政务外网的构建需要，提供服务网络总体设计方案、网络技术架构、网络业务规划、拓扑设计、网络设备配置数量、分层设计及功能、性能设计等，满足招标中服务用户所需带宽需求，符合适度先进性、合理性、可靠性及安全隔离性等服务和运维管理要求。

网络整体分为核心层、汇聚层以及接入层三层构成。考虑本项目服务区域覆盖虹口区，要求服务商为本项目设置核心节点不少于 2 个汇聚节点不少于 3 个。其中两个核心节点分别为区政府机房（飞虹路 518 号）以及本项目新增的核心节点 2，核心节点 2 拟租用运营商已有通讯机房。汇聚节点共计 3 个，其中汇聚节点 1 与核心节点 1 同址，用于汇聚区政府院内网络，汇聚节点 2 为劳动局机房，汇聚节点 3 为本次项目新增，为租用运营商已有通讯机房。

本项目网络技术部分主要分为光传输网络服务、SDN 业务网络服务、业务网络边界安全体系服务、网络安全管理中心服务以及网络基础光缆及机房设施服务五部分。网络所涉及软硬件设备质保期为 1 年。

所提供服务网络主要技术要求包括但不限于以下内容，要求投标人逐条予以响应。

1、网络底层基于全网底层光传输网络组网架构，要求采用单波速率 100G 及以上的 OTN 技术实现组网。网络具备向 200G 及以上带宽平滑扩容的能力。

2、业务网络需要按分层组网架构进行设计，分为核心层、汇聚层、接入层。

3、业务网络上层业务网络基于 IP 技术，采用数据平面和视频平面逻辑隔离、独立运行、互为备份的“一网双平面”高可靠架构构建。全网支持 IPv4/IPv6 双栈，并根据网络业务需求调研情况进行网络业务设计与地址规划。

4、按照网络安全等级保护三级要求，对业务网络边界包括但不限于：互联网边界、政务云边界、与市级政务外网边界等建立网络安全防护体系；

5、根据网络安全等级保护三级要求，虹口区电子政务外网建设安全管理中心，支持网络内流量探针检测及安全态势感知，对网络设备、安全设备进行运维管理，对安全事件进行事件分析、风险分析、通报和预警。并要求后续与市级安全监测平台对接。

6、要求所建政务外网与区运行和安全监测支撑系统实现对接，满足虹口区运行和安全监测支撑系统对安全设备、网络设备、主机、数据库和应用系统的日志采集功能。要求设备支持 REST API 接口和 HTTPS 数据传输协议，满足运行和安全监测支撑系统对接入节点数据、常规数据、机房数据、资源类、拓扑关系数据、性能类、告警类和安全数据等数据对接和数据交互要求。

7、投标人结合政务外网安全威胁调研和需求理解情况，提供服务网络安全设计方案，提供的软硬件产品从产品功能、产品可用性与可靠性及指标等维度满足本次项目需求及技术要求，组网产品选型具备合理性、高效性，满足招标书技术和服务相关需求，内容包括但不限于网络服务中的物理安全、传输安全、边界安全、接入安全以

及相关配套的虹口区电子政务外网安全平台建设及运营设计、制度机制、安全团队设计等。对用户网络安全业务理解充分、完善准确。

8、服务网络基础资源设计需提供符合下述采购技术要求中所提出的 IDC 机房及光缆技术标准要求。为网络核心、汇聚、接入层设备部署，为区级委办局、事业单位、区直属企业以及街道办事处用户接入以及为重点接入区域（电子政务云等）节点提供可靠、可实施、具备时效性、冗余性及长期可扩展性的基础资源点位服务。

光传输网络技术要求

光传输网络整体构架要求

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

光传输网络采用分层组网架构进行设计，分为核心层、汇聚层、接入层。核心节点、汇聚节点的设置，可根据政务外网接入单位的物理位置分布、机房和光纤链路资源的配置等因素酌情选择。

接入层可采用单个接入节点直连至汇聚节点的方式组网，或多个接入节点与汇聚节点成环的方式组网。

光传输技术规范要求

1、核心、汇聚层应承载于政务外网光传输网络之上；本项目核心节点、汇聚节点要求部署光传输网络站点设备;

2、采用单波速率 100G 及以上的 OTN 技术;

3、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;

4、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;

5、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;

6、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;

7、支持光纤线路诊断功能，能快速定位光纤线路故障;

8、要求采用 SDN 技术，实现对业务和链路的快速下发和调整;

9、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;

10、核心节点之间的互联应采用高可用的组网架构,相邻核心节点之间开通两个不同路由的光传输通道，保证两点间多链路可达，对传输的业务进行冗余保护;

11、汇聚节点之间应采用环形组网架构,每个汇聚节点到相邻的核心节点之间均开通两个不同路由的光传输通道。

光传输网络设备要求

（1）设备清单

序号	设备名称	单位	数量
1	核心光传输设备	台	2
2	汇聚光传输设备	台	2
3	光传输网络管理系统	套	1

（2）具体节点配置清单

节点	设备类型	需求分类	需求数量/节点	单位	需求说明
核心 1 核心 2	100G×8 波 OTN 设备（包括主控板、交叉板等）	光方向 (8 波)	2	个	必须有两个物理分离的光方向单元，光层除必备部件外须包含 OTDR 模块。
		线路口（100G）	5	个	5 个 100G 线路端口中：2 个为 100GE 接口提供线路带宽，3 个为 40GE 接口提供线路带宽。
		业务接口（100GE）	2	个	与各核心机房内路由器端口连接。（含光模块）
		业务接口（40GE）	6	个	与各核心/汇聚 1 机房内路由器端口连接。（含光模块）
汇聚 2 汇聚 3	100G×8 波 OTN 设备（包括主控板、交叉板等）	光方向 (8 波)	2	个	必须有两个物理分离的光方向单元，光层除必备部件外须包含 OTDR 模块。
		线路口（100G）	2	个	为 40GE 接口提供线路带宽。到两个核心各 1 个线路口。
		业务接口（40GE）	4	个	与各自机房内路由器端口连接。（含光模块）

（3）核心/汇聚光传输设备

指标项	指标要求

设备性能	1、高度不超过5U，支持交/直流，深度小于300mm，业务槽位≥12； 2、电层子架OTN交叉容量≥700G，单槽位带宽不低于50G，分组交叉容量≥800G ，SDH交叉容量不低于280G(高阶)/40G(低阶)； 3、单波可支持10G/100G/200G，支持支线路分离和支线路合一架构； 4、支持密集波分复用技术，系统容量最大支持80波；
可靠性	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；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
	主控、交叉、通信控制与时钟单元1+1保护，电源冗余保护；支持OTN、分组、SDH网络级保护
	业务板卡支持基于业务端口的物理层加密功能
技术先进性	宜采用SDN技术，实现对业务和链路的快速下发和调整；
业务类型	1、具有SDH、分组、OTN、PDH等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； 2、具备同一单板FE/GE/10GE/40GE/100GE、FC200\FC800\FC1200\FC1600\FC3200、STM-N(1/4/16/64)多业务接入能力； 3、单波10G/100G/200G速率传输；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；
交叉功能	所投设备具备OTN、分组、SDH统一交叉功能，支持SDH、分组、OTN等多种业务统一承载能力

（4）光传输网络管理系统

序号	指标要求

1	所有端到端业务需由统一专业网管系统进行配置管理，且本方案中所涉及的物理设备/板卡/端口能由统一专业网管实现全面管理。
2	网管系统需要为中文操作界面。
3	投标方应根据前述配置要求配置网管系统所需的软、硬件。
4	投标方应说明所供网管设备（包括网管服务器、网管终端、路由器、集线器等）的功耗、尺寸和重量。
5	投标方应对网管软、硬件配置及其性能进行详细说明，并说明配置理由。
6	要求投标方详细说明本次投标设备的网管功能情况，详细列出支持的各种配置、性能、故障、安全等管理的列表和功能清单。
7	网管系统须与用户网络运行支撑系统进行对接，实现数据互通以及业务联动等功能。投标人应无条件免费配合对接，并开放 MIB 库等接口数据。

SDN 业务网络技术要求

业务网络整体构架要求

虹口区电子政务外网业务网络采用分层架构设计，在网络层次上分为核心层、汇聚层、接入层。
核心层主要承担高速数据交换的任务，同时提供到上一级政务外网和互联网的连接。政务外网与互联网之间采用安全技术逻辑隔离。
为提升网络可靠性，政务外网应至少设置 2 个核心节点，并确保各个核心节点部署在不同物理位置的机房。
汇聚层主要将来自接入层的访问进行集中和汇聚，承担路由聚合和访问控制的功能。汇聚层节点的位置、数量选择可基于机房、传输资源及网络接入点的地理位置分布等因素酌情考虑。
接入层主要提供政务外网各使用单位的网络接入。虹口区电子政务外网业务网络提供 106 个区级委办局、事业单位、区直属企业、街道办事处以及社区服务中心的接入以及其他重点区域、平台及其他网络的对接。
接入层网络采用单链路或双链路上行的方式接入政务外网业务网络汇聚层。

业务网络技术规范

虹口区电子政务外网业务网络应满足各接入点汇聚接入及灵活互通的需求，具体要求如下:

- 业务网络采用核心、汇聚、接入的三层架构设计;
- 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;
- 业务网络采用 “一网双平面”的架构设计。数据平面承载网络数据流量，视频平面承载网络视频流量，两个平面在政务外网上逻辑隔离、独立运行，且互为冗余备份;
- 应基于TCP/IP技术构建政务外网业务网络，采用支持IPv4/IPv6双栈技术的网络设备;
- 业务网络应符合等保规范的要求;
- 应保证不同应用在业务网络的相互独立，可选用VLAN、VxLAN、VPN、网络切片等方式实现不同业务的隔离;
- 应从多个维度考虑设备的安全可控，采用国产领先的网络和安全设备、系统;
- 应采用SDN技术，实现业务快速部署，流量工程和智能流量调整能力;
- 应基于大数据分析技术和智能检测技术，对网络中不同业务的运行状态、服务质量，做到实时监控、主动运维。

核心节点设计

1、核心层设备承担用户流量安全、高速、可靠转发的功能;
2、核心节点设备选型应能满足面向未来业务发展平滑扩展的需要;
3、核心节点应采用高冗余设计，保证核心网络的高可靠性。

汇聚节点设计

汇聚节点连接核心节点与接入节点，采用双归方式接入核心节点以提高网络可靠性。按各接入点地理位置的分布情况设置汇聚节点。每个汇聚节点部署两台高端路由器设备，两台设备之间设置带宽为40Gbps的互联链路。
汇聚节点向上通过40Gbps链路分别连接至两个核心节点，向下通过N×10Gbps链路连接各汇聚层边界防火墙或汇聚交换机。

接入节点设计

虹口区各接入部门的接入设备以N×10Gbps链路连接至汇聚节点。
虹口区各接入节点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。

边界网络设计

虹口区电子政务外网边界区域包括互联网出口区、市区政务外网互联互通区域、政务云区域。出口路由器通过N×10Gbps链路分别连接各边界区域。

业务网络设备要求

设备清单

序号	类别	需求数量	单位
1	出口路由器	4	台
2	核心路由器	4	台
3	汇聚路由器	6	台
4	汇聚交换机	6	台
5	接入交换机 A	8	台
6	接入交换机 B	106	台
7	边界交换机	2	台
8	SDN 控制器	1	套
9	网络管理软件	1	套

注：要求本项目核心路由器、汇聚路由器、汇聚交换机以及SDN控制器等设备必须互相完全兼容。

1、出口路由器功能要求：

技术指标	参数指标要求
体系架构	支持主控板、业务板完全物理分离，主控板、业务板分布在不同的物理槽位
	为保障接口扩容，设备采用子母卡架构设计，子卡插在母板上，子卡母板均支持热拔插
	要求支持主控冗余，支持主备倒换，支持主控板、线卡板及接口模块、电源、风扇框的热插拔
交换容量	交换容量≥70Tbps
包转发率	包转发率≥6000Mpps
单槽位最大处理能力	≥240 Gbps
设备形态	整机框业务槽位数≥8
电源系统	支持内置交流电源，双电源，“1+1”备份，支持智能电源管理，且不需要占用业务槽位
接口类型	支持 FE、GE、10GE（LAN/WAN）、155M POS/CPOS、622M POS、ATM/POS、155M ATM/622M ATM 等接口
广域网优化	支持 DRE、LZ、TFO 等多种 WAN 优化手段
	支持 WEB CACHE
Segment Routing	支持单域及跨 BGP 域的 Segment Routing 技术
	支持 Segment Routing 与 LDP 混合组网
	支持对业务进行流量工程，支持基于按需下一跳，以及自动引流，并与 SR 灵活算法联动
	支持多种方法创建 SR Policy（NETCONF/CLI/BGP）
	支持 SRv6，支持 SRv6 承载 VPN 业务
NAT	支持随板分布式 NAT 功能

	设备支持 NPTv6-RFC6296 功能
组播 VPN	支持分布式 NG-MVPN 功能，不需要额外 License
虚拟化	支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合
实际配置	单台实际配置：双主控，双电源，接口板卡必须采用子母卡形式，万兆以太网光接口≥8 个，SFP+万兆多模光模块≥4 个

2、核心路由器功能要求：

技术指标	参数指标要求
体系架构	支持主控板、交换网板、业务板完全物理分离，主控板、交换网板、业务板分布在不同的物理槽位
	为保证设备可靠性，设备的转发全部有交换网板完成，主控板不集成转发芯片
	为保证可靠性，设备需支持板卡（含主控，线卡，交换网板等）直接热插拔，同时不需要插拔电源风扇等其他关键部件
	支持独立的交换网板≥4 个
交换容量	交换容量≥180Tbps
包转发率	包转发率≥30000Mpps
业务槽位	整机框全物理尺寸的线卡槽位数≥8（非子卡槽位），不含主控、交换网板槽位
	支持子母卡架构，母卡和子卡均支持热插拔
单槽位转发性能	设备支持单槽单向最大带宽≥400Gbps
电源系统	支持内置交流电源，不能配置外置交流电源，也不额外占用业务槽位
	实际配置电源个数≥4 个，电源系统支持 N+M 冗余，支持一体化供电方式，任意拔掉两个电源，设备能够正常运行
通风方式	支持前后通风
基本功能	支持 PPP、MP、HDLC、ETHERNET 等链路层协议
	支持链路聚合（Link aggregation），支持动态聚合、手工聚合、跨板聚合
	支持不同带宽的链路捆绑功能
	支持多路径负载分担功能（UCMP），支持非等速链路的负载分担，实现不同路径按带宽比例负载分担
	支持 IPV4 静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略，支持 4M IPv4 FIB
	支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+，支持 2M IPv6 FIB
	支持 L2VPN、L3VPN、OptionA、B、C 类跨域，支持 16K VPN，支持 4M VPN 路由
接口类型	支持 FE、GE、10Ge（LAN/WAN）、40Ge、100Ge、155M POS、622M POS、2.5G POS、10G POS、CPOS 接口、155M ATM、622M ATM、E1 等接口

	支持 155M POS/622M POS 端口灵活切换
	支持 ATM/POS 端口灵活切换
	支持 155M ATM/622M ATM 端口灵活切换
组播 VPN（MVPN）	支持分布式 MVPN 功能
虚拟化	支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合
Segment Routing	支持单域及跨 BGP 域的 Segment Routing 技术
	支持 Segment Routing 与 LDP 混合组网
	支持对业务进行流量工程，支持基于按需下一跳，以及自动引流，并与 SR 灵活算法联动
	支持多种方法创建 SR Policy（NETCONF/CLI/BGP）
	支持 SRv6，支持 SRv6 承载 VPN 业务
多业务扩展能力	支持与路由器一体化的防火墙、IPS 等安全业务插卡
QOS	支持优先级 Mark/Remark、CAR（Committed Access Rate）、GTS 等功能，支持 200ms 缓存
	为简化 ACL 配置，设备需支持全局 ACL 功能
	支持 FIFO、PQ、WFQ、LLQ 等各种队列调度机制，支持拥塞避免算法：Tail-Drop、RED、WRED，支持层次化 Qos（H-Qos），支持 QPPB，支持 MPLS TE 的 Qos 功能
BRAS	支持 PPPoE、PPPoEoVLAN、PPPoEoQ 接入认证，支持 PPPoX 功能，支持 PPPoA，PPPoEoA 接入认证
	支持二层 Portal、三层 Portal、QinQ Portal 接入认证
	支持 IPoE、IPoEoVLAN、IPoEoQ 接入认证，IPOE+WEB 支持 HTTP、HTTPS 弹窗认证页面
	支持子网专线、接口专线、L2VPN 专线等专线接入认证，支持 L2TP 技术
	支持二层无感知接入、三层无感知接入
	支持 iTA（智能靶向计费），按目的地址区分不同的业务类型，实现用户不同类型业务计费、带宽控制和 QoS 等
	二层、三层 IPv4/IPv6 一次认证，双栈放行，分别计费
	IPv4/IPv6 用户热备功能，用户掉线后不需要重新登录
	IPv4/IPv6 的 Portal 认证支持弹不同的认证页面
	白名单功能支持 IP、URL 放行
SDN	设备支持通过 Netconf（RFC 6241）协议下发配置
	设备支持 YANG 功能（RFC 6020）
	为实现设备间链路状态等信息共享，设备需支持 BGP Link-State 功能（RFC 7752)
	为实现单节点上安全策略同步功能，设备需支持 BGP FlowSpec 功能（RFC 5575)
	为实现报文最优路径转发，设备需支持 Segment Routing（RFC7855）协议

	为实现按业务优先级选择隧道路径，设备需支持 CBTS 功能（YD/T 1391.1）
	设备支持 Openflow 协议，报文可依据流表进行转发
	为保证业务调度的精细化控制，设备需要支持 13 层标签
	设备支持 EVPN/VxLAN（RFC 7348）功能，能够完成 MAC 地址远端学习，实现基于 VxLAN 的二三层 VPN
可靠性	支持 VRRP/VRRPv3、MPLS TE FRR、IP FRR（静态路由/策略路由/RIP/IS-IS/OSPF 等）
	为减小设备或线路故障对业务的影响、提高网络的可用性，需支持 BFD for BGP/IS-IS/OSPF/LDP/VRRP/Static Route
	支持热补丁功能，可在线进行补丁升级
	为提高设备软件稳定性及可靠性，主备倒换时业务不中断，需要支持 NSR 功能
	为提高设备硬件稳定性及可靠性，交换网板、板卡、子卡支持热插拔功能
	为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持 NQA 检测网络质量
网络安全	设备支持防攻击能力，包括：ARP 攻击、IPv6 报文攻击、超大 Trace 报文攻击、TCP SYN flood、Ping flood、DHCP DDOS、PADI DDOS 的防御等，支持 PADI、DHCP、PORTAL 防攻击
	支持 OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的 MD5 认证功能，支持 Keychain 功能，可以支持基于时间段的生效的密钥，支持安全网管 SNMPv3，支持 SSHv1/v2/v3，为用户登录提供安全加密通道
维护特性	为方便设备运维管理，设备需内置 TCL 语言功能，能够解析执行 TCL 语言脚本
	为方便设备运维管理，设备需内置 Python 语言功能，能够解析执行 Python 语言脚本
	为实现设备精细化管理，实现不同进程动态部署到不同的 CPU 上，设备需支持进程分布式优化功能
	为实现基于角色的权限灵活授权，并且和 AAA 联动，设备需支持 RBAC 功能
	为方便设备配置文件管理，支持 FTP、TFTP、Xmodem、SFTP 文件上下载管理，设备需支持配置回滚功能
实际配置	单台实际配置：双主控引擎，4 块交换网板，接口板卡必须采用子母卡形式，100G 以太网光接口≥4 个，40G 以太网光接口≥4 个，万兆以太网光接口≥20 个，QSFP28 100G 多模模块数≥4 个，QSFP+ 40G 多模模块数≥4 个，SFP+ 10G 多模模块数≥8 个

3、汇聚路由器功能要求：

技术指标	参数指标要求
体系架构	支持主控板、业务板完全物理分离，主控板、业务板分布在不同的物理槽位
交换容量	交换容量≥130Tbps
包转发率	包转发率≥18000Mpps
业务槽位	整机框全物理尺寸的线卡槽位数≥6（非子卡槽位），不含主控、交换网板槽位
	支持子母卡架构，母卡和子卡均支持热插拔
电源系统	支持内置交流电源，不能配置外置交流电源
	电源系统支持 N+M 冗余，支持一体化供电方式，支持单电源供电，电源槽位不占用业务或者子卡槽位
基本功能	支持 PPP、MP、HDLC、ETHERNET 等链路层协议
	支持链路聚合（Link aggregation），支持动态聚合、手工聚合、跨板聚合
	支持不同带宽的链路捆绑功能
	支持多路径负载分担功能（UCMP），支持非等速链路的负载分担，实现不同路径按带宽比例负载分担
	支持 IPV4 静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略
	支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+
接口类型	支持 FE、GE、10Ge（LAN/WAN）、40Ge、100Ge、155M POS、622M POS、2.5G POS、10G POS、CPOS 接口、155M ATM、622M ATM、E1 等接口
	支持 155M POS/622M POS 端口灵活切换
	支持 ATM/POS 端口灵活切换
	支持 155M ATM/622M ATM 端口灵活切换
组播 VPN（MVPN）	支持分布式 MVPN 功能
虚拟化	支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合
Segment Routing	支持单域及跨 BGP 域的 Segment Routing 技术
	支持 Segment Routing 与 LDP 混合组网
	支持对业务进行流量工程，支持基于按需下一跳，以及自动引流，并与 SR 灵活算法联动
	支持多种方法创建 SR Policy（NETCONF/CLI/BGP）
	支持 SRv6，支持 SRv6 承载 VPN 业务
多业务扩展能力	支持与路由器一体化的防火墙、IPS 等安全业务插卡
QOS	支持优先级 Mark/Remark、CAR（Committed Access Rate）、GTS 等功能
	为简化 ACL 配置，设备需支持全局 ACL 功能
	支持 FIFO、PQ、WFQ、LLQ 等各种队列调度机制，支持拥塞避免算法：Tail-Drop、RED、WRED，支持层次化 Qos（H-Qos）
SDN	设备支持通过 Netconf（RFC 6241）协议下发配置

	设备支持 YANG 功能（RFC 6020）
	为实现设备间链路状态等信息共享，设备需支持 BGP Link-State 功能（RFC 7752)
	为实现单节点上安全策略同步功能，设备需支持 BGP FlowSpec 功能（RFC 5575)
	为实现报文最优路径转发，设备需支持 Segment Routing（RFC7855）协议
	为实现按业务优先级选择隧道路径，设备需支持 CBTS 功能（YD/T 1391.1）
	设备支持 Openflow 协议，报文可依据流表进行转发
	设备支持 EVPN/VxLAN（RFC 7348）功能，能够完成 MAC 地址远端学习，实现基于 VxLAN 的二三层 VPN
可靠性	支持 VRRP/VRRPv3、MPLS TE FRR、IP FRR（静态路由/策略路由/RIP/IS-IS/OSPF 等）
	为减小设备或线路故障对业务的影响、提高网络的可用性，需支持 BFD for BGP/IS-IS/OSPF/LDP/VRRP/Static Route
	支持热补丁功能，可在线进行补丁升级
	为提高设备软件稳定性及可靠性，主备倒换时业务不中断，需要支持 NSR 功能
	为提高设备硬件稳定性及可靠性，交换网板、板卡、子卡支持热插拔功能
	为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持 NQA 检测网络质量
网络安全	设备支持防攻击能力，包括：ARP 攻击、IPv6 报文攻击、超大 Trace 报文攻击、TCP SYN flood、Ping flood、DHCP DDOS、PADI DDOS 的防御等
	支持 OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的 MD5 认证功能，支持 Keychain 功能，可以支持基于时间段的生效的密钥
维护特性	为方便设备运维管理，设备需内置 TCL 语言功能，能够解析执行 TCL 语言脚本
	为方便设备运维管理，设备需内置 Python 语言功能，能够解析执行 Python 语言脚本
	为实现设备精细化管理，实现不同进程动态部署到不同的 CPU 上，设备需支持进程分布式优化功能
	为实现基于角色的权限灵活授权，并且和 AAA 联动，设备需支持 RBAC 功能
	为方便设备配置文件管理，设备需支持配置回滚功能
实际配置	单台实际配置：双主控引擎，双电源冗余，接口板卡必须采用子母卡形式，40G 以太网光接口≥3 个，万兆以太网光接口≥4 个，QSFP+ 40G 多模模块数≥3 个，SFP+ 10G 多模模块数≥2 个

4、汇聚交换机功能要求：

技术指标	参数指标要求
业务插槽数	业务槽位≥3

交换容量	交换容量≥38Tbps
转发能力	转发能力≥7200Mpps
电源冗余	电源模块冗余
关键部件热插拔	主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔
主控引擎	主控引擎模块≥2，满足 1+1 冗余
接口要求	以太网支持千兆电口，千兆光口，万兆光口、40G 端口、100G 端口
	单槽位万兆线速端口密度≥48
	单槽位 40G 端口密度≥24
	单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性
链路聚合	聚合组数≥1000 组，每组成员≥32 个
	支持跨设备链路聚合技术，通过将两台物理设备在转发层面虚拟成一台设备来实现跨设备链路聚合，保持控制层面互相独立，提供设备级冗余保护和流量负载分担，同时提高系统的可靠性
ACL	支持双向 ACL，ACL≥4K
	支持端口 ACL、VLAN ACL
QOS	每端口支持 8 个优先级队列，3 个丢弃优先级，支持 SP、WRR、SP+WRR 三种队列调度算法
	支持精细化的流量监管，粒度可达 8K
	支持流量整形 Shapping
	支持 WRED 拥塞避免
	支持 802.1p、TOS、DSCP、EXP 优先级映射
可靠性	双引擎快速倒换，主备切换时候板内转发无丢包
	支持 NSF/GR for OSPF/BGP/IS-IS
	支持热补丁功能，可在线进行补丁升级
	支持 BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由
IPv6	支持 RIPng、OSPFv3、BGP4+、IS-ISv6 协议
	支持 IPv6 策略路由；
	支持 DHCPv6 功能、IPv6 portal 功能、IPv6 管理功能；
	支持基于 IPv6 的 VXLAN 二三层互通；
	支持基于 IPv6 的 VRRP 功能
虚拟化	多虚一技术(N:1)，支持 4 框虚拟化技术
	一虚多技术（1:N）
网络安全一体化	支持 FW、IPS、LB、SSL VPN、应用控制等安全业务插卡

可视化	支持 Telemetry 流量可视化功能
有线无线一体化	支持 AC 板卡，POE，POE+
	支持交换机内置 AC 功能，无需独立的 AC 板卡或带 AC 功能的接口板，即支持无线 AP 管理功能。
	支持有线无线一体化的终端准入认证
多业务融合化	支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署 Windows Server 及 AD Campus director，实现方案与设备一体化部署
终端管理及网络安全	支持 PC 终端、哑终端、网络设备等连接元素的准入控制和权限划分，确保网络的可信可控
	支持设备识别、归类、类型定义，可以对全网资产进行梳理，识别异常终端链接，确保网络的安全性
MPLS	支持 L3 VPN
	支持 VLL、VPLS
	支持 MCE
FCoE	支持 FCoE 功能
SDN/OPENFLOW	支持 OPENFLOW
	支持普通模式和 Openflow 模式切换
	支持多控制器（EQUAL 模式、主备模式）
	支持多表流水线
	支持 Group table
	支持 Meter
跨三层互联技术	支持主流的 MAC in IP 技术，如 EVI，实现跨三层网络的二层互联
VxLAN	支持 VXLAN，能够实现 VXLAN 二三层互通
安全特性	支持 IPv4 uRPF
	支持 DHCP Snooping
	支持 ARP 防攻击
	支持 IP Source Guard
	支持 CoPP
	支持广播风暴抑制
	支持 IEEE 802.1ae 介质访问控制安全技术
	支持端口隔离
	支持 IP+MAC+VLAN+PORT 的绑定
	支持报文过滤功能，黑洞路由、黑洞 MAC
管理特性	支持 Console/AUX/Telnet/SSH2.0

	支持风扇管理
	支持电源管理
	支持在线诊断
	支持 SNMPv1/v2/v3
	支持 RMON(RFC2819)
	支持端口镜像、VLAN 镜像、RSPAN、流镜像
NAS 认证	支持 mac、Portal、802.1x 认证方式
	支持本地认证、Radius 认证、Tacacs+认证
其它	所选用交换机与路由器必须品牌一致
实际配置	单台实际配置：双主控，双电源，万兆以太网光接口≥96 个，SFP+万兆单模光模块≥40 个

5、接入交换机A功能要求：

技术指标	参数指标要求
交换容量	交换容量≥432Gbps
转发性能	转发性能≥144Mpps
性能指标	MAC 地址表≥16K
	路由表容量≥1K
接口类型	48 个千兆 SFP 光口（其中有 2 个 combo 口），4 个万兆 SFP+光口
电源	为了提高设备可靠性，支持模块化可插拔双电源，并实际配置双电源
ERPS	实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms
CPU 防护	实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作
堆叠	最大堆叠台数≥9 台
	最大堆叠带宽≥40G
	支持通过标准以太端口进行堆叠（万兆或千兆均支持）
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预
	支持远程堆叠
VLAN 特性	支持基于端口的 VLAN，支持基于协议的 VLAN；
	支持基于 MAC 的 VLAN；
	最大 VLAN 数(不是 VLAN ID)≥4094
链路聚合	支持最多 8 个端口聚合；支持最多 128 个聚合组；支持 LACP
镜像功能	支持远程镜像
	支持流镜像
	支持端口镜像
组播协议	支持 IGMP v1/v2/v3，MLD v1/v2
	支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2
	支持 PIM Snooping

	支持 MLD Proxy
	支持组播 VLAN
	支持 MSDP，MSDP for IPv6
	支持 MBGP，MBGP for Ipv6
路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF
	支持 IPv6 静态路由、RIPng
可靠性	支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms；
	支持 Smartlink，收敛时间≤50ms
	支持 RSTP 功能、MSTP 功能、PVST 功能
访问控制策略	支持基于第二层、第三层和第四层的 ACL；
	整机提供 ACl 条目数不小于 1K 条；
	支持基于端口和 VLAN 的 ACL；
	支持 IPv6 ACL；
	支持出方向 ACL，以便于灵活实现数据包过滤；
	支持 802.1x 认证，支持集中式 MAC 地址认证；
SDN/OPENFLOW	支持 OPENFLOW 1.3 标准，支持普通模式和 Openflow 模式切换，支持多控制器（EQUAL 模式、主备模式）
	支持多表流水线
	支持 Group table
	支持 Meter
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
	支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
绿色节能	符合 IEEE 802.3az（EEE）节能标准
	端口定时 down 功能（Schedule job）
	支持端口休眠，关闭没有应用的端口，节省能源
其它	所选用交换机与路由器必须品牌一致
实际配置	单台实际配置：SFP+ 万兆单模模块≥2 个

6、接入交换机B功能要求：

技术指标	参数指标要求
交换容量	交换容量≥336Gbps
转发性能	转发性能≥108Mpps
性能指标	MAC 地址表≥16K
	路由表容量≥1K
接口类型	24 个 100/1000 SFP 光口（其中有 8 个 combo 口），4 个 10G/1G BASE-X SFP+端口
电源	为了提高设备可靠性，支持模块化可插拔双电源，并实际配置双电源
ERPS	实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms
CPU 防护	实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作

堆叠	最大堆叠台数≥9 台
	最大堆叠带宽≥40G
	支持通过标准以太端口进行堆叠（万兆或千兆均支持）
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预
	支持远程堆叠
VLAN 特性	支持基于端口的 VLAN，支持基于协议的 VLAN；
	支持基于 MAC 的 VLAN；
	最大 VLAN 数(不是 VLAN ID)≥4094
链路聚合	支持最多 8 个端口聚合；支持最多 128 个聚合组；支持 LACP
镜像功能	支持远程镜像
	支持流镜像
	支持端口镜像
组播协议	支持 IGMP v1/v2/v3，MLD v1/v2
	支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2
	支持 PIM Snooping
	支持 MLD Proxy
	支持组播 VLAN
	支持 MSDP，MSDP for IPv6
	支持 MBGP，MBGP for Ipv6
路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF
	支持 IPv6 静态路由、RIPng
可靠性	支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms；
	支持 Smart link，收敛时间≤50ms
	支持 RSTP 功能、MSTP 功能、PVST 功能
访问控制策略	支持基于第二层、第三层和第四层的 ACL；
	整机提供 ACl 条目数不小于 1K 条；
	支持基于端口和 VLAN 的 ACL；
	支持 IPv6 ACL；
	支持出方向 ACL，以便于灵活实现数据包过滤；
	支持 802.1x 认证，支持集中式 MAC 地址认证；
SDN/OPENFLOW	支持 OPENFLOW 1.3 标准，支持普通模式和 Openflow 模式切换，支持多控制器（EQUAL 模式、主备模式）
	支持多表流水线
	支持 Group table
	支持 Meter
管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
	支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
绿色节能	符合 IEEE 802.3az（EEE）节能标准
	端口定时 down 功能（Schedule job）

	支持端口休眠，关闭没有应用的端口，节省能源
其它	所选用交换机与路由器必须品牌一致
实际配置	单台实际配置：SFP+ 万兆单模模块≥2 个

7、边界交换机功能要求：

技术指标	参数指标要求
交换容量	交换容量≥2.56Tbps
转发性能	转发性能≥360Mpps
接口类型	24 个 10G/1G BASE-X SFP+端口
电源	为了提高设备可靠性，支持模块化可插拔双电源，并实际配置双电源
VLAN 特性	支持基于端口的 VLAN（4094 个） 支持 Default VLAN 支持 QINQ 支持灵活 QINQ 支持 VLAN MAPPING 支持 PVST+ 支持 RPVST+
镜像功能	支持流镜像
	支持 N:4 端口镜像
	支持本地和远程端口镜像
组播协议	支持 IGMP Snooping v2/v3， 支持 IGMP Snooping Fast-leave， 支持 IGMP Snooping Group-policy， 支持 PIM-SM,PIM-SSM， 支持 PIM snooping， 支持 MVRP， 支持 MFF，支持增强三层组播
路由协议	支持 IPv4、IPv6 静态路由，RIP 等三层动态路由协议 支持策略路由器; 支持 RIP v1/2、RIPng 支持等价路由、VRRP、OSPFv1/v2、OSPF v3、BGP、ISIS 等增强三层路由协议
可靠性	支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms；
	支持 Smart link，收敛时间≤50ms
	支持 RSTP 功能、MSTP 功能、PVST 功能
访问控制策略	支持基于第二层、第三层和第四层的 ACL；
	整机提供 ACl 条目数不小于 1K 条；
	支持基于端口和 VLAN 的 ACL；
	支持 IPv6 ACL；
	支持出方向 ACL，以便于灵活实现数据包过滤；

	支持 802.1x 认证，支持集中式 MAC 地址认证；
管理和维护	支持命令行接口（CLI）配置 支持 Telnet 远程配置 支持通过 Console 口配置 支持 802.1AG 及 802.3AH 支持 SNMP（Simple Network Management Protocol） 支持系统日志 支持分级告警 支持 USB 进行文件上传和下载
其它	所选用交换机与路由器必须品牌一致
实际配置	单台实际配置：SFP+ 万兆单模模块≥2 个

8、SDN控制器功能要求：

技术指标		参数指标要求
部署环境	集群方式	支持服务器集群工作方式，并配置 3 节点集群软件及授权
	部署方式	支持物理主机、虚拟机及容器化部署
基础能力	网络规模	支持管理不少于 2000 台路由网络设备
拓扑收集	自动拓扑收集	支持控制器通过 BGP-LS 协议自动收集实际的拓扑信息
	手动拓扑收集	支持由管理员手动在控制器添加设备、链路等拓扑信息，控制器对导入的网络拓扑和实际运行情况进行校对，最后形成整网的实际拓扑
拓扑管理	设备管理	支持对网络设备进行管理，包括增加、删除、属性修改等操作 支持管理员手动定义网络中各设备地理位置等信息，并在地图上进行呈现
	链路管理	支持对物理链路进行管理，包括增加、删除、属性修改等操作
隧道管理	隧道类型	支持在 IP 与 MPLS 网络中，使用 SR 隧道来对所有需要调度的应用流量进行封装
	隧道创建	支持控制器根据调度需要自动在设备间建立 SR 隧道，承载被调度的应用流量，支持 OSPF、IS-IS 的 SR-TE 隧道
L3VPN 业务部署	L3VPN 业务下发及管理	支持 PE 对接 CE 侧，自动化对 L3VPN 业务添加、修改、删除、回滚配置、查看操作
	应用绑定	支持 L3VPN 业务与应用组关联、修改关联、删除关联操作
QoS 业务部署	QoS 业务自动化部署	支持图形化配置 LAN 口业务自定义带宽值限速 支持图形化配置 WAN 口队列调度，按比例或带宽绝对值分配带宽，应用优先级进行业务保障 支持图形化配置 WAN 口限速
设备可视	设备状态可视	支持呈现 CPU、内存、温度 等基础资源的健康状态
	设备基础信息可视	设备名称、序列号等静态信息呈现 对 CPU、内存、温度等历史信息（包括过去 1 小时、过去 1 天、过去一周、过去一月）进行统计和呈现
链路可视	链路基础信息可视	支持链路名称、两端接口 IP 等静态信息呈现
	链路状态可视	支持链路通断，拥塞，质量状况呈现
	链路质量可视	链路质量（延时、抖动、丢包）详细信息的实时呈现，支持秒级呈现，对链路的历史质量信息（包括过去 1 小时、过去 1 天、过去一周、过去一月）进行统计和呈现
	链路流量可视	支持呈现链路实时流量、全网链路实时流量 TOPN、链路历史流量分布、链路承载应用历史流量分布，支持秒级呈现

	实时	应用组粒度粒呈现实时带宽信息，应用组实例粒度呈现实时带宽信息
	历史	时延、抖动、丢包、带宽利用率、应用组带宽/占比
应用流量可视	预定义应用流量	支持应用组实时流量及历史流量分布统计呈现
	未知应用流量	支持现网未知应用的实时流量分布统计呈现
应用质量可视	应用健康度	支持应用组内各实例质量的 SLA 符合度比例
应用路径可视	应用实例路径	对于调度应用组，呈现应用组实例的可调度路径 对于可视应用组，呈现实时运行路径，不做调度
应用定义	纯 IP 业务流分类	支持 IPv6 五元组、DSCP 任意组合进行业务流分类，自动映射到不同隧道自动进行流量调优。支持定义 IPv4/IPv6 应用。
	VPN 业务流分类	支持 IPv6 五元组、DSCP、VPN 任意组合进行业务流分类，自动映射到不同隧道自动进行流量调优。支持定义 IPv4/IPv6 应用。
流量调度	选路方式	支持自动计算路径和手工路径编排
	负载均衡	支持业务等价负载分担和非等价负载分担，控制器可根据链路带宽情况自动调整负载分担权重
	选路策略	支持永久、指定时间、周期性时生效等时间段策略 支持根据业务质量（时延、抖动、丢包）、带宽需求，为业务按需自动调整路径 共享风险组策略，主备路径避免选择同风险组链路
	路径自动调整方式	支持应用 SLA 不满足、链路带宽超过 80%、设备故障、链路故障、主备路径重合、非优选路径情况下，自动调整路径
	批量路径优化	支持对自动调度应用进行定时或周期性或手工进行全局路径优化 支持对多个自动调度应用组实例进行批量路径优化
故障自动诊断	设备故障	支持自动诊断设备连接故障，设备 CPU、内存、温度超过阈值
	链路故障	支持自动诊断链路中断，链路质量低于阈值
	应用质量故障	支持自动诊断应用质量是否满足需求
设备隔离冻结	设备隔离	支持可单独将某设备隔离，不再参与路径计算
告警管理	页面呈现	支持拓扑图中直接呈现故障信息
	告警推送	支持 E-mail 推送告警信息
	告警配置	支持告警阈值设置
设备管理	南向协议	支持 BGP-LS、Netconf、SNMP、Netstream、Telemetry、PCEP
	配置管理	支持同一设备 5 个不同时间的配置比对，可显示配置不同点

日志管理	用户操作日志	支持导出用户操作日志
	调度日志	支持导出历史流量调度日志
	控制器日志	支持导出控制器自身日志
报表导出	报表类别	支持链路质量报表、链路带宽报表、应用组流量报表、应用组内实例流量报表等
	时间段定制	支持提供固定时长（如过去 1 小时、过去 1 天、过去一周、过去一月、过去一年）或自定义时间段内的报表信息
控制器可靠性	控制器集群	支持控制器集群部署
	数据库异地灾备	支持定期自动或手工异地备份数据库
网络可靠性	设备堆叠	支持节点设备堆叠部署
	背靠背	支持节点设备背靠背部署
	一键逃生	支持一键取消控制器路径，切换传统转发模式
用户访问	用户认证	支持多用户通过用户名、密码认证
	账户分权	支持对不同用户分配不同管理权限
部署硬件	硬件服务器	配置数量不低于 4 台，每台要求如下： 机架式，≥2U，实际配置 CPU 性能不低于 5218(2.3GHz/16 核 /22MB/125W)2 颗，实际配置内存不低于 64GB 2933MHz DDR4，实际配置硬盘不低于 2*1.2TB 12G SAS HDD，实际配置不少于 1 个标配 SAS RAID 阵列卡，实际配置不少于 2 个≥800w 冗余电源，实际配置不少于 4 端口千兆网卡一块

9、网管软件功能要求：

技术指标	参数指标要求
分布式部署	需资源拓扑、告警、性能等功能组件支持多服务器负载分担部署，保证各网管组件性能；
多平台支持	支持 Windows、Linux 平台及 SQL Server、Oracle 数据库；
多厂商设备配置及软件管理	支持 H3C/HUAWEI/3COM/CISCO/HP 设备的批量配置和软件管理，包括的软件版本和软件库中最新可用的软件，更新设备的软件支持 220+设备厂商，8000+设备款型；
自定义用户主页	管理员可以在首页中通过拖拽，自定义需要在首页展示页面，同时支持 Widget 扩展；
自动发现拓扑	自动发现网络中的所有网络设备，并在拓扑中显示出来，可以自动将网络中的逻辑连接关系显示出来；
用户分权管理	可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理；
配置需求	可管理有线网络设备节点数量≥200
设备与用户统一管理	支持网络管理平台实现设备管理与用户管理联动，如通过点击拓扑楼层接入交换机查看该楼层所有接入用户帐户信息
设备与流量分析统一管理	支持设备与流量分析统一管理：支持网络管理平台实现设备管理与流量分析联动，如通过点击拓扑某链路可查看该链路的关键应用流

	量分布、关键用户流量使用等；
性能管理	支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警；
故障管理	支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转 E-mail，转短信，转上级网管或其它网管等支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能；
批量的设备配置备份和恢复	支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断；
运维报表	需支持多种报表样式，包括普通的行列报表、主/子报表、图形摘要报表、交叉表、TopN 和 BottomN 报表支持多种图形展示：包括条形图、饼图、曲线图、甘特图、面积图、圆环图、三维梯形图、三维曲面图、XY 散点图、雷达图、气泡图、股票图、漏斗图等；
周期性报表机制	支持天报表、周报表、月报表、季度报表、半年报表、年报表，可以设定周期性报表的开始时间、失效时间，可以将自身的组织名称和 Logo 融入到发布的报表中，可以定时生成后 Email 到指定邮箱；

业务网络带宽设计

本项目虹口区电子政务外网业务网络带宽（网络接口速率）设计如下：

链路类型	**速率**
核心节点之间	100Gbps
核心节点与下级汇聚节点之间	40Gbps
同一汇聚节点内主备冗余设备之间	40Gbps
汇聚节点与下级接入节点之间	N×10Gbps

业务网络边界安全技术要求

业务网络边界安全整体设计要求

1、分级分域保护原则

电子政务外网应根据联接网络对象的不同，以及承载信息系统的安全等级的不同，划分不同的安全区域和边界，并根据等保 2.0 规范相关要求，实施不同强度的安全保护。

2、网络边界划分

区级政务外网应将如下区域划定为安全边界，并部署符合等保 2.0 三级规范要求的安全设备，予以保护：

第一类区域：政务外网到互联网的接入边界，防范从互联网对政务外网的攻击；

第二类区域：各级政务外网互联的边界，如区级政务外网到市级政务外网的边界，

防范非法跨级访问对政务外网的非授权访问;

第三类区域：各单位政务网接入到对应区政务外网的边界，防范非法跨网用户对政务外网的非授权访问;

第四类区域：部分机构、部门等单位接入到政务外网的边界，防范非法接入单位用户对政务外网的非授权访问。

3、在服务期内设备质保、病毒库、特征库升级均在服务范围内。

业务网络边界安全规范要求

1、互联网接入区的安全规范

互联网接入区需实现抗 DDoS 攻击、网络访问控制、入侵检测和防御、防病毒、APT 检测、日志审计等功能。

互联网接入区域，需要满足以下技术规范:

（1）抗 DDoS 攻击

应在互联网接入区部署抗 DDoS 攻击设备，需要支持 DDoS 检测和清洗。抗 DDoS 攻击需要支持常见的 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）网络访问控制

应在互联网接入区部署防火墙，实现网络边界保护和访问控制功能。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经互联网接入区域的网络数据进行合法性检查。为了保证业务的可服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持 IPv6 协议栈、NAT64 转换技术。

（3）入侵检测和防御

应在互联网接入区部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

（4）防病毒

应在互联网接入区部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

（5）APT 检测

宜在互联网接入区旁路部署沙箱，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。

沙箱应支持和防火墙联动以实现对威胁的实时阻断。

（6）VPN 网关

应在互联网接入区部署 VPN 网关，针对从互联网接入的远程办公用户提供 SSL、IPSec 等形式的 VPN 接入网关功能。VPN 网关需支持国密算法。

（7）探针

宜在互联网接入区部署探针，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系统进行安全分析，识别潜在安全攻击风险。

（8）日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存 6 个月。

2、与市级政务外网互联的边界安全规范

区级政务外网接入市级政务外网时，应设置安全边界，实现网络访问控制能力，阻断非法访问。

对于区级政务外网接入市级政务外网，应在政务外网边界设置安全接入区，需实现 网络访问控制、入侵检测和防御、防病毒、APT 检测、日志审计等功能，具体要求如下:

（1）网络访问控制

应在该区域部署防火墙，实现网络边界保护和访问控制。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经接入边界的网络数据进行合法性检查。为了保证业务的可 服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持 IPv6 协议栈、NAT64 转换技术。

（2）入侵检测和防御

应在该区域部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

（3）防病毒

应在该区域部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

（4）APT 检测

宜在该区域旁路部署沙箱，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。沙箱应

支持和防火墙联 动以实现对威胁的实时阻断。

（5）探针

宜在该区域部署探针，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系统进行安全分析，识别潜在安全攻击风险。

（6）日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存 6 个月。

3、各单位接入政务外网边界的安全规范

对于各单位网络接入到政务外网，应在政务外网边界设置安全接入区，需实现网络访问控制、入侵检测和防御、防病毒、APT 检测、日志审计等功能，具体要求如下:

（1）网络访问控制

应在该区域部署防火墙，实现网络边界保护和访问控制。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经接入边界的网络数据进行合法性检查。为了保证业务的可 服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持 IPv6 协议栈、NAT64 转换技术。

（2）入侵检测和防御

应在该区域部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

（3）防病毒

应在该区域部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

（4）APT 检测

宜在该区域旁路部署沙箱，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。沙箱应支持和防火墙联 动以实现对威胁的实时阻断。

（5）探针

宜在该区域部署探针，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系统进行安全分析，识别潜在安全攻击风险。

（6）日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，

并要求审计日志至少保存 6 个月。

4、政务外网安全接入区边界的安全规范

其它机构、部门接入政务外网需求的，需要通过安全接入区接入电子政务外网。在安全接入区，需要实现网络访问控制、防病毒、入侵检测和防御、APT 检测、日志审计等功能。具体要求如下:

（1）网络访问控制

应在该区域部署防火墙，实现网络边界保护和访问控制。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经接入边界的网络数据进行合法性检查。为了保证业务的可服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持 IPv6 协议栈、NAT64 转换技术。

（2）入侵检测和防御

应在该区域部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

（3）防病毒

应在该区域部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

（4）APT 检测

宜在该区域旁路部署沙箱，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。沙箱应支持和防火墙联动以实现对威胁的实时阻断。

（5）探针

宜在该区域部署探针，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系统进行安全分析，识别潜在安全攻击风险。

（6）日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存 6 个月。

业务网络边界安全设备要求

需求设备清单

序号	类别	需求数量	单位	备注
1	负载均衡设备	2	台	
2	防病毒墙	2	台	
3	入侵防御	2	台	
4	防火墙	2	台	
5	上网行为管理	2	台	
6	网络探针 A	3	台	
7	商密 VPN 设备	2	台	
8	Anti-DDoS 设备	1	台	
9	沙箱 A	1	套	
10	防火墙/入侵防御/防病毒 A	2	台	
11	防火墙/入侵防御	2	台	

12	防火墙/入侵防御/防病毒 B	6	台	
13	网络探针 B	3	台	
14	沙箱 B	3	套	

注：安全设备中若需使用光模块，请投标人根据实际要求按需配置光模块，并含在该项安全设备报价中。

设备性能参数要求

（1）负载均衡设备

技术指标	参数指标要求
硬件参数	内存≥8G，硬盘容量≥64G SSD，电源：冗余电源，不少于 6 个千兆电口，不少于 4 个千兆光口，不少于 2 个万兆光口；
性能参数	4 层吞吐量≥20Gbps，四层并发连接数≥20000000，4 层新建连接数≥500000，7 层新建连接数≥550000；
多合一功能集成	单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权；
	提供针对 L4/L7 内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求；
链路负载均衡	支持静态 IP 和 PPPOE 两种线路接入方式；
	支持基于管理员自定义的时间计划来进行出站访问的流量调度分发；
	支持基于 URL 的链路调度功能，内置不少于 10 万条的国外 URL 网址库，无需手动导入并支持自动更新，管理员可查看。可根据 URL 将访问国外网站的请求调度到指定线路；
	支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度；
	支持链路负载投屏展示，能够分别基于链路监测、应用选路和 ISP 流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP 展示基于运营商分类

	选择链路的示意图；
服务器负载均衡	支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应时间、加权最小流量、按主机加权最小流量、源 IP 源端口哈希、源 IP 哈希、URI 哈希和 HOST 哈希等；
	对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包；
	支持优先级算法下最少可用节点保障，保证优先级高节点的可用性；
	支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、SIP、ICMPv6、TCP/UDP、FTP、HTTP、DNS、RADIUS，HTTPS、LDAP、ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制；
	支持复合监视器功能，可配置选择多个健康检查方式，同时可设置通过条件为同时成立、任意一个通过和自定义；并且能开启/关闭调试日志功能；
	节点支持域名和 IP 两种形式，支持根据 DNS 应答的 TTL 值和指定时间作为 DNS 查询间隔；
	支持 cookie 作用域和作用路径的自定义，支持 cookie 加密，提升 cookie 安全性；
	服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU 温度、CPU 和内存占用率、新建连接数、并发连接数、吞吐情况、SSL 新建和 SSL 吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量；
全局负载均衡	支持 DNS 缓存，可配置全局缓存最小时间和最大时间，并可设置 MSG 缓存大小、RR 缓存大小、密钥缓存大小、否定记录缓存大小和否定记录最大缓存时间；
	支持 TCP 和 UDP DNS 解析能力，支持设置 EDNS 缓冲区大小；

	支持启用/禁用 edns-ecs 方式提取/插入客户端请求真实源地址；

（2）防病毒墙

技术指标	参数指标要求
硬件规格	产品不少于 4 个千兆电口，4 个千兆光口，4 个万兆光口，支持 2 个 USB 口和 1 个 RJ45 串口，冗余电源，2U 机箱。
性能要求	病毒检测吞吐率≥10Gbps，
部署方式	支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。
链路聚合	具备链路聚合功能，将 2 个或者更多物理链路组合成一个更高带宽的逻辑链路接口，提高链路带宽和链路可靠性。
IPv6	支持 IPv4/IPv6 双栈工作模式。
	支持 IPv6 环境的应用控制策略设置，能针对 IPv6 的 IP 地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。
	支持 IPv6 环境的安全策略设置，实现入侵防御、防病毒、Web 应用防护等等安全功能。
DDoS 防御	支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护。
	支持 TearDrop 攻击、IP 数据块分片传输、Land 攻击、Smurf 攻击、WinNuke 攻击、超大 ICMP 数据攻击等异常报文攻击防护，支持 IP 协议异常报文和 TCP 协议异常报文攻击防护。
	支持 ARP 欺骗类攻击防护。
URL 过滤	内置海量互联网 URL 分类库，支持过滤上千万条恶意 URL。
文件过滤	具备文件过滤功能，可对视频文件、音频文件、图片文件、文本文件、可执行文件、驱动文件等类型文件进行安全过滤。
防病毒	支持对 HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP 协议进行病毒检测和查杀，支持最大 16 层的压缩文件查杀。
	支持病毒排除设置，支持基于文件 MD5 值和文件下载 URL 设置病毒白名单；
安全报表	产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全分析等。
用户管理权限	支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色；
集中管理	产品支持接入集中管理平台实现多设备的统一管理，集中管理平台支持硬件和云端两种部署方式。
	支持通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web 应用防护等安全策略。

（3）入侵防御

技术指标		参数指标要求
硬件指标	系统平台	系统应为机架式独立 IPS 硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统，稳定可靠。
	网络接口	引擎模块-2U，含交流冗余电源模块，不少于 2*USB 接口，1*RJ45 串口，2*GE 管理口，4 个扩展槽位；4 个万兆 SFPP 插槽；不含光模块。
产品性能		吞吐量：10G；最大并发 TCP 会话：1000 万；每秒新增 TCP 会话：400000；时延：<40 μs
支持入侵检测和高级威胁防护	入侵检测	系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为 9000 种以上。
		系统应支持多种抗逃避检测技术
		系统应提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测和阻断规则。
		系统应能够有效抵御 SQL 注入等多种常见的应用层安全威胁
		支持基于 SCADA 等工控协议的相关漏洞攻击检测与防护。
	防病毒	支持流式防病毒
		支持启发式防病毒
	DoS/DDoS	系统应提供 DoS/DDoS 攻击防护能力，支持 TCP/UDP/ICMP/ACK Flooding，以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击
		支持基于阈值和自学习检测
	数据泄露防护	系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。
		系统应提供关键文件保护功能，能够识别、阻断通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如 Excel、PDF、PowerPoint、Word 等，压缩文件类如 CAB、GZIP、RAR、ZIP、JAR 等，图像类如 BMP、GIF、JPEG 等，音频视频类如 MP3、AVI、MKV、MP4、MPEG、WMV 等，脚本类如 BAT、CMD、WSF 等，程序类如 APK、DLL、EXE、JAVA_CLASS 等。
	URL 分类	系统应提供 URL 分类库，提供中英文网页过滤数据库，实现高风险、不良网站过滤。
	统计及联动	支持对未知可疑文件统计
		支持与本地沙箱的联动配置
响应能力	攻击响应	系统应提供丰富的响应方式，包括：会话阻断、IP 隔离、邮件通知等功能，满足用户各种响应需求。
	攻击取证	系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析。
日志和报表	日志管理	系统应具备实时的日志归并功能，可以根据用户需要，按照告警事件的源/目的 IP、事件类型等信息，对告警日志执行归并，有效抵御告警风暴。

		系统应提供基于告警设备、时间、IP 地址、事件类型、用户身份等条件的日志检索功能，具备日志备份、清除和恢复功能。系统应具备递归查询功能，在查询结果中再次输入查询条件获得更详细的查询结果，进行细粒度分析。
	报表系统	系统应提供丰富的报表功能，支持 TopN 事件、TopN 源地址、TopN 目的地址、TopN 服务、事件类型分布与趋势、危险程度分类统计与趋势、风险级别统计与趋势以及交叉报表等多种报表模板；为便于分析，还应支持用户自定义报表模版，能够按照用户需求生成各种风格的统计报表。
		系统应提供定时自动发送报表功能，支持在指定的时间内将生成的报表以 html、word、pdf 等通用格式通过 FTP 或邮件发送给指定的管理员，以减少日常维护工作量。
		系统应提供标准 snmp trap（V1、V2、V3）和 syslog 接口，可接受第三方管理平台的集中事件管理。
部署能力	部署模式	系统应支持监听（Monitor）、直通（Direct）两种工作模式，能够快速部署在各种网络环境中。
		系统应支持独立式多路 IPS 工作模式，各路 IPS 相互独立，可单独配置策略。
		系统应支持 IPS 和 IDS 的混合运行模式，同时提供入侵防护和入侵检测功能。

（4）防火墙

技术指标	指标要求
硬件规格	产品不少于 4 个千兆电口，4 个千兆光口，4 个万兆光口
性能要求	网络层吞吐量≥40Gbps，应用层吞吐量≥15Gbps
部署方式	具备路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。
路由功能	支持静态路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议。
地址转换	支持 IPv4 / IPv6 下 NAT 地址转换，支持源地址转换 SNAT，目的地址转换 DNAT 和双向地址转换双向 NAT，支持 NAT64、NAT46 地址转换。
IPv6	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 环境的应用控制策略设置，能针对 IPv6 的 IP 地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。
VPN	IPSec VPN 支持智能选路功能，保障业务的高可靠性。
地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。
流量控制	具备基于国家/地区的流量管理功能
DDoS 防御	支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护。
策略生命周期管理	支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略

	的管理和运维。
双机部署	支持主主、主备两种双机模式部署。
安全报表	产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全风险分析等。
用户管理权限	支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色；
集中管理	产品支持接入集中管理平台实现多设备的统一管理，通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web 应用防护等安全策略。

（5）上网行为管理

技术指标		参数指标要求
网络吞吐量		≥25Gb
支持带宽		≥10 Gb
支持用户数		≥100,000
硬件接口		不少于 4 个千兆电口，4 个千兆光口，4 个万兆光口
部署方式	网关模式	支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能；
	网桥模式	支持网桥模式，以透明方式串接在网络中；支持电口、光口 bypass；
	旁路模式	支持旁路模式，无需更改网络配置，实现上网行为审计；旁路支持主主、主备模式部署；
	多路桥接	必须支持多路桥接功能，最多可支持 32 组网桥模式；
	多主模式	必须支持两台及两台以上设备同时做主机的部署模式；
实时监控	设备资源信息	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；
用户管理	本地认证	支持触发式 WEB 认证，静态用户名密码认证等；
	二维码认证	支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、免填写信息三种模式
网页管理	SSL 加密网页内容识别	识别并过滤 SSL 加密的钓鱼网站、非法网站等 支持 SSL 硬件加速卡解密，从而可提高 SSL 全流量解密性能； 必须支持旁路解密；
流量控制	流控通道实时可视化	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。
	P2P 智能流控	支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；
	流控黑名单	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
上网行为审计	应用审计	审计用户使用 P2P、流媒体、炒股、网络游戏、FTP、Telnet 等应用行为；
	时间审计	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；
日志管理	数据中心	设备必须支持内置数据中心和独立数据中心；

（6）网络探针 A

技术指标	指标要求
接口数量	不低于 6 个千兆电口，4 个千兆光口，2 个万兆光口
尺寸	2U
性能指标	应用层吞吐不低于 5G
部署模式	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
资产发现	具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等
基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意 URL 监测模式,可完成模式匹配并生成事件,可提取 URL 记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等
深度监测能力	可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗，IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型;
高级检测	支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求

	支持 DNS 审计日志，主要用于平台 dns flow 分析引擎进行安全分析；HTTP 审计日志，主要用于平台 http flow 分析引擎进行安全分析；SMB 审计日志，主要用于平台 SMB flow 分析引擎进行安全分析；同步 SMTP、POP3、IMAP 审计日志，主要用于平台 Mail flow 分析引擎进行安全分析，同步 AD 域协议审计日志，主要用于平台 AD 域分析引擎进行安全分析
Web 应用安全检测能力	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 web shell 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； 产品应具备独立的 Web 应用检测规则库，Web 应用检测规则总数在 3000 条以上；
僵尸网络检测	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，恶意软件识别特征总数在 35 万条以上；
违规访问检测	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式。
流量记录	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。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
集中管控	支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；
部署	支持旁路部署，对镜像流量进行监听 可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台

（7）沙箱 A

技术指标	指标要求
接口数量	2 个千兆电口，可扩展；
性能指标	虚拟沙箱个数为不低于 20 个 WinXP/Win7，适配流量不低于 2G，静态检测能力 500 万文件/天，动态检测能力 2 万文件/天；
文件处理	默认支持但不限于 Office 文档、WPS、PDF、HTML、JS、ZIP、7Z、RAR、CMD、PE、APK 等 68 种及以上文件类型检测，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 EML 格式文件检测，能自动提取附件并进行检测，能为每一条文件检测事件提供详细的知识库说明；
	支持文件检测告警日志上传功能，能够将检测告警日志发送给第三方 Syslog 服务器；
静态特征检测	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；
动态行为检测	具备杀软检测、CVE、沙箱检测、YARA 检测、机器学习、威胁情报检测等 7 种及以上综合检测能力，且每种检测能力可独立输出检测结果。
	沙箱引擎的虚拟机系统支持 Windows XP、Windows 7、Windows 10 等常见操作系统模板，且支持在不重启系统情况下的实时切换沙箱模版
	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；
	支持捕获样本所有原始网络流量并存储为 PCAP 包，支持在线查看 PCAP 包分析取证，至少包括源 IP、源端口、目的 IP、目的端口、16 进制和 ASCII 格式数据包内容；
	支持自动提取样本所释放的衍生文件并进行检测；支持 shellcode 提取，能将 shellcode 反汇编成汇编代码。
	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；
	支持用户自己编写 YARA 规则，扩展检测能力。
	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。）

机器学习检测	支持至少 5 种及以上机器学习模型，检测 PE、office、PDF 等格式文件。
	支持通过机器算法对恶意样本分类，分类方式至少包含病毒、木马、后门、蠕虫、广告等 5 种及以上。

（8）商密 VPN 网关

技术指标	参数指标要求
性能指标	理论加密流量不低于 350Mbps，最大理论并发用户数不低于 5000，IPSec 加密最大流量（Mbps）200；6 个千兆电口，4 个千兆光口；
用户授权	能够提供≥1250 个移动接入授权
基本特性	专业 VPN 设备，采用标准 SSL、TLS 协议，同时支持 IPSecVPN、SSLVPN 两种 VPN，非插卡或防火墙带 VPN 模块设备。
	支持终端使用包括 IE6、7、8、10、11 或其他 IE 内核的浏览器，以及最新版本的非 IE 内核浏览器，如 Windows EDGE，Google Chrome，Firefox，Safari，Opera 最新版登录 SSLVPN 系统，登录后可完整支持各种 IP 层以上的 B/S 和 C/S 应用。
	支持 Mac 系统主流浏览器，如 Chrome、Firefox 等最新版，免安装浏览器插件登录 SSLVPN。
	产品应支持国家商用密码算法包括：SM1,SM2,SM3,SM4 算法
终端安全	产品必须支持防中间人攻击，产品可在用户登录 SSLVPN 时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。
	支持用户终端登录前、登录后的安全性检测，检测范围包括：用户接入 IP、接入时间、接入线路 IP、进程、文件、注册表、操作系统、使用终端，可以检测出客户端是否安装指定的防火墙或杀毒软件。
	产品应提供 HTTPS 驱动病毒查杀工具，支持对 Windows 环境下的针对 HTTPS 拦截监听的驱动病毒进行扫描查杀，避免因为 HTTPS 驱动病毒导致无法正常接入和使用 SSL VPN。
权限、服务器安全	产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。
	支持主从认证账号绑定，必须实现 SSL VPN 账号与应用系统账号的唯一绑定，VPN 资源中的系统只能以指定账号登录，加强身份认证，防止登录 SSL VPN 后冒名登录应用系统。
高速性	针对 B/S 资源支持 WebCache 技术，动态缓存页面元素，提高 Web 页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果

身份认证	产品必须支持 LocalDB、USBKEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS 等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USBKEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证
高管理要求	支持 15 级以上的管理员分级分权限管理，从 Admin 派生树形结构下级管理员；上级管理员可分配下级管理员享有设备配置模块权限，可管理的用户、资源、角色权限，并可限制下级管理员是否允许创建下级管理员、创建资源、创建角色；上级管理员可限制下级管理员对权限内配置享有查看或配置权限

（9）Anti-DDoS 设备

技术指标	参数指标要求
设备要求	提供的产品为 2U 设备：含 2*USB 接口，1*RJ45 串口，2*GE 管理口，4 个网络接口卡插槽；
	设备攻击清洗能力不低于 8G；吞吐能力 20G；最大可升级为 12G 清洗容量。
部署方式	流量清洗产品支持串联部署方式。
	流量清洗产品支持旁路部署方式。
	流量清洗产品支持集群部署方式，可通过集群功能对清洗容量进行扩容。
攻击防范功能	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。
	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 攻击的不少于 9 种专有防护手段，能够对 HTTP 进行解码。
	设备具备对连接耗尽型攻击的防御能力。
	支持 URL 访问控制规则等多种分组过滤方式。
	支持使用 IP 信誉库对流量进行防护，并支持 IP 信誉查询，信誉库更新周期≤1 天
	支持在 web 界面查看目的 IP 的防护状态
	支持配合云清洗平台形成混合清洗解决方案，解决出口带宽拥塞情况下的攻击防护。
牵引回注功能	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
	设备支持与 Arbor 和 Genie 进行联动清洗
管理功能	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。
	对系统自身的管理方式支持串口命令行和 Web 图形化管理两种方式，无需安装专门的客户端管理系统，且图形化界面支持中文、英文和日文的切换。
	系统 Web 界面具备设备的远程升级功能。
	系统具备远程重启功能，并可在命令行和 Web 界面中进行操作。
	对设备的远程管理方式具备加密能力，通过 https 和 SSH 等加密方式实现。
	系统具备统一管理平台，在集群部署时支持对多台设备的集中管理，日志收集，运行状态监控，策略下发。
	管理系统支持以中文图表形式输出流量报表，可以选择日报、周报和月报
	系统支持用户分级分权管理，并具备合理的分级层次及权限划分粒度。

	系统具备安全日志功能，可完整地记录用户对设备的重要操作、访问信息。
	设备支持通过 snmp、syslog、API 等方式与第三方平台进行联动
	syslog 配置支持选择发送日志的类型。
	支持将告警日志自动发送给指定邮箱，并且日志类型、发送周期可选。
	支持通过设备 web 界面获取第三方接口文档规范。
	提供界面手动及自动抓包功能，抓包参数定义范围至少包含如下几项：接口、协议、抓包数量、源 IP、目标 IP、源或目标 IP、最大包长、流量方向、抓包时长、源端口、目的端口、源或目的端口。
	管理页面登录支持验证码校验，防止暴力破解。

（10）防火墙/入侵防御/防病毒 A

技术指标	参数指标要求
硬件要求	硬件参数：产品不少于 8 个千兆电口，8 个千兆光口，6 个万兆光口，2U 机箱，冗余电源。内存≥32G，硬盘容量≥128G SSD+480G SSD。
性能要求	网络层吞吐量≥60 Gbps，应用层吞吐量≥35 Gbps。
服务要求	提供 1 年规则库更新和 1 年软硬件质保服务。
硬件平台	产品应用多核并行处理架构，并采用国产处理器和国产操作系统。
链路状态探测	产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括 DNS 解析、ARP 探测和 PING 方式。
路由功能	产品支持静态路由、策略路由和多播路由协议，并支持 BGP、RIP、OSPF 等动态路由协议。
地址转换	产品支持多种地址转换功能，支持源地址转换 SNAT，目的地址转换 DNAT 和双向地址转换双向 NAT，支持 IPv4 / IPv6 下地址转换，至少包括 NAT64 和 NAT46 两种方式。
访问控制策略	产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。
安全防护	产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持超过 7200 种特征规则数量。
	产品支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。
	产品支持杀毒白名单设置，可以例外排除特定 MD5 和 URL 的病毒文件，针对特定文件不进行查杀。
	产品支持勒索病毒检测与防御功能。
	产品支持对多重压缩文件的病毒检测能力，支持不小于 15 层压缩文件病毒检测与处置。
	产品具备 Web 应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含 SQL 注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL 后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为。
	产品支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁。
对象识别	产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。

安全策略管理	产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。
	产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。
用户管理	产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。

（11）防火墙/入侵防御

技术指标	参数指标要求
硬件要求	硬件参数：产品不少于 8 个千兆电口，8 个千兆光口，6 个万兆光口，2U 机箱，冗余电源。内存≥32G，硬盘容量≥128G SSD+480G SSD。
性能要求	网络层吞吐量≥60 Gbps，应用层吞吐量≥35 Gbps。
服务要求	提供 1 年规则库更新和 1 年软硬件质保服务。
硬件平台	产品应用多核并行处理架构，并采用国产处理器和国产操作系统。
链路状态探测	产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括 DNS 解析、ARP 探测和 PING 方式。
路由功能	产品支持静态路由、策略路由和多播路由协议，并支持 BGP、RIP、OSPF 等动态路由协议。
地址转换	产品支持多种地址转换功能，支持源地址转换 SNAT，目的地址转换 DNAT 和双向地址转换双向 NAT，支持 IPv4 / IPv6 下地址转换，至少包括 NAT64 和 NAT46 两种方式。
访问控制策略	产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。
安全防护	产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持超过 7200 种特征规则数量。
	产品支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。
	产品支持杀毒白名单设置，可以例外排除特定 MD5 和 URL 的病毒文件，针对特定文件不进行查杀。
	产品支持勒索病毒检测与防御功能。
	产品支持对多重压缩文件的病毒检测能力，支持不小于 15 层压缩文件病毒检测与处置。
	产品具备 Web 应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含 SQL 注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL 后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为。
	产品支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁。
对象识别	产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。
安全策略管理	产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。

	产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。
用户管理	产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。

（12）防火墙/入侵防御/防病毒

技术指标	参数指标要求
硬件平台	产品采用多核并行处理架构
硬件规格	产品不少于 6 个千兆电口，4 个千兆光口，2 个万兆光口
性能要求	网络层吞吐量≥18Gbps，应用层吞吐量≥2.5Gbps
部署方式	具备路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。
路由功能	支持静态路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议。
地址转换	支持 IPv4 / IPv6 下 NAT 地址转换，支持源地址转换 SNAT，目的地址转换 DNAT 和双向地址转换双向 NAT，支持 NAT64、NAT46 地址转换。
IPv6	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 环境的应用控制策略设置，能针对 IPv6 的 IP 地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。
VPN	IPSec VPN 支持智能选路功能，保障业务的高可靠性。
地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。
DDoS 防御	支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护。
入侵防御	支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过 7000 种特征规则。
	支持僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。
防病毒	支持对 HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP 协议进行病毒检测和查杀，支持最大 16 层的压缩文件查杀。
	支持病毒排除设置，支持基于文件 MD5 值和文件下载 URL 设置病毒白名单；
策略生命周期管理	支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。
双机部署	支持主主、主备两种双机模式部署。
安全报表	产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全风险分析等。
用户管理权限	支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色；
集中管理	产品支持接入集中管理平台实现多设备的统一管理，通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web 应用防护等安全策略。

（13）网络探针 B

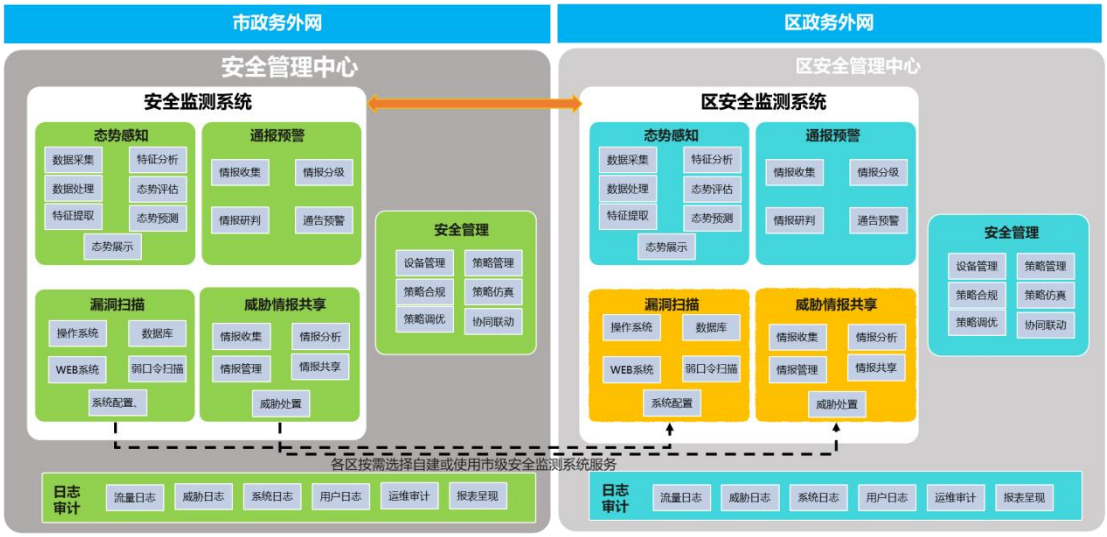
技术指标	参数指标要求
接口数量	不低于 4 个千兆电口，2 个千兆光口
性能指标	应用层吞吐不低于 1.5G
部署模式	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
资产发现	具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等
基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意 URL 监测模式,可完成模式匹配并生成事件,可提取 URL 记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。
深度监测能力	可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗，IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型;
高级检测	支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。
	支持 DNS 审计日志，主要用于平台 dns flow 分析引擎进行安全分析；HTTP 审计日志，主要用于平台 http flow 分析引擎进行安全分析；SMB 审计日志，主要用于平台 SMB flow 分析引擎进行安全分析；同步 SMTP、POP3、IMAP 审计日志，主要用于平台 Mail flow 分析引擎进行安全分析，同步 AD 域协议审计日志，主要用于平台 AD 域分析引擎进行安全分析
Web 应用安全检测能力	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； 产品应具备独立的 Web 应用检测规则库，Web 应用检测规则总数在 3000 条以上；
僵尸网络检测	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，恶意软件识别特征总数在 35 万条以上；

违规访问检测	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式。
流量记录	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。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
集中管控	支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；
部署	支持旁路部署，对镜像流量进行监听； 可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台。

安全管理中心技术要求

安全管理中心规范要求

根据等保 2.0 规范要求，区级政务外网应建设安全管理中心，对网络设备、安全设备进行运维管理，对安全事件进行事件分析、风险分析、通报和预警。



市、区两级安全管理中心架构图

安全管理中心包含态势感知、通报预警、威胁情报共享、漏洞扫描、安全管理控制、日志审计系统共 6 个模块，实现电子政务外网的全网威胁可视化、通报预警和统一安全运营能力。其中，态势感知、通报预警、威胁情报共享、漏洞扫描作为安全监测系统的关键部件，需要实现与国家政务外网安全监测系统的互通与信息共享。

对于区安全管理中心，漏洞扫描和威胁情报共享子系统可选择自建或使用市级安全检测系统提供的服务。其他子系统均需单独建设。

应通过市、区两级安全监测系统的对接，实现市、区两级安全管理中心的信息交

互和协同联动。

服务网络中提供安全监测系统，各模块的建设要求如下:

模块	**包含组件**
态势感知	探针、大数据分析、安全分析、可视化展示
通报预警	可由态势感知子系统提供通报预警接口
威胁情报共享	可由态势感知子系统提供威胁情报共享接口
漏洞扫描	漏洞扫描设备
安全管理控制	安全管理软件
日志审计系统	日志审计软件，服务器

1、态势感知

态势感知子系统须能从多维度和可视化方式，对全区政务外网进行全方位、全天候安全威胁感知和呈现。

态势感知子系统组成宜包括数据采集层、数据存储和挖掘层、态势展现层。数据采集层通过部署探针、接收安全设备日志、漏洞扫描设备扫描日志等方式获取原始数据；数据存储挖掘层建立在大数据分析系统之上，对 IP 地址库、GIS 地图库、恶意 IP、恶意文件库、资产库等基础数据信息进行安全和威胁的深度挖掘。态势展现层对安全分析结果进行威胁态势可视化呈现、通报预警和威胁情报的共享和发布。

态势感知子系统应能对网站及主机漏洞、流量异常、扫描探查、弱点攻击、僵尸网络、数据泄露、APT 攻击等各类安全攻击、威胁事件进行多视角的态势感知呈现，实现网站安全态势感知、内网威胁态势感知、Web 站点态势感知、脆弱性态势感知等功能。

2、通报预警

通报预警子系统可基于态势感知子系统的态势展现模块进行接口开发，或单独建设开发。通报预警子系统对安全态势、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，并及时将情况上报给上级安全管理中心，通告给本级政务外网主管单位和接入单位。从而实现对使用部门、上级单位、下级单位的通告预警。

通报预警按照安全风险、影响程度分为高危、中危和低危事件。

3、威胁情报共享

威胁情报共享子系统可基于态势感知子系统的态势展现模块进行开发，或单独建

设开发。威胁情报共享子系统实现安全情报的收集、情报分析与处理、情报数据管理等。情报信息主要包括恶意样本病毒、恶意 IP/URL/MD5 库，黑客组织信息、攻击方法手段、安全资讯等。

威胁情报共享子系统应能通过多种通道和技术搜集政务外网的安全情报信息，并共享给安全管理控制系统用于实时阻断、隔离相关攻击源。

4、漏洞扫描

漏洞扫描子系统可部署单独的漏洞扫描设备进行漏洞扫描，或集成在态势感知系统内部相关功能模块。

漏洞扫描子系统应支持对操作系统、数据库、网络设备、安全设备、Web 系统、弱口令等的漏洞扫描，支持对系统配置进行基线核查，并且能为系统管理员提供漏洞的详细报告和解决方案。漏洞扫描子系统需要支持资产自动发现功能，支持远程自动升级以及本地升级最新漏洞库。

5、安全管理控制

安全管理中心应部署安全管理控制子系统。安全管理控制子系统以独立软件的形式部署在一体机或虚拟机上。具体应具备以下能力：

（1） 设备管理

对设备的统一管理应支持以下能力：设备自动发现、设备的增删改查、双机热备组、设备组的增删改查、设备配置的一致性对比、设备单点登录，设备版本升级，设备配置文件备份。

（2） 策略管理

支持安全策略的管理，通过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。在执行动作上可以设置允许或禁止。同时也可以配置上对应的安全配置文件做内容安全防护，可对策略组视图和设备视图进行策略快速管理，策略变更统计、配置一致性统计、部署状态统计等管理能力。

（3） 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。策略提交后，匹配定义好的检查规则，及时反馈检查结果、安全等级等信息给安全审批责任人。支持低风险策略自动审批。

（4） 策略仿真

应能通过学习业务互访关系，对比待部署策略，以模拟部署的方式，在策略部署前评估策略对业务的影响，以降低策略部署后对业务带来的风险。

（5） 协同联动

应支持安全管理控制系统联动态势感知子系统，以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。

6、日志审计系统

安全日志系统须单独建设，提供集中化的统一日志管理系统，收集政务外网设备的日志信息，提供流量日志、威胁日志、系统日志、管理员运维日志的日志审计功能。按照等保要求，审计日志留存时间需满足至少 6 个月。

安全管理中心设备要求

序号	类别	需求数量	单位	备注
1	安全监测设备（态势感知）	1	套	含计算资源
2	通报预警模块			
3	威胁情报共享模块			
4	安全管理控制模块			
5	漏洞扫描设备	1	套	
6	日志审计设备	1	套	
7	数据库审计设备	1	套	
8	服务器审计功能模块	1	套	
9	应用审计功能模块	1	套	

注：安全设备中若需使用光模块，请投标人根据实际要求按需配置光模块，并含在该项安全设备报价中。

设备性能参数要求

（1）安全监测（态势感知）设备

技术指标		指标要求
安全监测模块	日志存储时长	不少于 180 天
	尺寸	不大于 2U
	硬盘容量	≥48T
	内存	≥256G
	接口数量	不低于 6 个千兆电口，4 个万兆光口
	电源	冗余电源

	综合安全态势大屏	支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势、设备运行态势，支持页面跳转到对应态势大屏，并具备大屏告警能力；
	横向威胁态势	支持图形化大屏展示横向威胁态势，包括业务与终端访问、发起威胁终端 TOP5、遭受威胁业务 TOP5、访问趋势图，并支持不同颜色标注横向攻击、违规访问、可疑行为、风险访问；
	业务	支持感知业务/服务器资产，可定义 IP 地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量识别操作系统、开放的服务与端口。
	安全域	支持安全域维度感知资产，可定义安全域名称、安全域属性、责任人、责任人邮箱、IP 范围、备注等信息，并支持导入导出 csv 配置文件。
	脆弱性总览	支持页面展示业务脆弱性风险分布，不同严重级别业务分布，漏洞类型分布图，漏洞整体态势等，支持 7 天、30 天统计；
	弱密码	支持镜像流量检测常见协议的弱密码,包括 HTTP、FTP、LDAP、VMWARE、ORACLE、VNC 等类型协议，检测列表包含账号、密码、服务器、所属分支和业务、最近登录源 IP、类型、最近发现时间等信息。
	风险业务视角	具备失陷(业务和用户)主机详细分析，包含攻击阶段分布、风险等级趋势、安全事件举证、遭受的外部攻击、存在的漏洞风险、行为画像（EBA）、开放端口等信息。攻击阶段包含存在漏洞、遭受攻击、C&C 通信、黑产牟利、内网探针、内网扩散、盗取数据；存在的漏洞风险包含漏洞风险、配置风险、明文传输、弱密码；行为画像 UEBA 包含外连、横向被访问、横向主动访问；支持对每个安全事件详细举证分析，包含风险危害、处置建议、专杀工具、安全知识库等
	风险安全域视角	支持安全域维度展示安全风险，包含安全域列表、安全域评分、事件类型 TOP5、IP 地址、IP 类型、风险等级、关键风险、状态等信息。
	威胁分析	横向威胁感知，展示包含横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包含发起与遭受横向威胁主机 TOP5，发起视角包含发起者 IP、发起者类型、所属分析、所属业务/终端组、横向威胁类型、遭受者数、遭受者类型、日志数。
		外连威胁感知，包含对外威胁总览、对外攻击、APTC&C 通信、可疑行为、隐蔽通信、违规访问、服务器风险访问；其中外连威胁总监包括外连威胁主机类型分布、存在外连威胁 IP TOP5、外连目标地区（国外）TOP5、外连威胁类型分布、非正常时间段外连主机 TOP5、外连威胁趋势。
	挖矿专项检测	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。
	日志检索	日志类型至少包含漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS 攻击、邮件安全、文件安全、网络流量、DNS 日志、HTTP 日志、用户日志、数据库日志、文件审计日志、POP3 日志、SMTP、IMAP、LDAP、FTP、Telnet、第三方等各类日志，并可按照以上类型日志的各个关键字段搜索日志。
	日志联动	支持与日志审计设备联动，可以接受来自日志审计设备的普通日志或者告警日志进行二次分析。
	主机安全风险报告	支持展示需要处理的风险主机与风险状况报告，报告内容包括业务与终端风险摘要、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。
	等级保护管理服务	支持对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理，最大程度发挥安全措施的保护能力

（2）通报预警模块功能要求

技术指标		指标要求
通报预警模块	通报总览	支持通报事件统计，包括待通报数量、待认领数量处理中数量、已超时数量、已归档数量；支持通报分支统计，包括通报分支次数 TOP5、分支处理时长 TOP5、通报事件危害影响面，通报分支趋势等。
	自动研判	支持安全事件、漏洞隐患、攻击威胁自动研判，可基于安全等级，如已失陷、高可疑、低可疑、高危、中危、低危等条件；支持自定义工单邮件通报预警模板，可定义主题、附件、正文等内容。
	分支权限管理	支持分权管理，可自定义分支管理权限，分支管理员具备独立的管理页面，分支管理员只能管理和查看所分支所属的业务和终端的安全信息，具备完整的功能展示，包括监控中心、处置中心、分析中心、资产中心和报告中心；总部管理员支持查看全局的安全信息，并支持通过页面跳转各个分支的独立管理页面

（3）威胁情报共享模块功能要求

技术指标		指标要求
威胁情报共享模块	威胁情报总览	支持威胁情报总览展示，内置威胁情报数量不少于 150W，支持展示 威胁情报命中数、今日命中数、命中威胁情报类别 TOP10、命中趋势、情报共享排行、活跃威胁情报 TOP20 等。
	威胁情报管理	支持自定义威胁情报，可定义域名、IP、URL、文件 MD5、

		确定性等级、威胁等级、事件类型、危害描述、处置建议等信息。
	威胁情报白名单	支持自定义威胁情报白名单，可自定义域名、URL、IP 和 MD5
	情报信息	支持情报信息展示，包含情报名称、情报来源、最近更新时间、情报内容，并可上报下达上下级平台。

（4）安全管理控制模块

技术指标		指标要求
安全管理控制模块	深度检测引擎升级	具备安全日志分析引擎、DnsFlow 行为分析引擎、HttpFLow 分析引擎、NetFLow 分析引擎、MailFLow 分析引擎、SmbFLow 分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等，支持定期自动升级或离线手动升级。
	平台级联	支持上下级平台级联功能，可支持资产信息、安全事件、脆弱性风险上报，其中资产信息包含受监控内部 IP 组、业务/服务器、终端、分析；安全事件包含已失陷事件、高可疑事件、低可疑事件；脆弱性风险包含漏洞风险、配置风险、弱密码和明文传输，并支持页面展示下级平台的当前状态、上报内容、最近上报时间等。
	防火墙设备联动	支持与现网内政务云接入区部署的防火墙进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击流量。
	策略自动填充	支持基于不同的安全事件，智能填充针对性的自动化响应处置策略，可自动选择推荐的联动设备。
	响应策略组合	支持自定义响应策略组合，可选择策略包括联动封锁、访问控制、上网提醒、冻结账号、一键查杀、调查取证，支持策略组合配置，支持基于特定时间段生效策略。
	开放共享	支持通过 RESTful API 接口形成对平台数据资源的“开放”与“共享”，第三方平台可获取受监控 IP 组、资产信息、风险业务与终端、漏洞详情、弱密码和明文传输等信息，实现数据更大价值。

（5）漏洞扫描共享模块功能要求

技术指标		指标要求
产品要求	基本要求	产品需使用专门的硬件，有自主知识产权的安全操作系统，采用 B/S 设计架构，并采用 SSL 加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理。
		1U 机架式设备，含 1 个 RJ45 串口，1 个 GE 管理口，6 个 10M/100M/1000M 自适应以太网电口扫描口，1 个接口扩展槽位（支持 4 电、4 光、8 电、8 光），含交流单电源。
		支持 IPv4 和 IPv6 环境的部署和扫描
	产品性能	允许最大并发扫描≥90 个 IP 地址，允许最大并发任务≥15 个任务，支持无限 IP 授权扫描。
		开启全插件漏洞扫描、弱口令探测和登录扫描后扫描速度不低于 1000 ip/h。
	漏洞管理和分析	支持检测的漏洞数大于 49000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准。
		同时支持远程扫描和采用 SMB、SSH、RDP、Telnet 等协议对 Windows、Linux 等系统进行登录扫描。
		提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。
		内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术。
		支持针对大数据组件框架的漏洞检测。
		支持扫描主流虚拟机管理系统的安全漏洞，如：VMWare ESX/ESXi，要求能够扫描大于 300 条相关漏洞。
		支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞。
		支持智能端口挖掘，可以智能发现非默认端口启动的服务
		具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用 SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。
		支持立即执行、定时执行、周期执行扫描任务，自定义的周期时间可精确至每*月第*个星期*的*点*分。
		支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务。
		支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行。
		支持复用已有任务配置用于新的扫描任务。
		提供通过资产树对资产进行分级管理，支持设备权重设置和可

		信设备登记，支持将资产信息批量导入到资产树，可在资产树上直接指定主机开展扫描任务。
		可以通过多种维度搜索定位资产和查看资产风险，包括并不限于：节点或设备名称、资产 IP 范围、资产管理员、资产操作系统类型、资产风险等级、漏洞名称、开放的端口、资产 banner 信息等。
		支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态。
		支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义。
	风险展示和报表	支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情。
		支持高级数据分析，可对同一 IP 的两次扫描结果进行风险对比分析，并可在线查看同一 IP 的多次历史扫描结果。
		支持将按 IP 范围、起止时间、任务名称、任务状态、漏洞模板、用户等筛选扫描任务,并对筛选结果进行汇总,和生成在线及离线报表。
		提供灵活的报表自定义，可定制报表标题、封面 logo、报表页眉和页脚、报表各章节显示内容。
		支持多用户分级权限管理，可为每个用户角色分配账号、任务级的权限分配、允许登录的 IP 范围和允许扫描的 IP 范围等

（6）日志审计模块功能要求

技术指标		指标要求
日志审计模块	性能参数	包含主机审计许可证书数量不低于 1000； 平均每秒处理日志数（eps）性能不低于 3000 2U，冗余电源，6 个千兆电口
	系统安全	支持通过 SSL 加密对数据传输等进行处理、采用 B/S 架构，HTTPS 访问
	支持对象	支持各类设备的日志采集要求，主要包括：安全设备：国内主流防火墙； 操作系统：Linux、Windows、Windows Server、Unix 等操作系统；数据库：Oracle、MySQL、SQLServer 等；应用系统：如 Apache、Tomcat、IIS、Weblogic 等；网络设备：主流的路由器、交换机、负载均衡等网络设备
	采集方式	支持 Syslog、SNMP Trap、数据库、文件、SMB、WMI、Console、日志导入、镜像流量等方式采集日志，审计中心可以支持多个日志采集器
	标准化	支持对日志格式进行标准化操作时，不破坏原始日志内容。从不同设备或系统的日志中抽取相关片段准确和完整地映射至日志的标准字段中，统一格式。
		支持对安全事件重新定级，能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义

	过滤	支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件
	归并	支持归并技术，一段时间内对重复日志进行归并
	日志查询	支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计；支持精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询
		支持全球地理位置库，支持不同设备相同 IP 的日志识别。
	关联分析	支持挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，关联的类型包括基于规则和基于统计的。
		支持将本地的日志上传至态势感知模块进行二次分析以及关联。
	告警响应	支持关联、审计策略命中后定义告警，响应方式包括：SYSLOG、邮件、自定义命令行。
		支持列表的方式展示告警；告警声音设置；告警过滤策略；支持实时监控，滚动显示实时的日志接入信息。
	人员审计	支持定义部门和人员的对应关系，支持定义人员与账号的对应关系。
	流量审计	支持 HTTP 网页标题、BBS、威胁情报、DGA、搜索关键词的网络会话分类展现
		支持 DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现
		支持 TLS 会话、数据库会话、邮件会话、FTP 会话、Telnet 会话，即时通讯会话的展现
	全文检索	支持全文检索功能，能对系统内的对象提供全文检索功能
	用户管理	支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如系统管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，安全审计员只负责查看相关的审计结果及告警内容；安全管理员只负责完成对系统本身的用户操作日志管理。

（7）数据库审计模块功能要求

技术指标		指标要求
配置要求	产品架构	要求设备为软硬件一体化产品，2U 上架设备。
	管理结构	中文界面，B/S 架构，采用 HTTPS 方式远程安全管理，无需安装客户端。
	网络接口	系统引擎模块含交流冗余电源模块，不少于 2*USB 接口，1*RJ45 串口，1*GE 管理口，6*GE 电口，1 个接口扩展槽位，2 个万兆 SFP+插槽（不含光纤接口模块）。
	性能指标	SQL 处理性能：不低于 50000 条/秒
		入库语句量：不低于 40000 条/秒
		并发会话：不低于 10000 个
		纯数据库网络流量处理能力：>=1.2GBit 每秒
	数据库自动发现	支持数据库自动发现。设备无需添加、即插即用。
数据库类型	支持的数据库类型	支持主流数据库： Oracle，SQLServer，MySQL、DB2、Sybase、Informix、PostgreSQL、HBase、MongoDB、DM、kingbase、OSCAR、Gbase、Hive、Redis、Cache、Highgo、MariaDB、Teradata、ElasticSearch
部署方式	旁路镜像	旁路部署模式，通过 TAP、SPAN 等技术将网络流量映射到审计设备，对数据库流量进行审计和告警
	Agent 方式	支持在目标数据库安装 Agent 解决无法通过旁路镜像获取流量的场景，如同服务器部署数据库和应用系统、云环境、虚拟化环境场景下数据库的审计。
	分布式部署	支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询。
		分布式部署下，审计引擎和审计中心都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展。
		系统采用大数据架构设计，审计中心支持集群部署，具备平滑升级和扩充存储能力。
审计能力	协议支持	支持在 IPV4 环境中部署，且支持所有数据库 IPV4 协议的审计。 支持在 IPV6 环境中部署，且支持所有数据库 IPV6 协议的审计。
	审计内容	支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小；
		会话的终端信息：IP、MAC、Port、工具名称（程序名）
		会话的主机信息、IP、MAC、Port、数据库名（实例名）
		会话的其它信息：登录时间、会话时长

		操作信息：操作类型（DDL、DML、DCL 等）、操作时间、执行时长、操作成功与失败、操作对象（表、函数、存储过程名称）、SQL 语句
		操作影响范围信息：查询、修改、删除操作的影响行数,以及返回行数
	运维协议支持	支持 ssh、telnet、nfs、smb、ftp、http 等运维协议的审计
	审计要素	执行人 who：审计到前端的应用用户、数据库用户名、主机名称、操作系统用户等；
		执行内容 what：具体的操作，访问的数据库、表、列、字段、包、存储过程、函数、视图；
		执行时间 when：每个操作发生的具体时间，操作时间、登录时间等；
		执行地点 where：操作的来源和目的，包括 IP 地址、MAC 地址、用户名、端口号、数据库类型；
		执行方式 how：通过哪些客户端应用程序或第三方工具执行得操作，如：DDL、DML、DCL；
		影响范围（影响行数）Range：该操作执行的影响范围，如查询、修改或删除的记录行数；
		执行结果 ResultSet：执行成功与否的结果以及返回结果集，如查询操作的返回内容；
	复杂 SQL 语句支持	准确审计长 SQL 语句
		有效分割、准确审计多 SQL 语句
		准确审计绑定变量的 SQL 语句
	应用用户关联审计	能以完全精确方式，审计到应用端相关信息，包括应用用户等。
		在并发 1000 个连接的情况下，准确率应达到 100%准确。
		支持 Weblogic、tomcat、Websphere 等主流的应用服务器。

（8）服务器审计模块

技术指标		指标要求
服务器审计	功能总览	支持针对 Windows、类 Unix（Solaris、ScoUnix、HP Unix、AIX、Linux）操作系统的服务器进行审计监控，包括：服务器资源审计监控（CPU、内存、操作系统版本信息、IP/MAC 地址等）、进程审计监控、文件访问审计监控、服务审计监控、用户登录审计等等。
	性能指标	支持不低于 100 台服务器的审计能力；
	用户监督	支持对被审计服务器上用户的变更，包括增加、删除、修改用户的行为进行监管，同时可以对被审计服务器进行控制，例如：禁止其增加用户，禁止修改用户等操作。

	进程监管	支持集中收集服务器上的进程信息，通过对进程黑白名单的设置，将进程设置为合法和非法进程，一旦服务器上启动非法（黑名单中的）进程，能及时阻断并报警，启动白名单中的进程则只是记录，但不阻断。
	共享监管	支持能够对服务器上的共享文件进行监控，可监管服务器的文件共享情况，包括共享文件路径、文件名等信息，同时可以监控是否允许服务器增加共享、删除共享等操作，出现违规情况能及时阻断并产生报警信息。
	地址监管	支持对受控服务器的 IP 地址进行监管，允许或禁止被审计服务器的 IP 地址修改行为，同时可以记录被审计服务器 IP 地址的修改信息。
	文件监管	支持能够根据文件的扩展名、文件名、路径名，对各类文件的写入、拷贝、删除、创建、读取、覆盖、移动或重命名进行审计并记录，出现违规操作能及时报警。
	服务监管	支持收集系统服务信息，包括服务名，服务描述，服务启动类型以及服务的当前状态，并由界面实时显示；当对受控服务器增加或者删除服务时，产生报警信息；通过设置服务的黑白名单，启动黑名单中的服务报警，一旦对白名单中的服务进行了属性的修改则产生报警。
	软件监管	支持收集被审计服务器软件安装情况并对软件安装信息变化进行审计，包括软件的安装和卸载，产生相应的报警信息。
	开关机监管	支持对服务器的开关机操作进行监控，通过策略设置，对非指定时间内开机的行为进行报警。
	性能监控	支持对 CPU 使用率、内存使用率、队列数量、页面扫描数量、可用交换分区大小、磁盘 I/O、进程数量等性能相关数据进行采集。
	硬件监管	支持能够对受控服务器的硬件设备进行监管，禁止或者允许指定设备的启用，如蓝牙设备，USB 设备，光驱，本地打印机等，并产生相应的报警信息。

（9）应用审计模块

技术指标	指标要求

应用审计模块	审计日志查询	支持能够根据指定查询条件（包括按时间范围、主体或客体、事件种类以及自定义关键词等）进行检索。
	审计报表输出	支持运用审计简约与聚类归并等审计数据分析处理手段，使审计报表更能直观地反映第三方应用系统的安全状态。通过报表统计模块对所有的事件信息进行查询、统计、分析等。
	用户行为审计	（1）支持提供用户访问网站的审计明细，包含：用户类型、用户名、网站名称、URL、访问终端 IP 地址、访问时间、访问结果。 （2）支持提供用户关键事件的审计明细。 （3）支持提供用户新增、更改、删除操作的审计明细。内容包含：操作用户类型、操作用户名、对象用户类型、对象用户名、操作主要内容、操作时间、操作结果。 （4）提供用户可访问资源清单的审计明细。内容至少包含：资源类型、资源名、资源发布时间、资源封停时间、资源访问用户白名单、资源访问用户黑名单。
	状态审计	（1）支持提供应用系统关键进程的审计明细，内容包含：进程类型、进程名、进程态、进程使用端口号、进程启动/暂停/阻塞/停止时间。 （2）支持提供应用系统关键进程内部线程的审计明细，内容包含：线程类型、线程名、线程态、线程使用端口号（若有）、线程启动/暂停/阻塞/停止时间。

IP 地址与网络协议业务规划要求

本项目所有网络设备配置 IPv4/IPv6 双栈接口地址，运行 IPv4/IPv6 双栈路由协议，保持 IPv4 和 IPv6 路由表。其中网络 IPv4 地址要求采用国家政务外网互联共享地址（59.X.X.X）以及上海政务外网本地网络地址（10.X.X.X/16）。其中 IPv6 地址则采用国家信息中心所分配的上海政务外网地址，上海为 240B:803C::/30。
要求投标人在对网络业务类规划、路由协议及虹口区电子政务外网现网 IP 资源等业务需求充分调研的情况下，就虹口区电子政务外网业务 IPv4/IPv6 地址规划、“一网双平面”可靠性实现、网络协议规划、业务带宽及 QOS 流量调整、主备保护等方面提出技术规划方案。并在方案可实施性、业务连续过渡性、可扩展性、可管理性进行综合评定。

网络基础光缆及机房设施要求

网络基础光缆总体要求

要求投标人提供网络基础光缆服务，服务内容包括本次新建 OTN 光传输网络以及政务外网各接入点上联汇聚机房的光纤链路。服务期为 1 年。投标人应具备覆盖全区范围的光纤接入能力，以满足本次项目改造以及今后政务外网新增接入节点业务所需。本项目所有光纤链路均采用裸光纤方式。本次所使用光缆应使用 G.652 或 G.655 规格的光缆，每公里光缆衰耗不大于 0.3dB。

核心、汇聚节点光纤要求

本项目共设置两个核心节点以及三个汇聚节点。
其中两个核心节点分别为区政府机房（飞虹路 518 号）以及本项目新增的核心节点 2;
核心节点 2 拟租用运营商已有通讯机房;
汇聚节点共计 3 个，其中汇聚节点 1 与核心节点 1 同址，用于汇聚院内网络；汇聚节点 2 为劳动局机房；汇聚节点 3 为本次项目新增，为租用运营商已有通讯机房;
要求每个核心、汇聚节点要求提供双路由光缆接入，且每路光缆芯数不低于 48 芯;
要求提供本次项目所有核心、汇聚节点光缆接入设计图纸。光缆设计图纸要求包括但不限于接入位置、接入点光缆路由走向，接入点就近管井信息、交接箱信息、光缆芯数等情况。

接入节点光纤要求

要求虹口区政务外网每个节点提供光纤链路。要求每个接入点分别通过运营商光缆的分别上联至就近汇聚机房，且每个接入点光纤芯数不少于 8 芯。
要求其中 8 个虹口区街道办事处、8 个街道社区事务中心拟采用双路由上联，拟采用两路不同光缆路由分别上联两个就近汇聚机房。且每路接入光缆不少于 8 芯;
要求提供本次项目 8 个虹口区街道办事处、8 个街道社区事务中心的光缆接入设计图纸。光缆设计图纸要求包括但不限于接入位置、接入点光缆路由走向，接入点就近管井信息、交接箱信息、光缆芯数以及上联机房等情况。
政务外网光纤链路接入节点清单:

序号	接入点名称	接入点地址	备注
1	区政府机房核心点		中心点
2	税务局	临平北路 35 号	
3	公安局	闵行路 260 号	
4	绿容局景观所	飞虹路 118 号瑞虹天地写字楼 1 层区绿容景观所 3 楼	
5	工商联	溧阳路 125 号	
6	北外滩办（投促办）	东大名路 908 号金岸 23 楼	
7	建筑署	唐山路 570 弄 1 号	
8	卫生疾控中心	长阳路 197 号	
9	老干部局	临平北路 28 号	

10	烟草局	欧阳路 85 号 B 幢	
11	区创业中心	长阳路 235 号 816	
12	应急救援支队	昆明路 399 号 3 楼弱电机房	
13	区纪委	新港路 186 号 4 楼机房	
14	社会主义学院	欧阳路 415 号	
15	民政局	巴林路 76 号后楼	
16	虹口综合大楼（南楼）	玉田路 222 号	
17	绿化署	中山北二路 1775 号	
18	数据局飞虹路 370 号办公点	飞虹路 370 号	
19	虹房集团	曲阳路 1 号	
20	卫生局	巴林路 76 号前楼（2 号楼）	
21	长远集团-体育局	东江湾路 444 号	
22	房地局	东体育会路 359 号 313 机房	
23	市场监督管理局	大连西路 296 号	
24	区法院	北宝兴路 531 号	
25	水务所	广中支路 28 号	
26	环保检测站	中山北一路 212 号	
27	区残联	广灵四路 116 号	
28	司法局矫正中心	广灵四路 500 号	
29	民政收入核对	水电路 1558 号 1 楼	
30	虹口科投有限公司	水电路 1388 号 8 楼	
31	区人才服务中心	中山北一路 1230 号柏树大厦 A 座 1707 室	
32	虹口公证处	溧阳路 1222 号	
33	武装部	广中支路 28 号	
34	环境监察支队	宝山路 748 号 7 楼	
35	区府临平路大楼	临平北路 7 号	
36	区社会福利中心	广灵四路 268 号	
37	区体育发展中心	乍浦路 471 号	
38	区社会体育管理中心	东江湾路 444 号体育局 205	
39	区少体校	东体育会路 119 弄 37 号	
40	虹口体育馆	东体育会路 715 号	
41	区旅游公共服务中心	四川北路 2286 号	
42	区文化馆	水电路 1412 号	
43	图书馆	水电路 1412 号	
44	儿童福利院	幸福村 286 号	
45	四大纪念馆	四川北路 1468 号	
46	北外滩集团（本部）	东大名路 817 号 3 楼(高阳大楼)	
47	检察院	邯郸路-135 号园区 6 号楼	
48	四川北街道	溧阳路 1338 号	双路由
49	北外滩街道	新建路 100 号	双路由
50	嘉兴街道	天宝路 868 号	双路由
51	曲阳街道	巴林路 60 弄 22 号	双路由

52	欧阳街道	四平路 421 弄 21 号	双路由
53	江湾街道	丰镇路 300 号	双路由
54	凉城街道	凉城路 661 弄	双路由
55	广中街道	同丰路 667 弄	双路由
56	四川北社区事务中心	新广路 296 号	双路由
57	北外滩社区事务中心	新建路 195 号	双路由
58	嘉兴社区事务中心	三河路 380 号	双路由
59	曲阳社区事务中心	伊敏河路 88 号	双路由
60	欧阳社区事务中心	曲阳路 483 弄 1 号	双路由
61	江湾社区事务中心	奎照路 280 号	双路由
62	凉城社区事务中心	凉城路 465 弄 41 号甲	双路由
63	广中社区事务中心	水电路 120 号	双路由
64	北外滩街道城运分中心	东长治路 623 号	双路由
65	教育局	祥德路 96 弄 11 号南楼 1 楼弱机房	双路由
66	区府临平路大楼	临平北路 7 号	
67	社会福利院	密云路 623 号	
68	宇航大厦(绿容/国安/环境)	四川北路 525 号宇航大厦 2 楼	

区级业务专网裸光纤专线要求

本项目中拟提供区公务网、市场监督局专网以及检察院链路裸光纤链路服务，服务期为 1 年。每条链路需提供两芯光缆链路；服务要求如下:

- 实际光缆线路指标:

光纤波长	光纤衰减系数	跳接点衰减系数
1310nm	不高于 0.3dB/km	不高于 0.5dB/个

- 线路服务要求:

a、使用光纤规格为 ITU-T G.652 单模光纤
b、光纤线路质量按国家标准使用寿命额定 15 年（至少）
c、线路尽可能敷设在地下，并通过不同物理路由直接引入机房
d、点-点光缆路由距离不超过 40 公里
e、单根光纤总衰耗不高于 18dB

（1）公务网接入节点清单

序号	接入点名称	接入点地址	上联机房
1	武装部-曲阳街道	巴林路 60 弄 22 号	武装部
2	区政府-法院	北宝兴路 531 号	区政府
3	区政府-法院 2	北宝兴路 531 号	区政府
4	武装部-市场监督局	大连西路 296 号	武装部

5	区政府-区安全局	唐山路 902 号	区政府
6	区政府-体育局	东江湾路 444 号	区政府
7	区政府-房管局	东体育会路 359 号	区政府
8	武装部-江湾镇街道 2	丰镇路 300 号	武装部
9	区政府-工商联 2	溧阳路 125 号	区政府
10	区政府-川北街道	溧阳路 1338 号	区政府
11	武装部-凉城街道 2	凉城路 661 弄	武装部
12	区政府-区税务局	临平北路 35 号	区政府
13	区政府-公安分局	闵行路 260 号	区政府
14	区政府-区委党校	欧阳路 415 号	区政府
15	区政府-绿化市容局	沙泾路 94 号	区政府
16	区政府-欧阳街道	四平路 621 弄 8 号	区政府
17	区政府-检察院 2	唐山路 902 号	区政府
18	区政府-区教育局	祥德路 96 弄 11 号南楼 1 楼弱电机房	区政府
19	区政府-嘉兴街道	天宝路 545 号	区政府
20	武装部-广中路街道办事处综治中心	同丰路 667 弄	武装部
21	区政府-北外滩街道 2	新建路 100 号	区政府
22	区政府-老干部局 2	临平北路 28 号	区政府
23	区纪委-武装部	新港路 186 号 7 楼机房	武装部
24	档案局-武装部	凉城路-2130 号彩虹湾公共服务中心 6 楼	武装部

（2）市场监督局专网接入节点清单

序号	接入点名称	接入点地址	备注
1	市场监督管理局	大连西路 296 号	中心点
2	川北市场监督所-市场监督局	百官街路 18 号 2 楼	
3	欧阳市场监督所 -市场监督局	欧阳路 158 号	
4	北外滩市场监督所-市场监督局	周家嘴路 366-368 号	
5	嘉兴市场监督所-市场监督局	天宝路 466 弄 9 号 7 楼弱电机房（建邦大厦）	
6	区服务大厅-市场监督局	三河路 388 号	
7	凉城工商所-市场监督局	水电路 1312 弄 73-75	
8	执法大队-市场监督局	天宝西路 279 号 3 楼	
9	江湾工商所-市场监督局	新市南路 845 号 3 楼	
10	曲阳工商所-市场监督局	玉田路 252 号 2 楼	
11	消保委-市场监督局	乍浦路 490 号	
12	广中工商所-市场监督局	同心路 1128 弄 8 号	

（3）检察院专网接入节点清单

序号	接入点名称	接入点地址	对端节点
1	检察院专线（邯郸路-吴淞路未检中心）	邯郸路 135 号园区 6 号楼	未检中心
2	检察院专线（邯郸路-看守所）	邯郸路 135 号园区 6 号楼	看守所
3	检察院/保密局-区政府（保密专线）	邯郸路 135 号园区 6 号楼	区政府

核心、汇聚网络机房要求

要求服务商为本项目设置核心节点不少于 2 个，汇聚节点不少于 3 个。其中核心机房可提供 6 个 2000*1200*600（高*深*宽）19 英寸标准机柜，单机柜最大功耗为 3KW。汇聚机房可提供 5 个 2000*1200*600（高*深*宽）19 英寸标准机柜，单机柜最大功耗为 3KW。

所提供机房须满足相应区域为独立空间；机架数量满足所投设备的安装使用，并考虑拓展需求；机柜为独用的标准 19 英寸机柜；每机柜供电不低于 3KW；提供双路供电；UPS 备电时间大于 2 小时；具备门禁系统、监控系统；具备柴发（可为移动柴发）；温度湿度满足通信设备日常工作需求；具备 24 小时值守；值守人员熟知机房内电源、地线、光纤缆的位置、规格、归属等；具备消防灭火设施和防水防潮设备，避免高温、暴雨时产生安全隐患。

要求本次项目中投标人所提供核心、汇聚机房为投标人自有产权或长期租赁。要求投标人提供核心、汇聚机房房产证明或租赁合同。如为租赁关系，则要求自开标之日起至租赁合同终止之日不应少于 5 年。

所有核心、汇聚节点要求投标人提供具体业务机房规划。且所有机房要求满足以下要求:

1、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。

2、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；

3、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；配置双路市电供电，建立备用供电系统，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，同时发电车 2 小时内到现场，确保电力不中断。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。

4、设备与介质管理

政务外网各级机房采用有效的区域监控，配合招标方需求提供调用对接，同时配备防盗报警系统，阻止非法用户的各种临近攻击。

与市级政务外网对接要求

请投标人提供虹口区政务外网与市级政务外网对接实施方案，具体内容要求包括:

（1）虹口区电子政务外网与市级政务外网对接网络拓扑以及业务流量分析

（2）与市级政务外网对接方案，包括但不限于接入方式、对接带宽，IP 地址及路由协议规划，业务流程规划等。

（3）虹口区电子政务外网与市级政务外网对接具体实施步骤说明。

与市级政务外网管理系统承载网对接要求

请投标人提供虹口区政务外网运行和安全监测支撑系统与市级政务外网管理系统承载网对接实施方案，具体内容要求包括:

（1）虹口区政务外网运行和安全监测支撑系统与市级政务外网管理系统承载网对接网络拓扑图。

（2）与市级政务外网管理系统承载网对接方案，包括但不限于接入方式、对接带宽，IP 地址及路由协议规划，职责分工规划等。

（3）虹口区政务外网运行和安全监测支撑系统与市级政务外网管理系统承载网对接具体实施步骤说明。

项目服务与管理要求

项目服务与管理方案编制要求

投标人应充分调研用户现网情况，理解用户现行业务状况，详细设计并提供运维服务方案，包括但不限于服务内容、保障措施、人员管理、质量管理、日常维护方案、安全运营、网络安全保障、应急响应方案、档案管理、服务质量及考核承诺等方面，方案设计考虑运营整体团队的组织设置与功能架构，提供设计周密、岗位明晰、职责、制度流程等，具备长期可操作性和运营支撑能力。并对下述网络整体项目服务运营及服务质量要求提供实质性响应方案，并提供质量措施、保证措施。

服务团队要求

投标人为虹口区电子政务外网的 7*24 小时安全稳定运行提供充足的服务团队保障，并建立完备的组织体系架构。整体网络服务主要人员建议不少于 16 人，其中包括项目负责人 1 名、项目运营经理 1 名、网络运维工程师建议不少于 6 名、网络安全工程师建议不少于 4 名、驻场工程师建议不少于 4 名。

项目负责人对网络运行服务进行全面管理，协调网络运行过程中出现的各类重大、紧急问题。项目负责人具备有效的全国计算机技术与软件专业技术资格（水平）考试证

书中“信息系统项目管理师（高级）”证书，具有本科及以上学历，且具备从事项目负责人或运维经理经验不少于 5 年。
项目运营经理对网络运行服务进行具体处理、落实和管理，并协调网络运行过程中出现的各类问题。项目运营经理具备国家或地方人社局颁发的高级工程师证书，且具备从事项目经理或运维经理经验不少于 5 年。
网络运维工程师在本项目中提供现场故障抢修、技术支持、现场巡检等服务。人数建议不少于 6 人。要求服务工程师具备国家或地方人社局颁发的中级及以上专业技术职称证书且有 3 年以上网络、机房、安全系统等实际维护经验。
网络安全工程师在本项目中提供网络安全事件的处置以及日常网络安全防护工作，人数建议不少于 4 人。要求具备国家或地方人社局颁发的中级及以上专业技术职称证书并具备 3 年以上网络安全项目经验。
驻场工程师，在本项目中要求至少有 2 人负责 7*24 小时驻场在核心节点区政府（飞虹路 518 号），负责网络故障响应、院内网络维护、远程技术支持等。至少有 2 人负责 7*24 小时驻场在虹口区，负责各接入点网络故障响应、院外网络维护、远程技术支持等。驻场工程师人数建议不少于 4 人。要求驻场工程师均具备国家或地方人社局颁发的中级及以上专业技术职称证书，且有 3 年以上网络、机房、安全系统等实际维护经验。

网络服务质量要求

投标人提供的通信网络服务保障网络运行中无重大事故，核心节点可用率不低于 99.99%，汇聚业务接入设备可用率不低于 99%，要求核心节点到汇聚节点的时延指标≤10ms，丢包指标≤0.1%。

网络故障处理要求

1、投标人对故障处理提供相应流程处理方案，包括但不限于故障响应、故障智能预警、重复故障申告、故障处理回访、故障处理报告、投诉处理等，投标人应具备快速定位故障原因的能力。
2、投标人 7*24 小时响应用户单位的网络故障报修，提供报修专线及专业的客户服务。

网络保障要求

提供 7*24 小时故障响应服务，安排专人进行维修。要求在接到用户报修通知后，服务人员要求在 30 分钟内进行应急响应，并在 2 小时内到达现场处理故障，重大故障要求在 4 小时内处理完毕恢复使用，一般故障在 8 小时内处理完毕恢复使用。并在故障发生后 3 天内提供故障报告。

网络日常运行管理要求

投标人应具备网络监控、安全管理、变更管理、故障处理、资源管理、性能管理、流程管理和报告管理等服务能力。

机房值守与巡检

投标人提供服务网络的相关机房配备 7*24 小时现场维护值守人员，并按周对网络进行主动巡检，提供周巡检记录。

技术支持

（1）投标人负责网络的维护、安全运行和支撑工作;
（2）投标人负责对网络故障进行及时诊断、定位和排查处理;
（3）投标人组织实施网络业务的变更，制定维护作业计划并落实;
（4）投标人负责各类网络资源的动态维护与管理;
（5）投标人负责分析研究网络运行状态，周期性形成网络运行的分析报告;
（6）投标人负责网络的评估，提出升级、改造方案并组织实施;
（7）投标人应制定网络应急保障预案并进行演练、实施;
（8）投标人负责收集、整理本级网络及下一级上报的网络数据，形成网络运行维护数据资源， 并对接上报至上一级网络运行维护数据资源库;
（9）投标人负责技术资料的收集、整理和归档工作。

网络安全运营防护要求

1、投标人提供的通信网络，全网符合网络安全等级保护三级要求，具备安全主动防御以及安全可控的政务应用承载能力，能有效防范和拦阻外部攻击，包括但不限于防范黑客通过投标人所属链路攻破信息系统事件。
2、投标人具备安全事件响应与处置能力，包括但不限于防范病毒在投标人所属通信网络扩散等事件。
3、投标人根据招标方的要求定期进行的应急预案修订，并进行每年不少于 2 次的网络安全应急演练。
4、投标人根据招标方要求进行重大安全保障、安全质量管理及安全平台建设等工作，制定相关保障及工作方案。
5、投标人组织安全工作专项团队，对网络安全进行专业化运维。具备网络安全风险评估机制，持续开展网络安全监测，对全网安全运行状况进行分析、研判和通报，实现全网到终端的安全分析预警和安全管理，并根据招标方的要求，按需提供相关网络安全分析报告。
6、投标人每年组织一次由第三方机构进行的网络安全测评以及每年组织一次网络安全自测。
7、投标人根据招标方要求配合开展季度安全检查工作。

现网业务连续性服务要求

投标人应充分调研现网运行情况并结合对本项目的理解，提供对现有网络及系统进行规范性迁移，具有合理性、可实际操作及组织保障管理的实施方案，提出满足本次项目需求的最短网络迁移割接计划，并对最终时间周期作出承诺。包含部署迁移过

程的协调管理、风险评估与监控，以及确保应用迁移风险最小化。对虹口区电子政务外网中的重要节点，包括区级委办局、区直属单位以及全区街道居委主要提供迁移方案设计、割接经验，同时对此类节点今后搬迁、新建等提供的相关实施方案。如投标人具备与政务外网服务相关的运行和安全支撑系统的对接及服务经验，提供对接方案设计。投标人对政务运行和安全支撑系统充分理解，提供整体、完备及后续业务可延性的支撑方案。

其他增量服务

投标人根据自身实际情况，提出可在服务周期内提供的其他服务。

企业实力要求

投标人需提供近 3 年内承接的有效的类似项目业绩，以证明其有能力承接该项目。

项目实施要求

服务开通实施计划

投标人按本招标要求中所规定的各项服务要求，在收到中标通知书的 20 个自然日内完成本次招标中所提出的服务对象及范围内用户提供虹口区电子政务外网网络通信服务开通验收并投入使用。如项目涉及工程实施内容，要求投标人提出详细的项目实施计划，对整个项目进行阶段性划分，说明各个阶段的任务、工作过程和方法，明确各阶段的职责划分、工作内容、形式和进度时间计划。实施应至少细化到日，并且应根据投标人要求进行调整和细化，要求给出时间具体安排及工期。
投标人于收到中标通知书后的 5 个日历日内向招标方提供集成建设方案（包括测试方案、实施方案、业务迁移方案、应急预案、保障方案、人员安排、施工计划等）。承诺投标人收到中标通知书后 10 个日历日内项目所涉及所有设备到货并提供相应清单。

服务连续性要求

如涉及业务割接，投标方应针对本次服务内容提供符合虹口区政务外网现网要求的无缝业务割接方案，须承诺所进行的网络割接等操作不影响网络正常运行，并提供相应承诺书。承诺所进行的网络割接等操作尽量避免影响现有网络通信、互联网访问、政务应用等业务正常运行，保证政务外网服务的连续性。根据方案对于现网造成影响用户与应用范围、影响时间以及整体方案安全性进行整体评估。
1、 应完整详细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，并具备合理性。（包括核心、汇聚、接入点以及政务云、市政务外网对接、互联网出口等）
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，并具备可行性。
3、网络割接方案要求考虑对用户业务的中断性影响。政务外网作为政府应用基础保

障网络，投标人确保平滑割接，将影响控制在最小，不影响用户正常业务的开展。
4、方案内容包括但不限于网络拓扑、施工材料、迁移实施步骤、网络配置、线路切换、应急演练、验证方式、迁移时间、回退方案和保障计划等。

项目验收及服务要求

服务开通验收

本项目要求整体网络服务开通时间在收到中标通知书的 20 个自然日内，且中标方全部满足以下服务开通验收要求:

1、要求全网全部接入点网络服务按时开通;

2、要求本技术需求所需设备包括光传输设备、网络设备、安全设备等皆按要求完成安装、调试并投入使用;

3、要求中标方向招标方提供完整验收文档，包括但不限于网络技术方案、网络设计图纸、业务迁移方案、应急预案以及项目保障方案、项目测试、验收方案以及项目运行服务方案;

4、要求整体网络通过网络安全等级保护三级测评，并出具评测报告。

服务交付验收

1、投标人根据对本项目需求理解提供相应的网络运营服务规范。

2、投标人对服务网络中核心设备制定“一机一档”机制，形成建档标准，确保设备信息真实全面、合理有效。

3、投标人配合招标方每年的项目验收工作，提供验收所需的年度运维服务报告（加盖运维公司章）、月度报告、季度报告或专题报告、第三方测试报告、故障报告、工程建设台账等。

服务指标要求

1、区级政务外网核心节点可用率不低于 99.99%;

2、区级政务外网汇聚业务接入设备可用率不低于 99%;

3、区级政务外网核心节点到汇聚节点的时延指标≤10ms，丢包指标≤0.1%;

4、按要求区级政务外网各保障等级的用户均进行 7*24 小时运行保障服务，发现网络异常即时告警，并根据用户重要等级不同，提供不同等级的主动保障抢修及电话通知服务，具体用户等级划分由招标方确认。

- 特级保障用户：监控发现告警时，即刻通知用户，正常情况 1 小时内到达故障现场，60 分钟内完成报修处置;
- 一级保障用户：监控发现告警时，7×12 小时（8:00 至 20:00）时间段内通知用户，正常情况 1 小时内到达故障现场，100 分钟内完成报修处置;
- 二级保障用户：监控发现告警时，在 5×8 小时（9:00 至 17:00）时间段内通知用户，正常情况 1.5 小时内到达故障现场完成报修处置，120 分钟内完成报修处置;

- 三级保障用户：提供 7×24 小时客户服务报修热线，正常情况 1.5 小时内到达故障现场，200 分钟内完成报修处置;

5、要求 7*24 小时响应用户单位的网络故障报修，提供报修专线及专业的客户服务，并要求在 20 秒内实现人工接通;

6、投标人接到招标方开具的工单后，要求在 5 个工作日内完成到用户接入点电路的资源调查工作，及时制定并提交符合用户需求、具备可实施性的具体方案，要求在 30 个工作日内完成网络接入施工，因市政管道资源条件限制、接入单位不具备接入条件等特殊原因影响网络接入的，可以根据实际情况适当延时但不得超过 90 个工作日;

7、要求投标人每个自然日针对监测到的网络安全事件和告警信息完成当日处置工作;

8、要求投标人在服务期间不得出现由于安全漏洞（包括但不限于网络攻击）未及时发现并处置，造成网络中断、非法控制、信息泄露、数据篡改等重大安全事件;

以上网络服务指标要求投标人逐条响应并出具相应网络服务指标承诺书。

服务承诺要求

1、投标人提供的服务和相应的硬件、软件，应符合国家、行业或者企业标准，在稳定性、网络安全性、环保等领域不存在任何缺陷。

2、提供的服务不存在任何侵犯第三方权利（包括但不限于知识产权等）的情况，任何第三方如提出侵权指控，投标人需及时进行处理，给招标方造成损失的，投标人应赔偿一切损失。

3、在本项目约定的履行期限内或者履行期限届满后，对网络带宽、硬件软件数量、覆盖区域等方面的扩充或者增加，投标人承诺将按与本项目同等的优惠条件提供光纤接入和技术服务。

对投标单位的其它要求

内容要求
业务设计分析 （1）投标人对现有网络架构与分区情况、网络与安全设备部署情况、网络流量情况、IP 地址与路由规划、网络所承载应用情况的了解，要求充分、完整、准确。 （2）根据以上了解情况，投标人需要从网络、安全、运营服务等三个方面对项目进行分析，要求分析充分，服务目标精确。
业务连续性 （1）投标方案设计及实施中充分考虑业务连续性要求，对现有区级政务外网网络和用户业务的连续性运行、网络安全稳定性影响最小。可达成服务的工作时间计划周期最短，根据方案进行综合评价。 （2）网络服务系统在网络容灾备份设计上的先进性、可靠性和安全性情况，要求充分考虑业务连续性要求，根据方案进行综合评价。 （3）投标方应保障现有区级政务外网网络和用户业务无中断。
网络技术架构 （1）要求对现有政务外网运行技术架构的了解和分析充分、资料详实，对方案设计有深入把握。网络技术架构需要高可用、强扩展并适度超前，管理功能要求高效可实现性高，根据方案进行综合评价。 （2）网络技术架构满足项目服务的支撑与后续业务扩展，部署或变更实施所需时效性最强、对政务外网运行影响度最低，根据方案进行综合评价。
网络业务规划方案 （1）要求对区级政务外网业务类规划以及网络 IP 资源等业务情况了解充分、资料详实。业务规划方案对网络“一网双平面”实现、业务带宽及 QOS 流量调整、SDN 配置调整、主备保护、IP 地址规划等方面提供技术方案的实质性响应，根据方案可实施性、业务连续过渡性、可扩展性、可管理性情况综合评价。 （2）服务技术方案业务规划执行实现的时间计划安排，要求满足业务开通时间需要，对网络风险影响程度最低。
与市级政务外网对接方案 （1）作为“全市一张网”的市区两级政务外网，投标人所提出的与市级政务外网对接实施方案要求完整、可行、安全。 （2）从对接业务类型、网络协议、IP 地址规划等方面进行方案描述。
与市级政务外网管理系统承载网对接方案 （1）投标人所提出的与市级政务外网管理系统承载网对接实施方案要求完整、可行、安全。 （2）从对接业务类型、对接网络拓扑图，接入方式，对接带宽，IP 地址及路由协议规划，职责分工规划，具体实施步骤等方面进行方案描述。
机房要求 投标人所提供运营商租用核心、汇聚机房距离要达到用户的基本功能实现要求，可提供自有产权证明或机房长期租赁合同或者由投标单位承诺中标后提供符合要求的自有产权证明或机房长期租赁合同。
服务所用机房、光缆资源情况 （1）投标人需要提供本项目 2 个核心节点和 3 个汇聚节点（其中核心节点 1 与汇聚节点 1 同址）、8 个街道办事处及 8 个社区事务服务中心共计 20 个接入点光缆

接入设计图纸。 （2）投标所提供接入点光缆设计图纸符合要求，包括接入光缆、双路由走向、管井信息、交接箱信息、光缆芯数等内容
安全方案设计 对政务外网安全威胁与风险情况有详实了解、资料充分，对全网业务安全性理解深入完善。要求在网络物理安全、传输安全、各主要区域对接边界安全、用户接入安全等方面有实质性的设计响应，设计详尽完善，安全方案部署对政务外网现网业务的影响和风险程度最低，实施具有可行性、时效性强。
安全等保防护情况 投标人所提供电子政务外网安全方案的合规性在以往政务外网服务项目中获得验证的，提供类似项目并通过安全等级保护测评报告。
全网业务及服务开通 （1）投标人制定的全网服务开通方案具备技术可行性和实践操作性。重点评估方案对现有网络设施、系统运行、业务流量、安全策略的影响程度。 （2）投标人承诺的服务开通所需的具体时限优于或者满足采购文件要求，且科学、合理（考虑到业务规模、技术复杂度、资源投入等）。 （3）投标人需要提供保障按时开通的具体计划、资源配置（人力、软硬件资源到位计划），包含应对计划外延误的应急预案或措施。 （4）投标人在服务开通实施计划中，需要明确提出对现有网络生产环境影响最小及服务连续性保障的承诺与自罚条款。
运维服务方案整体设计 项目网络运营服务方案要求完整、合理，包括服务内容、服务团队、日常运维方案、应急响应方案、网络安全防护方案、文档和资料管理、培训等内容。
服务运营与质量、安全保证措施 根据投标人提供的服务质量保证措施进行综合评分：服务质量保证措施完整并有自罚承诺、可操作性强，人员服务质量保障制度完善，提供完善的延伸服务，根据措施完整性情况评审。
业务迁移方案 （1）如涉及业务割接，投标方应针对本次服务内容提供符合本区政务外网现网要求的无缝业务割接方案，须承诺所进行的网络割接等操作不影响网络正常运行，并提供网络无缝业务迁移承诺函。 （2）投标人所提供业务迁移方案（含核心、汇聚、接入层、互联网出口、政务云应用等）要求完整、可行，割接步骤具体详实，实施保障措施完备。
服务方案组织与架构 要求运营整体团队的组织设置与功能架构方面设计周密，岗位职责、制度流程明确，具备长期可操作性。
服务团队及人员配置 （1）要求运维团队建议：不少于 16 人，团队数量和人员专业性配置齐全，提供每一位团队人员有关资质、社保证明、学历、专业、职称及主要从业经历。 （2）项目负责人要求建议：具备信息系统项目管理师（高级）证书，具有本科及以上学历，且具备从事项目负责人或运维经理经验不少于 5 年。 （3）项目运营经理要求建议：具备高级工程师证书，且具备从事项目经理或运维经理经验不少于 5 年。 （4）网络运维工程师要求建议：不少于 6 人，网络运维工程师配置合理，具备中级及以上专业技术职称证书且有 3 年以上网络、机房、安全系统等实际维护经验。

（5）网络安全工程师要求建议：不少于 4 人，网络安全工程师配置合理，具备中级及以上专业技术职称证书并具备 3 年以上网络安全项目经验。。 （6）驻场工程师要求建议：不少于 4 人，驻场工程师配置合理，提供 7*24 小时驻场服务。要求驻场工程师均具备中级及以上专业技术职称证书，且有 3 年以上网络、机房、安全系统等实际维护经验。
类似项目业绩实力 投标人近 3 年内承接的有效的类似项目业绩。需提供相关业绩的合同关键页扫描件（至少包含合同双方签章页、项目名称及内容、合同金额、合同签订日期），否则将不予认可。

本项目为非仅面向中小企业，所属行业为 软件和信息技术服务业（用于中小企业声明函），属于服务类项目。中小企业声明函的红色区域需认真填写（中小企业声明函详见采购文件格式附件）。

中小企业声明函（工程、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**上海市虹口区城市运行综合管理中心**的 **二级政务网年租费（2025-2026 年）** 采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：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. **（二级政务网年租费（2025-2026 年））**，属于**（软件和信息技术服务业）**；承建（承接）企业为_____（企业名称），从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于_____（*中型企业、小型企业、微型企业*）；……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

注：各行业划型标准

(十二)软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。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。

第五章　政府采购合同主要条款指引

包 1 合同模板：

[合同中心-合同名称]

合同统一编号： [合同中心-合同编码]

合同内部编号：

合同各方：

甲方：[合同中心-采购单位名称]	乙方：[合同中心-供应商名称]
地址：[合同中心-采购单位所在地]	地址：[合同中心-供应商所在地]
邮政编码：[合同中心-采购人单位邮编]	邮政编码：[合同中心-供应商单位邮编]
电话：[合同中心-采购单位联系人电话]	电话：[合同中心-供应商联系人电话]
传真：[合同中心-采购人单位传真]	传真：[合同中心-供应商单位传真]
联系人：[合同中心-采购单位联系人]	联系人：[合同中心-供应商联系人]

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

1．乙方根据本合同的规定向甲方提供以下服务：

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： 甲方指定。

2．3 服务期限 ：按照采购文件等相关要求。
本服务的服务期限：[合同中心-合同有效期]。

3．质量标准和要求

3．1 乙方所提供的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]

（1）本合同付款按照上述付款内容和付款次序分期付款或一次性付款。

8．甲方（甲方）的权利义务

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

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

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

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

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

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

9．乙方的权利与义务

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

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

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

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

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

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

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

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

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

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

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

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

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

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

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供服务。

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

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

12．误期赔偿

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

13．不可抗力

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

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

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

14．履约保证金

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为元人民币的履约保证金。履约保证金应自出具之日起至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。

签约各方：

甲方（盖章）： 乙方（盖章）：

法定代表人或授权委托人（签章）： 法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]** 日期：[合同中心-签订时间]

合同签订点:网上签约

第六章 投标文件格式附件

附件 1：

二级政务网年租费（2025-2026 年）

项目编号：310109000250605115128-09255652（标项　）

资

质

文

件

投标人全称：

地　　址：

时　　间：

1、资质文件目录

（1）投标声明书（格式见附件，含无重大违法记录及不诚信行为声明)；

（2）“信用中国”网站（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）投标人信用查询情况。（以开标当日采购人或采购代理机构或由采购人委托的评标委员会核实的查询结果为准）

（3）法定代表人授权委托书(格式见附件)；

（4）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

（5）联合投标协议书（若需要）；

（6）联合投标授权委托书（若需要）；

（7）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

（8）财务状况，税收及社保缴纳声明函。

（9）前三内经营活动中无重大违法记录和无不诚信行为的声明。

附件 2：

声 明 书

致上海市虹口区政府采购中心：

（投标人名称）系中华人民共和国合法企业，经营地址_____。

我（姓名）系（投标人名称）的法定代表人，我方愿意参加贵方组织的（二级政务网年租费（2025-2026 年））（编号为310109000250605115128-09255652）的投标，为此，我方就本次投标有关事项郑重声明如下：

1、我方已详细审查全部招标文件，同意招标文件的各项要求。

2、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。

3、若中标，我方将按招标文件规定履行合同责任和义务。

4、我方不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。

5、投标文件自开标日起有效期为 90 天。

6、我方参与本项目前 3 年内的经营活动中没有重大违法记录及不诚信行为；

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

8、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。

法定代表人签名（或签名章）：_____ 日 期：

投标人全称（公章）：

附件 3：

法定代表人授权委托书

上海市虹口区政府采购中心：

我____（姓名）系____（投标人名称）的法定代表人，现授权委托本单位在职职工 _____（姓名）为授权代表，以我方的名义参加项目编号：_____项目名称：_____项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对授权代表的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。授权代表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。

授权代表无转委托权，特此委托。

授权代表签名：_____ 职务：

授权代表身份证号码：_____电话：

邮箱（方便告知投标单位后续相关事宜）：

法定代表人签名（或签名章）：_____ 职务：

法定代表人身份证号码：_____电话：

投标人全称（公章）：_____ 日 期：_____

附件 4：

联 合 投 标 协 议 书

甲方：

乙方：

（如果有的话，可按甲、乙、丙、丁…序列增加）

各方经协商，就响应 _____组织实施的编号为 号的招标活动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产品和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，甲方承担的工作和义务为:

乙方承担的工作和义务为：

五、有关本次联合投标的其他事宜：

六、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。

七、本协议签约各方各持一份，并作为投标文件的一部分。

甲方单位：　　（公章）　　乙方单位：　　（公章）

法定代表人：　　（签章）　　法定代表人：　　（签章）

日　期：　　年　　月　　日　　日　期：　　年　　月　　日

附件 5：

联合投标授权委托书

本授权委托书声明：根据 _____与_____签订的《联合投标协议书》的内容，主办人_____的法定代表人_____现授权 _____为联合投标代理人，代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与这有关的一切事务， 联合投标各方均予以认可并遵守。

特此委托。

授权人（签名）：

日期：　　年　月　日

授权代表（签名）；

日期：　　年　月　日

联合体甲方单位：　　（公章）　联合体乙方单位：　　（公章）

法定代表人：　　（签章）　法定代表人：　　（签章）

日　期：　年　月　日　　日　期：　年　月　日

附件 6：

二级政务网年租费（2025-2026年）

项目编号：310109000250605115128-09255652（标项　）

技术及商务文件

投标人全称：

地　　址：

时　　间：

2、技术及商务文件目录

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标方认为需要的其他文件资料。

附件 7：

评分对应表

投标人全称（公章）：_____ 标项：

评分项目	投标文件对应资料	投标文件页码
对应第三章评分办法及评分标准（报价除外）		
……		

授权代表签名：_____ 日期：

附件 8：

投 标 项 目 明 细 清 单

投标人全称（公章）：_____ 标项：

货物类

序号	货物名称	品牌	规格型号	单位及数量	性能及指标	产地

服务类

序号	服务内容	服务人员数量	工作量

注：在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。

授权代表签名：_____ 日期：

附件 9：

技 术 响 应 表

投标人全称（公章）：_____ 标项：

招标文件要求	投标文件响应	偏离情况

注：投标人应根据投标设备的性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

授权代表签名：_____ 日 期：

附件 10：

项目组人员清单

投标人全称（公章）：_____ 标项：

姓名	职务	专业技术资格	证书编号	参加本单位工作时间	劳动合同编号

注：在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

授权代表签名：_____ 日　　期：

附件 11：

商务响应表

投标人全称（公章）：_____ 标项：

项目	招标文件要求	是否响应	投标人的承诺或说明
供货时间(项目工期)及地点			
付款条件			
违约责任及争议解决方式			
项目维护计划			
响应情况			
本地化服务要求			
技术培训			
公司技术力量情况			
经验或业绩要求			
……			

授权代表签名：_____ 日期：

附件 12：

投标人业绩情况一览表

投标人全称（公章）：

采购单位名称	设备或项目名称	采购数量	单价	合同金额（万元）	附件页码		采购单位联系人及联系电话
					合同	验收报告	
备注	提供投标人同类项目合同复印件、用户验收报告（如有）。						

授权代表签名：_____　　时　间：_____

附件 13：

二级政务网年租费（2025-2026年）

项目编号：310109000250605115128-09255652（标项　）

报价文件

投标人全称：

地　　址：

时　　间：

3、报价文件目录

（1）投标报价明细表（见附件 14）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）中小微企业声明函（见附件 15）；

（4）残疾人福利企业声明函（见附件 16）。

附件 14：

投 标 报 价 明 细 表

投标人全称（公章）：

招标编号及标项：

二级政务网年租费（2025-2026 年）包 1

备注	投标人专用邮箱	服务期限（月）	最终报价（总价、元）

授权代表签名：　　日期：

附件 15：

中小企业声明函（货物）

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

1. *（标的名称）*，属于*（采购文件中明确的所属行业）*行业；制造商为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于*（中型企业、小型企业、微型企业）*；

2. *（标的名称）*，属于*（采购文件中明确的所属行业）*行业；制造商为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于*（中型企业、小型企业、微型企业）*；

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

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

备注：请认真填写中小企业声明函，中小企业声明函填写不全或者填写错误，在审查认定时对投标单位不利，均有可能导致投标废标风险。

中小企业声明函（工程、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，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. *（标的名称）*，属于*（采购文件中明确的所属行业）*；承建（承接）企业为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于*（中型企业、小型企业、微型企业）*；

2. *（标的名称）*，属于*（采购文件中明确的所属行业）*；承建（承接）企业为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于*（中型企业、小型企业、微型企业）*；

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

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。

备注： 请认真填写中小企业声明函，中小企业声明函填写不全或者填写错误，在审查认定时对投标单位不利，均有可能导致投标废标风险。

附件 16：

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，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　期：

附件 18：

政府采购活动现场确认声明书

上海市虹口区政府采购中心：

本人经由_____（单位）负责人_____（姓名）合法授权参加_____项目（编号：_____）政府采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

一、本单位与采购人之间 □不存在利害关系 □存在下列利害关系_____：

A.投资关系　　B.行政隶属关系　　C.业务指导关系

D.其他可能影响采购公正的利害关系(如有,请如实说明)_____。

二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位 □与其他所有供应商之间均不存在利害关系 □与_____（供应商名称）之间存在下列利害关系_____：

A.法定代表人或负责人或实际控制人是同一人

B.法定代表人或负责人或实际控制人是夫妻关系

C.法定代表人或负责人或实际控制人是直系血亲关系

D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

E.法定代表人或负责人或实际控制人存在近姻亲关系

F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入 50%以上）或重要财务往来关系（如融资）等其他实质性控制关系

I.其他利害关系情况_____。

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

四、我发现_____供应商之间存在或可能存在上述第二条第_____项利害关系。

（供应商代表签名）

年　月　日

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：

前三年内无重大违法记录及无不诚信行为声明函

我方（供应商名称）承诺在参加本项目政府采购活动前三年内，在经营活动中无重大违法记录及无不诚信行为，我方遵守相关国家法律法规，符合《中华人民共和国政府采购法》及相关法规规章规定的有关政府采购供应商应当具备的条件，符合拟申请项目的供应商相关要求。

我方（供应商名称）已通过（包括但不限于“信用中国”、“中国政府采购网”、“国家企业信用公示系统”等）法定途径，全面自查确认：我方在参加本次政府采购活动前三年内，在经营活动中没有重大违法记录。

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：