



项目编号：310115000260430107934-15350750

# 中国（上海）自贸区基 础云平台 2026 年建设 项目

## 招标文件 (正式稿)

采购人：上海市浦东新区大数据中心  
集中采购机构：上海市浦东新区政府采购中心

2026年05月19日

2026年05月2026年05月19日

## 电子投标特别提醒

### 一、注册登记与安全认证

为确保电子采购平台数据的合法、有效和安全，各参与主体均应在上海市政府采购管理信息平台（以下简称“电子采购平台”）上注册登记并获得账号和密码。采购人、投标人、集中采购机构还应根据《上海市数字证书使用管理办法》等规定，向本市依法设立的电子认证服务机构申请用于身份认证和电子签名的数字证书（CA 证书），并严格按照规定使用电子签名和电子印章。

### 二、招标文件下载

投标人使用数字证书（CA 证书）登陆《上海政府采购网》（上海政府采购云平台），在电子政府采购平台下载并保存招标文件。如招标公告要求投标人在下载招标文件前进行报名登记，并查验资格证明文件的，投标人应当按照招标公告的要求先行登记后，再下载招标文件。

### 三、招标文件的澄清、补充与修改

采购人和集中采购机构可以依法对招标文件进行澄清、补充与修改。澄清、补充与修改的文件将在电子采购平台上予以公告，并通过电子采购平台发送至已下载招标文件的供应商工作区。

### 四、投标文件的编制、加密和上传

投标人下载招标文件后，应使用电子采购平台提供的投标工具客户端编制投标文件。

在投标截止前，投标人在“网上投标”栏目内选择要参与的投标项目，按照网上投标系统和招标文件要求填写网上投标内容。对于有多个包件的招标项目，投标人可以选择要参与的包件进行投标。只有投标状态显示为“标书提交”时，才是有效投标。

投标人和电子采购平台应分别对投标文件实施加密。投标人通过投标工具，使用数字证书（CA 证书）对投标文件加密后，上传至电子采购平台，再经过电子采购平台加密保存。由于投标人的原因，造成其投标文件未能加密，导致投标文件在开标前泄密的，由投标人自行承担责任。

投标人在网上投标系统中，应提交投标文件彩色扫描件（PDF 文件），投标文件组成内容详见招标文件要求。本项目恕不接受电子采购平台以外其他形式的投标。

投标人应根据招标文件的要求编制投标文件，投标文件内容应规范完整、简洁明了、编排合理有序，其中的扫描文件应清晰完整。考虑到电子采购平台运行现状，上传电子加密标书最大支持150M，详细技术问题可咨询电子采购平台运维单位。

**投标人组成联合体形式投标，由联合体中的主体方进行网上投标操作，投标流程和要求参照以上条款。**

投标文件内容不完整、格式不符合要求，导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

### 五、投标截止

投标截止后电子采购平台不再接受供应商上传投标文件。

投标截止与开标的时间以电子采购平台显示的时间为准。

### 六、开标

开标程序在电子采购平台进行，投标人在完成网上投标后，按照招标文件规定的时间和地点，由其法定代表人，或经授权的代理人携带要求的材料及设备【笔记本电脑、无线网卡、数字证书（CA 证书）】，登录《上海政府采购网》（上海政府采购云平台）（<http://www.zfcg.sh.gov.cn>）参加开标。

**为确保您所参与的招投标工作的顺利进行，避免在此期间因数字证书办理更新、变更等而导致您的投标文件解密失败，特提示您：在开标业务未完成期间，请勿进行数字证书的更新、变更等操作。**

**您可以在投标前或开标业务完成后再进行数字证书更新、变更等操作，以避免因此给您的招投标工作带来不便。**

### 七、投标文件解密

投标截止、电子采购平台显示开标后，投标人进行签到操作，操作时长以平台显示时间（目前为 30 分钟）为准。投标人签到完成后，由集中采购机构解除电子采购平台对投标文件的加密，投标人应在电子采购平台规定时间内使用数字证书（CA 证书）对其投标文件解密，操作时长以平台显示时间（目前为 30 分钟）为准。投标人应在规定时间内完成上述签到或解密操作，逾期未完成签到或解密的投标人，其投标将作无效标处理。

### 八、开标记录的确认

投标文件解密后，电子采购平台根据各投标人通过投标客户端填写并提交的《开标一览表》中的报价，自动汇总生成《开标记录表》。为此，投标人应正确填写，使投标客户端的《开标一览表》和投标文件中的《开标一览表》所填报价保持一致。

**投标人应及时检查《开标记录表》的数据与其投标文件中的《开标一览表》是否一致，并作出确认。投标人因自身原因未作出确认的，视为其认可《开标记录表》内容。**

### 九、其他

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

本项目实施过程中因以下原因导致的不良后果，集中采购机构不承担责任，投标人参加本项目投标即被视作同意下述免责内容：

- 1、电子采购平台的程序设置对本项目产生的影响；
- 2、集中采购机构以外的单位或个人，在电子采购平台中的不当操作，对本项目产生的影响；
- 3、电子采购平台发生技术故障或遭受网络攻击对本项目所产生的影响；
- 4、其他无法预计或不可抗拒的因素。

### 十、电子采购平台技术咨询联系方式

联系电话：95763（市级）

## 投标邀请

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》和《上海市电子政府采购管理暂行办法》之规定，受采购人的委托，集中采购机构对采购项目进行国内公开招标采购，特邀请合格的供应商前来投标。

### 一、合格的投标人必须具备以下条件：

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

3.1 本项目面向大、中、小、微型企业，事业法人、其他组织或自然人采购。

3.2 本项目**不允许**联合体形式投标。

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

### 二、项目概况：

1、项目名称：中国（上海）自贸区基础云平台 2026年建设项目

2、招标编号：310115000260430107934-15350750

3、预算编号：包1：1526-W00026421；包2：1526-W00026422；包3：1526-W00026423

4、项目主要内容、数量及简要规格描述或项目基本概况介绍：

本项目共包含3个包件，同一投标人允许最多中标2个包件：

包1：包名称为中国（上海）自贸区基础云平台2026年建设项目区域一，预算金额为50,685,537.92元。

包2：包名称为中国（上海）自贸区基础云平台2026年建设项目区域二，预算金额为55,046,105.01元。

包3：包名称为中国（上海）自贸区基础云平台2026年建设项目区域三，预算金额为51,958,551.61元。

本项目各包件最高限价同预算金额。

包1：

包名称：中国（上海）自贸区基础云平台2026年建设项目区域一

招标范围及内容主要包括：（1）云资源服务（2）算力资源服务（3）网络服务（4）安全服务（5）密码服务（6）运行维护服务（7）服务模式。详见第二章项目招标需求。

包2：

包名称：中国（上海）自贸区基础云平台 2026 年建设项目区域二

招标范围及内容主要包括：（1）云资源服务（2）算力资源服务（3）网络资源服务（4）安全服务（5）密码服务（6）运行维护服务（7）服务模式。详见第二章项目招标需求。

包3：

包名称：中国（上海）自贸区基础云平台 2026 年建设项目区域三

招标范围及内容主要包括：（1）云资源服务（2）算力资源服务（3）网络资源服务（4）安全服务（5）密码服务（6）服务模式。详见第二章项目招标需求。

按照《中小企业划分标准规定》（工信部联企业〔2011〕300号），本项目采购的中国（上海）自贸区基础云平台 2026年建设项目（标的）属于**软件和信息技术服务业**。

5、交付地址：上海市浦东新区迎春路520号（采购人指定地址）。

6、服务期限：**合同签订后，自各项服务交付之日起一年**。以乙方向甲方提供资源下发测试等相关证明材料为准。

7、采购预算金额：157,690,194.54元（国库资金：157,690,194.54元；自筹资金：0元）

8、采购项目需要落实的政府采购政策情况：节能产品政府采购、环境标志产品政府采购、促进中小企业发展、促进残疾人就业。

### 三、招标文件的获取

时间：**2026-05-19**至**2026-05-26**，每天上午**00:00:00~12:00:00**，下午**12:00:00~23:59:59**（北京时间，法定节假日除外）。

合格的供应商可于招标公告发布之日起至公告截止时间内，登录《上海政府采购网“对标改革专窗”》（<http://www.zfcg.sh.gov.cn>）在网上招标系统中上传如下材料：无

合格供应商可在招标公告规定的时间内下载招标文件并按照招标文件要求参加投标。

凡愿参加投标的合格供应商应在招标公告规定的时间内按照规定获取招标文件，逾期不再办理。未按规定获取招标文件的投标将被拒绝。

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

### 四、投标截止时间及开标时间：

1、投标截止时间：**2026-06-01 10:00:00**（电子采购平台显示时间）。

2、开标时间：**2026-06-01 10:00:00**（电子采购平台显示时间）。

### 五、投标地点和开标地点

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

2、开标地点：上海政府采购网（<http://www.zfcg.sh.gov.cn>）。届时请投标人代表持投标时所使用的数字证书（CA证书）参加开标。

3、开标所需携带其他材料：

**自行携带无线上网的笔记本电脑、无线网卡、数字证书（CA证书）。**

### 六、发布公告的媒介：

以上信息如果有变更我们会通过《上海政府采购网》通知，请供应商关注。

### 七、其他事项

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

### 八、联系方式

采购人：	上海市浦东新区大数据中心	集中采购机构：	上海市浦东新区政府采购中心
地址：	上海市浦东新区迎春路520号7楼	地址：	上海市浦东新区民生路1399号16楼
邮编：	200135	邮编：	200135
联系人：	成金燕	联系人：	宋杨宏
电话：	58206726	电话：	68549758
传真：	/	传真：	68542614

## 第一章投标人须知及前附表

### 一、投标人须知前附表

本表关于项目的具体要求是对投标人须知的具体补充，两者如有矛盾，应以本表为准。

条款号	内容规定	备注
1.1	项目名称：中国（上海）自贸区基础云平台 2026年建设项目	
6.1	关于现场踏勘 （1）集合时间：****年**月**日**:**（北京时间） （2）地点：***** （3）联系人：***** （4）联系电话：*****	<u>（本项目不适用）</u>
7.1	关于澄清答疑 （1）提问递交截止时间：2026年5月27日10时整（北京时间） （2）提问递交方式：以书面形式（必须加盖投标人公章）递交至“《投标邀请》/八联系方式”集中采购机构地址。	
7.2	答疑会时间：****年**月**日**:**（北京时间） 地点：上海市浦东新区民生路1399号16楼***室	<u>（本项目不适用）</u>
10.1.1	投标人提交的投标文件商务部分应包括以下内容（不局限于以下内容）： （1）投标承诺书 （2）投标函 （3）法定代表人身份证明及授权委托书 （4）投标保证金（ <b>支票、汇票、本票、保函等非现金形式</b> ) <u>（本项目不适用）</u> （5）投标人基本情况表 （6）投标人应提交的资格证明材料 ①财务状况及税收、社会保障资金缴纳情况声明函； （7）开标一览表 （8）投标报价明细表 （9）根据招标文件要求，投标人提供以下证明材料： ① <u>国家强制认证的产品承诺书</u> ； （10）拟分包项目一览表 <u>（本项目不适用）</u> （11）投标人可提交的商务部分其他证明材料（不仅限于以下资料） ①中小企业声明函（注：仅中、小、微型企业须提供）； ②投标人综合实力介绍，包括投标人认为可以证明其履约能力和水平的《近三年类似项目承接及履约情况一览表》（详见“投标文件格式”），获得的有关荣誉证书，质量管理体系和质量保证体系等方面的认证证书 ③投标人认为可以证明其信誉和信用的其他材料； ④残疾人福利性单位声明函；（注：仅残疾人福利单位提供） ⑤制造商授权书等证明文件（ <b>如果有</b> ）。	投标文件内容不完整、格式不符合要求，导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

条款号	内容规定	备注
	⑥《关于符合本国产品标准的声明函》或财政部会同有关部门规定的有关证明文件； <u>（本项目不适用）</u> ⑦关于符合本国产品标准的成本占比的承诺函（采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到80%以上时提供） <u>（本项目不适用）</u>	
10.1.2	投标人提交的投标文件技术部分应包括（不局限于以下内容）： （1）技术方案（包括：总体方案、分项实施方案等）； （2）拟投入本项目的人员组成情况（包括《拟派人员汇总表》、《项目主要人员基本情况表》、《项目其他工作人员基本情况表》）； （3）项目服务质量保证措施（包括《项目实施进度计划表》、《风险管理表》）； （4）拟投所有产品材料清单、偏离表（包括《拟投所有设备材料清单》、《技术偏离表》等）； <b>（如果有）</b> （5）拟投入本项目的设备材料情况； <b>（如果有）</b> （6）售后服务（包括：质保期内的服务方案） （7）其他需说明的问题或需采取的技术措施。	投标文件内容不完整、格式不符合要求，导致投标文件被误读、漏读，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。
12.1	投标有效期：投标截止日期之后的90天（日历天）	
13.1	投标保证金：**元	<u>（本项目不适用）</u>
13.3	投标保证金提交方式： <b>支票、汇票、本票、保函等非现金形式</b> 投标保证金有效期：同“投标有效期” <b>注：投标保证金（纸质原件）须在投标截止时间前提交集中采购机构</b> <b>提交地址：上海市浦东新区民生路 1399 号**室</b> 联系人：*****	各包件的投标保证金应独立开具 <u>（本项目不适用）</u>
15.1	投标截止时间详见《投标邀请》	
★21.1	开标结束后，采购人或集中采购机构对投标人的资格进行审查。投标人不满足下列情形之一的，其投标文件不予符合性审查。 （1）投标人符合招标文件“投标人须知”第3条规定的资格条件的； （2）投标人按“投标人须知前附表”第10.1.1（6）条款规定提交资格证明材料。	1、本条款所提及内容均为实质性响应条件。 2、投标人证明材料提供不完整，关键信息模糊、难以辨认或甄别的，视作未按要求提供资格证明材料。
★21.3	评标委员会如发现投标人及其投标文件 <b>不满足</b> 下列情形之一的，经评标委员会审定后，该投标文件作无效标处理。 （1）投标文件中的下列内容按招标文件要求签署、盖章的（具体详见“投标文件格式”要求）： ➤ 投标承诺书	本条款所提及内容均为实质性响应条件，若所列实质性检查内容判断标准与其他各处有矛盾

条款号	内容规定	备注
	<ul style="list-style-type: none"> <li>➢ 投标函</li> <li>➢ 授权委托书</li> <li>➢ 开标一览表</li> </ul> <p>(2) 投标人未提交两个以上不同的投标报价；（注：招标文件要求提交备选投标的除外）</p> <p>(3) 投标人接受招标文件规定的投标有效期的；</p> <p>(4) 接受招标文件规定的项目实施或服务期限；</p> <p>(5) 未出现投标报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的；</p> <p>(6) 各包件投标报价未超过招标文件中规定的【<b>预算金额</b>】；</p> <p>(7) 经评标委员会审定，投标报价未存在招标文件“第二章”第 19.4 条款所列情形之一的；</p> <p>(8) 按规定缴纳投标保证金；<u>（本项目不适用）</u></p> <p>(9) 根据招标文件要求，投标人提供以下证明材料：  <u>①国家强制认证的产品承诺书；</u>            (10) 按“投标人须知”第 21.4 条款规定，对投标报价算术性错误修正予以确认的；            (11) 投标人接受“项目招标需求”中明确的结算原则和支付方式的；            (12) 投标人未出现《政府采购货物和服务招标投标管理办法》第三十七条所列的串通投标情形之一的；            (13) 投标人未出现提供虚假材料、行贿等违法行为；            (14) 未因电子文档本身的计算机病毒、或电子文档损坏等原因造成投标文件无法打开或打开后无法完整读取的；            (15) 满足招标文件规定的以下要求；  <u>①接受并满足招标文件的实质性响应要求和条件；</u>            (16) 经评标委员会审定，投标人未提供整体进口产品；            (17) 遵守《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》规定的。</p>	<p>之处，<b>以此处所列要求为准。</b></p>
24.3	本项目授权评标委员会依照评标办法确定中标人	
29.1	<p>采购货物数量的更改：依据《中华人民共和国政府采购法》，合同履行期间，如服务内容发生增加，按照合同约定需按实结算的项目，其核增内容的合同总金额不得超过原合同采购金额的<b>10%</b>，反之，则需重新组织采购。</p>	
31.1	<p>履约保证金金额：（单位：**元）</p> <p>履约保证金提交方式：<b>支票、汇票、本票、保函等非现金形式</b></p> <p>履约保证金提交时间：签订合同协议书之前</p>	<p><u>（本项目不适用）</u></p>

## 二、投标人须知

## （一）说明

### 1 总则

1.1 本项目（即“投标人须知前附表”写明的项目，以下简称“前附表”）已纳入本年度政府集中采购预算。本项目年度预算已经批准，招标范围、招标方式和招标组织形式已经核准。

1.2 本招标文件及今后的招标补充文件等是本项目招标过程中的规范文件，是采购人与中标人签订服务承包合同的依据，作为项目承包合同附件之一，具有同等法律效力。

1.3 各投标人应认真踏勘项目现场，熟悉项目现场及作业空间等情况，并在投标文件中考虑可能影响投标报价的一切因素。中标后，不得以不完全了解现场及周边等情况为理由要求提出经济补偿，否则，由此引起的一切后果由中标人负责。

1.4 各投标人必须认真阅读全部招标文件（包括招标补充文件），并不得擅自改变上述文件条款的规定，一旦作出投标决定，即视作投标人已完全理解和确认招标文件（含招标补充文件等）的一切内容并要求，已不需要作出任何其它解释和修改。凡投标人对上述文件条款的文字与数字的误读、漏读而引起投标文件的错误、遗漏、费用计算有误等，形成投标报价内容的差异，均属投标人失误，采购人和集中采购机构对此均不承担任何责任。开标后，除招标文件明确作相应调整外，一律不得作出其他任何调整。

1.5 投标人不得相互串通投标报价，不得排挤其他投标人的公平竞争，损害采购人或其他投标人的合法权益，投标人不得与采购人串通投标。评标委员会在评标阶段，对投标文件的审查、澄清、评议的过程中，一旦发现投标人有上述行为或对采购人、评标委员会以及其他有关人员施加影响的任何行为，其投标文件作无效标处理。

1.6 采购人不一定接受最低报价投标或收到的全部投标。

1.7 本次招标采购确定的是完成本项目的承包供应商，如果涉及到与本项目相关的部分设备产品或服务采购，国家、上海市或行业管理部门另有相关要求的，中标人在履约过程中的相关采购工作也应从其规定。

1.8 依据《中华人民共和国政府采购法》，政府采购应当采购**本国货物和服务**。本国产品标准按照《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）的规定执行。

1.9 根据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的有关要求，采购人和集中采购机构将在开标后、评标开始前，通过“信用中国”网站（[www.creditchina.gov.cn](http://www.creditchina.gov.cn)）、中国政府采购网（[www.ccgp.gov.cn](http://www.ccgp.gov.cn)）查询相关投标人信用记录，并对供应商信用记录进行甄别，对被列入“信用中国”网站（[www.creditchina.gov.cn](http://www.creditchina.gov.cn)）失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网（[www.ccgp.gov.cn](http://www.ccgp.gov.cn)）政府采购严重违法失信行为记录名单，以及上述网站查询中其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动。各供应商的信用信息查询记录作为采购文件一并归档。两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

1.10 本招标文件中的不可抗力是指不能预见、不能避免并不能克服的客观情况。应包括重大自然灾害（如台风、洪水、地震等）、政府行为（如征收、征用）、社会异常事件（如战争、罢工、骚乱）。

1.11 本招标文件中的政策性调价是指经政府授权的相关部门对职工最低工资标准、社保金和公积金缴存基数和比例的调整。

1.12 本招标文件未尽之处，或者与相关法律、法规、规范性文件要求不一致的，均按相关法律、法规、规范性文件要求执行。

1.13 本招标文件中出现前后矛盾的，以在招标文件中出现顺序在后的解释为准（招标文件中有特别说明的除外）。

**1.14 本招标文件中标有“★”的内容为实质性响应要求和条件。**

1.15 本招标文件由采购人和集中采购机构负责解释。

## 2 招标范围和内容

2.1 本项目招标范围和-content 详见招标文件“第二章”。

## 3 投标人的资格要求

3.1 合格的投标人应满足《投标邀请》中“合格的投标人必须具备以下条件”的要求。

3.2 投标人应当提供相应资格证明材料，具体详见“投标人须知前附表”第10.1.1（6）条款要求。

3.3 为该采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该项目的其他采购活动。

3.4 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。

3.5 符合《关于对接国际高标准经贸规则推进试点地区政府采购改革的指导意见》（沪财采〔2024〕12号）第17条规定的供应商，不得参加本项目的采购活动。

## 4 合格的货物和服务

4.1 投标人所提供的货物和服务应当没有侵犯任何第三方的知识产权、技术秘密等合法权利，同时应当符合招标文件的招标需求，并且其质量完全符合国家标准、行业标准或地方标准。

## 5 投标费用

5.1 投标人在投标过程中的一切费用，不论中标与否，均由投标人承担。

## 6 现场踏勘（本项目不适用）

6.1 采购人或集中采购机构将在“前附表”中载明的地址和时间，统一组织投标人对现场及其周围环境进行现场踏勘，以便使投标人自行查明或核实有关编制投标文件和签订合同所必需的一切资料。

6.2 现场踏勘期间的交通、食宿由投标人自行安排，费用自理。

6.3 如果投标人认为需要再次进入现场考察，应向采购人事先提出，采购人应予支持，费用由投标人自理。

6.4 除采购人的原因外，投标人自行负责在现场踏勘中所发生的人员伤亡和财产损失。

## 7 答疑会（本项目不适用）

7.1 在“前附表”规定的截止时间以前，投标人可以通过“前附表”明确的方式和途径向集中采购机构提出关于招标文件、提供资料及项目现场踏勘中存在的影-响本次投标的疑点问题。

7.2 采购人和集中采购机构在“前附表”规定的时间、地点召开答疑会。

7.3 采购人和集中采购机构将对收到的书面问题作统一解答，但不包括问题的来源。采购人和集中采购机构也可以主动对招标文件进行澄清、修改与补充。

## （二）招标文件

### 8 招标文件的内容

8.1 本项目招标文件包括下列文件及所有按本须知第7.3和9.1条款发出的招标补充文件。

8.1.1 电子投标特别提醒

### 8.1.2 投标邀请

### 8.1.3 投标人须知及前附表

### 8.1.4 项目招标需求

### 8.1.5 采购合同

### 8.1.6 投标文件格式

### 8.1.7 项目评审

### 8.1.8 附件（如果有）

8.2 投标人应仔细阅读招标文件，按招标文件的规定与要求编写投标文件。如果投标文件与招标文件的规定与要求不符合，则投标人应自行承担投标风险。凡与招标文件的规定有重大不符合的投标文件，按本招标文件有关规定办理。

## 9 招标文件的澄清和修改

9.1 在投标截止时间之前，采购人或集中采购机构可以对已发出的招标文件进行必要的澄清或者修改，但不得改变采购标的和资格条件。澄清或者修改将通过“上海市政府采购网”以公告形式发布，如果澄清或者修改的内容可能影响投标文件编制，且距投标截止时间不足15天的，则将顺延提交投标文件的截止时间，延长后的具体投标截止时间以最后发布的澄清或修改公告中的规定为准。

9.2 澄清或者修改内容为招标文件的组成部分，对招投标各方起约束作用，当原招标文件与澄清或者修改内容表述不一致时，以最后发布的内容为准。

## （三）投标文件的编制

### 10 投标文件的组成

10.1 投标文件由商务部分和技术部分组成。

10.1.1 投标人提交的投标文件商务部分，应包括内容详见“前附表”要求。

10.1.2 投标人提交的投标文件技术部分，应包括内容详见“前附表”要求。

#### 10.2 投标文件编制的注意事项

10.2.1 投标人按上述内容及顺序排列编制投标文件，投标文件内容应规范完整、简洁明了，编排合理有序，其中的扫描文件应清晰完整。

#### 10.2.2 技术部分标书应遵循以下要求

（1）投标人应针对本项目的具体情况，通过对核心参数指标分析，从材料或配件选择、生产工艺、整体产品可实现的各项功能指标、实施过程的质量控制管理、安装调试、售后服务等方面编制技术标。

（2）技术部分标书内容要求表达精炼、准确、简要。

（3）技术部分标书文字部分统一采用宋体小四号字体，行距采用 1.5 倍行距。

10.2.3 投标人应按照电子采购平台要求的格式填写相关内容，凡招标文件要求签字、盖章之处，均应由投标人的法定代表人或法定代表人正式授权的代表签字和加盖公章。

10.2.4 投标人应按招标文件要求的内容、格式和顺序编制投标文件，凡招标文件提供有相应格式（详见“投标文件格式”）的，投标文件均应完整的按照招标文件提供的格式填写，并按要求在电子采购平台进行有效上传。

10.2.5 投标文件内容不完整、格式不符合，而导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任，投标人应承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

## 11 投标报价

11.1 除招标需求另有说明外，投标报价应包括完成招标范围内全部工作内容；为达到招标要求所发生的一切辅助性、配合性的相关费用；按规定应计取的规费、保险、税金等；并且充分考虑合同包含的责任、义务和一般风险等各项全部费用。投标报价原则及计算方法见本招标文件“第二章”要求。

11.2 如项目中包含多个包件，且投标人同时响应两个（含两个）以上包件的，各包件应单独报价。

11.3 本项目的采购预算金额或最高限价详见《投标邀请》中“项目概况”，投标报价或各包件报价均不得超过公布的预算金额或最高限价。

11.4 投标人所报的投标报价（包括各子目单价及取费标准）在合同执行过程中是固定不变的（合同或招标文件中约定的变更除外），不得以任何理由予以变更。

11.5 本项目的报价按人民币计价，单位为元。

## 12 投标有效期

12.1 投标文件在前附表中所述的投标有效期内保持有效，投标有效期不足的投标将被作为无效标。

12.2 在原定投标有效期满之前，如出现特殊情况，集中采购机构可以向投标人提出延长投标有效期的要求，对此投标人应立即向集中采购机构作出答复，这种要求和答复均应以书面形式进行。投标人可以拒绝集中采购机构的要求，且不会被作不良诚信记录和不予退还投标保证金的处理，但拒绝延长投标有效期的投标文件将不会列入评审范围。接受延长投标有效期的投标人不允许修改其投标文件，但评标委员会认为需对投标文件作出澄清的除外。

## 13 投标保证金（本项目不适用）

13.1 投标人应提交“前附表”规定金额的投标保证金，并作为其投标的一部分。

13.2 投标保证金是为了保护采购人和集中采购机构免遭因投标人的行为而蒙受损失。采购人和集中采购机构在因投标人的行为受到损害时可根据投标人须知第 13.5 条款的规定不予退还投标人的投标保证金，统一上缴国库。

13.3 投标保证金应按“前附表”中规定的其中一种方式提交，投标保证金有效期为投标有效期满后（“前附表”规定的天数）天。

13.4 凡没有根据本须知第 13.1 和 13.3 条款的规定提交投标保证金的投标，应按本须知第 21 条的规定视为无效标。

13.5 下列任何情况发生时，投标保证金将不予退还：

13.5.1 投标人在招标文件中规定的投标有效期内撤回其投标；

13.5.2 中标后不能按照投标文件的承诺签订合同的。

13.6 投标保证金的退还

13.6.1 未中标人的投标保证金在中标通知书发出后五个工作日内退还。

13.6.2 中标人的投标保证金在合同签订后五个工作日内退还。

## 14 投标文件的编制、加密和上传

具体详见《电子投标特别提醒》中相关要求。

## 15 投标截止时间

15.1 投标人应在规定的投标截止时间前，使用电子采购平台提供的客户端投标工具编制加密、上传投标文件，并打印“投标确认回执”。

15.2 在特殊情况下，采购人和集中采购机构如果决定延后投标截止时间，至少应在原定的投标截

止时间 3 日前将此决定书面通知所有的投标人。在此情况下，采购人、集中采购机构和投标人受投标截止时间制约的所有权利和义务，适用于延长后新的投标截止时间。

15.3 投标截止与开标的时间以电子采购平台显示的时间为准。

#### **16 迟到的投标文件**

16.1 投标截止后，不再接受投标人上传投标文件。

#### **17 投标文件的修改与撤回**

17.1 在投标截止时间之前，投标人可以使用电子采购平台提供的客户端招标工具，对投标文件进行修改。投标文件修改完成后，应在规定的时间内重新加密、上传投标文件，并确保投标状态显示为“正式投标”。

17.2 在投标截止时间之前，投标人可以使用电子采购平台提供的客户端招标工具，对投标文件进行撤回。

17.3 在投标有效期内，投标人不能修改或撤回投标文件，否则将按照本须知的规定作不良诚信记录。

### **（四）开标与评标**

#### **18 开标**

18.1 开标程序在电子采购平台进行，所有上传投标文件的投标人应登录电子采购平台参加开标。

#### **19 投标文件解密和开标记录的确认**

19.1 投标截止、电子采购平台显示开标后，投标人进行签到操作，操作时长以平台显示时间（目前为 30 分钟）为准。投标人签到完成后，由集中采购机构解除电子采购平台对投标文件的加密。投标人应在规定时间内使用数字证书（CA 证书）对其投标文件解密，操作时长以平台显示时间（目前为 30 分钟）为准。投标人应在规定时间内完成上述签到或解密操作，逾期未完成签到或解密的投标人，其投标将作无效标处理。

19.2 投标人因自身原因，未能在电子采购平台规定的解密时限内，将其投标文件解密的，视为放弃投标。

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

19.4 投标人应及时检查《开标记录表》的数据与其投标文件中的《开标一览表》是否一致，并作出确认。投标人因自身原因未作出确认的，视为其确认《开标记录表》内容。

#### **20 评标委员会组成**

20.1 评标委员会由 5 人以上（含 5 人）的单数组成，其中政府采购评审专家所占比例不少于成员总数的三分之二。采购人派代表参加评标委员会，集中采购机构不参与评标。

#### **21 投标文件的资格审查及符合性审查**

★21.1 开标结束后，采购人或集中采购机构对投标人的资格进行审查。投标人不满足“前附表”所列情形之一的，其投标文件不予符合性审查。

21.2 在评审中，评标委员会将根据招标文件规定，对每份投标文件进行符合性审查，详细审查每份投标文件是否实质性响应了招标文件的要求。投标文件与招标文件要求的全部条款、条件和规格相符且没有重大偏离为实质性响应；投标文件对招标文件要求的实质性条文存在偏离、保留或者反对为非实质性响应。

★21.3 评标委员会如发现投标人不满足“前附表”所列情形之一的，经评标委员会审定后，将作无效标处理。

21.4 对于实质上响应招标文件要求的投标文件，投标报价有计算上和累计上的算术性错误的差错，经评标委员会审定，按下列方法进行修正。

21.4.1 电子采购平台自动汇总生成的《开标记录表》内容与投标文件中的《开标一览表》内容不一致的，以《开标记录表》内容为准；

21.4.2 《开标记录表》内容与《投标报价分类明细表》及投标文件其它部分内容不一致的，以《开标记录表》内容为准；

21.4.3 单价金额小数点或者百分比有明显错位的，以《开标记录表》的总价为准，并修改单价；投标文件中如果同时出现上述两种或两种以上错误或矛盾的，则根据以上排序，按照序号在先的方法进行修正。

上述修正或处理结果对投标人具有约束作用，投标人不确认的，其投标文件无效。

## ★ 22 异常低价投标审查

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

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

（2）投标报价低于通过符合性审查且报价次低供应商投标报价 50% 的，即  $\text{投标报价} < \text{通过符合性审查且报价次低供应商投标报价} \times 50\%$ ；

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

（4）其他评标委员会认为供应商报价过低，有可能影响产品质量或者不能诚信履约的情形。

22.2 评标委员会启动异常低价投标审查后，应当要求相关供应商在评审现场合理的时间内对投标价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等。

22.3 如果投标人不能在评标委员会规定的时间内提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

## 23 投标文件的澄清

23.1 对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者修改。

23.2 投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。投标人的澄清、说明或者补正内容作为投标文件的组成部分，对投标人具有约束力。

23.3 经评标委员会审定，可以接受投标文件中不构成实质性偏差的小的不正规、不一致或不规范的内容。

## 24 评委评审

24.1 评标委员会对通过资格性及符合性检查的投标文件，根据招标文件规定的评标办法进行综合评审，未经评标委员会确认的价格和优惠条件在评标时不予考虑。

24.2 计算评标总价时，以满足采购人要求提供的全部服务内容为依据，评标价包括实施和完成全部内容所需的劳务、管理、利润、风险等相应费用，对所有列入评审范围的投标文件应适用相同计算口径，在同一基准上进行评定。

24.3 本项目中标人的确定方式详见“前附表”。

## （五）询问与质疑

### 25 询问与质疑

25.1 投标人对政府采购活动事项有疑问的，可以向采购人或集中采购机构提出询问。询问可采取电话、当面或书面等形式。采购人或集中采购机构将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

25.2 投标人认为招标文件、采购过程和中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起 10 日内，以**书面形式**（具体格式可通过中国政府采购网 [www.ccg.gov.cn](http://www.ccg.gov.cn) 右侧的“下载专区”下载）向采购人或集中采购机构提出质疑，否则视为未递交。（采购人联系方式详见“投标邀请”）

**质疑函的递交应当采取当面递交形式，否则视为未递交。质疑联系部门：上海市浦东新区政府采购中心办公室或者采购人相关部门。**

**集中采购机构地址：上海市浦东新区民生路 1399 号 16 楼 16A15 室**

**集中采购机构联系电话：（021）68542111。**

25.3 投标人应知其权益受到损害之日，是指：

25.3.1 对招标文件提出质疑的，为收到招标文件之日或者招标文件公告期限届满之日。

25.3.2 对采购过程提出质疑的，为各采购程序环节结束之日。

25.3.3 对中标结果提出质疑的，为中标结果公告期限届满之日。

25.4 投标人不得以捏造事实、提供虚假材料或者以非法手段取得证明材料进行质疑。

25.5 投标人应当在法定质疑期内一次性提出针对同一采购程序环节的质疑，超过次数的质疑将不被受理。

25.6 投标人提起的询问和质疑，应该按照《政府采购质疑和投诉办法》（财政部令第 94 号）的规定办理。质疑函的内容和格式若不符合《投标人须知》第 25.2 条规定的，采购人或集中采购机构将当场一次性告知投标人需要补正的事项，投标人超过法定质疑期或未按要求补正并重新提交的，视为放弃质疑。

## （六）诚信记录

### 26 诚信记录

26.1 投标人在本招标项目的竞争中应自觉遵循诚实信用原则，不得存在腐败、欺诈或其他严重违背诚信原则的行为。“腐败行为”是指提供、给予任何有价值的东西来影响采购人员在采购过程或合同实施过程中的行为；“欺诈行为”是指为了影响采购过程或合同实施过程而谎报、隐瞒事实，损害采购人的利益，包括投标人之间串通投标（递交投标书之前或之后），人为地使投标丧失竞争性，损害采购人从公开竞争中所能获得的权益。

26.2 如果采购人或集中采购机构有证据表明投标人在本招标项目的竞争中存在腐败、欺诈、报名截止之日前三年内在政府采购活动中有不良行为记录的或其他严重违背诚信原则的行为，则将拒绝其投标。

26.3 投标人有下列情形之一，采购人和集中采购机构将取消其评标资格，并将相关情况报浦东新区政府采购监督管理部门：

26.3.1 提供虚假材料谋取中标、成交的；

26.3.2 采取不正当手段诋毁、排挤其他投标人的；

- 26.3.3 与采购人、其他投标人或者集中采购机构恶意串通的；
- 26.3.4 向采购人、集中采购机构行贿或者提供其他不正当利益的；
- 26.3.5 在招标采购过程中与采购人进行协商谈判的；
- 26.3.6 拒绝有关部门监督检查或者提供虚假情况的；
- 26.3.7 开标后擅自撤销投标，影响招标继续进行的；
- 26.3.8 中标、成交后无正当理由拒绝签订政府采购合同的；
- 26.3.9 无正当理由拒绝履行合同的；
- 26.3.10 提供假冒伪劣产品或走私物品的；
- 26.3.11 拒绝提供售后服务，给采购人造成损害的；
- 26.3.12 政府采购管理部门认定的其他有违诚实信用的行为。

## （七）授予合同

### 27 中标通知书

27.1 在公告中标（成交）结果的同时，采购人、采购代理机构应向中标（成交）供应商发出中标（成交）通知，且一并以书面方式告知未中标（成交）供应商未中标（成交）的原因（但不得泄露其他供应商的商业秘密），前述原因包括以下与该供应商相关的内容：资格审查、符合性审查的情况及被认定为无效投标（响应）的原因，评审得分与排序，评标委员会对该供应商的总体评价。

27.2 中标通知书是合同文件的组成部分，对采购人和中标人均具有法律效力。中标通知书自发出后，如采购人自行改变中标结果或中标人自行放弃中标项目的，将依法承担法律责任。

### 28 合同授予的标准

28.1 除第 26 条的规定之外，采购人将把合同授予按第 24.3 条款确定的中标人。

### 29 授标合同时更改采购服务数量的权利

29.1 依据《中华人民共和国政府采购法》，需要从原供应商处添购的，添购资金总额不超过原合同采购金额的 10%。

### 30 合同协议书的签署

30.1 采购人与中标人应当在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同。

30.2 采购人和中标人应当按照政府采购相关法律法规的规定签订书面合同，合同的标的物、价款、质量、履行期限等主要条款应当与招标文件和中标人的投标文件的内容一致。

30.3 对于因采购人原因导致变更、中止或者终止政府采购合同的，采购人应当依照合同约定对供应商受到的损失予以赔偿或者补偿。

### 31 履约保证金

31.1 中标人在收到中标通知书后三十日内，并在签订合同协议书之前，应按“前附表”规定向采购人提交履约保证金，联合体的履约保证金由联合体主办人提交或联合体成员共同提交（招标文件另有规定的除外）。合同存续期间，履约保证金不得撤回。

31.2 如果中标人未按上述规定签订合同或提交履约保证金，采购人和集中采购机构将取消原中标决定。

## 第二章项目招标需求

### 一、说明

#### 1 总则

1.1 投标人应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由投标人自行负责。

1.2 投标人对所提供的系统应当享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

1.3 投标人提供的货物应当是全新的、未使用过的，货物和相关服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

1.4 投标人应如实准确地填写投标货物的规格型号、技术参数、品牌、产地等相关信息，因上述信息内容填写不完整、不准确，而导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

★1.5 若本项目涉及国家强制认证产品（信息安全产品、3C 认证产品、强制节能产品、电信设备进网许可证等），则根据国家有关规定，投标人提供的产品必须满足强制认证要求。（详见第一章投标人须知及前附表 21.3（9））

★1.6 投标人提供的产品和服务必须符合国家强制性标准。

1.7 采购人在技术需求和图纸或图片（如果有）中指出的工艺、材料和货物的标准以及参照的技术参数或型号仅起说明作用，并没有任何限制性和排他性，投标人在投标中可以选用其他替代标准、技术参数或型号，但这些替代要在不影响功能实现的前提下，并在可接受范围内接受偏离。

1.8 投标人在投标前应认真了解采购人的使用需求、使用条件（使用空间、能源条件等）和其他相关条件，一旦中标，应按照招标文件和合同规定的要求提供货物及相关服务。

1.9 投标人应根据本章节中详细技术规格要求，采用市场主流产品或按照要求提供定制产品参加竞标。同时，**请投标人务必注意：无论是正偏离还是负偏离，都不得与招标要求相差太大，否则将可能影响投标人的得分。**一旦中标，投标人应按投标文件的承诺签订合同并提供相应的产品和服务。

1.10 本项目如涉及软件开发，则开发软件（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）的全部知识产权归采购人所有。投标人向采购人交付使用的软件系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。支撑该系统开发和运行的第三方编制的软件的知识产权仍属于第三方。如采购人使用该软件系统构成上述侵权的，则由投标人承担全部责任。

1.11 投标人认为招标文件（包括招标补充文件）存在排他性或歧视性条款，自收到招标文件之日或者招标文件公告期限届满之日起 10 日内，以书面形式提出，并附相关证据。

### 二、项目概况

#### 2 项目名称

中国（上海）自贸区基础云平台 2026 年建设项目

#### 3 项目地点

上海市浦东新区迎春路 520 号（采购人指定地址）。

## 4 招标范围与内容

### 4.1 项目背景及现状

浦东新区按照政务系统服务器存储资源集约化建设、统筹使用的原则，通过向通信运营商租用服务和自建的方式，统一建设浦东“政务云”。成为浦东新区城市治理数字化底座的核心基础设施。

本期项目在 2025 年度浦东政务云云资源和服务的基础上，根据国产化发展的要求，缩减非国产化资源量，补充国产化资源和算力资源，增强资源使用效能评估，持续为新区各委办局提供稳定可靠的云服务。

### 4.2 项目招标范围及内容

本项目共包含 3 个包件，同一投标人允许最多中标 2 个包件：

包1：包名称为中国（上海）自贸区基础云平台2026年建设项目区域一，预算金额为50,685,537.92元。

包2：包名称为中国（上海）自贸区基础云平台2026年建设项目区域二，预算金额为55,046,105.01元。

包3：包名称为中国（上海）自贸区基础云平台2026年建设项目区域三，预算金额为51,958,551.61元。

#### 4.2.1 包 1 招标范围及内容

##### （1）云资源服务

为浦东政务云平台（区域一）提供非国产化及国产化云资源服务，包括：CPU、内存、普通存储、高性能存储（SSD）及备份服务。提供云管平台功能，提供全栈 IPv6 功能，支持 PAAS 能力提供，提供外部快照功能。

##### （2）算力资源服务

为浦东政务云平台（区域一）提供算力资源服务，包括：推理用算力、训练用算力。

##### （3）网络服务

为浦东政务云平台（区域一）提供网络资源服务，包括：互联网带宽（骨干级）、网络资源、应用负载均衡服务、安全交换区（网闸）、网管服务。

##### （4）安全服务

为浦东政务云平台（区域一）提供安全服务，包括：网络访问控制服务、入侵防御服务、常规安全漏洞扫描、用户管理服务、用户身份认证服务、在线防护 WAF。

配置安全技术团队保障政务云安全，提供的非国产化和国产化云计算服务均满足网络安全等级保护三级要求并通过测评认证。其国产化平台需整体按照《信息安全技术云计算服务安全能力要求》(GB/T31168)进行建设，需满足《信息安全技术信息系统密码应用基本要求》(GB/T39786-2021)第三级要求的内容。

##### （5）密码服务

为浦东政务云平台（区域一）提供密码服务，包括：安全认证网关服务、可信密码服务、签名验签服务、时间戳服务等密码服务。

##### （6）运行维护服务

建立专职的运行维护团队，满足浦东新区政务云统一管理运维服务要求。根据实际工作需要签订服务水平协议（SLA），确保政务云安全、稳定、可靠运行。

需提供基于算力设施的运维服务，为创新技术试点应用提供服务。

##### （7）服务模式

本次项目采购模式为购买服务，即乙方按照甲方要求，自行建设机房、部署软硬件环境。

#### 4.2.2 包 2 招标范围及内容

##### （1）云资源服务

为浦东政务云平台（区域二）提供非国产化及国产化云资源服务，包括：CPU、内存、存储。

##### （2）算力资源服务

为浦东政务云平台（区域二）提供算力资源服务，包括：推理用算力、训练用算力、渲染用算力。

##### （3）网络资源服务

为浦东政务云平台（区域二）提供网络资源服务，包括：互联网线路、公有 IP、政务外网链路、应用负载均衡服务、安全交换区（网闸）。

##### （4）安全服务

为浦东政务云平台（区域二）提供安全服务，包括：入侵防御服务、常规安全漏洞扫描、网络访问控制服务、数据库审计服务、日志审计服务、用户管理服务、用户身份认证服务、在线防护 WAF、网页防篡服务。

配置安全技术团队保障政务云安全，提供的非国产化和国产化云计算服务均满足网络安全等级保护三级要求并通过测评认证。

##### （5）密码服务

为浦东政务云平台（区域二）提供密码服务，包括：安全认证网关服务、可信密码服务、文件加密存储/签名验签服务、时间戳服务等密码服务。

提供的国产化云计算服务满足商用密码应用安全性要求并通过测评认证。

##### （6）运行维护服务

建立专职的运行维护团队，满足浦东新区政务云统一管理运维服务要求。根据实际工作需要签订服务水平协议（SLA），确保政务云安全、稳定、可靠运行。

需提供基于算力设施的运维服务，为创新技术试点应用提供服务。

##### （7）服务模式

本次项目采购模式为购买服务，即乙方按照甲方要求，自行建设机房、部署软硬件环境。

#### 4.2.3 包 3 招标范围及内容

##### （1）云资源服务

为浦东政务云平台（区域三）提供国产化云资源服务，包括：CPU、内存、数据存储服务、数据库存储服务。

##### （2）算力资源服务

为浦东政务云平台（区域三）提供算力资源服务。

##### （3）网络资源服务

为浦东政务云平台（区域三）提供网络资源服务，包括：网络接入与地址分配服务、应用负载均衡服务、政务专网接入服务。

为创新技术试点应用提供保障服务。涉及量子通讯、保障数据要素赋能、智能化应用与治理等应用场景。

##### （4）安全服务

为浦东政务云平台（区域三）提供安全服务，提供统一安全防护服务，保障政务云安全，提供的

非国产化和国产化云计算服务均满足网络安全等级保护三级要求并通过测评认证。

#### （5）密码服务

为浦东政务云平台（区域三）提供密码服务，包括：安全认证网关服务、可信密码服务、文件加密存储/签名验签服务、时间戳服务等密码服务。提供的国产化云计算服务满足商用密码应用安全性要求并通过测评认证。

#### （6）服务模式

本次项目采购模式为购买服务，即乙方按照甲方要求，自行建设机房、部署软硬件环境。

4.3 本项目工期为：**合同签订后，自各项服务交付之日起一年**。以乙方向甲方提供资源下发测试等相关证明材料为准。

### 5 承包方式

5.1 依据本项目的招标范围和内容，中标人以包系统设计、包供货、包安装集成调试、包质量、包安全的方式实施总承包。

5.2 **本项目不允许分包。**

### 6 合同的签订

6.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与招标文件和中标人投标文件的内容一致，并互相补充和解释。

### 7 结算原则和支付方式

#### 7.1 结算原则

7.1.1 本项目合同结算价以审计价为准，中标人的中标单价不变，实际工作量以采购人或第三方按照招标文件规定的验收标准核定为准。

7.1.2 发生设备维修的，如该设备尚在质保期内的，采购人不另行支付相关费用；如在质保期外的，单价按照投标文件中明确的备品备件单价（含维修人工费）计取，数量按实结算。如投标文件中没有类似备品备件单价可参照的，则由合同双方协商确定维修单价。

#### 7.2 支付方式

7.2.1 本项目合同金额采用**分期付款**方式，在采购人和中标人合同签订，且财政资金到位后，按下款要求支付相应的合同款项。

7.2.2 分期付款的时间进度要求和支付比例具体如下：

（1）第一笔付款-交付付款（80%）：合同签订后，甲方收到乙方关于系统交付报告和发票，经甲方审核均符合要求后 30 日内，向乙方支付合同金额 80%。

（2）第二笔付款-最终验收付款（20%）：项目验收通过，且甲方收到乙方发票后 30 日内，按照验收通过并审定的价格向乙方支付合同尾款。

7.3 中标人因自身原因造成返工的工作量，采购人将不予计量和支付。

7.4 采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时 1 年期贷款市场报价利率。

## 三、技术质量要求

### 8 适用技术规范和规范性文件

- （1）国家标准化管理委员会《电子政务标准化指南-信息共享（征求意见稿）》
- （2）国家标准化管理委员会《XML 在电子政务中的应用指南》

- (3) 《政府信息交换语言标准》
- (4) 《政务信息资源交换体系》 GB/T21062
- (5) 《信息安全等级保护管理办法》（公通字[2007]43 号）
- (6) 《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008）
- (7) 《中国计算机信息系统安全保护条例》国务院令 147 号 1994 年 2 月 18 日
- (8) 《关于加强计算机信息网络保密管理的通知》（中保委发[2002]4 号）
- (9) 《计算机软件保护条例》（国务院令 2001 年第 339 号）
- (10) 《计算机场地通用规范》（GB2887-2000）
- (11) 《电子计算机机房设计规范》（GB50174-93）
- (12) 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
- (13) 《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）
- (14) 《中国密码法》
- (15) 建设单位提供的设计要求及相关资料
- (16) 国家相关的政策及法规等

各投标人应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本招标文件中列明，中标人应无条件执行。标准、规范等不一致的，以要求高者为准。

**9 招标内容与质量要求**

**9.1 工作量清单**

**9.1.1 包 1 工作量清单**

**包 1 工作量清单**

序号	具体内容		单位	资源总量	备注	
1	服务 1	云平台资源	CPU	核	5960	
2			内存	GB	55698	
3			应用存储空间	TB	6615	
4			数据库存储	TB	1638	
5			数据备份服务	TB	1500	
6			整机柜租用	个	2	
7		GPU 资源	CPU	核	120	
8			GPU（训练）	块	10	
9			内存	GB	1920	
10		国产化资源	CPU	核	640	
11			内存	GB	10240	
12			数据库存储	TB	208	
13			应用存储空间	TB	399	
14		网络服务	应用负载均衡服务	IP	97	
15			网络资源	Gps	1	
16			互联网带宽（骨干级）	Gps	1	
17			安全交换区（网闸）	IP	100	
18		安全服务	网管服务	套	1	
19			网络访问控制服务	套	6	
20			入侵防御服务	套	6	

序号	具体内容		单位	资源总量	备注		
21			常规安全漏洞扫描	次	100		
22			用户管理服务	套	6		
23			用户身份认证服务	套	6		
24			在线防护 WAF	套	6		
25	运维服务	运维服务	套	1			
26	服务 2	云平台资源（国产化）	CPU	核	2944		
27			内存	GB	47104		
28			应用存储空间	TB	300		
29			数据库存储	TB	200		
30			数据备份服务	TB	400		
31	网络服务		应用负载均衡服务	IP	45		
32			安全交换区（网闸）	IP	45		
33	安全服务		网络访问控制服务	套	19		
34			入侵防御服务	套	19		
35			常规安全漏洞扫描	次	988		
36			用户管理服务	套	19		
37			用户身份认证服务	套	19		
38			在线防护 WAF	套	19		
39	密码服务		安全认证网关服务	套	15		
40			时间戳服务	套	15		
41			签名验签服务	套	15		
42			可信密码服务	套	15		
43	服务 3	云平台资源（国产化）	CPU	核	576		
44			内存	GB	6144		
45			数据库存储	TB	74		
46		GPU 资源（国产化）		CPU	核	1536	
47				GPU（推理）	块	64	
48				内存	GB	8192	
49		运维服务	运维服务	套	1	保障算力等创新业务	

说明：上表中所列为本次招标的主要工作内容，投标人不得减少主要工作内容数量。

9.1.2 包 2 工作量清单

包 2 工作量清单

序号	具体内容		单位	资源总量	备注	
1	服务 1	计算资源服务（非国产化）	CPU	核	4892	
2			内存	GB	34513.17	
3			应用存储空间（HDD）	TB	2219.72	
4			数据库存储（SSD）	TB	103.66	
5	计算资源服务（国产化）		CPU	核	582	
6			内存	GB	3641.34	
7	计算资源服务（推		CPU	核	392	

序号	具体内容		单位	资源总量	备注	
8	理服务器)	内存	GB	7168		
9		GPU（推理）	块	56		
10	计算资源服务（训练服务器）	CPU	核	240		
11		内存	GB	3072		
12		数据库存储（SSD）	TB	23.04		
13		GPU（训练）	块	24		
14	网络资源服务	互联网带宽	Gbps	2		
15		互联网公有 IP 服务	个	512		
16		政务外网链路	条	2		
17		应用负载均衡服务	每 IP	42		
18		安全交换区（网闸）	每 IP	214		
19	信息安全技术服务	入侵防御服务	套	40		
20		用户管理服务	套	40		
21		常规安全漏洞扫描	次	2080		
22		网络访问控制服务	套	8		
23		数据库审计服务	套	8		
24		日志审计服务	套	8		
25		用户身份认证服务	套	8		
26		在线防护 WAF	套	8		
27		网页防篡服务	套	8		
28	密码服务	安全认证网关服务	套	8		
29		可信密码服务	套	8		
30		文件加密存储/签名验签服务	套	8		
31		时间戳服务	套	4		
32	运维服务	运维服务	人	4		
33	服务 2	计算资源服务（国产化）	CPU	核	3293	
34			内存	GB	26214.4	
35			应用存储空间（HDD）	TB	300	
36			数据库存储（SSD）	TB	100	
37		计算资源服务（推理服务器）	CPU	核	896	
38			内存	GB	17408	
39			数据库存储（SSD）	TB	264.04	
40			GPU（推理）	块	112	
41		计算资源服务（训练服务器）	CPU	核	896	
42			内存	GB	11264	
43			数据库存储（SSD）	TB	122.88	
44			GPU（训练）	块	64	
45		机房机柜服务	整机柜租用	个	9	
46		信息安全技术服务	网络访问控制服务	套	15	
47			数据库审计服务	套	15	
48			日志审计服务	套	15	

序号	具体内容		单位	资源总量	备注	
49			用户身份认证服务	套	15	
50			在线防护 WAF	套	15	
51			网页防篡服务	套	15	
52		密码服务	安全认证网关服务	套	15	
53			可信密码服务	套	15	
54			文件加密存储/签名验签服务	套	15	
55			时间戳服务	套	8	
56		服务 3	计算资源服务（推理服务器）	CPU	核	1792
57	内存			GB	14336	
58	应用存储空间（HDD）			TB	1536	
59	数据库存储（SSD）			TB	174.08	
60	GPU（推理）			块	128	
61	计算资源服务（渲染服务器）		CPU	核	192	
62			内存	GB	3072	
63			数据库存储（SSD）	TB	23.04	
64			GPU（渲染）	块	24	
65	计算资源服务（训练服务器）		CPU	核	1088	
66			内存	GB	13824	
67			数据库存储（SSD）	TB	93.44	
68			GPU（训练）	块	72	
69	运维服务		运维服务	人	2	

说明：上表中所列为本次招标的主要工作内容，投标人不得减少主要工作内容数量。

### 9.1.3 包 3 工作量清单

#### 包 3 工作量清单

序号	具体内容		单位	资源总量	备注
1	服务 1	物理托管	机房机柜服务	个	5
2		网络资源服务	互联网公有 IP 服务	个	254
3			互联网带宽（骨干级）	GB	4
4			政务专线	10GB/条	4
5			应用负载均衡服务	每 IP	103
6			安全交换区	每 IP	254
7		计算资源服务	CPU	核	10984
8			内存	G	67660
9		存储资源服务	应用存储空间	TB	3373.7
10			高性能数据库存储	TB	523
11		安全服务	网络访问控制服务	租户	130
12			入侵防御服务	租户	130
13			用户管理服务	租户	130
14			用户身份认证服务	租户	130
15			数据库审计服务	实例	100
16			常规安全漏洞扫描	次	2400

序号	具体内容		单位	资源总量	备注
17	密码服务	在线防护 WAF	套	148	
18		网页防篡服务	套	148	
19		安全认证网关服务	套	10	
20		时间戳服务	套	1	
21	计算资源服务	CPU	核	2515	
22		内存	G	20700	
23		GPU 算力服务器 CPU	核	1536	
24		GPU 算力服务器内存	G	10240	
25		GPU 算力服务器存储	TB	19.88	
26		GPU（推理）	块	48	
27		GPU（训练）	块	32	
28	密码服务	安全认证网关服务	套	15	
29		签名验签服务	套	15	
30		可信密码服务	套	15	
31		时间戳服务	套	15	
32	网络资源服务	政务专线	条	1	

**说明：上表中所列为本次招标的主要工作内容，投标人不得减少主要工作内容数量。**

9.2 具体技术质量需求

9.2.1 总体要求

系统架构要求：满足电子政务云总体架构，以政府购买服务的方式，统一为浦东新区各委办局提供服务。

浦东政务云平台架构要求：政务云平台网络区域按电子政务网络安全要求划分为电子政务外网和互联网两个区域，通过管理平台对资源进行统一管理，在符合网络安全等级保护基本要求的前提下，政务外网和互联网之间的业务交互需使用安全隔离方法保证安全和数据传输；云平台内的核心系统尽量采用同一厂商的产品。中标人提供的物理设备需要按独立的机房区域划分给云平台使用。为保证中国（上海）自贸区基础云平台 2026 年建设项目整体平稳运行及后续交付验收审计等工作，涉及到硬件设备的具体要求：1、确保所有提供的设备均符合国家及行业标准，并通过了相关的认证测试；2、国产化云计算资源部分需提供符合国家国产化要求的硬件设备，满足信创工作安全合规的产品；3、本次采购资源量为实际能够使用资源量，为保障政务云平台业务正常使用，政务云平台水位线为 70%，即可用资源量为平台实际资源量的 70%。4、平台租用服务需与现有平台保持统一运营和运维，配套软件及云服务提供商与现平台保持一致，充分考虑与现有平台软硬件的兼容性和拓展性，中标方需提供项目设备品牌及设备配置清单等，配套运维支撑服务。

(1) 包 1

服务 1 部分	<p>1、云资源需求：资源池物理建设规模满足 CPU 数量 6720 核，内存 67858 GB，普通存储 7014 TB，高性能存储 1846TB，备份资源 1500TB，GPU 服务器不少于 5 台，其中 GPU 卡合计不少于 10 块，规格不低于 P40。应满足区级的业务需求，在各项资源发放水位高于 70%时及时报告招标人。中标人应按照招标人的要求，根据实际需求进行扩容。</p> <p>2、云运维管理平台服务：云服务商应使用自主的、适应国际标准的商业化虚拟化软件，并搭建统一的个性化云运维管理平台提供服务。云运维管理平台能够基于自</p>
---------	--

	<p>主架构的虚拟化软件，提供云运营管理服务和云运维管理服务，能够对 IT 基础设施进行统一管理。</p> <p>3、安全服务：政务云平台需符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求。</p>
<p>服务 2 部分</p>	<p>1、国产化云主平台建设</p> <p>云资源需求：资源池物理建设规模满足 CPU 2944 物理核，内存 47104GB，HDD 集中式存储 2 套、可用容量不低于 200TB，全闪集中式存储 2 套、可用容量不低于 200TB，对象存储可用容量不低于 100TB，应满足区级的业务需求，在各项资源发放水位高于 70%时及时报告招标人。中标人应按照招标人的要求，根据实际需求进行扩容。</p> <p>备份需求：提供不低于 400TB 的备份能力，支持整机、数据库和文件级备份。</p> <p>运行维护服务：中标人应建立专职的运行维护团队，满足浦东新区政务云统一管理运维服务要求。包括但不限于为浦东新区政务云提供业务培训、基础运维、业务迁移咨询等必要的运维服务。招标人和中标人双方根据实际工作需要签订服务水平协议（SLA），确保政务云安全、稳定、可靠运行。</p> <p>平台安全服务：中标人应配置专职安全技术团队保障政务云安全。政务云平台需整体按照《信息安全技术云计算服务安全能力要求》(GB/T31168)进行建设,符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和商用密码应用安全性评估三级标准。</p> <p>2、租户密码服务</p> <p>密码服务要求：投标人提供的密码服务中包含冗余部署的云密码机，云密码机可以根据国家、地方、行业的相关规定供同一使用单位申请的不同密码服务使用，投标人应当确保所提供的云密码机计算能力符合密码服务的性能需求。</p> <p>密码机资源水位达到阈值的 80%时，应答方应及时进行扩容。</p> <p>对本项目中提供的服务，应答方应根据采购方的要求，向采购方提供全面、有效、及时的技术支持。在提供服务期间，要求应答方独立设置 1 名专人驻场做技术支持。该名驻场人员需具有同类项目驻场运维经验，负责项目整体驻场运维支撑服务。</p> <p>服务运行期间，如发生软件优化、升级、扩展等有关情况，应答方须提前向采购方提供必要的技术资料。</p> <p>3、关于故障等级分类及故障处理要求</p> <p>故障等级分为三级：</p> <p>特别重大故障事件：故障造成系统失效或崩溃，应用系统无法正常启动运行、网络故障、丢失数据等，且没有临时替代解决方案；系统崩溃（死机和自动重启）且不能再启动、磁盘信息丢失、系统或应用服务无法启动、网络链接失效、文件损毁等。</p> <p>重大故障事件：故障造成系统发生中断或系统死机但重启后正常；应用部分不稳定；系统运行正常，但不能进行操作（控制台无响应）。</p> <p>一般故障事件：除特别重大故障事件、重大故障事件以外的故障，故障对系统业务无明显影响，仅造成系统报错、非关键应用无法启动、使用不便、操作不畅等。</p> <p>故障处理要求如下表：</p>

	<table border="1"> <tr> <th>级别</th> <th>业务恢复时间</th> <th>解决时间</th> <th>响应时间</th> </tr> <tr> <td>特别重大故障事件</td> <td>30 分钟</td> <td>3 天</td> <td>5 分钟</td> </tr> <tr> <td>重大故障事件</td> <td>60 分钟</td> <td>1 周</td> <td>10 分钟</td> </tr> <tr> <td>一般故障事件</td> <td>360 分钟</td> <td>2 周</td> <td>30 分钟</td> </tr> </table> <p>所有恢复故障所需的服务均由应答方负责。</p> <p>应答方应在建议书中详细说明技术指导和技术支持的范围和程度。</p> <p>在服务期内，网络和扩容及软件升级时，应答方必须根据采购方要求派技术人员到场指导。</p> <p>重保支撑：服务期内，应答方需配合采购方进行重保支撑工作，包括不限于系统巡检、重保人员支撑等。</p>	级别	业务恢复时间	解决时间	响应时间	特别重大故障事件	30 分钟	3 天	5 分钟	重大故障事件	60 分钟	1 周	10 分钟	一般故障事件	360 分钟	2 周	30 分钟
级别	业务恢复时间	解决时间	响应时间														
特别重大故障事件	30 分钟	3 天	5 分钟														
重大故障事件	60 分钟	1 周	10 分钟														
一般故障事件	360 分钟	2 周	30 分钟														
服务 3 部分	<p>1、云资源需求：资源池物理建设规模满足 CPU 数量 2112 核，内存 14336 GB，高性能存储 74TB，GPU 服务器不少于 8 台，其中 GPU 卡合计不少于 64 块，规格不低于 910B2。应满足区级的业务需求，在各项资源发放水位高于 70%时及时报告招标人。中标人应按照招标人的要求，根据实际需求进行扩容。</p> <p>2、运行维护服务：提供基于算力设施的运维服务，为创新技术试点应用提供服务。</p>																

(2) 包 2

服务 1 部分	<p>非国产化云资源需求：提供不少于 19538 核 vCPU（超分比为 6，<math>19538/6=3256</math> 核 CPU）、16593.17GB 内存、1528.52TB 普通存储、96.16TB 高性能存储的可用资源，以及 1636 核 CPU、17920GB 内存、691.2TB 普通存储、7.5TB 高性能存储的物理机资源。</p> <p>国产化云资源需求：提供不少于 1747 核 vCPU（超分比为 3，<math>1747/3=582</math> 核 CPU）、3641.34GB 内存的可用资源。</p> <p>算力资源需求：（1）提供不少于 392 核 CPU、7168GB 内存、56 块推理卡的推理用算力资源，推理卡显存不小于 48GB，并组建 100G 的 RoCE 算力网；（2）提供不少于 240 核 CPU、3072GB 内存、23.04TB 高性能存储、24 块训练卡的训练用算力资源，训练卡显存不小于 80GB，并组建 200G 的 RoCE 算力网。</p> <p>网络资源需求：（1）公网 IP 地址需求：提供至少 512 个互联网 IP 地址，后续可根据实际使用情况扩容；（2）互联网带宽：提供至少 2 线 1Gbps 带宽的链路接入公网，互为灾备，后续可根据实际使用情况扩容；（3）政务外网带宽：提供至少 2 条万兆带宽的裸光纤链路，通过双路由接入的方式从云平台所在机房至招标人指定的申港大道 200 号政务外网机房；（4）提供至少 42 个 IP 的应用负载均衡服务；（5）提供至少 214 个 IP 的安全交换区（网闸）。</p> <p>安全服务需求：提供至少 40 套入侵防御服务、40 套用户管理服务、2080 次常规安全漏洞扫描、8 套网络访问控制服务、8 套数据库审计服务、8 套日志审计服务、8 套用户身份认证服务、8 套在线防护 WAF、8 套网</p>
---------	---

	<p>页防篡服务。</p> <p>密码服务需求：提供至少 8 套安全认证网关服务、8 套可信密码服务、8 套文件加密存储或签名验签服务、4 套时间戳服务。</p> <p>运行维护服务需求：中标人应建立专职的运行维护团队，并提供不少于 4 人的运维服务，负责浦东新区政务云平台、网络、安全及备份部分的运维，满足浦东新区政务云统一管理运维服务要求。包括但不限于为浦东新区政务云提供业务培训、基础运维、业务迁移咨询等必要的运维服务。招标人和中标人双方根据实际工作需要签订服务水平协议（SLA），确保政务云安全、稳定、可靠运行。</p>
<p>服务 2 部分</p>	<p>国产化云资源需求：提供不少于 9879 核 vCPU（超分比为 3，9879/3=3293 核 CPU）、26214.4GB 内存、300TB 普通存储、100TB 高性能存储的可用资源。</p> <p>算力资源需求：（1）提供不少于 896 核 CPU、17408GB 内存、264.04TB 高性能存储、112 块推理卡的推理用算力资源，推理卡显存不小于 48GB；（2）提供不少于 896 核 CPU、11264GB 内存、122.88TB 高性能存储、64 块训练卡的训练用算力资源，训练卡显存不小于 96GB，并组建 400G 的 RoCE 算力网。</p> <p>机柜租用需求：提供至少 9 个机柜的租用服务。</p> <p>安全服务需求：提供至少 15 套网络访问控制服务、15 套数据库审计服务、15 套日志审计服务、15 套用户身份认证服务、15 套在线防护 WAF、15 套网页防篡服务。</p> <p>密码服务需求：提供至少 15 套安全认证网关服务、15 套可信密码服务、15 套文件加密存储或签名验签服务、8 套时间戳服务。</p>
<p>服务 3 部分</p>	<p>算力资源需求：（1）提供不少于 1792 核 CPU、14336GB 内存、1536TB 普通存储、174.08TB 高性能存储、128 块推理卡的推理用算力资源，推理卡显存不小于 96GB，并组建 400G 的 RoCE 算力网；（2）提供不少于 192 核 CPU、3072GB 内存、23.04TB 高性能存储、24 块渲染卡的渲染用算力资源；（3）提供不少于 1088 核 CPU、13824GB 内存、93.44TB 高性能存储、72 块训练卡的训练用算力资源，训练卡显存不小于 96GB，并组建 400G 的 RoCE 算力网。</p> <p>运行维护服务需求：中标人应建立专职的运行维护团队，并提供不少于 2 人的运维服务，提供基于算力设施的运维服务，为创新技术试点应用提供服务。</p>

**(3) 包 3**

<p>服务 1 部分</p>	<p>物理托管需求：提供机房机柜服务，资源量不少于 5 个，满足设备上架、供电、散热等托管运行要求。</p> <p>网络资源需求：提供互联网公有 IP 服务不少于 254 个；互联网骨干级带宽不少于 4GB；政务专线 4 条，每条带宽 10GB；应用负载均衡服务不少于 103 个 / IP；安全交换区不少于 254 个 / IP。</p>
----------------	--

	<p>计算资源需求：提供 XC 云计算资源，资源池规模满足 CPU 不少于 10984 核，内存不少于 67660GB，满足业务稳定运行需求。</p> <p>存储资源需求：提供应用存储空间不少于 3373.7TB，高性能数据库存储不少于 523TB，满足业务数据存储与数据库高性能读写要求。</p> <p>安全服务需求：提供统一安全防护服务，资源满足网络访问控制服务 130 个租户、入侵防御服务 130 个租户、用户管理服务 130 个租户、用户身份认证服务 130 个租户、数据库审计服务 100 个实例、常规安全漏洞扫描 2400 次、在线防护 WAF148 套、网页防篡改服务 148 套。</p> <p>密码服务需求：提供租户密码应用支撑服务，资源满足安全认证网关服务不少于 10 套，时间戳服务不少于 1 套。</p> <p>云运维管理平台服务：云服务商应使用自主的、适应国际标准的商业化虚拟化软件，并搭建统一的个性化云运维管理平台提供服务。云运维管理平台能够基于自主架构的虚拟化软件，提供云运营管理和云运维管理服务，能够对 IT 基础设施进行统一管理。</p> <p>安全服务：政务云平台需符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求。中标人所提供的加密服务及提供加密服务所需的软/硬件设备符合《中华人民共和国密码法》及国家密码管理部门的相关要求。</p>
<p>服务 2 部分</p>	<p>计算资源需求：提供通用算力与 GPU 算力服务，通用算力资源池满足 CPU 不少于 2515 核，内存不少于 20700GB；GPU 算力资源池满足 GPU 服务器 CPU 不少于 1536 核、内存不少于 10240GB、存储不少于 19.88TB，GPU 推理卡不少于 48 块，GPU 训练卡不少于 32 块。</p> <p>密码服务需求：提供密码应用与可信认证服务，资源满足安全认证网关服务不少于 15 套、签名验签服务不少于 15 套、可信密码服务不少于 15 套、时间戳服务不少于 15 套。</p> <p>网络资源需求：提供政务专线接入服务，政务专线资源量不少于 1 条，满足政务业务网络互通要求。满足量子通讯、数据要素赋能、智能化应用与治理等应用场景要求。</p> <p>平台租用服务部分 1 需与平台租用服务 2 保持统一运营和运维，配套软件及云服务提供商保持一致，充分考虑与现有平台软硬件的兼容性和拓展性。</p>

**9.2.2 指标要求**

服务指标要求如下：包 1，包 2，包 3 均适用

指标名称	指标要求
平台可用性	<p>中标人应承诺在合同期内用户云服务可用时间的概率不低于 99.9%，即实际可用时间/(实际可用时间+不可用时间)。</p>
数据存储持久性	<p>中标人承诺在合同期内数据保存不丢的概率不低于 99.99%，即完好数据/(完好数据+丢失数据)。</p>

数据可迁移性	中标人承诺用户能够控制数据的迁移，保证启用或弃用该云服务时，数据能迁入和迁出。
数据私密性	中标人应承诺用户应有加密或隔离等手段保证同一物理资源池的用户数据互不可见。
资源交付服务响应时间	资源开通、变更完成后交付用户时间-收到需求时间，标准需求不超过 3 个工作日。
故障恢复时间	<p>一般事件需在 360 分钟内恢复、重大事件需在 60 分钟内恢复、特别重大事件需在 30 分钟内恢复。</p> <p>说明：</p> <p>一般事件：故障对系统业务无明显影响，仅造成系统报错、非关键应用无法启动、使用不便、操作不畅等。</p> <p>重大事件：故障造成系统发生中断或系统死机但重启后正常；应用部分不稳定；系统运行正常，但不能进行操作（控制台无响应）。</p> <p>特别重大事件：故障造成系统失效或崩溃，应用系统无法正常启动运行、网络故障、丢失数据等，且没有临时替代解决方案；系统硬件故障、系统崩溃（死机和）自动重启）且不能再启动、磁盘信息丢失、系统或应用服务无法启动、网络链接失效、文件损毁等。</p>

**9.2.3 整体架构概述**

浦东新区按照政务系统服务器存储资源集约化建设、统筹使用的原则，通过租用服务和自建的方式，统一建设浦东政务云。

根据政府业务特性，平台划分为政务外网业务区和互联网业务区，两个区之间严禁直接通信，所有需要交换的数据均通过网闸实现安全交互。

云上主要有非国产化资源、国产化资源及算力资源，并提供安全能力及密码能力。

**10 技术指标要求**

**10.1 包 1 技术指标要求**

**10.1.1 系统功能与技术指标——服务 1 部分**

**10.1.1.1 云平台能力要求**

**10.1.1.1.1 平台能力要求**

整体平台支持 x86 架构与 ARM 架构混合部署和统一管理，支持 Intel、AMD、海光、鲲鹏、飞腾等业界主流 CPU 服务器，并可提供以下能力：弹性计算服务、块存储服务、网络资源服务、主机备份服务、运维管理服务功能等。

**10.1.1.1.2 平台高可靠要求**

云平台使用的网络安全设备、服务器、存储等设备都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可以接管业务；云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响；

云平台提供备份/快照功能，能对政务云平台中的云主机进行备份，防止存储故障导致数据丢失。

**10.1.1.1.3 资源能力要求**

分类	资源总量	单台配置	备注
----	------	------	----

分类	资源总量	单台配置	备注
非国产化资源	不少于 5960 核物理 CPU，不少于 55698 GB 内存	不低于 2 路 18 核 768G	
	不少于 6615TB 普通存储容量	配置全容量许可快照功能,配置全容量许可的克隆功能,配置全容量许可的在线重删压缩功能,后续扩容无需额外购买许可	
	不少于 1638TB 高性能存储容量		
	不少于 1500TB 备份存储容量	1.可兼容适配现网备份平台; 2.支持兼容适配现网云平台内外部快照功能; 3.备份服务端、介质服务端支持海光、鲲鹏架构下麒麟操作系统等; 4.配置不低于 1500TB 的容量授权	
	GPU 服务器不少于 5 台,其中 CPU 不少于 120 核,内存不少于 1920GB	GPU 卡合计不少于 10 块,规格不低于 P40	
国产化资源	不少于 640 核物理 CPU，不少于 10240GB 内存	不低于 2 路 24 核 768G	
	不少于 399TB 普通存储容量	不少于 2 个控制器,单控不低于 256G 缓存,配置 RAID-TP(三盘校验),配置重删、压缩、自动分层和克隆授权;	
	不少于 208TB 高性能存储容量	不少于 2 个控制器,单控不低于 256G 缓存,配置 RAID-TP(三盘校验),配置重删、压缩、自动分层和克隆授权;	

### 10.1.1.2 云业务管理平台能力要求

#### 10.1.1.2.1 云业务管理平台软件能力要求

云业务管理平台软件需支持与中标人所提供的云运维监控平台对接的能力、以及在基础设施层各类服务器及其虚拟化环境中部署的能力。云管理平台可提供北向接口、API 接口，接入浦东大数据中心统一云管平台。

提供云业务管理平台软件，支持云业务管理和业务云上资源监控等相关服务，能够对云上业务进行有效管理；

云业务管理平台支持用户自助服务，用户可通过自助服务门户完成云资源申请、使用、修改、销毁等操作，服务门户支持为用户提供云主机、VPC、云防火墙、云负载均衡、应用管理、云数据库、中间件、大数据、微服务引擎、DevOps 等服务；

为提升云管平台高可靠性，云管理平台管理节点和 OpenStack 控制组件需支持以容器形式集群部署，云管理平台支持业界前沿的容器技术 Containerd、Docker 及容器编排引擎 Kubernetes，支持 Spring Cloud、Dubbo 和 Istio 等主流微服务治理框架；

如有证明云平台软件功能的测试报告、证书等材料请提供。

支持 IPv4/IPv6 双栈业务部署，支持按需扩展中间件、容器等 PaaS 功能；

支持对用户按需提供业务服务，实现容器、微服务、DevOps 组合式的业务能力；

支持与现网云业务管理平台平滑演进，支持现网平台授权通过升级等方式可利旧使用，支持对接

SDN 平台实现业务自动化上线和管理，支持网络 Overlay 和主机 Overlay；

云管理平台可提供北向接口、API 接口，接入浦东大数据中心统一云管平台。

### 10.1.1.3 虚拟化平台要求

#### 10.1.1.3.1 虚拟化平台软件要求

虚拟化平台支持安装在通用的 x86、ARM 架构服务器，支持海光、鲲鹏、飞腾等业界主流 CPU 服务器，支持 x86 架构和 ARM 架构服务器集群统一管理，支持统一提供虚拟机、裸金属资源管理，包括对裸金属服务器的增加、删除、启动、关闭、重启、安装镜像等全生命周期管理能力；

支持集群动态资源调度功能，可基于主机的 CPU 利用率、内存利用率、磁盘 I/O、磁盘容量利用率、磁盘请求、网络流量等资源对虚拟机进行动态资源调度，实现自动化资源分配和负载均衡功能，支持当虚拟机的 CPU、内存利用率超过设置的阈值时，在虚拟机操作系统本身支持资源热添加的前提下，系统将自动为该虚拟机增加相应的 CPU 和内存资源，无需人工干预；

支持宿主机自治功能，在虚拟化管理平台故障时，可以通过主机自治平台对所在宿主机和虚拟机进行管理运维；支持查看宿主机正在使用的服务及端口号，并设置访问端口的 IP 范围，防止未授权的访问和攻击；

虚拟化平台支持虚拟交换机的图形化展示，集中化展示虚拟交换机端口使用情况，通过点击虚拟交换机端口，可以快速查看端口详细信息和端口流量实时监控，提供可视化的监控界面降低运维难度，快速掌握网络流量情况；

支持一云多芯、多运行时、管算分离以及智能计算功能，支持外部快照功能，支持未来国产化资源池演进需求；

支持与现网虚拟化平台平滑演进，支持现网平台授权通过升级等方式可利旧使用，支持对接云平台实现业务资源统一管理。

### 10.1.1.4 云网络系统要求

#### 10.1.1.4.1 云网络系统要求

SDN 控制器支持通过弱控方式对云内业务接入、核心设备、出口设备和骨干线路等需要支持冗余备份，云内业务骨干线路带宽  $\geq 80\text{Gb}$  带宽，服务器业务网  $\geq 20\text{Gb}$  带宽，服务器存储网  $\geq 50\text{Gb}$  带宽，核心交换机支持持续扩容，全面支持 IPv4/IPv6 双栈业务部署；

业务网络设备统一纳管，又支持与云业务管理平台对接，实现云业务对网络的自动化调度；

### 10.1.1.5 网络资源要求

#### 10.1.1.5.1 应用负载均衡要求

需提供应用负载均衡服务，将来自用户的访问请求合理地分发到各台云主机上，从而提升整个业务系统的服务能力和可用性。

#### 10.1.1.5.2 网络资源要求

互联网带宽：需提供不低于 1Gbps 带宽，分配一个/56 位的 IPv6 地址段，提供 256 个 IPv6 地址；

政务外网带宽：需开通不少于 1 条的裸光纤链路，通过双路由接入的方式从云平台所在机房至招标人指定的政务外网机房；

需大幅降低互联网出口防火墙重复配置 NAT 策略的性能压力；

支持不小于 40G 的入侵防御处理能力，支持互联网网络出口全万兆链路的能力，为政务云不断发展的互联网业务提供持续安全防护能力。

#### 10.1.1.5.3 安全交换区要求

需提供安全交换区服务，通过安全交换区的数据交换策略，从物理上隔离、阻断具有潜在攻击可能的一切连接，并进行强制内容检测，从而实现最高级别的安全，有效的将两网之间实现了安全隔离与业务数据安全、可靠的交换。

#### 10.1.1.5.4 网管服务要求

配套提供网管服务。服务内容包含业务分析中心、移动运维中心、资源审计中心、自助服务中心巡检等维保服务内容。

##### （1）业务分析中心

业务分析中心可对单个业务进行管理，能够关联分析业务性能、业务告警、CMDB 变更、流程工单数据，进行端到端智能分析，帮助运维人员完成对某个业务故障发现、故障定位分析、故障预防相关工作。

##### （2）移动运维中心

移动运维中心支持用户通过移动端来创建工单、处理待办、查看已办、知识库和公告，方便快捷，在移动端能够处理哪些流程可以在后台进行配置，同时还支持通过移动端提交服务请求、查看知识库和公告，便捷迅速。对于同一流程节点在移动端和 web 端使用不同的表单页面，运维人员可在后台对移动端的表单界面展示字段进行配置，灵活调整。

##### （3）资源审计中心

支持将线下审计数据以 excel 方式批量导入资源审计中心中，系统根据导入数据自动生成审计结果，对于审计结果为“有差异”的数据，可以手工确认该数据或生成流程工单进行管控确认。

在资源详情中支持查看该资源的历史审计记录，并可查看审计数据详情。对于审计结果为“有差异”的数据，详情中该差异数据将被红色高亮显示，便于运维人员的快速定位，增大运维响应效率。

##### （4）自助服务中心

自助服务中心为业务部门用户提供自助申请 IT 服务，业务部门用户可以通过自助服务中心进行申报故障、自助发起服务请求、查询进展、查询知识、查看公告信息和个人信息修改等。同时运维人员可以将服务请求发布成服务目录，发布成服务目录后，业务用户可以在自助服务中心自助申请。

#### 10.1.1.6 安全服务要求

浦东政务云平台应符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求，核心技术应具有国内自主知识产权，并具备保障系统运行的数据库、操作系统等完整方案；针对数据分析、共享交换等应用，应提供更高标准。

##### 10.1.1.6.1 网络访问控制要求

需提供网络访问控制，配置合规策略与安全接入实现云数据中心的整体安全防护，同时为每个申请安全服务的租户提供独立的 vFW 服务，实现租户业务的隔离与安全能力。

##### 10.1.1.6.2 入侵防御要求

需提供入侵防御防护能力，为数据中心内部提供更坚固的安全保护机制，叠加深度检测功能可以更有有效的保护内部服务器避免受到病毒、蠕虫、程序漏洞等来自应用层的安全威胁。

##### 10.1.1.6.3 常规安全漏洞扫描要求

需提供漏洞扫描服务，对网络或主机系统进行安全漏洞监测和分析，根据扫描网络或主机的安全漏洞，为用户提供详细的漏洞扫描报告，同时针对扫描结果提供修复建议，用户可以在被攻击前及时进行修复等处理，保证业务安全运行。

##### 10.1.1.6.4 用户管理的要求

需提供用户管理，云平台需对用户账号实行严格的统一身份认证、最小权限分配、多因素验证，确保访问可控。

#### 10.1.1.6.5 用户身份认证的要求

需提供集中化账号管理、高强度认证加固、细粒度授权控制和多种形式审计记录，使内部人员、第三方人员的操作处于可管、可控、可见、可审的状态，保障操作系统、数据库、应用系统等资产的安全运维。

#### 10.1.1.6.6 在线防护 WAF 的要求

需提供在线防护 WAF，对网站进行安全防护，提供对 WEB 攻击的全面防御，包括 SQL 注入、CSRF、XSS、Webshell、系统命令注入、远程文件包含、盗链、HTTP 畸形报文、CC 等等。

#### 10.1.1.7 设备托管服务要求

需提供数据中心机房空间服务，提供额外设备托管空间服务；需提供机房整机柜出租服务，提供额外设备托管机柜，托管机柜数量不少于 2 个，单机柜功耗不低于 3000W。

#### 10.1.1.8 服务 1 机房技术要求

(1) 机房空间要求：机柜总数量不少于 93 个，实际使用机柜数量可根据项目需求提供。每机柜提供双路供电模式（2N 架构）。

(2) 中标人提供的机房可以通过冷通道等多种形式按照要求对资源进行物理和逻辑隔离，可在机房内划分独立区域，满足多个云平台资源区和独立资源区域划分要求。独立区域具有门禁控制，可使用指纹识别、门禁卡、密码相结合的方式授权管理，控制权按照招标人要求进行管理。需要提供不低于 100M 互联网专线，用于运维办公使用。

(3) 机房环境要求：

项目	设计指标
环境要求	机房在温度 $23 \pm 1^{\circ} \text{C}$ ，相对湿度 40%-55% 的环境下运行，为通信设备创造良好的温度湿度环境。
结构	数据中心承重严格按照国家 A 级计算机机房标准进行设计建设，2 层设备区楼板荷重 $\geq 1000 \text{kg/m}^2$ ，电力电池区 $\geq 1600 \text{kg/m}^2$ ，完全满足作为 IDC 机房的承重要求，满足国标要求的抗震要求，能够防御雷击、防御重大洪涝灾害
空气调节	机房配置 12 台显冷量为 79.4KW 的下送风机房专用空调和 2 台显冷量为 28KW 的下送风机房专用空调，N+1 冗余，总共可提供制冷量 850KW。机房内采用高效的前送风、后回风的气流组织方式，机架采用面对面、背对背的布局方式形成冷热通道，同时封闭冷通道，有效的提高空调的效率，减少服务器的风扇功耗。能保障机房在温度 $23 \pm 1^{\circ} \text{C}$ ，相对湿度 40%-55% 的环境下运行，为通信设备创造良好的温度湿度环境。
供电电源	两路独立、可靠的 10kV 市电电源，两路市电电源的供电容量均为 4000kVA，共安装 4 台 2000kVA 变压器，两路电源均为常用电源，并列运行，互为主备用。
后备用电	配置 2 台 0.4kV/2000kW 固定式柴油发电机组作为应急保障电源，柴油发电机组所使用的地下储油系统为 2 个 30 立方米直埋式地下储油罐。
接地	接地电阻 $\leq 1$ ，接地电位差 1V
机房布线	采用光缆/六类对绞电缆，采用 1+1 冗余。

项目	设计指标
照明要求	采用 T5 型高效照明系统，机房照度达到 500Lux，眩光限制按 I 级标准，机房内设置备用照明，其照度为一般照明的 15%，机房设置疏散照明和安全出口标志灯，其照度不低于 0.5LUX。
机房监控	专业保安人员 24 小时在岗，提供 7×24 小时机房专用保安值班和巡逻；出入口、机房、配套区域采用门禁系统和视频监控系统；机柜区域配备专用门禁和 24 小时监控系统，视频监控画面可远程调用。
安全防范	采用 SYRIS 门禁系统控制级别设定和身份识别；机房安防监控系统可开放相应的接口或者服务提供监控服务，监控录像保存时间 6 个月以上，门禁系统记录保存 1 年以上。消防系统为全淹没式气体自动灭火系统，灭火药剂采用七氟丙烷作为洁净气体。
消防	具备火灾报警及消防联动控制系统。消防系统为全淹没式气体自动灭火系统，灭火药剂采用七氟丙烷作为洁净气体。

在本次项目建设提供的资源外，中标人需在建设区域内储备一定数量的非国产化和国产化计算和存储资源，以应对政务业务应急和突发性需求，包括但不限于：不少于 960 核 CPU 物理核，不低于 11520GB 物理内存的国产化计算资源；不少于 16 台国产化 GPU 服务器资源（单台规格不低于 CPU 4\*48 核，内存 32\*64GB，GPU 8\*64GB，SSD 存储 2\*480GB+2\*3.84TB）。

## 10.1.2 系统功能与技术指标——服务 2 部分

### 10.1.2.1 云主平台建设

#### 10.1.2.1.1 云平台能力要求

支持多种国产化架构部署，并可提供以下能力：弹性计算服务、块存储和对象存储等。

#### 10.1.2.1.2 云业务管理平台要求

提供一套云业务管理平台软件，提供云业务管理和业务云上资源监控等相关服务，能够对云上业务进行有效管理。云业务管理平台软件需支持与中标人提供的云运维监控平台对接的能力、以及在基础设施层各类服务器及其虚拟化环境中部署的能力。云管理平台可提供北向接口、API 接口，接入浦东大数据中心统一云管平台。

#### 10.1.2.1.3 虚拟化平台要求

虚拟机之间可以做到隔离保护；虚拟机具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址等；当虚拟机操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性；支持将多个物理服务器组成集群，CPU、内存、磁盘资源可以通过碎片整理、数据平衡技术提升集群资源利用率；虚拟化软件可以在线进行版本升级。

#### 10.1.2.1.4 云网络系统要求

核心骨干设备、出口设备、骨干线路等需要支持冗余备份，云内骨干线路带宽 $\geq 80\text{Gb}$ 带宽（双链路），服务器接入 $\geq 50\text{Gb}$ 带宽（业务接入和存储网接入），核心骨干设备可以保证大规模业务迁移，无缝扩容需求；支持对云平台内的网络设备进行统一管理；网络控制器需集群部署。云平台综合运维区需与现浦东政务云管理区实现互通。同时，综合运维区网络出口接入需提供互联网网络出口。

#### 10.1.2.1.5 网络服务需求

##### 10.1.2.1.5.1 网络出口要求

本期云平台网络出口需提供国产化云平台较独立的网络出口，并预留相同带宽的网络出口线路作

为容灾线路。

#### 10.1.2.1.5.2 应用负载均衡要求

需提供应用负载均衡服务，将来自用户的访问请求合理地分发到各台云主机上，从而提升整个业务系统的服务能力和可用性。

#### 10.1.2.1.5.3 安全交换区要求

需提供安全交换区服务，通过安全交换区的数据交换策略，从物理上隔离、阻断具有潜在攻击可能的一切连接，并进行强制内容检测，从而实现最高级别的安全，有效的将两网之间实现了安全隔离与业务数据安全、可靠的交换。

#### 10.1.2.1.6 平台高可靠要求

云平台使用的网络安全设备、服务器、存储等设备都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可以接管业务。云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响。云平台提供备份/快照功能，能对政务云平台中的裸金属服务器和虚拟化服务器进行备份，防止存储故障导致数据丢失。

#### 10.1.2.1.7 备份要求

共需提供备份存储不少于 400T，承载政务外网区主机备份、政务外网区业务数据备份、互联网区主机备份、互联网业务数据备份。

#### 10.1.2.1.8 设备托管

需提供数据中心机房空间服务，此次提供 4 个机柜，可用于部署托管设备使用，并预留设备托管空间，提供用于后续额外设备托管机柜。

#### 10.1.2.1.9 云安全需求

云平台整体按照《信息安全技术云计算服务安全能力要求》（GB/T 31168）进行建设。符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求；满足《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）第三级要求的内容。

#### 10.1.2.1.9.1 平台安全要求

为了保证平台的安全、稳定运营，制定完善的安全运维管理体系，制定完善的安全管理制度规范，对不同的安全区域、安全保护对象明确安全责任人；提供符合信息安全等级保护三级要求的云平台基础安全和应用系统安全的服务内容。

需提供安全监控，安全监控内容包含但不限于网络流量监控、各个安全设备的日志记录监控、安全设备运维操作监控和云资源运行状态监控等，并提供安全事态分析，满足用户不同安全级别业务系统的安全需求。

中标人建设的浦东政务云平台需满足包括但不限于如下安全要求：物理安全、网络安全、主机安全、平台安全等内容。

1) 物理安全：中标人用于建设浦东政务云的机房需具备防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应等能力。

2) 网络安全：中标人需针对浦东政务云平台按照国家网络安全等级保护基本要求要求建立一套网络安全防护体系，对网络边界处提供访问控制、病毒过滤、防攻击、防入侵、防篡改、内外网数据安全隔离交换等立体安全防护，保护平台内部网络通信安全。提供入侵流量监测功能；态势感知通过大数据的离线数据分析能力，对收集的安全日志，进行建模分析，通过大数据手段得出未知威胁攻击、

黑客入侵的结论。

**访问控制：**浦东政务云平台在各网络边界处应部署安全访问控制设备，包括防火墙、IPS、VPN 网关、安全网关等，能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。支持按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统资源访问。

**安全审计：**中标人需对浦东政务云平台使用网络设备运行状况、网络流量、用户行为等进行日志记录，能够根据记录数据进行分析并生成审计报告，同时对系统审计的记录进行有效安全保护，避免受到未预期的删除、修改或覆盖等不安全操作。

**入侵防范：**须提供 IPS 入侵防范、检测系统或安全网关系统，实现的实时防范功能应包括：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等非法网络攻击行为，当检测到攻击行为时，系统将详细记录相关信息，同时在发生严重入侵事件时具备报警、记录功能。

**恶意代码防范：**中标人应提供对各种恶意代码进行检测和清除功能，系统应支持自动及手工方式对恶意代码库的升级和检测系统的更新功能。

**网络设备防护：**中标人所使用的网络设备均应支持对登录用户的身份鉴别功能，支持采用加密用户口令鉴、RADIUS 身份认证等方式，可通过命令行、Web、中文图形化配置软件等方式进行配置和管理，并可通过 ACL 访问控制列表的方式实现对网络设备的管理员登录地址进行限制，所有网络设备用户均应具备唯一标识。

**常规安全漏洞扫描：**中标人应提供对系统漏洞、Web 漏洞、数据库漏洞以及弱口令等安全漏洞扫描和脆弱性检测，系统漏洞知识库需涵盖各种主流的数据库厂商，涵盖各种常见的漏洞类型。

**用户管理：**中标人应提供用户的安全、合规接入功能，通过 SSL VPN 服务提供统一的接入接口，可实现通过专用线路安全访问，也可以通过专属操作间提供更加安全、合规的运维响应服务；

**用户身份认证：**中标人应提供授权、可控的用户身份认证和管理操作留痕可溯服务，提供对物理设备访问时的安全跳转平台，一方面可以防止非法用户直接登录物理设备带来的安全隐患，另一方面可以有效授权并记录合法用户的操作。

**在线防护 WAF：**中标人应提供在线防护 WAF，对网站进行安全防护，提供对 WEB 攻击的全面防御，包括 SQL 注入、CSRF、XSS、Webshell、系统命令注入、远程文件包含、盗链、HTTP 畸形报文、CC 等等。

3) 主机安全：对主机的物理安全，主机访问控制方面进行保护。

**主机访问控制：**主机系统应启用主机系统的访问控制功能，依据安全策略控制用户对资源的访问权限，通过系统的技术维护措施严格限制默认账户的访问权限。

4) 平台安全：包括虚拟化及云运维管理平台的安全保护，支持物理资源与虚拟资源统一管理。

**虚拟化安全：**支持有代理或者无代理安全方式进行虚拟环境的整体防护。

**浦东政务云平台安全：**如果云运维管理平台需要数据库的支持，应保护好云运维管理平台的数据库安全，设置强壮复杂的密码策略、备份数据库和配置相关的网络安全服务；云运维管理平台的访问许可应加强管理，删除不需要的用户账号。

5) 委办局单位部署在浦东政务云平台中的应用系统在执行国家及本市有关电子政务信息安全管理办法的过程中，若发现重大安全事故或者安全隐患时，中标人需要配合进行安全整改。

#### 10.1.2.1.9.2 安全硬件要求

序号	设备类型	数量	备注(用途)
----	------	----	--------

序号	设备类型	数量	备注(用途)
1	政务外网出口 抗 DDOS	2 台	《GB/T 22239-2019 等保基本要求》规范中要求的 8.1.33 入侵防范 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
2	政务外网出口 防火墙	2 台	本期云平台在政务外网区出口规划 2 台防火墙用于内网区和政务外网区业务互通。
3	政务外网出口 IPS	2 台	《GB/T 22239-2019 等保基本要求》规范中要求的 8.1.33 入侵防范 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；通过 IPS 进行入侵防御检测，并进行阻止攻击；分别在政务外网区和互联网区配置。
4	政务外网核心 防火墙	2 台	本期云平台在政务外业务区规划 2 台防火墙，实现云内租户间安全防护。
5	政务外网负载 均衡	2 台	本期云平台在政务外业务区规划 2 台负载均衡，实现云内业务负载均衡可靠性。
6	管理防火墙	2 台	本期云平台在管理区内新增 2 台管理防火墙，按照主备部署原则，实现业务区和管理区的安全隔离，需具备安全威胁防护板，配套 IPS、AV license。
7	网闸	2 台	规划政务外网区和互联网区跨区访问均经过网闸实现，按照最小化建设需求，本期新增 2 台网闸。
8	综合运维防火 墙	2 台	规划 2 台防火墙作为运维区的统一安全入口，统筹管理两个管理区。
9	互联网出口抗 DDOS	2 台	《GB/T 22239-2019 等保基本要求》规范中要求的 8.1.33 入侵防范 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
10	互联网出口防 火墙	2 台	本期云平台在互联网网区出口规划 2 台防火墙用于内网区和政务外网区业务互通。
11	互联网出口 IPS	2 台	《GB/T 22239-2019 等保基本要求》规范中要求的 8.1.33 入侵防范 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；通过 IPS 进行入侵防御检测，并进行阻止攻击；分别在政务外网区和互联网区配置。
12	互联网核心防 火墙	2 台	本期云平台在互联网业务区规划 2 台防火墙，实现云内租户间安全防护。
13	互联网负载均 衡	2 台	本期云平台在互联网业务区规划 2 台负载均衡，实现云内业务负载均衡可靠性。

#### 10.1.2.1.9.3 国密相关要求：

对浦东云平台所在机房部署符合 GMT 0036-2014《采用非接触卡的门禁系统密码应用技术指南》标准要求的电子门禁系统对进出机房人员进行身份鉴别，实现对电子门禁纪录进行完整性保护。

部署符合密码相关国家、行业标准要求的国密视频监控系统，对视频记录进行完整性保护，防止记录数据被非授权篡改导致数据不可信，提高记录数据的真实可靠性。

同时，部署服务器密码机、签名验签服务器、时间戳服务器等设备以保障云平台密码应用安全及合规。平台密码能力，需通过商用密码应用安全性评估三级。

### 10.1.2.2 租户密码服务

#### 10.1.2.2.1 密码支撑服务内容

##### （1）安全认证网关服务

围绕通信网络传输安全、安全区域边界及应用安全支撑等方面实现基于数字证书的身份认证与访问控制。业务应用方面，作为应用代理，联动业务系统，验证终端用户数字证书的有效性、合法性，并进行鉴权与访问控制，保证用户资源身份可信、业务可控、行为不可否认。

##### （2）签名验签服务

由云签名验证服务提供虚拟化的实例服务，以云安全组件的模式部署，围绕通信网络传输安全、安全区域边界及应用安全支撑等方面实现基于数字证书的身份认证与访问控制。

通过统一密码服务调用签名验证服务镜像，对内部流转与审批过程，通过签名验证服务实现关键行为的责任认定，确保内部流转的抗抵赖性；同时，利用签名验证技术对用户的身份鉴别事件、访问控制事件、重要系统资源敏感标记的变更事件、重要应用程序的加载和卸载事件等审计记录进行签名、加密，从而防止审计数据被篡改、泄露或非授权访问。

##### （3）可信密码服务

可信密码服务需支持两种加密方式：数据加密服务和存储加密服务。

###### 1) 数据加密服务

###### 数据加解密

在业务应用中基于虚拟密码机，提供对关键数据的透明加密及解密服务，对字段级的敏感数据进行实现加密存放。

###### 获取数据加密密钥

###### 获取系统的数据加密密钥

说明：数据加密密钥是用于加密传入数据的敏感字段信息的密钥，由密钥管理生成并管理，数据加密密钥将从密码管理系统来获取。

本地数据加密：本地数据加密，由数据加密密钥在本地对数据进行加密。

本地数据解密：本地数据解密，由数据解密密钥在本地对数据进行解密。

获取公钥信息：获取公钥信息，得到应用系统身份密钥的公钥。

远程数据加密：数据加密，由数据加密密钥在密码管理系统对数据进行加密。

说明：用于对现存数据进行加密，得到密文数据后保存。

###### 数据转加密（会话密钥到数据加密密钥）

数据转加密，将由会话密钥加密的用户数据转为数据加密密钥加密；

说明：解密客户端的数字信封得到会话密钥，将由会话密钥加密的用户数据转为数据加密密钥加密。

###### 2) 存储加密服务

面向非结构化类型的数据提供加密服务的安全存储系统服务支持面向文件的网络安全存储（NAS 安全存储）和面向块的安全存储网络（IPSAN/FCSAN 安全存储）的加密存储能力，通过密码技术保证文件机密性，避免文件采用明文方式存储在硬盘上，相关用户可查看或篡改文件内容；支持结构化、半结构化和非结构化等复杂机构数据的加密存储，应用范围广泛；提供密码运算、密钥管理、身份认证等服务器密码机功能及安全审计功能，对存储安全支撑提供安全可靠密码保障服务。

##### （4）时间戳服务

时间戳服务为业务系统提供时间戳的签发及验证服务，满足在众多业务场景中，对于业务发生的时间准确性、权威性、可信性以及可追溯性的要求。

**10.1.2.2.2 系统功能与技术指标**

服务名称	指标参数
安全认证网关服务	具备国家密码管理局颁发的《商用密码产品认证证书》
	具备公安部颁发的《网络安全专用产品安全检测证书》
	支持 SM2、SM3、SM4 算法，具有密钥协商、身份认证、SSL 隧道加密等功能。
	应支持口令、证书、短信、SSL 双向认证等方式
	支持国密 SM2/3/4 算法，支持 GM/T 0024-2014 《SSLVPN 技术规范》定义的国密 SSL 协议
	支持在同一个服务实例中，同时支持国际标准协议（TLS 1.0/1.1/1.2）以及国家密码管理局制定的国密 SSLVPN 协议。根据客户端的支持情况自动适应。
	支持将非国密浏览器的传输通道升级为国密 SSL 协议通道
	支持在同一个服务实例中，配置 RSA 和 SM2 两张站点证书，并同时启用，根据客户端的算法能力进行自动适应。
	支持超过 100 万条目数的证书黑名单
	支持代理后端启用 SSL 的应用，包括后端启用双向认证（客户端认证）的应用
	支持保护 B/S、FTP、远程桌面以及通用 C/S 应用的传输通道，并对用户提供透明无感的体验
	支持对后端应用进行连接复用，降低后端应用的长连接数量
	支持对后端应用进行静态数据缓存。降低后端应用的流量
	支持对浏览器端的流量进行压缩，降低出口带宽占用
	支持安全的页面密码代填技术（浏览器端无法获取代填内容），以实现旧应用改造
	支持以 HTTP 注入（Cookie/Header）的方式将用户的证书信息传送给后台应用，同时可以对注入的信息进行签名，防止伪造用户登录
支持自定义访问日志模板	
支持国产操作系统；支持国产 CPU	
在 8 核 CPU，16G 内存的云平台虚拟机环境下：最多并发连接数不低于 5 万次连接；吞吐率不低于 400 MB/秒；新建连接数不低于 300 次连接/秒。	
签名验签服务	具有国家密码管理局颁发的《商用密码产品型号证书》
	提供基于数字证书的身份认证功能，支持不同 CA 的证书验证，支持 HTTP/LADP 等多种方式的证书有效性验证
	提供证书解析功能，获取证书中的任意主题信息以及扩展项信息
	支持签名验签（身份鉴别）、数据加密解密、数字信封、数据完整性保护，兼容多种签名格式，验签格式自适应
	支持证书白名单功能（提供截图）
	支持证书延期策略（提供截图）
	提供文件数据签名与签名验证功能

服务名称	指标参数
	提供数字信封功能对数据进行加密传输，只有指定的信封接收者可解密数据
	API 支持 HTTPS 协议（提供截图）
	支持多种加密设备：加密卡、加密机；支持密码卡+CPU 同时使用（提供截图）
	全面系统管理及审计功能：支持日志 SYSLOG 远程发送、日志归档、系统备份恢复、支持 IPV6、三权管理、SNMP 监控（提供截图）
	支持国产操作系统；支持国产 CPU
	8 核 CPU，16G 内存的云环境虚拟机下：SM2 算法签名效率 $\geq 2000$ 次/秒；SM2 算法验签效率 $\geq 3000$ 次/秒；
可信密码服务	具有国家密码管理局颁发的《商用密码产品型号证书》
	提供对接主流国产数据库，支持 SM4 算法数据加密的互认证证明材料
	支持用户主密钥、数据加密密钥的密钥管理，应用按需选择安全的密钥管理策略，可实现不同应用间密钥数据安全隔离存储
	提供用户主密钥管理，用户主密钥主要用于加密保护数据密钥，也可直接用于加密少量的数据。由 KMS 托管的用户主密钥有不同的类型（如加解密、签名/验签等），用户和应用系统可以根据自己的需要，使用不同类型的密钥完成特定的功能。
	通过对密钥状态的控制，达到对数据加密权限的管理。密钥生命周期管理中提供创建密钥、禁用密钥、删除密钥、修改密钥备注、导入密钥（密钥来源为外部导入）等。
	支持用户主密钥别名属性（可选）。别名与主密钥是多对一的关联关系，对别名提供了生命周期管理操作（新增，删除，更新，查看）。
	支持用户主密钥标签属性，将角色密钥权限细分到密钥标签级别，支持标签信息的维护以及密钥权限的细分。
	提供简便的密码运算 API，可以直接调用对应的密码运算类接口进行密钥相关的密码运算。
	提供密钥信封功能。
	支持密钥轮转功能。
	支持基于密钥管理系统的接口或客户端工具，获取数据密钥实现对应用数据的加解密。
	支持在数据库系统中内置密钥管理系统的数据库加密引擎工具，实现对数据库数据的加解密、签名验签等密钥运算服务。
	支持国产操作系统；支持国产 CPU
在 8 核 CPU，16G 内存的云环境虚拟机下：并发数 $\geq 128$ 个会话连接；SM4 加解密速度 $\geq 60$ Mbps；数据库加解密速率 $\geq 60$ Mbps；数据库操作性能损耗 $\leq 20\%$	
时间戳服务	具有国家密码管理局颁发的《商用密码产品型号证书》
	系统同时支持 SM2 算法、RSA（2048 位密钥长度）算法
	提供基于数字证书的身份认证功能，支持不同 CA 的证书验证，支持 CRL/OCSP 等多种方式的证书有效性验证
	支持时间戳策略 OID 的配置
	支持 ASN.1 时间戳请求签发

服务名称	指标参数
	支持通过原文摘要直接签发时间戳
	支持对时间戳中证书、原文摘要、策略 OID、签名时间等信息的解析及获取
	支持 RSA 证书、SM2 单证、SM2 双证的导入
	支持时间戳管理与审计
	支持时间戳归档、备份
	提供 RESTFUL、JAVA 等主流开发 API
	支持三权认证、时间源配置
	支持国产操作系统；支持国产 CPU
	8 核 CPU，16G 内存的云平台虚拟机环境下：时间戳生成速率不低于 240 次/秒；验证速率不低于为 110 次/秒；时间同步间隔时间不大于 30 分钟；时间误差不大于 100 毫秒。

**10.1.2.2.3 机房要求**

项目	参数要求	
供电	市电	两路市电由 2 个供电局向、2 个不同路由同时供电，保证电源不同时受到损坏，供电系统可用性（由市电至机柜计算）≥99.99%
	UPS	机房 UPS 采用双总线冗余（2N）供电系统的要求。即每套 UPS 供电系统由一台 UPS 主机、蓄电池组、UPS 出线柜、UPS 输出屏及电池开关组成。每 2 套 UPS 供电系统共同担负同一通信设备的供电，理论上每套系统均分负载，各承担全部负载的 50% 负载，蓄电池组处于浮充状态；当其中 1 套 UPS 供电系统发生故障时，另一套 UPS 供电系统将承担通信系统的全部负载供电，每台 UPS 的最大负载率不超过 80%，后备时间为 15 分钟。
	直流蓄电池	UPS 系统所配置的电池组，按输入市电中断后，满负荷状态下电池放电持续时间应不小于 15 分钟设计，电池具备大电流深度放电能力，并安装有电池监控监测电池的健康状况。
	柴油发单机	数据中心柴油发电机配备 N+1 冗余后备柴油发电机系统，安装 9 台 2000kW 柴油发电机组。发电机组应连续和不限时运行，发电机组的输出功率满足最大平均负荷的需要。负荷包含 UPS 系统、制冷系统、消防系统、监控系统、应急照明系统等。
	机柜 PDU	新增 PDU 采用交流 32A 单相输入，IEC320C13 10A 卡扣插座[12 位]，IEC320 C19 卡扣插座[4 位]，整条 PDU 输出位数 16 位。
制冷	机房空调	数据中心配置有冷冻水系统、冷却水系统各一套，两个系统互为备用，在主用系统发生故障时，备用系统可无缝切换，确保整个数据中心制冷的高可用性；机房末端空调全部采用冷冻水+冷却水双冷源型机房专用空调，采用高效的下送风、上回风的气流组织方式，机房内架空地板高度为 800mm，机架采用面对面、背对背的布局方式形成冷热通道，有效的提高空调的效率，减少服务器的风扇功耗。机房专用空调配备满足 N+X（X=1~N）冗余要求，两路供电来自市电，末端切换。
安防	视频监控	机房动环系统配置温、湿度监控系统，漏水检测系统，电力设备运行监控系统，空调设备运行监控系统；所提供的模块需配门禁系统；提供的模块需配有 CCTV

项目		参数要求
		监控系统，视频无死角监控，存储时间≥90 天。
	机房动力监控	数据中心集中监控系统主要监控场地内的低压配电柜输入端的电压、电流、频率、有功功率、无功功率变化情况，各温湿度监测点的温湿度变化情况，精密空调回风温度的变化情况，UPS 输入输出电压、电流等变化，UPS 状态及电池状态，场地内漏水位置，油机停启状态，剩余油量，市电供应状态等。
	门禁	满足机房采用刷卡管理方式，即进出机房均要刷卡，其中进入机房采用双因素识别（刷卡+密码）方式。
	保安	享受提供的 7×24 小时端到端全程保障服务
消防	消防要求	机房安装火灾自动报警系统和使用全淹没式 IG-541 气体灭火系统，并配备规定数量的手动消防器材。机房内 60 平方米以上的机房区域有两个以上的消防逃生出口，并保证机房内各分区到消防逃生出口的道路畅通。机房设置火灾自动报警系统，在各个分区的房间内活动地板下和顶面等部位安装烟感探测器和温感探测器。
运行维护	巡检	机房每天进行 3 次及以上例行巡检，并对机房设备运行状态、环境状态进行详细记录。
	应急机制	做好机房应急预案，在网络、电力、安全等各方面提供协助，确保采购人应急人员、设备和供应商能在最短时间内能够进入机房进行应急处置。

### 10.1.2.3 计算资源参数指标

序号	项目	资源总量	单台配置
1	云整体架构国产化建设，包含 CloudOS 云平台、CAS 虚拟化平台、AD-DC 平台、UC 网管平台、iSOC 安全威胁发现与运营管理平台，支持 IPv4/IPv6 双栈、支持外部快照；		
2	管理区资源-平台管理	CPU 不低于 1088 核、内存不低于 8704GB	不低于 2 路 32 核 512G 内存，2*480GB SATA SSD，14*3.84TB SATA SSD
	管理区资源-资源管理	CPU 不低于 896 核、内存不低于 14336GB	不低于 2 路 32 核 1024G 内存，2*480GB SATA SSD；
3	计算资源	CPU 不低于 2944 核、内存不低于 47104GB	不低于 2 路 32 核 1024G 内存，2*480GB SATA SSD；
4	HDD 集中式存储	不少于 200TB 可用	不低于 68 块 2.4TB SAS(不低于 10000RPM)，不少于 2 个控制器，单控不低于 256G 缓存，配置 RAID-TP(三盘校验)，配置重删、压缩、自动分层和克隆授权；【本次需配置 2 套，并满足 200TB 可用】
5	全闪集中式存储	不少于 200TB 可用	不低于 46 块 3.84TB SSD，不少于 2 个控制器，单控不低于 256G 缓存，配置 RAID-TP(三盘校验)，配置重删、压缩、自动分层和克隆授权；【本次需配置 2 套，并满足 200TB 可用】
6	对象存储	不少于 100TB 可用	不少于 100TB 可用；

序号	项目	资源总量	单台配置
7	备份	不低于 500TB	不低于 400TB，支持整机、数据库、文件级备份；
8	云配套软件	云配套软件	
9	云配套网络设备	云配套网络设备	
10	云配套安全设备	云配套安全设备	
11	政务外网出口	复用现有政务云政务外网出口	
12	互联网出口	复用现有政务云互联网出口	

#### 10.1.2.4 平台密码要求

本次项目包含密码机、签名验签与时间戳和密码配套，配置要求如下：

##### 10.1.2.4.1 密码机要求

（1）技术标准：同时符合 GM/T 0030《服务器密码机技术规范》、GM/T 0028《密码模块安全技术要求》技术要求。

（2）支持密码算法：支持 SM2 国密非对称算法，支持 RSA1024、RSA2048、RSA4096 等国际非对称算法；支持 SM1、SM4 等国密对称算法，支持 DES、3DES、AES 等国际对称算法；支持 SM3 国密摘要算法，支持 SHA1、SHA256、SHA512 等国际摘要算法，支持 RSA 密钥生成与查看，提供 1024 位、2048 位、4096 位 RSA 密钥生成算法及密钥备份和恢复。

（3）随机数生成：采用国家密码管理局批准的 WNG-9 硬件物理噪声源生成真正随机数，保证随机数质量可用性。

（4）扩展能力：提供 API 接口：支持多种 API 接口，服务器密码机基本接口 SDF 接口以及标准的 PKCS#11 等接口。同时可根据用户需求定制接口。

##### 10.1.2.4.2 签名验签与时间戳要求

（1）技术标准：同时符合 GM/T 0029《签名验签服务器技术规范》、GM/T 0033《时间戳接口规范》、GM/T 0028《密码模块安全技术要求》等相关技术要求。

（2）支持密码算法：支持 SM1、SM2、SM3、SM4 密码算法。

（3）数字签名/验证：提供基于 SM2 算法的数字签名和认证功能，可用于证书生成和验证、身份认证等。

（4）密钥生成与管理：提供 SM2 密钥生成及密钥备份和恢复功能。在密钥导入、导出时，私钥是加密的。

（5）运行状态监控：支持 CPU 和内存的利用率、磁盘占用率、网络状态、用户登录状态等的实时监控。

（6）开发接口：支持多种 API 接口，含 PKCS#1、PKCS#7、PKCS#10、PKCS#11、JCE 等接口。提供符合 GM/T 0033-2014《时间戳接口规范》的时间戳服务接口以及 C、JAVA 接口，可根据用户需求定制接口。

（7）时间戳签发和验证：支持基于 SM2 算法的时间戳服务，为应用系统提供时间戳签发、验证时间戳服务，实现对数据、消息、文件等多种格式原文数据的时间戳签发服务。

（8）时间同步：支持时间同步功能，支持 NTP 协议，支持多个第三方时间源的配置管理，能够

与第三方授时中心、卫星授权时间源(北斗、GPS)进行时间同步，确保签发时间戳时所获取的时间有效、精确。

(9) 高可用：支持双机热备部署；支持负载均衡。

**10.1.2.4.3 密码配套要求**

本次项目需包含国密浏览器密码模块 20 个，智能密码钥匙 USBKey20 个，个人数字证书（5 年）20 个，设备数字证书（5 年）2 个；SSL 证书（5 年）2 个。

**10.1.2.5 服务 2 机房技术要求**

项目		参数要求
供电	市电	两路市电由 2 个供电局向、2 个不同路由同时供电，保证电源不同时受到损坏，供电系统可用性（由市电至机柜计算）≥99.99%
	UPS	机房 UPS 采用双总线冗余（2N）供电系统的要求。即每套 UPS 供电系统由一台 UPS 主机、蓄电池组、UPS 出线柜、UPS 输出屏及电池开关组成。每 2 套 UPS 供电系统共同担负同一通信设备的供电，理论上每套系统均分负载，各承担全部负载的 50% 负载，蓄电池组处于浮充状态；当其中 1 套 UPS 供电系统发生故障时，另一套 UPS 供电系统将承担通信系统的全部负载供电，每台 UPS 的最大负载率不超过 80%，后备时间为 15 分钟。
	直流蓄电池	UPS 系统所配置的电池组，按输入市电中断后，满负荷状态下电池放电持续时间应不小于 15 分钟设计，电池具备大电流深度放电能力，并安装有电池监控监测电池的健康状况。
	柴油发单机	数据中心柴油发电机配备 N+1 冗余后备柴油发电机系统，安装 9 台 2000kW 柴油发电机组。发电机组应连续和不限时运行，发电机组的输出功率满足最大平均负荷的需要。负荷包含 UPS 系统、制冷系统、消防系统、监控系统、应急照明系统等。
	机柜 PDU	新增 PDU 采用交流 32A 单相输入，IEC320C13 10A 卡扣插座[12 位]，IEC320 C19 卡扣插座[4 位]，整条 PDU 输出位数 16 位。
制冷	机房空调	数据中心配置有冷冻水系统、冷却水系统各一套，两个系统互为备用，在主用系统发生故障时，备用系统可无缝切换，确保整个数据中心制冷的高可用性；机房末端空调全部采用冷冻水+冷却水双冷源型机房专用空调，采用高效的下送风、上回风的气流组织方式，机房内架空地板高度为 800mm，机架采用面对面、背对背的布局方式形成冷热通道，有效的提高空调的效率，减少服务器的风扇功耗。 机房专用空调配备满足 N+X（X=1~N）冗余要求，两路供电来自市电，末端切换。
安防	视频监控	机房动环系统配置温、湿度监控系统，漏水检测系统，电力设备运行监控系统，空调设备运行监控系统；所提供的模块需配门禁系统；提供的模块需配有 CCTV 监控系统，视频无死角监控，存储时间≥90 天。

项目		参数要求
	机房动力监控	数据中心集中监控系统主要监控场地内的低压配电柜输入端的电压、电流、频率、有功功率、无功功率变化情况，各温湿度监测点的温湿度变化情况，精密空调回风温度的变化情况，UPS 输入输出电压、电流等变化，UPS 状态及电池状态，场地内漏水位置，油机停启状态，剩余油量，市电供应状态等。
	门禁	满足机房采用刷卡管理方式，即进出机房均要刷卡，其中进入机房采用双因素识别（刷卡+密码）方式。
	保安	提供 7×24 小时端到端全程保障服务
消防	消防要求	机房安装火灾自动报警系统和使用全淹没式 IG-541 气体灭火系统，并配备规定数量的手动消防器材。机房内 60 平方米以上的机房区域有两个以上的消防逃生出口，并保证机房内各分区到消防逃生出口的道路畅通。机房设置火灾自动报警系统，在各个分区的房间内活动地板下和顶面等部位安装烟感探测器和温感探测器。
运行维护	巡检	机房每天进行 3 次及以上例行巡检，并对机房设备运行状态、环境状态进行详细记录。
	应急机制	做好机房应急预案，在网络、电力、安全等各方面提供协助，确保采购人应急人员、设备和供应商能在最短时间内能够进入机房进行应急处置。

机房需提供独立操作间，并提供 100M 配备安全网关（防火墙）的互联网专线，用于运维使用。

**10.1.3 系统功能与技术指标——服务 3 部分**

基于服务 2 中现有资源，补充国产化资源和国产化算力资源，包括：补充在国产化平台上 6 台 ARM 裸金属服务器、8 台国产化算力服务器及配套网络设备与授权，以及运维服务。

**10.1.3.1 裸金属服务器要求**

要求国产化资源提供物理 CPU 数量不少于 576 核，内存不少于 6144GB，高性能存储容量不少于 74TB。单台服务器配置不低于 2 路 48 核 1024G 内存，2\*480GB SATA SSD，2\*1.92TB SATA SSD，2\*3.84TB SATA SSD。

**10.1.3.2 国产化算力服务器要求**

为满足浦东新区政务领域 AI 算力逐步向国产化算力演进的需求，补充 8 台具备多机多卡互联及高性能并行文件存储能力的国产化算力设备。要求单台 GPU 服务器满足以下配置：

CPU 不低于 4 路 48 核心；内存不少于 2048G；硬盘不少于 2\*480G SSD，3.84TB SATA SSD\*2，每台服务器搭载不少于 8 张加速卡，FP16 算力不低于 376TFlops，配备不低于 64GB HBM2e 高带宽显存，显存带宽不低于 2.4TB/s，能提供超高的数据吞吐能力。

**10.1.3.3 运维服务需求**

中标人需提供基于算力设施的运维服务，为创新技术试点应用提供服务。涉及保障数据要素赋能、智能化应用与治理、量子通讯等应用场景，协同开展算力部署、国产算力适配、配合通用智能体开发，配合行业部门开展垂类大模型搭建，行业智能体的训练，智能体安全管理等工作。

**10.1.3.4 服务 3 机房技术要求**

项目		参数要求
供电	市电	两路市电由 2 个供电局向、2 个不同路由同时供电，保证电源不同时受到损坏，供电系统可用性（由市电至机柜计算） $\geq 99.99\%$
	UPS	机房 UPS 采用双总线冗余（2N）供电系统的要求。即每套 UPS 供电系统由一台 UPS 主机、蓄电池组、UPS 出线柜、UPS 输出屏及电池开关组成。每 2 套 UPS 供电系统共同担负同一通信设备的供电，理论上每套系统均分负载，各承担全部负载的 50% 负载，蓄电池组处于浮充状态；当其中 1 套 UPS 供电系统发生故障时，另一套 UPS 供电系统将承担通信系统的全部负载供电，每台 UPS 的最大负载率不超过 80%，后备时间为 15 分钟。
	直流蓄电池	UPS 系统所配置的电池组，按输入市电中断后，满负荷状态下电池放电持续时间应不小于 15 分钟设计，电池具备大电流深度放电能力，并安装有电池监控监测电池的健康状况。
	柴油发单机	数据中心柴油发电机配备 N+1 冗余后备柴油发电机系统，安装 9 台 2000kW 柴油发电机组。发电机组应连续和不限时运行，发电机组的输出功率满足最大平均负荷的需要。负荷包含 UPS 系统、制冷系统、消防系统、监控系统、应急照明系统等。
	机柜 PDU	新增 PDU 采用交流 32A 单相输入，IEC320C13 10A 卡扣插座[12 位]，IEC320 C19 卡扣插座[4 位]，整条 PDU 输出位数 16 位。
制冷	机房空调	数据中心配置有冷冻水系统、冷却水系统各一套，两个系统互为备用，在主用系统发生故障时，备用系统可无缝切换，确保整个数据中心制冷的高可用性；机房末端空调全部采用冷冻水+冷却水双冷源型机房专用空调，采用高效的下送风、上回风的气流组织方式，机房内架空地板高度为 800mm，机架采用面对面、背对背的布局方式形成冷热通道，有效的提高空调的效率，减少服务器的风扇功耗。 机房专用空调配备满足 N+X（X=1~N）冗余要求，两路供电来自市电，末端切换。
安防	视频监控	机房动环系统配置温、湿度监控系统，漏水检测系统，电力设备运行监控系统，空调设备运行监控系统；所提供的模块需配门禁系统；提供的模块需配有 CCTV 监控系统，视频无死角监控，存储时间 $\geq 90$ 天。
	机房动力监控	数据中心集中监控系统主要监控场地内的低压配电柜输入端的电压、电流、频率、有功功率、无功功率变化情况，各温湿度监测点的温湿度变化情况，精密空调回风温度的变化情况，UPS 输入输出电压、电流等变化，UPS 状态及电池状态，场地内漏水位置，油机停启状态，剩余油量，市电供应状态等。
	门禁	满足机房采用刷卡管理方式，即进出机房均要刷卡，其中进入机房采用双因素识别（刷卡+密码）方式。

项目		参数要求
	保安	提供 7×24 小时端到端全程保障服务
消防	消防要求	机房安装火灾自动报警系统和使用全淹没式 IG-541 气体灭火系统，并配备规定数量的手动消防器材。机房内 60 平方米以上的机房区域有两个以上的消防逃生出口，并保证机房内各分区到消防逃生出口的道路畅通。机房设置火灾自动报警系统，在各个分区的房间内活动地板下和顶面等部位安装烟感探测器和温感探测器。
运行维护	巡检	机房每天进行 3 次及以上例行巡检，并对机房设备运行状态、环境状态进行详细记录。
	应急机制	做好机房应急预案，在网络、电力、安全等各方面提供协助，确保采购人应急人员、设备和供应商能在最短时间内能够进入机房进行应急处置。

**10.2 包 2 技术指标要求**

**10.2.1 系统功能与技术指标**

**10.2.1.1 云平台能力要求**

非国产化平台要求：支持 x86 架构部署，并可提供以下能力：弹性计算服务、块存储服务。

国产化平台要求：支持 x86、ARM 架构部署，并可提供以下能力：弹性计算服务、块存储服务、对象存储服务等。

**10.2.1.2 云业务管理平台要求**

云业务管理平台提供云业务管理和业务云上资源监控等相关服务，能够对云上业务进行有效管理。提供统一门户，为用户提供自助服务门户、大屏展示、单点登录等功能；提供资源管理，对资源池中的虚拟机、子网等生命周期（创建、修改、删除、开启、关闭等）进行管理；提供运维管理，提供云资源的监控和告警功能，并提供监控大屏进行数据实时展示；提供运营管理，面向运营管理员提供服务支撑；提供管理中心，管理云管平台自身的系统配置。

云业务管理平台软件需支持与中标人所提供的云运维监控平台对接的能力、以及在基础设施层各类服务器及其虚拟化环境中部署的能力。云管理平台可提供北向接口、API 接口，接入浦东大数据中心统一云管平台。

**10.2.1.3 虚拟化平台要求**

非国产化平台要求：虚拟机之间可以做到隔离保护；虚拟机具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址等；支持将多个物理服务器组成集群，CPU、内存、磁盘资源可以通过碎片整理、数据平衡技术提升集群资源利用率；虚拟化软件可以在线进行版本升级。

国产化平台要求：支持一云多芯，同时支持 X86、ARM 等主流国产芯片，实现异构集群统一管理；虚拟机具备丰富的操作系统兼容能力，支持麒麟、统信等主流国产化操作系统；虚拟机支持共享 CPU 模式；支持提供多种虚拟机规格，并支持虚拟机在线变更服务器 CPU 和内存配置；支持弹性伸缩功能，根据业务的需求和策略，自动调整计算资源大小，并支持用户定时执行伸缩规则，从而实现自动扩展或者收缩计算资源；块存储支持用户自助管理，包括创建、挂载、卸载、删除等；并支持对主机的系统盘和数据盘进行备份，保障数据的安全性；对象存储支持主流的 S3 协议访问对象文件，并支持对象分段上传；负载均衡调度算法支持轮询算法、最少连接算法、哈希算法。

**10.2.1.4 云网络系统要求**

核心骨干设备、出口设备、骨干线路等需要支持冗余备份，云内骨干线路带宽 $\geq 40\text{Gb}$  带宽，服务器业务 $\geq 10\text{Gb}$  带宽，核心骨干设备可以保证大规模业务迁移，无缝扩容需求；支持对云平台内的网络设备进行统一管理；网络控制器需集群部署。

#### 10.2.1.5 出口网络要求

公网 IP 地址需求：不少于 1 个 C 类互联网 IP 地址，后续可根据实际使用情况扩容。

互联网带宽：需提供至少  $2*1\text{Gbps}$  带宽接入公网，互为灾备，后续可根据实际使用情况扩容。

政务外网带宽：需开通不少于 2 条的裸光纤链路，通过双路由接入的方式从云平台所在机房至招标人指定的申港大道 200 号政务外网机房，万兆带宽。

#### 10.2.1.6 平台高可靠要求

云平台使用的网络安全设备、服务器、存储等设备都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可以接管业务。云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响。

#### 10.2.1.7 平台安全要求

非国产化平台和国产化平台均需符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求。

为了保证平台的安全、稳定运营，需制定完善的安全运维管理体系及安全管理制度规范，对不同的安全区域、安全保护对象明确安全责任人；提供符合信息安全等级保护三级要求的云平台基础安全和应用系统安全的服务内容。

需提供安全监控，安全监控内容包含但不限于网络流量监控、各个安全设备的日志记录监控、安全设备运维操作监控和云资源运行状态监控等，并提供安全事态分析，满足用户不同安全级别业务系统的安全需求。

中标人建设的浦东政务云平台需满足包括但不限于如下安全要求：物理安全、网络安全、主机安全、平台安全等内容。

1) 物理安全：中标人用于建设浦东政务云的机房需具备防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应等能力。

2) 网络安全：中标人需针对浦东政务云平台按照国家网络安全等级保护基本要求要求建立一套网络安全防护体系，对网络边界处提供访问控制、病毒过滤、防攻击、防入侵、防篡改等立体安全防护，保护平台内部网络通信安全。

访问控制：浦东政务云平台在各网络边界处应部署安全访问控制设备，包括防火墙、IPS 等，能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。支持按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访问。

安全审计：中标人需对浦东政务云平台使用网络设备运行状况、网络流量、用户行为等进行日志记录，能够根据记录数据进行分析并生成审计报告，同时对系统审计的记录进行有效安全保护，避免受到未预期的删除、修改或覆盖等不安全操作。

入侵防范：配备有 IDS 或 IPS 入侵防范、检测系统，实现的实时防范功能应包括：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等非法网络攻击行为，当检测到攻击行为时，系统将详细记录相关信息，同时在发生严重入侵事件时具备报警、记录功能。

3) 主机安全：中标人需对浦东政务云平台主机的物理安全进行防护，主机系统应启用访问控制

功能，依据安全策略控制用户对资源的访问权限，通过系统的技术维护措施严格限制默认账户的访问权限。

4) 平台安全：包括虚拟化及云运维管理平台的安全保护，如果云运维管理平台需要数据库的支持，应保护好云运维管理平台的数据库安全，设置强壮复杂的密码策略、备份数据库和配置相关的网络安全服务；云运维管理平台的访问许可应加强管理，删除不需要的用户账号，同时针对云平台本身应用提供应用安全防护能力。

5) 委办局单位部署在浦东政务云平台中的应用系统在执行国家及本市有关电子政务信息安全管理办法的过程中，若发现重大安全事故或者安全隐患时，中标人需要配合进行安全整改。

#### 10.2.1.8 应用安全要求

为了使在政务云环境下的应用系统能够满足信息安全等级保护三级要求，需针对应用系统提供安全防护能力，具体需求如下：

1) 入侵防御服务：针对应用提供实时的互联网出口及政务外网出口入侵防御，对网络流量进行检测，过滤各种可疑流量，并实时监控内网安全状况，防止大规模僵尸网络的形成，同时为全网检测提供数据支撑。

2) 用户管理服务：为每个使用单位下不同租户之间资源进行默认隔离。一个租户下可以设立不同项目，每个项目可视为一个资源集，通过 VPC 的功能进行隔离。并且提供在租户下创建和管理用户的功能、提供角色创建及管理功能、提供登录策略的创建及管理功能；为用户登陆后的工作台，显示关键的运营数据；根据使用单位需求开启 ssh, ftp 等服务。

3) 常规安全漏洞扫描：对政务外网及互联网出口 IP 地址、主机或按用户要求进行漏洞扫描，并提供漏扫报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

4) 网络访问控制服务：针对应用提供实时的互联网出口访问控制、政务外网出口访问控制、虚拟网络间访问控制等，针对 HTTP、FTP、TELNET、SMTP、POP3、P2P 等网络协议进行识别和过滤；按照等级保护三级相关要求，在网络边界实时监测恶意代码、敏感内容并进行实时告警。

5) 数据库审计服务：通过在用户数据库主机上安装探针程序，将外部访问数据库流量镜像到相关审计设备的一种安全审计服务，对用户访问数据库行为的记录、分析和汇报，提高数据资产安全。

6) 日志审计服务：对网络日志、安全日志、主机日志和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件；为运维提供全局的视角，一站式提供数据收集、清洗、分析、可视化和告警功能，并且日志留存 180 天。

7) 用户身份认证服务：用户管理的配套登录认证服务，为用户管理服务提供身份认证支撑，为政务云用户安全接入云平台的统一身份认证，通过双因素认证方式实现用户认证，防止用户身份冒用。

8) 在线防护 WAF：网站前端提供在线 WAF 防护系统，用于防御 SQL 注入、XSS 跨站脚本、常见 Web 服务器插件漏洞、木马上传、非授权核心资源访问等 OWASP 常见攻击，并过滤海量恶意 CC 攻击，避免网站资产数据泄露，保障网站的安全与可用性。

9) 网页防篡改：在网站服务器上部署网页防篡改软件，为用户提供网页内容监测，及时修复被篡改网页内容，同时记录篡改事件的相关日志，为监管部门提供调查的凭据。

##### 10.2.1.8.1 功能与技术指标要求

服务名称	指标参数
在线防护 WAF	内置 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、

服务名称	指标参数
	<p>WEBSHELL 后面攻击、COOKIE 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，支持超过 3000 种 Web 服务器漏洞特征规则</p> <p>支持对 HTTP 和 HTTPS 异常请求协议检测和防护攻击，检测内容包含 HTTP 和 HTTPS 请求信息的方法及参数长度等</p> <p>支持基于源 IP、Referer、URL 等多种组合条件对 CC 攻击进行检测，检测指标为检测时间和触发阈值</p> <p>支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞</p>
日志审计服务	<p>支持对用户分组的权限角色设置，统一提供日志来源、告警、已存搜索、仪表盘、趋势图、自定义字典、字段提取规则、报表、定时任务等各种资源的权限控制功能</p> <p>支持查询脱敏数据，修改他人密码，下载数据，资源导入导出权限的控制</p> <p>支持定义该角色用户单次检索最大可以横跨多长时间范围</p> <p>支持通过 url 控制每个用户角色访问具体功能页面地址的权限</p> <p>支持将指定的日志来源可读权限分享给指定用户，支持设定分享的有效时长，过期自动回收</p> <p>用户可利用主机名、应用名、标签三项内容的任意组合，定义搜索范围和授权不同用户的日志访问范围。被限定范围的用户只能在限定范围内查询，且不能建立新的日志来源。 用户可以使用日志来源来区分研发，测试和生产等不同类型的日志</p> <p>支持设置自定义索引的切分周期和过期时间：小时、天、周、月、年</p> <p>支持定义一个 appname，零到多个 tag 为接入规则，指定匹配该规则的输入以低/中/高优先级写入索引</p> <p>支持根据一到多项的 appname、tag 或日志原文的正则匹配规则，完成数据分发导入</p> <p>支持设置自定义索引的冷却时间，冷却索引可以通过延缓加载速度来释放部分内存资源</p> <p>支持设置自定义索引的过期大小，索引空间超过这个大小后将被清理</p> <p>支持 syslog 上传，文件目录监听，snmptrap 接收，snmpget 接收，脚本上传，web 上传，数据库采集，对接 kafka / mq 消息队列，对接 flume 数据源，对接 hdfs 数据源，对接 redis 数据源，对接 odps 数据源，对接 nmon 数据源，对接 netflow 数据源，对接 countly 数据源，对接 Docker 数据源，对接 logstash 数据源，对接 Packetbeat 嗅探，beats 上传，压缩文件采集，systemd-journald 日志上传，对接 H3Csessionflow 数据源</p> <p>支持 linux 性能监控、支持 windows 性能监控</p> <p>支持定时调用用户自定义脚本，将其输出作为日志上传</p> <p>支持操作系统网络及进程连接数据采集</p>

服务名称	指标参数
	<p>多行日志管理，对于如应用服务器经常产生对多行日志，通过配置 agent 合并规则，可将多行日志合并为一个事件整体发送到统一日志平台</p>
	<p>支持自动识别多行规则，支持自动识别字符编码，支持自动识别及自定义时间戳解析规则</p>
	<p>支持正则表达式，kv/xml/json 自动解析，数值转化，url 解码，user agent 解析，时间戳识别，字段分拆，syslog pri 解析，geo 地理位置信息解析，固定电话归属地解析，手机号归属地解析，hex 转换，字段脱敏配置，内容替换，新增扩展字段，自定义字典，结构体解析，重定向，script 脚本解析，dissect 解析，extract 正则解析，base64 解码</p>
	<p>所有的解析功能，必须在 Web 界面完成，不得编译源代码、提交版本等方式完成，需要极其精简的方式完成日志解析工作。</p>
	<p>支持通过划选字段自动生成正则表达式，支持批量验证正则</p>
	<p>支持可选在某字段值大于、小于、等于、包含、非空、正则匹配等条件下才运用某个解析器；支持在解析器解析成功时，给事件添加新字段值，字段名称和值均支持变量引用</p>
	<p>支持界面查看字段提取规则的性能统计情况</p>
	<p>全文检索、短语(多个词中间空格)搜索、字段过滤、逻辑运算搜索、数值范围搜索(数值比较运算，如&gt;,&lt;,&lt;=,&gt;=等)、通配符搜索、简单正则表达式；</p>
	<p>高级搜索，包括支持管道符、产生新增字段、分组查询、子查询、联合查询、字段挑选、条件过滤、结果排序、数据量过滤、字段重命名、分桶查询、统计查询、移动标准差、移动均值、时序预测、去重、行列转换、自动回归、动态提取，json 提取，序列映射，多值拆分，多值归并，时序图，制造结果，输入映射，输出映射，时序弯曲</p>
	<p>流式搜索，支持搜索任务暂停，恢复，中止，支持对搜索结果下载（txt，csv 或 json 格式）</p>
	<p>支持在事件列表上点击日志原文部分内容，生成附加查询语句，产生新增字段，通过算术运算、字符串拼接、empty、abs、ceil、floor、min、max、log、coalesce、if、case、len、upper、lower、substring、trim、match、tolong、todouble、tostring、formatdate、parsedate、format、typeof、isnum、isstr、relative_time、cidrmatch、urldecode 等函数方式生成新字段</p>
	<p>支持在查询时对日志原文中部分字段信息进行提取，并可实时对提取出来的字段信息进行进一步分析</p>
	<p>支持由用户自定义搜索宏，在搜索语句中可以通过反引号引用</p>
	<p>预置事件技术统计，时间分段统计，数值分段统计，时间直方图，数值直方图，字段值分类统计，字段数值统计，累计百分比统计，百分位查询统计，行政区域分布图</p>
	<p>自定义图形支持以饼图、条带图、折线图、区域图、柱状图、散点图、单值图、区线图、和弦图、迷你图、桑基图、玫瑰图、力引导图、和弦图、循序</p>

服务名称	指标参数
	图等任意形态进行数据可视化
	支持服务器性能指标（CPU、内存、I/O、流量等）的收集与分析，实现同比、环比分析，实现趋势预测、指标超出合理区间外的告警。
	支持操作系统日志（linux、aix、windows 等）的收集与分析，实现安全审计、操作行为、用户行为分析。
	支持进程信息（进程名、进程号、进程启动命令、进程开始时间、进程占用 CPU 大小等）的收集与分析，实现进程的统一管理、未知进程告警。
	支持中间件访问日志、运行日志的收集与分析，实现访问请求关系、运行状态的分析。
	支持服务器网络连接信息（netstat）的收集与分析，支持进程等连接状态的关联分析，分析进程关系，生存网络主机拓扑和进程连接拓扑
	支持设置仪表盘标签页的自动刷新频率：30 秒、1 分钟、5 分钟
	支持手动调整趋势图位置和大小，支持时间过滤，字段过滤的全局配置
	支持点击操作自动跳转到某个仪表盘，并将所选的下钻变量值（\${click.name1}, \${click.value1}, \${click.name2}, \${click.value2}, \${row.<fieldname>}），传递给目标地址的一到多个过滤/输入项
	支持趋势图下钻配置，包括跳转到原始日志，跳转到本仪表盘趋势图，跳转到其他仪表盘趋势图
	支持事件数告警、字段统计告警、连续统计告警、基线对比告警、统计告警
	支持告警抑制，告警扩展搜索，告警等级配置，支持告警恢复通知
	支持告警等级设置，多阈设置，分等级推送
	支持扩展搜索，并支持将扩展搜索结果绘制成趋势图，插入告警内容中
	支持对指定时间范围内，指定告警分组内的所有监控项暂停运行
	对告警事件支持信息归并，告警处理，告警忽略，填写处理意见，触发处理操作
	对告警记录支持同比，环比方式分析告警状态的等级分布，以及浮动涨跌幅
	支持邮件，短信，syslog，自定义插件等方式告警发送方式
	支持从所有统计视图上点击保存成定时任务，采用标准的 crontab 式语法设定任务运行时间
	支持对定时任务统计结果进行二次统计，提升统计速度
	支持根据指定的 JDBC 配置推送定时任务结果到外部数据库表
	支持从趋势图清单拖拽添加多个报表元素到报表中
	支持复选 PDF、HTML、DOCX、XLSX 等邮件格式发送报表
	支持选择多种内置的报表布局方式，支持移动报表元素排序，改变其在布局中的位置
	支持定义拓扑图节点的归属分组，同分组的节点将自动聚合在一个图层内
	支持定义拓扑图节点的数值展示布局，包含上下左右的不同组合

服务名称	指标参数
	支持定义在非编辑模式下，点击节点时，钻取跳转的目的地址
	支持对布局中的每个数值，均可定义其搜索语句、时间范围、颜色范围等配置
	支持设定定时刷新拓扑图数据的频率
	支持知识包括标题、标签、事件代码、描述、解决方案的管理
	支持选择特定分组，查看组内知识
	支持关键字搜索知识的全文内容，并高亮展示搜索结果列表
	支持界面化 agent 管理，包括启动，停止，升级，agent 分组等
	支持界面配置 agent 发送速率限制和数据压缩功能
	支持某个数据采集源采集的启动和停止，支持界面指定清空 agent 上单个采集配置缓存或整体缓存，支持下发特定的单一数据源配置信息至指定 agent 列表
	支持界面化监控日志集群各模块的性能状态，支持各模块告警自动发现
	支持界面化升级软件版本，启停服务，支持界面化横向扩展机器，支持界面化模块参数配置
	配置类 API 包括，字段提取规则映射 API，告警配置 API，agent 采集配置 API，用户管理 API，资源分组 API，日志来源 API
	搜索类 API 包括，上下文查询 API，下载任务 API，搜索 API
	支持插件安装为一个新的 grafana 数据源类型；支持对数据源搜索并展示 timeseries 和 table 两种类型效果
	具备日志生命周期管理功能，能够对索引数据每天进行备份、历史数据永久归档、数据恢复功能，且完全通过 WEB 界面配置操作完成
	列表展示日志经过聚类后的模式结果
	对每个聚类内部事件的趋势图采用 sparkline 效果展示
	展示每个聚类内部事件数，以及事件数在全部数据中的占比
	支持点击后，查看该聚类内的全部日志原文
	单机环境下，以每条日志 300 字节为例，每秒 EPS>3000
	通过编写正则表达式，对数据进行字段抽取等格式化定义操作，以每条日志 300 字节为例，每秒 EPS>3000
	在数据总量为 5 千万条的环境下，通过 5 个（包含 and、or、not、数值范围、全文模糊匹配）条件，进行检索。检索完成时间小于 10 秒
	在数据总量为 5 千万条的环境下，能够快速地完成即席分级统计(不小于三层)。统计任务延时小于 10 秒
	支持对用户分组的权限角色设置，统一提供日志来源、告警、已存搜索、仪表盘、趋势图、自定义字典、字段提取规则、报表、定时任务等各种资源的权限控制功能
	支持查询脱敏数据，修改他人密码，下载数据，资源导入导出权限的控制

服务名称	指标参数
	支持定义该角色用户单次检索最大可以横跨多长时间范围
用户管理及身份认证服务	<b>Web 访问方式:</b> 通过系统的 Web 页面控件直接访问服务器或通过 WEB 页面调用本地工具（含数据库官方客户端）直接访问服务器
	多类型浏览器支持: IE (6-9)、firefox、chrome、safari
	web 方式访问支持所有远程协议
	web 访问方式支持历史访问配置参数自动记忆功能
	web 访问方式支持直接输入目标 IP 快速连接功能
	通过 web 方式使用 SSH 协议支持 clone session 功能; 支持直接调用 SFTP 功能; 支持设定窗口颜色、保存屏幕内容、打印屏幕内容、复制粘贴等功能
	通过 web 方式使用图形化远程操作协议, 支持自适应浏览器窗口大小
	通过 web 方式使用 RDP 协议支持剪切板、磁盘映射功能
	客户端访问方式: 支持通过管理员常用的客户端(如 SecureCRT、PUTTY、Mstsc、PLsql、SQLplus 等)直接连接堡垒机再访问到服务器
	支持客户端(SecureCRT、putty)clone session 功能
	支持 secure shell client 软件中直接调用 sftp 功能
	登录资源菜单访问: 客户端访问审计系统即可显示用户能访问的主机资源菜单, 用户通过字符菜单或图形菜单选择列表方式直接访问服务器
	菜单方式访问支持所有协议
	支持多种认证方式: 本地密码认证、UsbKey 认证、第三方 CA 证书认证、RSA 动态口令认证、安盟动态口令认证、RADIUS 认证、LDAP 认证、AD 域认证以及短信认证
	内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色
	支持 SSO 功能, 运维人员不必输入服务器帐号及密码, 无需进行二次登录认证
	支持基于用户(用户组)、目标设备(设备组)、系统帐号、协议类型、生效时间范围、源 IP 地址等条件组合设置访问控制策略
	支持粗放式访问授权模式, 授权条件仅基于运维用户(用户组)和目标主机 IP 地址段, 不限制使用的系统账号及协议等其它条件
	支持审批模式: 运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行, 否则无法进行任何操作
	支持备注模式: 运维用户访问服务器前必须先填写该次访问的维护目的等内容, 否则不能进行访问操作
支持工单授权功能: 通过运维人员申请或管理员下发工单的方式来赋予运维人员访问目标服务器的权限, 且有工单生效时间限制	
支持协同操作功能	
支持批量执行功能及对批量执行结果进行成功或失败判断	

服务名称	指标参数
	<p>支持按用户（用户组）、目标设备（设备组）、系统帐号、命令集和生效时间等内容或按访问授权策略设定安全事件规则；支持指令黑白名单</p> <p>支持对违规操作的指令（黑名单）进行告警、忽略处理、自动阻断或指令审批</p> <p>支持以屏幕、邮件、SYSLOG、Snmp Trap、短信方式实时发送告警信息</p> <p>针对 SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计；记录发生时间、发生地址、服务端 IP、客户端 IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息</p> <p>针对 RDP、VNC、X11 等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端 IP、客户端 IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息</p> <p>能够记录 RDP 协议中的活动窗口名称、删除文件等动作，并能记录 RDP 会话中的键盘输入信息</p> <p>支持以 WEB 在线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件</p> <p>支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作</p> <p>支持下载回放文件到本地保存，并通过厂家专用播放器查看，防止会话视频记录泄密</p>
数据库审计服务	<p>支持主流数据库 Oracle、SQL-Server、DB2、MySQL、informix、sybase、Postgresql、Cache、MongDB、K-DB、达梦、人大金仓、南大通用</p> <p>支持同时审计多种数据库及跨多种数据库平台操作</p> <p>支持 HTTP 请求审计，可指定 GET、POST、URL、响应码进行精细审计；</p> <p>支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌</p> <p>支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；</p> <p>深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库类型、操作类型、SQL 语句、SQL 模版、客户端程序名、响应码、影响行数、返回行数、SQL 预计响应时间；</p> <p>支持三层架构下的真实 IP 追踪；</p> <p>允许查看 SQL 语句会话日志；</p> <p>支持客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数、影响行数、响应内容等实现对敏感数据库操作的精细监控；</p> <p>支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况；</p>

服务名称	指标参数
	支持以源 IP、业务主机、操作类型、SQL 模版、数据库用户为维度的数据库行为排行；
	支持以源 IP、业务主机、操作类型、SQL 模版、数据库用户为维度的数据库行为趋势；
	支持执行 SQL 语句失败分析，包括登录失败排行，SQL 语句失败排行；
	支持吞吐量分析，包括 SQL 语句吞吐量排行、SQL 语句吞吐量趋势、SQL 操作类型吞吐量排行、SQL 操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势；
	支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询；
	支持报表收藏，报表导出 PDF；
	支持报表订阅，自定义报表；
	精细化日志秒级查询
	通过 SQL 串模式抽取保障磁盘 IO 的读写性能；分离式存储 SQL 语句保障数据审计速度快
	TB 级日志秒级查询、支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多 SQL 语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询
	自定义报表拖拽
	通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。
	支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询。
	支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。
	内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；
	支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断；
	可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施

服务名称	指标参数
	<p>数据库威胁分析：可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助企业快速溯源。</p> <p>支持基于 SQL 命令的 webshell 检测</p> <p>支持 SIP 联动实现数据外发泄密分析</p> <p>支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询</p> <p>支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行</p> <p>支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险趋势</p>
网页防篡改服务	<p>支持各类网页文件的保护，包括静态和动态网页以及各类文件信息</p> <p>同时支持防护模式和监控模式两种模式的防篡改模式</p> <p>系统支持在断线情况下对网页文件目录的防护功能</p> <p>支持文件多线程同步，并可以设置文件空闲同步时间周期、发布时间周期等设置</p> <p>支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码</p> <p>一键启停所有对监控端的保护</p> <p>在与其它模块网络断开的情况下能防止文件被篡改</p> <p>支持基于目录、进程、IP、用户等进行设置篡改规则</p> <p>提供自我保护机制，网页防篡改客户端需有第三方认证码方可卸载</p>
网络访问控制+入侵防御服务	<p>支持基于区域、IP 地址、域名、端口、用户、应用、服务、时间、分组等多个维度设置应用控制策略。</p> <p>流量管理功能</p> <p>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。</p> <p>产品内置应用特征识别库，支持不少于 3000 种应用规则，支持对游戏、P2P 下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。</p> <p>支持基于区域和 IP 地址配置连接控制策略，对特定 IP 地址设置最大并发连接数，实现内部资源保护和系统资源合理分配。</p> <p>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。</p> <p>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</p>

服务名称	指标参数
	TCP 协议异常报文攻击防护。
	支持 ARP 欺骗类攻击防护。
	单防火墙组件的吞吐能力根据客户要求进行弹性设定，最高可支持 10G 安全业务防护能力
	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。
	支持自定义病毒白名单，可基于文件 MD5 值和下载 URL 设置文件杀毒排除策略。
	支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告。

### 10.2.1.9 平台密码要求

国产化平台需符合《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）要求。

需部署服务器密码机、SSL VPN、安全认证网关、签名验签服务器、数据库加密网关、文件加密存储网关，配置要求如下：

#### 10.2.1.9.1 密码机要求

1) 技术标准：同时符合 GM/T 0030《服务器密码机技术规范》、GM/T 0028《密码模块安全技术要求》技术要求。

2) 支持密码算法：支持 SM2 国密非对称算法，支持 RSA1024、RSA2048、RSA4096 等国际非对称算法；支持 SM1、SM4 等国密对称算法，支持 DES、3DES、AES 等国际对称算法；支持 SM3 国密摘要算法，支持 SHA1、SHA256、SHA512 等国际摘要算法，支持 RSA 密钥生成与查看，提供 1024 位、2048 位、4096 位 RSA 密钥生成算法及密钥备份和恢复。

3) 随机数生成：采用国家密码管理局批准的双硬件物理噪声源生成真正随机数，至少采用两个独立的物理噪声源芯片实现，保证随机数质量。对外生成随机数的接口，应采用硬件生成密码计算涉及的随机数，包括非对称密钥对生成、非对称加密、签名运算，都必须采用硬件生成的随机数。

4) 扩展能力：支持 GM/T 0018、GBT 36322、JCE、PKCS#11、RESTful 等接口。

#### 10.2.1.9.2 SSL VPN 要求

1) 技术标准：符合 GM/T 0026《安全认证网关产品规范》和 GM/T 0028《密码模块安全技术要求》安全等级第二级要求。

2) 支持多类型证书：支持 RSA、SM2、ECC 多种格式的站点证书，支持无私钥证书文件、PFX 格式证书、证书与密钥双文件、双证书、双证书-密钥不落地多种格式站点证书。

3) 反向代理：支持通过反向代理的方式，隐藏后端应用的真实地址，支持基于 SSL 协议配套客户端软件，实现基于 TCP 协议应用的透明代理访问，用户直接访问服务器目标，不改变用户使用习惯。

4) 黑名单：支持黑名单文件管理，支持黑名单自动更新，支持从 WEB 站点下载、从 LDAP 服务器下载以及手工导入黑名单三种模式；黑名单容量不小于 100 万条，每条查询速度不大于 5ms。

5) 高可用：支持双机热备，支持第三方负载均衡。

#### 10.2.1.9.3 安全认证网关要求

1) 技术标准：符合《GM/T 0026》安全认证网关产品规范要求，《GM/T 0028》密码模块技术要求

安全等级第二级要求。

2) 可信身份传递：将用户个人数字证书信息通过绑定在 HEADER, COOKIE 中等方式传递至后端应用；绑定信息可以使用 HMAC-SM3 算法保护信息真实性和完整性，防止伪造用户登录。

3) 站点证书：支持 RSA、SM2 多种格式的站点证书，支持无私钥证书文件、PFX 格式证书、证书与密钥双文件、双证书、双证书-密钥不落地多种格式站点证书。

4) 应用优化：支持 HTTP 压缩、Web 高速缓存、HTTP 请求和响应改写、HTTP 反向代理转发和 HTTP 重定向等，更好地支撑业务系统对接。

5) IP 透传：在代理 TCP 应用、HTTP 应用时，使用客户端真实 IP 端口访问后端应用服务器。

6) 高可用：支持双机热备，支持第三方负载均衡。

#### 10.2.1.9.4 签名验签服务器要求

1) 技术标准：符合《GM/T 0028》密码模块技术要求安全等级第二级要求，遵循 GM/T 0029 《签名验签服务器技术规范》。

2) 支持密码算法：包含 SM2, 国际 ECC, RSA2048, SM1, SM4, AES, DES, 3DES 等。

3) 接口服务：支持 PKCS#1 签名验签、PKCS#7 签名验签，支持 XML 签名验签、PDF 签名验签、APK 签名验签。

4) 数据密钥管理：支持对非对称密钥、对称密钥进行生命周期管理。

5) 监控与告警功能：支持对系统 CPU、内存、磁盘、服务状态、证书过期、电源异常情况进行告警。

6) API 及 SDK：支持 RESTFUL、TCP 方式的接口调用和 Java 和 C 语言的 SDK。

7) 高可用：支持双机热备，支持第三方负载均衡。

#### 10.2.1.9.5 密钥管理系统

1) 技术标准：产品符合 GM/T 0034 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》，《GM/T 0028》密码模块技术要求安全等级第二级要求。

2) 支持密码算法：支持国产 SM2、SM4、RSA、AES、DES 算法。

3) 数据库透明加解密引擎能力：支持通过数据库加解密引擎进行数据库透明加解密，支持数据库全库加解密，数据表整表加密和列加密。

4) API 及 SDK：支持 http、https、thrift 多种通讯协议,并支持国密 SSL 配置。

5) 安全性设计：支持三层密钥结构的密钥保护机制，包括系统根密钥、用户主密钥、数据密钥；支持租户级和应用级密钥隔离。

6) 兼容性：密钥管理系统服务端和 SDK 可与部署在 redhat、麒麟、统信、CentOS 操作系统环境上的应用集成。

#### 10.2.1.9.6 文件加密存储网关要求

1) 技术标准：符合 GM/T 0028 《密码模块安全技术要求》安全等级第二级要求。

2) 支持密码算法：支持 SM1/SM2/SM3/SM4 等国密算法。

3) 完整性功能：基于 SM3-HMAC 的文件存储完整性功能，完整性状态包括正常、新增、删除、修改等；

多种存储设备支持：包括本地磁盘和 SAN 存储。

双因素登录：管理员支持 USBKey+数字证书和用户名口令两种身份认证方式。

4) 零改造集成：应用零代码改造集成。

**10.2.1.10 应用密码要求**

根据当前业务系统建设情况与信息安全发展趋势，为全面满足国家密码法律法规、网络安全等级保护制度以及行业数据安全规范中对密码应用的强制性要求，构建安全、可信、合规的密码支撑体系，需为云上的租户提供密码应用服务。具体需求如下：

- 1) 安全认证网关服务：需实现对各业务系统访问入口的集中管控，支持基于数字证书、动态口令等多因素的强身份认证，解决认证分散、强度薄弱的问题。
- 2) 可信密码服务：为应用提供标准的密钥管理、密码运算（如加密、解密、哈希）等基础能力，确保应用层密码使用的规范性与安全性。
- 3) 文件加密存储/签名验签服务：实现对重要电子文件的透明加密存储与安全共享，并为关键业务流程提供数字签名与验证功能，确保数据的机密性、完整性和操作的不可否认性。
- 4) 时间戳服务：为全系统提供权威、可信、准确的时间源，确保所有日志记录、数字签名及交易行为具有法律效力的时间凭证，支撑安全审计与责任认定。

**10.2.1.10.1 功能与技术指标要求**

服务名称	指标参数
安全认证网关服务	具备国家密码管理局颁发的《商用密码产品认证证书》 具备公安部颁发的《网络安全专用产品安全检测证书》
	支持 SM2、SM3、SM4 算法，具有密钥协商、身份认证、SSL 隧道加密等功能。
	应支持口令、证书、短信、SSL 双向认证等方式
	支持国密 SM2/3/4 算法，支持 GM/T 0024-2014 《SSLVPN 技术规范》定义的国密 SSL 协议
	支持通过反向代理的方式，隐藏后端应用的真实地址，用户仅知道网关暴露的地址。支持基于 SSL 协议配套客户端软件，实现基于 TCP 协议应用的透明代理访问，用户直接访问服务器目标，不改变用户使用习惯。
	支持将非国密浏览器的传输通道升级为国密 SSL 协议通道
	支持在同一个服务实例中，配置 RSA 和 SM2 两张站点证书，并同时启用，根据客户端的算法能力进行自动适应。
	支持超过 100 万条目数的证书黑名单
	支持代理后端启用 SSL 的应用，包括后端启用双向认证（客户端认证）的应用
	支持保护 B/S、FTP、远程桌面以及通用 C/S 应用的传输通道，并对用户提供透明无感的体验
	支持对后端应用进行连接复用，降低后端应用的长连接数量
	支持采用会话级事件证书或代理证书，一次一密向后端传递用户真实身份
	支持 HTTP 压缩、Web 高速缓存
	支持明文流量镜像，将 SSL 流量解密后发送给外部风险分析服务进行分析
	支持以 HTTP 注入（Cookie/Header）的方式将用户的证书信息传送给后台应用，同时可以对注入的信息进行签名，防止伪造用户登录
	支持配置和审计日志的完整性检查
	支持国产操作系统；支持国产 CPU
在 8 核 CPU，16G 内存的云平台虚拟机环境下：最多并发连接数不低于 5 万次连接；吞	

服务名称	指标参数
	吐率不低于 400 MB/秒；新建连接数不低于 300 次连接/秒。
签名验签服务	具有国家密码管理局颁发的《商用密码产品型号证书》
	支持证书校验，包括：证书链校验、证书有效性校验、CRL/OCSP 校验
	支持证书解析功能，包括：证书 DN，证书 SN，生效时间、失效时间、证书扩展项
	支持多种 SM2 算法的加密格式，包括国密格式和 ASN.1 格式
	支持通过手动上传 CRL、自动从 HTTP/LDAP 更新 CRL 等方式管理证书黑名单，最大可支持 5 千万条目的 CRL
	支持应用级策略配置包含： <ol style="list-style-type: none"> <li>1. 签名策略：如签名格式、是否包含时间、是否返回证书</li> <li>2. 加密策略：如加密格式、是否包含时间、是否返回证书</li> <li>3. 验证策略：忽略证书有效期、验签到具体时间、延期天数</li> <li>4. 弱算法过滤：指定若干算法为弱算法，并拒绝提供对应算法的服务请求</li> <li>5. IP 白名单：限制应用的源 IP 地址</li> </ol>
	提供文件数据签名与签名验证功能
	提供数字信封功能对数据进行加密传输，只有指定的信封接收者可解密数据
	支持管理应用访问签名验签服务的 AK/SK 凭证，包括查看和更新
	支持按需创建/删除新的管理类角色并对角色权限进行动态话配置
	全面系统管理及审计功能：支持日志 SYSLOG 远程发送、日志归档、系统备份恢复、支持 IPV6、三权管理
	支持国产操作系统；支持国产 CPU
	8 核 CPU，16G 内存的云环境虚拟机环境下：SM2 算法签名效率≥2000 次/秒；SM2 算法验签效率≥3000 次/秒
可信密码服务	具有国家密码管理局颁发的《商用密码产品型号证书》
	提供对接主流国产数据库，支持 SM4 算法数据加密的互认证证明材料
	支持三层密钥结构的密钥保护机制，包括系统根密钥、用户主密钥、数据密钥；支持租户级和应用级密钥隔离。
	数据库透明加解密引擎能力： <ul style="list-style-type: none"> <li>支持通过数据库加解密引擎进行数据库透明加解密</li> <li>支持数据库全库加解密，数据表整表加密和列加密。</li> <li>支持常见的国产化数据库使用国密 SM4 算法加解密。</li> </ul>
	支持 http、https、thrift 多种通讯协议,并支持国密 SSL 配置，SDK 支持 Java、C 语言
	密钥管理系统服务端和 SDK 可与部署在 redhat、麒麟、统信、CentOS 操作系统环境上的应用集成
	应用通过接口、SDK 和数据库加解密引擎访问管理系统，均支持基于 GM/T 0024 标准的通信保护
	应用访问服务支持基于 GM/T 0024 标准的通信保护
	支持对应用访问凭证进行管理

服务名称	指标参数
	支持密钥轮换功能
	支持调用加解密、签名验签、杂凑运算等密钥运算能力
	单次 API 调用的平均响应时间不超过 200ms
	支持国产操作系统；支持国产 CPU
	在 8 核 CPU，16G 内存的云平台虚拟机环境下：并发数≥128 个会话连接；SM4 加解密速度≥60Mbps；数据库加解密速率≥60Mbps；数据库操作性能损耗≤20%
时间戳服务	具有国家密码管理局颁发的《商用密码产品型号证书》
	支持 RESTFUL、TCP 方式的接口调用和 Java 和 C 语言的 SDK
	支持对导入系统的证书链进行生命周期管理，包括导出、导入、删除、查询等操作
	支持配置各类时间源，支持 NTP 和 SNTP 协议，能够通过授时中心、卫星（北斗、GPS）CDMA 等方式进行时间同步，确保时间的有效性
	支持管理应用访问签名验签服务的 AK/SK 凭证，包括查看和更新
	支持按需创建/删除新的管理类角色并对角色权限进行动态话配置
	支持通过备份文件进行恢复
	支持配置 IPv4/IPv6 白名单，限制特定的 IP 才能访问本服务
	支持对数据和文件进行签名验签，最大签名数据或文件可达到 1G 字节。
	支持 GB/T20520、GM/T0033、RFC3161 标准、RFC2630 标准等格式的时间戳签发和验证功能
	授时精度:<5us，守时精度:<28us，卫星同步精度纳秒级，NTP 同步精度毫秒级
	支持 IPV4/IPV6 方式的管理和服务接口配置
	支持国产操作系统；支持国产 CPU
	8 核 CPU，16G 内存的云平台虚拟机环境下：时间戳生成速率不低于 240 次/秒；验证速率不低于为 110 次/秒；时间同步间隔时间不大于 30 分钟；时间误差不大于 100 毫秒

**10.2.1.11 运维服务需求**

中标人应建立专职的运行维护团队，负责浦东新区政务云平台、网络、安全、备份及算力部分的运维，并为创新技术试点应用提供服务。

**10.2.1.12 设备托管服务要求**

需提供机房整机柜出租服务，提供额外设备托管机柜，托管机柜数量不少于 9 个，单机柜功耗不低于 4000W。

**10.2.1.13 机房技术要求**

项目		参数要求
供电	市电	机房配备双路市电，机架供电可用率为 99.97%，即用户托管的电源系统每月电力中断时间累积不超过 13 分钟
	UPS	机房托管 IT 设备的不间断供电系统应采用冗余等级为 N+1 的交流 UPS 系统
	直流蓄电池	提供双路一类市电保障；电压等级 10KV，市电容量两路共 10000KVA 及以上

	柴油发电机	机房所在建筑或园区采用柴油发电机作为后备电源，油机数量满足 N+1 配 路，并可持续不间断供电 6 小时及以上
	机柜 PDU	每个机柜提供两条 PDU。机柜两路供电，都有不间断电源保障。（含 PDU 电 源系统）
制冷	机房空调	机房所在建筑内制冷系统配置高效能精密空调按照双路市电及油机进行不间 断的电源供给，保障空调运行不受电力影响，配路的精密空调满足 N+1 的冗 余配置，冷通道相对湿度：相对湿度（不大于 60%），露点温度（5.5-15℃） 且不得结露。服务器进风温度：21℃--26℃
安防	视频监控	机房、网络接入间、主要走道和其它重要部位应安装摄像机监视，重要机架及 机柜应单独设摄像机监视，录像保存时间不得少于 30 天
	机房动力监 控	具备配电开关监控、配电参数监测（包括动力配电）、UPS 监控、配电头柜监 控
	门禁	机房重要部位应安装门禁设备，划分不同人员进出不同区域的权限
	保安	安保人员每周 7 天×24 小时值守和监控
消防	消防要求	机房内应配备气体灭火系统，消防系统具备自动报警功能
运行 维护	巡检	机房每天进行 3 次及以上例行巡检，并对机房设备运行状态、环境状态进行 详细记录
	应急机制	做好机房应急预案，在网络、电力、安全等各方面提供协助，确保采购人应急 人员、设备和供应商能在最短时间内能够进入机房进行应急处置

10.2.2 资源配置要求

服务	分类	资源总量	单台配置	备注
服务 1	非国 产化 云资 源	不少于 3256 核 CPU、 16593.17GB 内存的可用资源	单台配置不低于 2 路 10 核、 256GB 内存	
		不少于 1528.52TB 普通存储的 可用资源	集中式存储，提供不少于 1100TB 可用的 HDD 存储	
			分布式存储，单台配置不低于 12 块 12TB 的 HDD 数据盘	
		不少于 96.16TB 高性能存储的 可用资源	分布式存储，单台配置不低于 8 块 7.68TB 的 SSD 数据盘	
		不少于 1636 核 CPU、17920GB 内存的物理机资源	单台配置不低于 2 路 6 核、 128GB 内存	
		不少于 691.2TB 普通存储的物 理机资源	物理机挂载存储，提供不少于 691.2TB 的 HDD 数据盘	
		不少于 7.5TB 高性能存储的物 理机资源	物理机挂载存储，提供不少于 7.5TB 的 SSD 数据盘	
	国产化 云资 源	不少于 582 核 CPU、3641.34GB 内存的可用资源	单台配置不低于 2 路 32 核、 768GB 内存	

服务	分类	资源总量	单台配置	备注
	算力资源	不少于 392 核 CPU、7168GB 内存、56 块推理卡的推理用算力资源	单台配置不低于 2 路 28 核、1024GB 内存、8 块推理卡，单卡显存不低于 48GB	
		不少于 240 核 CPU、3072GB 内存、23.04TB 高性能存储、24 块训练卡的训练用算力资源	单台配置不低于 2 路 40 核、1024GB 内存、7.68TB 的 SSD 数据盘、8 块训练卡，单卡显存不低于 80GB	
服务 2	国产化云资源	不少于 3293 核 CPU、26214.4GB 内存的可用资源	单台配置不低于 2 路 64 核、1024GB 内存	
		不少于 300TB 普通存储的可用资源	分布式存储，单台配置不低于 12 块 12TB 的 HDD 数据盘	
		不少于 100TB 高性能存储的可用资源	分布式存储，单台配置不低于 8 块 7.68TB 的 SSD 数据盘	
	算力资源	不少于 896 核 CPU、14336GB 内存、215.04TB 高性能存储、112 块推理卡的推理用算力资源	单台配置不低于 2 路 32 核、1024GB 内存、2 块 7.68TB 的 SSD 数据盘、8 块推理卡，单卡显存不低于 48GB	
		不少于 896 核 CPU、8192GB 内存、122.88TB 高性能存储、64 块训练卡的训练用算力资源	单台配置不低于 2 路 56 核、1024GB 内存、2 块 7.68TB 的 SSD 数据盘、8 块训练卡，单卡显存不低于 96GB	
		为服务 1 的推理用算力资源增补不少于 3072GB 内存、49TB 高性能存储	内存及存储增补，提供不少于 3072GB 内存、49TB 的 SSD 数据盘	
		为服务 1 的训练用算力资源增补不少于 3072GB 内存	内存增补，提供不少于 3072GB 内存	
服务 3	算力资源	不少于 1024 核 CPU、12288GB 内存、122.88TB 高性能存储、128 块推理卡的推理用算力资源	单台配置不低于 2 路 64 核、1536GB 内存、4 块 3.84TB 的 SSD 数据盘、16 块推理卡，单卡显存不低于 96GB	
		不少于 768 核 CPU、2048GB 内存、1536TB 普通存储、51.2TB 高性能存储	单台配置不低于 2 路 48 核、256GB 内存、12 块 16TB 的 HDD 数据盘、2 块 3.2TB 的 SSD 数据盘	
		不少于 192 核 CPU、3072GB 内存、23.04TB 高性能存储、24 块渲染卡的渲染用算力资源	单台配置不低于 2 路 32 核、1024GB 内存、2 块 3.84TB 的 SSD 数据盘、8 块渲染卡	
		不少于 1088 核 CPU、13824GB	单台配置不低于 2 路 48 核、	

服务	分类	资源总量	单台配置	备注
		内存、93.44TB 高性能存储、72 块训练卡的训练用算力资源	1536GB 内存、2 块 3.84TB 的 SSD 数据盘、8 块训练卡，单卡显存不低于 96GB	

### 10.3 包 3 技术指标要求

#### 10.3.1 系统功能与技术指标

##### 10.3.1.1 云平台能力要求：

支持 x86 架构与 ARM 架构混合部署，并可提供以下能力：弹性计算服务(ECS)、对象存储软件(OSS)、块存储(EBS)、文件存储(NAS)功能等。

##### 10.3.1.2 云业务管理平台要求：

提供一套云业务管理平台软件，提供云业务管理和业务云上资源监控等相关服务，能够对云上业务进行有效管理。云业务管理平台软件需支持与中标人所提供的云运维监控平台对接的能力、以及在基础设施层各类服务器及其虚拟化环境中部署的能力。云管理平台可提供北向接口、API 接口，接入浦东大数据中心统一云管平台。

##### 10.3.1.3 虚拟化平台要求：

虚拟化平台需支持国产化操作系统。虚拟机之间可以做到隔离保护；虚拟机具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址、MAC 地址等；当虚拟机操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性；支持将多个物理服务器组成集群，可基于 CPU、内存、磁盘等资源利用率进行动态资源调整；虚拟化软件可以在线进行版本升级。

##### 10.3.1.4 云网络系统要求：

需采用国产化网络设备；核心骨干设备、出口设备、骨干线路等需要支持冗余备份，云内骨干线路带宽 $\geq 40\text{Gb}$  带宽，服务器业务 $\geq 10\text{Gb}$  带宽，核心骨干设备可以保证大规模业务迁移，无缝扩容需求；支持对云平台内的网络设备进行统一管理；网络控制器需集群部署。

##### 10.3.1.5 出口网络需求：

公网 IP 地址需求：不少于 1 个 C 类互联网 IP 地址，后续可根据实际使用情况扩容。

互联网带宽：考需提供至少 2\*2GE 带宽接入公网，后续可根据实际使用情况扩容。

政务外网带宽：需开通不少于 4 条 10GE 传输资源，双路由接入，2 条从云平台所在机房至招标人指定的浦东大数据中心世纪大道 2001 号某机房，2 条从云平台所在机房至招标人指定的申港大道 200 号某机房。

政务专线要求：需满足量子通讯、数据要素赋能、智能化应用与治理等应用场景保障要求。

##### 10.3.1.6 平台高可靠要求：

云平台使用的网络安全设备、服务器、存储等设备都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可以接管业务。云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响。云平台提供备份/快照功能，能对政务云平台中的物理和虚拟服务器进行备份，防止存储故障导致数据丢失。

##### 10.3.1.7 云安全需求：

符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求；满足《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）第三级要求的内容。

### （1）平台安全要求：

为了保证平台的安全、稳定运营，制定完善的安全运维管理体系，制定完善的安全管理制度规范，对不同的安全区域、安全保护对象明确安全责任人；提供符合信息安全等级保护三级要求的云平台基础安全和应用系统安全的服务内容。

需提供安全监控，安全监控内容包含但不限于网络流量监控、各个安全设备的日志记录监控、安全设备运维操作监控和云资源运行状态监控等，并提供安全事态分析，满足用户不同安全级别业务系统的安全需求。

中标人建设的浦东政务云平台需满足包括但不限于如下安全要求：物理安全、网络安全、主机安全、平台安全等内容。

1) 物理安全：中标人用于建设浦东政务云的机房需具备防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应等能力。

2) 网络安全：中标人需针对浦东政务云平台按照国家网络安全等级保护基本要求要求建立一套网络安全防护体系，对网络边界处提供访问控制、病毒过滤、防攻击、防入侵、防篡改、内外网数据安全隔离交换等立体安全防护，保护平台内部网络通信安全。提供入侵流量测功能；态势感知通过大数据的离线数据分析能力，对收集的安全日志，进行建模分析，通过大数据手段得出未知威胁攻击、黑客入侵的结论。

访问控制：浦东政务云平台在各网络边界处均应部署安全访问控制设备，包括防火墙、IPS、VPN 网关、安全网关等，能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。支持按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访问。

安全审计：中标人需对浦东政务云平台使用网络设备运行状况、网络流量、用户行为、特权命令等进行日志记录，能够根据记录数据进行分析并生成审计报告，同时对系统审计的记录进行有效安全保护，避免受到未预期的删除、修改或覆盖等不安全操作。

边界完整性检查：中标人通过部署网络行为管理系统、安全审计系统应能够对非授权设备私自连到内部网络的行为及内部网络用户私自连到外部网络的行为进行检查，能根据用户信息、主机信息、IP 信息等准确确定出非法互联位置，并对其进行有效的网络阻断控制。

入侵防范：配备有 IDS 或 IPS 入侵防范、检测系统或安全网关系统，实现的实时防范功能应包括：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等非法网络攻击行为，当检测到攻击行为时，系统将详细记录相关信息，同时在发生严重入侵事件时具备报警、记录功能。

恶意代码防范：中标人在网络的边界处对各种恶意代码进行检测和清除功能，系统应支持自动及手工方式对恶意代码库的升级和检测系统的更新功能。

网络设备防护：中标人所使用的网络设备均应支持对登录用户的身份鉴别功能，支持采用加密用户口令鉴、RADIUS 身份认证等方式，可通过命令行、Web、中文图形化配置软件等方式进行配置和管理，并可通过 ACL 访问控制列表的方式实现对网络设备的管理员登录地址进行限制，所有网络设备用户均应具备唯一标识。

3) 主机安全：对主机的物理安全，主机访问控制方面进行保护。

主机访问控制：主机系统应启用主机系统的访问控制功能，依据安全策略控制用户对资源的访问权限，通过系统的技术维护措施严格限制默认账户的访问权限。

4) 平台安全：包括虚拟化及云运维管理平台的安全保护，支持物理资源与虚拟资源统一管理。

虚拟化安全：支持有代理或者无代理安全方式进行虚拟环境的整体防护。

浦东政务云平台安全：如果云运维管理平台需要数据库的支持，应保护好云运维管理平台的数据库安全，设置强壮复杂的密码策略、备份数据库和配置相关的网络安全服务；云运维管理平台的访问许可应加强管理，删除不需要的用户账号。

浦东政务云平台访问控制安全：用户在访问浦东政务云平台资源过程中支持使用数字证书进行身份认证，包括但不限于中标人维护人员、委办局操作人员、政务云管理单位监管人员。

5) 委办局单位部署在浦东政务云平台中的应用系统在执行国家及本市有关电子政务信息安全管理办法的过程中，若发现重大安全事故或者安全隐患时，中标人需要配合进行安全整改。

## **(2) 国密安全要求：**

基于密码技术为根本，以《网络安全等级保护基本要求》为目标，充分遵循《信息系统密码应用基本要求》的相关要求，建设面向云租户的云密码服务体系，总体构建以密码技术为核心的云密码服务支撑体系，融合密码应用的不同类别和多种场景。

### **1) 整体体系定位：**

本次密码保障体系基于国产密码算法进行建设，为面向上云的信息系统提供密码保障机制，配合整体的国密改造工作，服务对象为浦东新区各委办局适配国密要求的信息系统及国产终端环境。建设一套满足国密要求的云密码保障体系。

### **2) 选用安全合规的密码产品服务：**

本次建设的密码保障体系，所有密码设备均满足商用密码产品认证的合规产品，并提供密码支撑服务。

### **3) 国产密码适配改造：**

本次建设的密码保障体系包括应用系统国密改造适配工作，提供独立的密码改造技术要求、密码接入流程、适配环境，帮助各委办局能快速的推进信息系统国密改造。

## **10.3.1.8 设备托管服务要求：**

需提供数据中心机房空间服务，提供额外设备托管空间服务；需提供机房整机柜出租服务，提供额外设备托管机柜，托管机柜数量不少于 5 个，单机柜功耗不低于 6000W。

## **10.3.1.9 机房技术要求：**

(1) 机房空间要求：政务外网、互联网区域使用物理隔离的不同机房，机柜总数量不少于 120 个，实际使用机柜数量可根据项目需求提供。每机柜提供双路不间断供电，功率不低于 6KW。

(2) 中标人提供的机房可以按照招标人的要求对资源进行物理和逻辑隔离，满足多个云平台资源区和独立资源区域划分要求。独立区域具有门禁控制，控制权按照招标人要求进行管理。

(3) 中标人提供的机房应具备符合国密要求的门禁系统。

### **(4) 机房链路要求：**

政务外网接入：要求承载政务云平台的网络和市政务外网骨干传输网络高效安全地衔接，满足各政务部门接入政务云业务系统的网络需要。根据相关安全管理部门的要求，中标人应支撑安全管理部门放置相关设备到中标人机房或进行专网的接入。

互联网接入：要求承载政务云平台的网络和市政务外网互联网统一出口高效安全地衔接，满足各政务部门业务系统接入互联网的需要，需提供互联网骨干级带宽服务及异网接入能力。

### **(5) 机房环境要求：**

项目	设计指标
环境要求	温度：开机时 23° C ±1° C，停机时 5° C ~35° C；相对湿度：开机时 40% ~55%，停机时 40% ~70%；温度变化率<5° C/h，不得结露。
结构	抗震：乙级以上，抗震烈度 7 度及以上，机房活荷载标准值≥8kN/m <sup>2</sup> ，电池室≥12kN/m <sup>2</sup> ，机房外墙不宜设采光窗，耐火等级：一级。
空气调节	机房专用空调 N+1 冗余，制冷量按 300W/m <sup>2</sup> 估算，总冷量负偏差不大于 5%；空调系统供电应采取双路市电自动切换线路供电，每台空调应采用独立回路供电；
	机房和辅助区应设置空气调节系统，主机房与其它房间、走廊间的压差不应小于 4.9Pa，机房应保持正压，与室外静压差不应小于 9.8Pa；
	主机房内的空气含尘浓度，在表态条件下测试，每升空气中大于或等于 0.5 μm 的尘粒数，应少于 18,000 颗。
供电电源	机房市电容量≥10000KVA，由 2 个供电局向、2 个不同路由同时供电，保证电源不同时受到损坏，配备电源自动切换系统。（需提供双路市电及市电容量证明材料）
后备用电	配备不间断电源系统，N+1 的冗余备份 UPS 系统数量大于一套，所有设备机架供电应由两套不同 UPS 提供，电池满负荷放电时间不少于 30 分钟；
	配备柴油发电机组，保障本系统满负荷情况下可靠供电运行 72 小时。
电源质量	稳态电压偏移范围 3%，稳态频率偏移范围 0.5Hz，输出电压波形失真度≤5%，允许断电持续时间 0~4ms；防雷、防浪涌：保护级别（IEC/VDE 标准）达到 I 级 B 类标准。
接地	接地电阻≤1Ω，接地电位差 1V。
机房布线	采用光缆或六类及以上对绞电缆，采用 1+1 冗余。
照明要求	眩光限制按 I 级标准，照度按机房≥300Lux 及按现场布局排列，机房内应设置备用照明，其照度为一般照明的 15%。机房应设置疏散照明和安全出口标志灯，其照度不应低于 0.5LUX。
机房监控	空气质量：对温度、相对湿度、压差、含尘度；漏水监测报警；监控 IT 设备、空调、动力、供配电系统、不间断电源、电池、柴油发电等设备；采用 KVM 切换系统。
安全防范	在主要出入口、机房、配套区域采用门禁系统和视频监控系统，机柜区域配备专用门禁和 24 小时监控系统，视频监控画面可远程调用，中标人需开放相应的接口或者服务提供监控服务，监控录像保存时间大于 3 个月。
消防	应配置气体消防系统和火灾自动报警系统。

### 10.3.2 硬件设备参数指标

租用服务部分 1				
序号	设备名称	具体配置要求	数量	备注

1	软件虚拟化服务器（X86 架构）	<p>CPU: <math>\geq</math>[hygon7280]*2; <math>\geq</math>[32]*2 核;</p> <p>内存: 内存<math>\geq</math>1024GB; 频率<math>\geq</math>2666MHz;</p> <p>硬盘: 480G[480G_sata_ssd]*1; 1600G[1600G_nvme_ssd]*1;</p> <p>网络接口: <math>\geq</math>10GE*2; 双端口 10G 光口独立网卡;</p> <p>电源和风扇: 配置冗余电源和风扇;</p> <p>磁盘控制器类型: sas 卡 (none-raid) *1, 支持的硬盘数量<math>\geq</math>12</p> <p>硬件要求: 服务器满足 XC 要求。</p>	42	
2	软件虚拟化服务器（ARM 架构）	<p>CPU: <math>\geq</math>[kunpeng920]*2; <math>\geq</math>[48]*2 核;</p> <p>内存: 内存<math>\geq</math>384GB; 频率<math>\geq</math>2933MHz;</p> <p>硬盘: 240G[240G_sata_ssd]*1; 1600G[1600G_nvme_ssd]*1;</p> <p>网络接口: <math>\geq</math>10GE*2; 双端口 10G 光口独立网卡;</p> <p>电源和风扇: 配置冗余电源和风扇;</p> <p>磁盘控制器类型: sas 卡(none-raid)*1, 带宽<math>\geq</math>6Gbps, non-raid 直通, 满足机型磁盘配置需求和盘序要求。</p> <p>硬件要求: 服务器满足 XC 要求。</p>	80	
3	基础管控服务器/管控主机服务器	<p>CPU: <math>\geq</math>[hygon5280]*2; <math>\geq</math>[16]*2 核;</p> <p>内存: 内存<math>\geq</math>512GB; 频率<math>\geq</math>2666MHz;</p> <p>硬盘: 480G[480G_sata_ssd]*1; 3840G[3840G_nvme_ssd]*4;</p> <p>网络接口: <math>\geq</math>10GE*2; 双端口 10G 光口独立网卡;</p> <p>电源和风扇: 配置冗余电源和风扇;</p> <p>磁盘控制器类型: sas 卡 (none-raid) *1, 支持的硬盘数量<math>\geq</math>12</p> <p>硬件要求: 服务器满足 XC 要求。</p>	25	
4	管理基础服务器	<p>CPU: <math>\geq</math>[hygon7280]*2; <math>\geq</math>[32]*2 核;</p> <p>内存: 内存<math>\geq</math>768GB; 频率<math>\geq</math>2666MHz;</p> <p>硬盘: 480G[480G_sata_ssd]*1; 8000G[8T_sata_hdd]*12; 1920G[1920G_nvme_ssd]*2; 3840G[3840G_nvme_ssd]*2;</p> <p>网络接口: <math>\geq</math>1GE*2, <math>\geq</math>10GE*4; 1GE: 主控芯片型号 Intel I350/82580/82576, 物理网口 10/100/1000Mbps, 支持 PXE, 支持虚拟化应用;10GE: 双端口 10G 光口独立网卡;</p> <p>电源和风扇: 配置冗余电源和风扇;</p> <p>磁盘控制器类型: sas 卡 (none-raid) *1, 支持的硬盘数量<math>\geq</math>12</p> <p>硬件要求: 服务器满足 XC 要求。</p>	8	
5	专有网络管理服务器	<p>CPU: <math>\geq</math>[hygon7280]*2; <math>\geq</math>[32]*2 核;</p> <p>内存: 内存<math>\geq</math>512GB; 频率<math>\geq</math>2666MHz;</p>	4	

		<p>硬盘：240G[240G_sata_ssd]*1；1600G[1600G_nvme_ssd]*1；</p> <p>网络接口：≥1GE*2，≥10GE*2，≥40GE*4；1GE：主控芯片型号 Intel I350/82580/82576，物理网口 10/100/1000Mbps，支持 PXE，支持虚拟化应用；10GE：双端口 10G 光口独立网卡；</p> <p>电源和风扇：配置冗余电源和风扇；</p> <p>磁盘控制器类型：sas 卡（none-raid）*1，支持的硬盘数量≥12；</p> <p>硬件要求：服务器满足 XC 要求。</p>		
6	对象存储服务器	<p>CPU：≥[hygon7280]*2；≥[32]*2 核；</p> <p>内存：内存≥256GB；频率≥2666MHz；</p> <p>硬盘：480G[480G_sata_ssd]*2；12000G[12T_sata_hdd]*12；3840G[3840G_nvme_ssd]*2；</p> <p>网络接口：≥10GE*2；双端口 10G 光口独立网卡；</p> <p>电源和风扇：配置冗余电源和风扇；</p> <p>磁盘控制器类型：≥sas 卡（none-raid）*1，支持的硬盘数量≥12；</p> <p>硬件要求：服务器满足 XC 要求。</p>	18	
7	块存储（SSD）服务器	<p>CPU：≥[hygon7280]*2；≥[32]*2 核；</p> <p>内存：内存≥256GB；频率≥2666MHz；</p> <p>硬盘：480G[480G_sata_ssd]*2；3840G[3840G_nvme_ssd]*10；</p> <p>网络接口：≥10GE*2；双端口 10G 光口独立网卡；</p> <p>电源和风扇：配置冗余电源和风扇；</p> <p>磁盘控制器类型：sas 卡（none-raid）*1，支持的硬盘数量≥12；</p> <p>硬件要求：服务器满足 XC 要求。</p>	30	
8	块存储（高效云盘）服务器	<p>CPU：≥[hygon7280]*2；≥[32]*2 核；</p> <p>内存：内存≥256GB；频率≥2666MHz；</p> <p>硬盘：≥480G[480G_m.2_ssd]*1；≥8000G[8T_sata_hdd]*36；≥3840G[3840G_u.2_ssd]*2；</p> <p>网络接口：≥1GE*2：物理网口 10/100/1000Mbps，支持 PXE，支持虚拟化应用；≥10GE*2；双端口 10G 光口独立网卡；</p> <p>电源和风扇：配置冗余电源和风扇；</p> <p>磁盘控制器类型：≥sas 卡（none-raid）*1，支持的硬盘数量≥12；</p> <p>硬件要求：服务器满足 XC 要求。</p>	24	
9	文件存储服	<p>CPU：≥[hygon5280]*2；≥[16]*2 核；</p>	12	

	服务器	<p>内存：内存 ≥ 512GB；频率 ≥ 2666MHz；</p> <p>硬盘：480G[480G_sata_ssd]*1；8000G[8T_sata_hdd]*12；1920G[1920G_nvme_ssd]*2；</p> <p>网络接口：≥10GE*2；双端口 10G 光口独立网卡；</p> <p>电源和风扇：配置冗余电源和风扇；</p> <p>磁盘控制器类型：≥sas 卡（none-raid）*1，支持的硬盘数量 ≥12；</p> <p>硬件要求：服务器满足 XC 要求。</p>		
10	出口交换机	<p>1) 转发性能：交换容量 ≥ 4Tbps；包转发率 ≥ 1800Mpps；</p> <p>2) 硬件规格：高度 ≤ 1U，固定接口交换机；电源 1+1 备份，风扇框 4+1 备份；整机最大功耗 ≤ 220W；支持前后、后前风道；</p> <p>3) 端口配置要求：40/100 GE 光接口 ≥ 6 个；10GE 光端口数量 ≥ 48 个；</p> <p>4) 二层功能：支持 Access、Trunk 和 Hybrid 三种模式，支持 QinQ，支持 M-LAG 或 vPC 等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现），支持 DLDP，支持动态 MAC、静态 MAC 和黑洞 MAC 表项；</p> <p>5) 三层功能：支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+ 等 IPv6 动态路由协议，支持 IP 报文分片重组，支持 BFD for OSPF，BGP，IS-IS，Static Route，支持 IPv6 ND、PMTU 发现。</p>	4	
11	核心交换机	<p>1) 转发性能：交换容量 ≥ 600Tbps；包转发率 ≥ 200000 Mpps；</p> <p>2) 硬件规格：业务槽位数 ≥ 8；交换网板插槽数量 ≥ 6，且支持网板 N+M 冗余；风扇框冗余设计，要求风扇框个数 ≥ 2；无中板架构；10G/40G/100G 端口时延均小于 1.2us；DC，AC，HVDC 电源模块均支持 M+N 和 N+N；主控引擎与交换网板硬件分离，主控板故障或者更换不影响整机转发性能；严格前后风道；</p> <p>3) 端口配置要求：≥ 4 个 36 端口 40GE 以太网光接口板；</p> <p>4) 二层功能：支持端口聚合，802.3ad，支持 M-LAG 或 vPC 等类似技术（跨框链路聚合，支持 N:1 镜像、流镜像、远程端口镜像；</p> <p>5) 三层功能：支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+ 等 IPv6 动态路由协议，支持路由协议多实例、策略路由，支持 VRRP，支持 IP 分片和重组。</p>	4	

12	万兆接入交换机	<p>1) 转发性能：交换容量<math>\geq 4\text{Tbps}</math>；包转发率<math>\geq 1800\text{Mpps}</math>；</p> <p>2) 硬件规格：高度<math>\leq 1\text{U}</math>，固定接口交换机；电源 1+1 备份，风扇框 4+1 备份；整机最大功耗<math>\leq 220\text{W}</math>；支持前后、后前风道；</p> <p>3) 端口配置要求：40/100 GE 光接口<math>\geq 6</math> 个；10GE 光端口数量<math>\geq 48</math> 个；</p> <p>4) 二层功能：支持 Access、Trunk 和 Hybrid 三种模式，支持 QinQ，支持 M-LAG 或 vPC 等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现），支持 DLDP，支持动态 MAC、静态 MAC 和黑洞 MAC 表项；</p> <p>5) 三层功能：支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+ 等 IPv6 动态路由协议，支持 IP 报文分片重组，支持 BFD for OSPF，BGP，IS-IS，Static Route，支持 IPv6 ND、PMTU 发现。</p>	24	
13	综合接入交换机	<p>1) 转发性能：交换容量<math>\geq 350\text{Tbps}</math>；包转发率<math>\geq 110000\text{Mpps}</math>；</p> <p>2) 硬件规格：业务槽位数<math>\geq 4</math>；交换网板插槽数量<math>\geq 6</math>，且支持网板 N+M 冗余；风扇框冗余设计，要求风扇框个数<math>\geq 2</math>；无中板架构；10G/40G/100G 端口时延均小于 1.2us；DC，AC，HVDC 电源模块均支持 M+N 和 N+N；主控引擎与交换网板硬件分离，主控板故障或者更换不影响整机转发性能；</p> <p>3) 端口配置要求：<math>\geq 2</math> 个 36 端口 40GE 以太网光接口板；<math>\geq 1</math> 个 48 端口 10GE 以太网光接口板；</p> <p>4) 二层功能：支持端口聚合，802.3ad，支持 M-LAG 或 vPC 等类似技术，支持 N:1 镜像、流镜像、远程端口镜像；</p> <p>5) 三层功能：支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+ 等 IPv6 动态路由协议，支持路由协议多实例、策略路由，支持 VRRP，支持 IP 分片和重组。</p>	4	
14	专线接入交换机	<p>1) 转发性能：交换容量<math>\geq 4\text{Tbps}</math>；包转发率<math>\geq 1800\text{Mpps}</math>；</p> <p>2) 硬件规格：高度<math>\leq 1\text{U}</math>，固定接口交换机；电源 1+1 备份，风扇框 4+1 备份；整机最大功耗<math>\leq 220\text{W}</math>；支持前后、后前风道；</p> <p>3) 端口配置要求：40/100 GE 光接口<math>\geq 6</math> 个；10GE 光端口数量<math>\geq 48</math> 个；</p> <p>4) 二层功能：支持 Access、Trunk 和 Hybrid 三种模式，支持 QinQ，支持 M-LAG 或 vPC 等类似技术（跨框链路聚合，</p>	4	

		<p>要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现），支持 DLDP，支持动态 MAC、静态 MAC 和黑洞 MAC 表项；</p> <p>5) 三层功能：支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议，支持 IP 报文分片重组，支持 BFD for OSPF, BGP, IS-IS, Static Route, 支持 IPv6 ND、PMTU 发现。</p>		
15	带外管理核心交换机	<p>1) 转发性能：交换容量≥650Gbps；包转发率≥180Mpps；</p> <p>2) 硬件规格：高度 1U，固定接口交换机；为了提高设备可靠性，支持模块化可插拔双电源；支持 48 个 10/100/1000Base-T 以太网端口，6 个万兆 SFP+；</p> <p>3) 二层功能：支持 MAC 地址≥32K，支持 ARP 表项≥8K，支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN，支持组播 VLAN，支持 IEEE 802.1d(STP), 802.w(RSTP), 802.1s(MSTP)，支持 IGMP v1/v2/v3、PIM-SM；</p> <p>4) 三层功能：支持静态路由、RIP v1/v2、OSPF、BGP、OSPFv3，支持 IPv4 路由表≥8K，支持 IPv6 路由表≥2K，支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、Static Route，支持 IPv6、支持 IPv4/IPv6 双栈。</p>	4	
16	带外汇聚交换机	<p>1) 转发性能：交换容量≥650Gbps；包转发率≥180Mpps；</p> <p>2) 硬件规格：高度 1U，固定接口交换机；为了提高设备可靠性，支持模块化可插拔双电源；支持 48 个 10/100/1000Base-T 以太网端口，6 个万兆 SFP+；</p> <p>3) 二层功能：支持 MAC 地址≥32K，支持 ARP 表项≥8K，支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN，支持组播 VLAN，支持 IEEE 802.1d(STP), 802.w(RSTP), 802.1s(MSTP)，支持 IGMP v1/v2/v3、PIM-SM；</p> <p>4) 三层功能：支持静态路由、RIP v1/v2、OSPF、BGP、OSPFv3，支持 IPv4 路由表≥8K，支持 IPv6 路由表≥2K，支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、Static Route，支持 IPv6、支持 IPv4/IPv6 双栈。</p>	4	
17	边界防火墙	<p>1) 整机性能：防火墙吞吐量≥2.4Tbps，每秒新建连接数≥4500 万，最大并发连接数≥18 亿；</p> <p>2) 路由功能：支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议；策略路由支持的匹配条件：源 IP/目的 IP，</p>	4	

		<p>服务类型，应用类型，入接口；</p> <p>3) IPv6: 支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议；</p> <p>4) NAT: 支持全面 NAT 功能，对多种应用层协议支持 ALG 功能；</p> <p>5) VPN: 支持 IPSEC 双机热备，实现会话同步，设备切换 VPN 业务不中断；支持 URL 识别能力和 URL 地址识别库，云端 URL 识别库≥1.4 亿；</p> <p>6) 协议识别: 可识别应用层协议数量≥6000 种；</p> <p>7) 可靠性: 支持 BFD 链路检测，支持 BFD 与 VRRP 联动实现双机快速切换，支持 BFD 与 OSPF 联动实现双机快速切换；支持平滑升级，升级窗口中支持不同版本的软件形成双机热备；实配应用层协议识别及流量控制功能；</p> <p>8) 硬件要求: 关键器件使用国产芯片。</p>		
18	专线防火墙	<p>1) 整机性能: 防火墙吞吐量≥50Gbps，最大并发连接数≥1800 万，每秒新建连接数≥50 万；IPSec VPN 吞吐量≥30Gbps，SSL VPN 吞吐量≥3Gbps；IPSec VPN 隧道数≥20000，SSL VPN 并发在线用户数≥5000；</p> <p>2) 路由功能: 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议；策略路由支持的匹配条件: 源 IP/目的 IP, 服务类型，应用类型，用户(组)，入接口，DSCP 优先级；IPv6: 支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议；支持 IPv6 over IPv4 隧道，6RD 隧道；</p> <p>3) URL 过滤: 支持 URL 识别能力和 URL 地址识别库，云端 URL 识别库≥1.4 亿；</p> <p>4) 协议识别: 可识别应用层协议数量≥6000 种；</p> <p>5) 可靠性: 支持 BFD 链路检测，支持 BFD 与 VRRP 联动实现双机快速切换，支持 BFD 与 OSPF 联动实现双机快速切换；</p> <p>6) 硬件要求: 关键器件使用国产芯片。</p>	4	
19	流量分析平台（含探针）	<p>流量分析系统管理平台：</p> <p>1) 硬件要求: 关键器件使用国产芯片</p> <p>2) 处理器: CPU≥2 颗</p> <p>3) 内存: ≥128GB DDR4</p> <p>4) 硬盘: ≥32TB</p> <p>5) 监控场景: 支持数据中心网络拓扑的 visio 级定制，监控视图中支持标识镜像点位置、网元位置及连线关系。</p> <p>6) 监控视图: 能够根据运维重点组合最需要的数据投屏呈</p>	2	

		<p>现，支持自定义组合各种业务性能、链路流量的关键指标，指标图表呈现具备 3 种或以上可选方式。</p> <p>7) 业务 SLA 报表：支持自动生成指定业务的运行状态报告，能够记录业务所包含的应用数量、业务的总运行时间、故障时间、无故障时间、故障率和无故障率等信息；以及每个应用的总运行时间。</p> <p>8) 调用其他平台接口：流量分析系统支持与主流负载均衡器进行 API 对接，梳理负载均衡器前后的虚拟系统及真实服务器地址的对应关系，以可视化的方式展示，并提供负载均衡器前后的指标多段关联分析功能。</p> <p>9) 平台接口调用：流量分析系统支持 resful API、kafka 等标准数据接口，将任意维度及指标的分析统计数据输出至外部平台，支持秒级的接口调用频率及秒精度的统计数据查询输出。</p>		
		<p>流量分析探针：</p> <p>1) 硬件要求：关键器件使用国产芯片</p> <p>2) 处理器：CPU ≥2 颗</p> <p>3) 内存：≥256GB DDR4</p> <p>4) 硬盘：≥128TB</p> <p>5) 性能要求：流量处理：≥10Gbps；数据包处理：≥600 万 pps；TCP/UDP 会话处理≥100 万/秒。</p> <p>6) 解码器要求：系统中内置自主知识产权的数据包解码器，支持在线进行数据包的快速解码分析。</p> <p>7) 数据链路层采集分析：系统支持基于原始数据包的 mac 层地址统计分析，分析维度包括 mac 地址、mac 会话。</p> <p>8) IP 层采集分析：可以检索并展示流量，包率等曲线，并根据用户所选时间关联分析统计数据。</p>		
20	日志审计	<p>1) 系统结构：国产化硬件平台、国产化安全操作系统及功能软件构成</p> <p>2) 内存：≥64G</p> <p>3) 硬盘：系统盘≥240G SSD；数据盘≥16T，支持 Raid5</p> <p>4) 系统性能：日志采集均值≥20000EPS，峰值≥35000EPS，配置不少于 500 个日志源授权。</p> <p>5) 数据采集：支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 26 类 300 种日志对象的日志数据采集。</p> <p>6) 数据存储：支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个</p>	2	

		<p>月和永久保存等参数。</p> <p>7) 数据查询：支持对常用查询条件进行保存，可重复使用；支持查询条件缓存，通过快速调用系统右侧隐藏栏中缓存的查询条件，提升常用条件的检索速度。</p> <p>8) 数据分析：提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则；支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警。</p> <p>9) 告警管理：支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定。</p> <p>10) 统计报表：系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。</p>		
21	网闸	<p>1) 系统性能：传输速率<math>\geq 6400\text{Mbps}</math>，传输延时<math>\leq 0.5\text{ms}</math>。</p> <p>2) 安全浏览：支持 http 消息头、消息体，上下行方向，命令及关键字的管控，支持允许、阻断、告警三种处理方式。</p> <p>3) FTP 访问：支持基于 FTP 协议和 TFTP 协议的文件传输功能。</p> <p>4) 数据库访问：支持对数据库用户名、命令、关键字等内容进行管控，包括允许、阻断、告警。</p> <p>5) 安全邮件访问：支持发件人、收件人、邮件标题、邮件正文、邮件附件等数据内容过滤。</p> <p>6) 音视频通话访问：支持 SIP 和 RTSP 协议。</p> <p>7) 自定义访问：支持自定义的 TCP、UDP 协议的数据访问功能，用户自定义应用无需对自定义协议软件进行二次修改开发。</p> <p>8) 文件同步：无需在用户服务器上安装任何插件，安全隔离与信息交换系统不开放任何服务端口；支持 NFS、FTP 等多种文件服务器类型，支持实时同步和周期性同步；</p> <p>9) 数据库同步：无需在用户服务器上安装任何插件；支持同构、异构数据库之间的同步；支持同侧数据库之间的数据同步；支持数据库同步冲突策略处理，包括覆盖、忽略处理方式。</p> <p>10) 安全防护：支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制；支持病毒库升级，并提供后续升级服务。</p> <p>11) 日志审计：支持日志记录本地数据库存储，也可以将日志传输到独立的日志服务器上，传输日志格式支持 syslog 和</p>	2	

		welf, 支持日志加密传输。		
22	入侵防御系统	<p>1) 性能要求: 整机最高可扩展至 500Gbps; 单槽位扩展 IPS 吞吐量≥80Gbps。</p> <p>2) 入侵防护功能: 配置入侵防护功能模块; 能够防范各种应用层攻击, 包括但不限于: 后门程序, 木马程序, 间谍软件, 蠕虫, 僵尸主机, 异常代码, 协议异常, 扫描, 可疑行为审计类等, 能够对跨站攻击、SQL 注入等 WEB 攻击行为进行有效防护。</p> <p>3) DDoS 防护: 配置攻击防护功能模块; 支持 SYN Flood、SYN ACK、UDP Flood 等 DDoS 防护, 支持 HTTP Flood、HTTPS Flood 等应用层 DDoS 防护。</p> <p>4) 防病毒功能: 支持对 SMTP、POP3、HTTP、FTP 协议实现病毒扫描检测。</p> <p>5) 响应方式: 支持日志告警、会话阻断、IP 隔离、等多种响应方式。</p> <p>6) 升级服务: 支持应用威胁签名库的在线升级、离线升级多种升级方式; 支持每周定期升级威胁签名库、病毒库, 遇到重大安全事件, 支持即时升级。</p> <p>7) 报表: 支持安全威胁的分析报表, 提供基于威胁名称、威胁类型、威胁应用类型等呈现方式; 支持应用流量的分析报表, 支持按日、周、月、导出报表。</p> <p>8) 硬件要求: 关键器件使用国产芯片。</p>	4	
23	租户侧加密机	<p>1) 符合国家密码管理局相关管理要求。</p> <p>2) 整机性能: SM2 签名速率≥15000 次/秒; SM2 验签速率≥14000 次/秒; SM3 计算速率≥700 Mbps; SM4 算法加解密速率≥700Mbps; 单台最大支持虚拟加密机(VSM)数量≥32 个,最少支持虚拟加密机(VSM)数量≤16 个;</p> <p>3) 密钥算法支持: 支持国密算法 SM1、SM2、SM3、SM4;</p> <p>4) 虚拟化功能: 单台云密码机可虚拟多个密码机 VSM, 提供弹性分配、虚机迁移、运算速度分配等云化功能, 提高密码设备资源利用率。VSM 可根据应用的需求动态伸缩, 按需调配资源, 同时应用所需的加解密功能也应能动态的按需加载;</p> <p>5) 密钥管理: 支持密钥的安全生成(二级、三级模块)、存储、备份、恢复;</p> <p>6) 安全性: 提供丰富基于口令、智能密码钥匙、数字证书等多种身份认证机制, 各 VSM 安全隔离, 各 VSM 密钥安全隔离;</p>	4	

		<p>7) 接口支持：支持 JCE、PKCS#11CSP、国密 SDF 等多种标准密码应用接口；密码机服务应符合《GB/T 36322-2018_信息安全技术密码设备应用接口规范》；</p> <p>8) 管理要求：密码管理中心实现贯穿整个密码服务体系的管理中心，对设备和密码平台的使用均能进行管理；</p> <p>注册管理：要求应用及密码设备在使用密码服务前，需要先接入服务进行注册认证,确保自己是合法对象，否则无法接入密码服务体系，应用无法使用密码服务。</p> <p>虚拟服务管理：支持实时监控虚拟服务的状态是否关闭。当虚拟服务退出或者异常关闭的时候，资源回收服务会自动释放被租户占用的密码算法能力，更改剩余密码算法能力和各个密码设备负载信息；</p> <p>密钥管理：支持租户密钥生命周期安全管理包括密钥生成、传输、存储、使用、导入、导出、销毁，系统保证租户密钥私钥不以明文形式出现在密码设备之外，不被任何人非法使用。</p>		
24	态势感知平台（含探针）	<p>态势感知平台：</p> <p>1) 首页工作台：支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示。</p> <p>2) 安全态势可视化：支持立体、平面、球面等多种维度的网络实体关系透视。</p> <p>3) 监测中心：支持告警数据自动化归并，并通过告警列表条目颜色区分“已读告警”和“未读告警”。</p> <p>4) 分析中心：应内置包括规则模型、关联模型、统计模型、情报模型、AI 模型等不少于 5 类安全分析模型</p> <p>5) 响应中心：支持通过单条告警、聚合告警添加白名单，快速过滤误报；支持前端拖拽式交互设计安全风险研判策略和联动响应剧本。</p> <p>6) 运营中心：支持用户自定义编辑报告模板，选择的相应统计报表组成要展示的报告内容。</p> <p>7) 资产中心：支持人工录入、流量自动发现、主动扫描、web 自动发现、资产同步等不少于 5 种的资产数据接入方式。</p> <p>硬件要求：关键器件使用国产芯片。</p> <hr/> <p>探针：</p> <p>1) 性能要求：吞吐率≥5Gbps</p> <p>2) 探测扫描检测：具备端口扫描、主机存活扫描、服务扫描、Web 扫描、扫描器指纹检测等 600 种以上的探测扫描检</p>	2	

	<p>测规则，可针对任意单条规则进行启用和禁用。</p> <p>3) 恶意程序检测：具备挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell、恶意邮件等 17000 种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。</p> <p>4) 配置风险检测：具备弱口令风险、明文传输风险、HTTP 配置风险、中间件配置风险、数据库配置风险、服务配置风险等 300 种以上配置风险检测规则。</p> <p>5) 主机和账号异常检测：支持端口异常、主机对外扫描、主机对外攻击等主机异常检测，对任意单条检测规则支持启用和禁用。</p> <p>6) 告警研判：支持从请求头、请求体、响应头、响应体四个方面展示告警详情，并对攻击报文进行高亮显示；对攻击结果的判定，支持识别成功、尝试和失败行为；支持对威胁告警进行调查分析，针对威胁告警支持原始数据包取证分析，告警详情支持查看、下载 PCAP 包，在告警页面支持一键添加白名单。</p> <p>7) 告警归并：支持展示高度聚合告警列表，对告警进行自动归并；支持多维度告警查询，支持威胁告警快速过滤，包括筛选、排除操作（需提供软件功能截图证明支持以上全部功能）。</p> <p>8) 资产发现：支持根据探针的内部 IP 配置或从态势感知平台同步的内部 IP 配置从流量中进行资产信息的识别，资产信息包括 IP、MAC 地址、首次发现时间、最近活跃时间、资产类型、发现来源、服务与端口、标签。</p> <p>9) 流量采集：支持自定义流量采集策略，包括过滤策略和采集策略，支持根据 IP 和协议进行过滤，包括 DNS、FTP、HTTP、HTTPS、IMAP、KRB5、LDAP、POP3、RDP、SMB、SMTP、SSH、TELNET、TLS 等。</p> <p>10) 指纹识别：支持对 Web 类、FTP、TELNET 等类型的资产指纹进行识别，识别信息包括指纹名称、分类、标签、厂商名称、官网链接、产品链接、产品描述、对应资产接口等；支持区分每个资产接口的最新指纹和历史指纹。</p> <p>11) 文件还原：支持文件还原，用户可新增指定后缀文件进行文件还原，具体协议包括 HTTP、SMTP、POP3、IMAP、FTP、SMB、NFS 等，还原文件支持推送沙箱进行安全检测。</p> <p>数据同步：自定义配置：可在前端页面自定义配置与态势感知平台之间的数据传输类型、各类型数据均支持任意字段的发送配置。</p> <p>硬件要求：关键器件使用国产芯片。</p>		
--	--	--	--

25	漏洞扫描设备	<p>1) 性能要求：任务并发数≥15，单任务并发 IP 数≥90；</p> <p>2) 系统漏扫功能要求：用户可自定义扫描范围、扫描端口、扫描使用的参数集等具体扫描选项。具备弱口令扫描功能，支持弱口令扫描协议数量≥22 种，包括 FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP 等协议进行弱口令扫描，允许用户自定义用户、密码字典（需提供软件功能截图证明支持以上全部功能）；</p> <p>3) 网站漏扫功能要求：支持将漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级。支持 Web2.0 扫描，采用自主研发的网页执行模块，执行网页中的 JavaScript 脚本获取其中的链接。支持对 Struts2 远程命令执行漏洞进行命令执行和文件上传的渗透测试验证操作；</p> <p>4) 数据库扫描功能要求：支持达梦、人大金仓的授权数据库漏洞扫描；配置授权扫描时能够远程登录目标数据库以验证能否成功登录目标数据库，防止因输错密码或网络限制等未能成功授权扫描。数据库扫描的漏洞库数量大于 3000 条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNNVD 等国际、国内漏洞库标准兼容。数据库扫描支持的检测类型大于 10 种，至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL-SQL 注入、危险程序、安全信息查看等。基线核查要求：支持主流操作系统的基线配置检查，包括但不限于 Windows、Linux、Suse、HP-UX、Solaris、AIX、Debian。支持的数据库基线配置检查包括但不限于 Informix、DB2、MySQL、SQL Server、Oracle。在资产管理页面可直接对单个资产或批量资产下发扫描任务。</p> <p>5) 报表管理：支持导出的报告类型≥5 种，包括 HTML、WORD、PDF、EXCEL、XML 报告格式。</p> <p>6) 硬件要求：关键器件使用国产芯片。</p>	2	
26	SSL VPN	<p>1) 符合国家密码管理局相关管理要求。</p> <p>2) 总体要求：支持 SM2、SM3、SM4 算法，具有密钥协商、身份认证、SSL 隧道加密等功能。</p> <p>3) 性能要求：最大并发用户数≥6000；最大并发连接数≥5800；每秒新建连接数≥100；吞吐率≥ 55Mbps。</p> <p>4) 功能要求：支持国密 SSL 协议；支持端到端的全链路加</p>	2	

		密。支持日志完整性保护、syslog 功能；具备 SSL 服务端动态选择证书的能力（SM2、RSA 自适应）。应用支持：支持 B/S 应用；支持 C/S 应用，支持 FTP、telnet、远程桌面以及通用的 C/S 应用；支持基于 IP 的所有应用。		
27	平台侧堡垒机	1) 硬件要求：关键器件使用国产芯片。 2) 性能：最大支持 150 路图形会话或 400 路字符会话并发；最大支持 300 个被管资源数。 3) 硬盘：内置≥4TB 硬盘。 4) 其他：支持液晶屏。	2	
租用服务部分 2				
序号	设备名称	具体配置要求	数量	备注
1	软件虚拟化服务器（X86 架构）	CPU: ≥[hygon7280]*2; ≥[32]*2 核; 内存: 内存≥1024GB; 频率≥2666MHz; 硬盘: 480G[480G_sata_ssd]*1; 1600G[1600G_nvme_ssd]*1; 网络接口: ≥10GE*2; 双端口 10G 光口独立网卡; 电源和风扇: 配置冗余电源和风扇; 磁盘控制器类型: sas 卡 (none-raid) *1, 支持的硬盘数量 ≥12 硬件要求: 服务器满足 XC 要求。	15	
2	软件虚拟化服务器（ARM 架构）	CPU: ≥[kunpeng920]*2; ≥[48]*2 核; 内存: 内存≥768GB; 硬盘: 240G[240G_sata_ssd]*1; 1600G[1600G_nvme_ssd]*1; 网络接口: ≥10GE*2; 双端口 10G 光口独立网卡; 电源和风扇: 配置冗余电源和风扇; 磁盘控制器类型: sas 卡 (none-raid)*1, 带宽≥6Gbps, non-raid 直通, 满足机型磁盘配置需求和盘序要求。 硬件要求: 服务器符合 XC 要求。	10	
3	GPU（推理）服务器	CPU: ≥[64]*2 核; 内存: 内存≥1024GB; 硬盘: 480G[480G_sata_ssd]*1; 1920G[1920G_nvme_ssd]*1; GPU: 8*推理 GPU, 单 GPU 卡显存≥64GB, 单 GPU 卡 FP16 算力（非稀疏）≥196TFLOPS; 网络接口: ≥10GE*2; 双端口 10G 光口独立网卡; 电源和风扇: 配置冗余电源和风扇; 磁盘控制器类型: sas 卡 (none-raid) *1。	6	

		硬件要求：服务器符合 XC 要求。		
4	GPU（训练）服务器	CPU: $\geq[48]*4$ 核; 内存: 内存 $\geq 1024GB$ ; 硬盘: 240G[240G_sata_ssd]*1; 960G[960G_nvme_ssd]*1; GPU: 8*训练 GPU, 单 GPU 卡显存 $\geq 64GB$ , 单 GPU 卡 FP16 算力（非稀疏） $\geq 376TFLOPS$ ; 网络接口: $\geq 10GE*2$ ; 双端口 10G 光口独立网卡; 电源和风扇: 配置冗余电源和风扇; 磁盘控制器类型: sas 卡（none-raid）*1。 硬件要求：服务器符合 XC 要求。	4	
5	备份硬件服务器	CPU: $\geq[hygon 7360]*2, \geq[24]*2$ 核; 内存: 内存 $\geq 512GB$ ; 硬盘: 960G[480G_sata_ssd]*2; 3840G[3840G_nvme_ssd]*2; 16000G[16T_sata_hdd]*12; 网络接口: $\geq 10GE*2$ ; 双端口 10G 光口独立网卡; 电源和风扇: 配置冗余电源和风扇; 磁盘控制器类型: sas 卡（none-raid）*1 硬件要求：服务器符合 XC 要求。	12	
6	万兆接入交换机	1) 转发性能: 交换容量 $\geq 4Tbps$ ; 包转发率 $\geq 1800Mpps$ ; 2) 硬件规格: 高度 $\leq 1U$ , 固定接口交换机; 电源 1+1 备份, 风扇框 4+1 备份; 整机最大功耗 $\leq 220W$ ; 支持前后、后前风道; 3) 端口配置要求: 40/100 GE 光接口 $\geq 6$ 个; 10GE 光端口数量 $\geq 48$ 个; 4) 二层功能: 支持 Access、Trunk 和 Hybrid 三种模式, 支持 QinQ, 支持 M-LAG 或 vPC 等类似技术（跨框链路聚合, 要求配对设备有独立的控制平面, 不能用堆叠等多虚一技术实现), 支持 DLDP, 支持动态 MAC、静态 MAC 和黑洞 MAC 表项; 5) 三层功能: 支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议, 支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议, 支持 IP 报文分片重组, 支持 BFD for OSPF, BGP, IS-IS, Static Route, 支持 IPv6 ND、PMTU 发现。	6	

10.3.3 软件技术方案

序号	模块名称	具体功能要求	备注
1	云业务管理	1) 功能要求:	

序号	模块名称	具体功能要求	备注
	平台	<p>A. 支持查看历史告警。</p> <p>B. 提供云环境中的云产品资源实例提供租户级的资源监控能力；提供云产品资源实例提供租户级的告警通知能力。</p> <p>C. 支持以组织和资源维度统计统计资源报表、配额报表和云监控报表；支持异步导出的各类统计分析报表</p> <p>D. 支持创建/修改/删除/查询资源集；支持查看/跳转到资源集所有的资源实例；通过资源集管理用户、用户组；支持对于不同的 region 区域，设置每个云产品可以使用的资源量，支持对于 region 和集群，设置不同的名称，便于管理</p> <p>E. 创建/修改/删除/恢复/禁用/激活/查询用户、查询/修改/重置密码、变更归属、角色授权、用户组管理、登录策略设置</p> <p>F. 支持创建/修改/删除/查询用户组、添加/删除用户；支持用户组与角色关联</p> <p>G. 按时间/按组织维度计量、计量报表查询、计量报表导出</p> <p>2) 安全性要求：</p> <p>A. 提供统一的用户密码策略配置，支持强密码、密码有效时间以及锁定策略；</p> <p>B. 提供日志审计功能，保留所有用户的操作日志，并支持日志的过滤和导出功能。</p> <p>C. 创建/修改/删除/禁用/激活登录策略、支持白名单、支持黑名单、关联用户、关联组织；支持按照登陆时间和 IP 地址的白名单/黑名单策略；支持设置能看见并使用这个登陆策略的组织</p>	
2	云运维管理系统	<p>1) 支持展示云平台部署产品概览。</p> <p>2) 支持看出每个集群的详细信息。</p> <p>3) 支持任务管理，支持展示系统中任务的整体运行情况。</p> <p>A. 支持查看当前系统中等待介入、运行中、失败和已完成任务数量的统计信息。单击各统计数值，会跳转到对应的任务页面。</p> <p>B. 支持查看最近 24 小时内正在运行中的任务。</p> <p>C. 支持查看最近 7 天任务的运行趋势。</p> <p>D. 支持修改任务的灰度策略即调整机器的执行批次。</p> <p>E. 支持查看任务的执行情况。</p> <p>F. 支持导出历史告警列表。</p> <p>4) 告警监控管理：</p> <p>A. 支持查看告警源详情。</p> <p>B. 支持根据监控项类型、产品、服务、等级、状态、开始日期、结束日期及过滤内容来进行过滤查询。</p> <p>C. 支持告警处理，导出告警列表里的告警信息，支持告警屏蔽，支持</p>	

序号	模块名称	具体功能要求	备注
		<p>为已屏蔽的告警解除屏蔽。</p> <p>D. 支持按关键字查询相应的告警事件，可以根据业务需要，查询、添加、修改以及删除告警联系人和联系人组。</p> <p>5) 云资源管理：</p> <p>A. 支持云主机库存情况查看，云主机库存详情中主要提供按区域、实例类型和日期分页查询某类实例在某个日期的库存情况。</p> <p>B. 支持块存储、NAS、对象存储库存情况查看，历史可用库存（TB）显示近五天存储的库存可用情况；当前已用库存（TB）显示当前存储已用库存和百分比；存储库存详情中可按日期分页查询存储库存详情。</p> <p>C. 支持负载均衡服务库存情况查看。</p> <p>D. 支持显示云平台物理网络拓扑，支持显示网络设备网元和互联链路，网络设备和互联链路应支持按颜色区分链路状态。</p> <p>E. 支持动态拓扑和基准拓扑展示功能，动态拓扑可以动态刷新拓扑状态，基准拓扑表示网络的目标状态。</p> <p>6) 用户权限管理：</p> <p>A. 支持用户管理、用户组管理、双因素认证、角色管理、部门管理、菜单管理、Region 授权管理、云操作系统日志、操作日志、授权信息。</p> <p>B. 统一账号管理&amp;角色权限管理，能实现对云平台所有的组件进行运维或者免登录跳转运维。</p> <p>7) 支持云平台运维工作自动化，可向批量资源完成运维操作，提供基础设施，云环境，操作系统，应用层的自动化运维能力。</p> <p>A. 脚本管理，提供脚本库存放运维脚本，支持系统内置脚本，并支持运维人员自定义和导入脚本。</p> <p>B. 软件包管理：提供软件仓库能力，可以上传和下载软件包，支持压缩包，JAR 包等格式。</p> <p>C. 运维作业：支持运维作业定义，运维作业可以手动触发和定时触发。</p> <p>D. 运维流程编排：支持图形化方式编排运维流程。</p>	
3	弹性计算服务	<p>1) 功能要求：</p> <p>A. 支持云主机生命周期管理和维护。</p> <p>B. 支持对云主机 CPU、内存、硬盘等基础指标进行监控，同时支持对云主机系统中的各进程 CPU、内存、打开文件数进行监控，为用户提供系统级、主动式、细粒度监控服务。</p> <p>2) 可靠性：</p> <p>A. 支持云主机按宿主机，机架，网络交换机物理拓扑的调度能力，提升业务的可靠性。控制台上分散策略支持严格分散和尽量分散两种</p>	

序号	模块名称	具体功能要求	备注
		<p>可选。</p> <p>B. 支持云主机热迁移，运维人员可以手工指定迁移任务的带宽限制，降低迁移流量对正常业务的干扰。</p> <p>C. 支持云主机高可用（宕机迁移），当某台物理节点发生意外故障，在其上运行的云主机能够在其他正常的物理节点上重新启动，保障业务的连续性。</p> <p>3) 安全性</p> <p>A. 支持云主机磁盘国密算法加密，能够对云盘中的数据、云盘和实例间传输的数据、云盘创建的所有快照进行加密处理，保障数据的安全性。</p> <p>B. 支持云主机网络防 ARP 欺骗，云平台应阻止用户非法修改 IP 地址和 MAC 地址后发出的数据包，提升安全性。</p> <p>C. 支持用户通过 VNC 方式远程访问云主机，同时支持用户设置云主机 VNC 密码（非系统密码），并能在用户 VNC 访问时进行 VNC 密码认证，保证终端用户对云主机的安全访问。</p> <p>D. 支持用户通过快照对云主机的数据进行备份，通过快照进行云服务器的数据恢复，可以为每块磁盘创建 64 个快照。</p>	
4	弹性计算块存储服务	<p>1) 总体要求：为云主机提供的低时延、持久性、高可靠性的数据块级存储设备。</p> <p>2) 功能要求：支持在线扩展容量，扩容期间无需关闭虚拟机，无需卸载云盘；系统盘在线扩容不停业务。支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能。</p> <p>3) 功能指标：单个云盘最高支持 32TB 容量。</p> <p>4) 安全性：支持分布式 EC 和三副本数据冗余保护，三副本模式下，数据三副本支持分布在 3 个机柜或 3 对接入交换机上。</p>	
5	文件存储服务	<p>1) 总体要求：为云主机提供的低时延、持久性、高可靠性的数据文件级存储设备。</p> <p>2) 功能要求：</p> <p>A. 支持 NFS v3.0/4.0, SMB2.1/3.0 协议。</p> <p>B. 支持多个文件系统组成全局命名空间。</p> <p>C. 支持将 NAS 指定文件或目录归档到对象存储，可以按照不同时间段规则进行选择性的归档。</p> <p>D. 支持目录级容量 Quota 管理。</p> <p>3) 可靠性：提供三副本数据保护，数据三副本支持分布在 3 个机柜或 3 对不同接入交换机上。（如有系统功能界面截图等相关证明材料，请在投标文件中提供）</p>	

序号	模块名称	具体功能要求	备注
		4) 安全性：支持通过权限组对访问主机的 IP 地址进行读写访问权限控制，允许授权对象对文件系统进行只读操作或读写操作，当同一个授权对象匹配到多条规则时，高优先级规则将覆盖低优先级规则。	
6	对象存储服务	<p>1) 总体要求：对象存储服务支持 RESTful API 接口、兼容 Amazon S3 接口，通过开发工具包 SDK 或直接通过 RESTful API 进行基础和高级对象存储操作，提供 key-value 键值对形式的对象存储服务</p> <p>2) 功能要求：</p> <p>A. 支持原生图片处理服务：创建图片处理规则、图片格式转换、图片效果处理、添加文字或图片水印、高级编辑自定义图片处理样式等。</p> <p>B. 支持对象的简单上传、追加上传、下载、删除、列举、复制，获取对象的元数据、创建多段上传任务。支持列举存储空间、创建存储空间、删除存储空间、列举存储空间内对象、获取存储空间的元数据。</p> <p>C. 支持生命周期管理、定义和管理存储空间内所有对象或对象的某个子集的生命周期、变更容量和变更归属。</p> <p>D. 3) 功能指标：单个对象最大支持 48.8TB，单租户支持最大 10000 个 bucket 并提供界面截图；每个 bucket 的生命周期最多可容纳 1000 规则。</p> <p>4) 安全性：支持客户端加密功能，可以使用客户端加密 SDK，在本地进行数据加密，并将加密后的数据上传到对象存储，既支持云平台密钥管理系统托管的用户主密钥，也支持用户自主管理的密钥。支持服务器端的加密功能，用户能够使用密钥管理系统上创建的密钥进行加密。可以使用国密算法对 bucket 内保存的数据以及单独 object 进行加密存储。</p>	
7	专有网络服务	<p>1) 总体要求：支持用户创建自己的专有网络，同时支持自定义配置 IP 地址、子网、路由表。支持不同 VPC 之间的安全隔离。</p> <p>2) 功能要求：</p> <p>A. 支持 ENI 弹性网卡 (elastic network interface) 绑定云服务器，在多个云服务器间自由迁移。支持为 ENI 绑定 EIP。</p> <p>B. 支持 IPSEC VPN 服务，支持 IPsec-VPN 建立专有网络 (VPC) 到本地数据中心的 VPN 连接，IPsec-VPN 支持 IKEv1 和 IKEv2 协议，同时支持 API 方式配置。</p> <p>C. 支持 SSL VPN 服务，支持通过 SSL-VPN 功能远程接入 VPC，修改 SSL 服务端的名称、本端网段、客户端网段信息，支持创建 SSL 客户端证书，支持 AES128、ASE192、AES256 加密算法。支持 API 方式配置。</p>	

序号	模块名称	具体功能要求	备注
		D. 支持共享 VPC，支持按租户和资源集的 VPC 资源共享。VPC 的所有者可以将 VPC 共享给同一组织的租户。 E. 支持在控制台上针对 VPC 配置多个 CIDR 地址段；支持新 CIDR 地址段的扩容。 F. 支持用户可以创建网络 ACL 配置入向/出向规则，进行网络访问控制功能，从而实现对一个或多个子网流量的访问控制。	
8	负载均衡服务	1)总体要求:负载均衡服务采用通用服务器架构实现。提供 4 层 TCP/UDP 和 7 层 HTTP/HTTPS 协议类型的服务。 2) 功能要求: A. 七层负载均衡模式下支持配置域名或者 URL 转发策略,将来自不同域名或者 URL 的请求转发给不同的 ECS 处理。 B. 四层负载均衡支持 TCP/UDP 监听在后端应用服务器无插件模式下直接获取客户端源 IP 地址。七层负载均衡支持后端服务器应用程序通过 HTTP 头字段的 X-FORWARD-FOR 获取客户端源 IP 地址,支持从 HTTP 头字段扩展方式获取负载均衡实例 Id 和负载均衡 VIP 地址信息。 C. 四层负载均衡支持提供主备服务器 Active-Standby 模式,负载均衡监听的后端添加主备两台后端应用服务器,当主机健康检查正常时,流量将直接转发至主机;当主机健康检查失败,流量将切换至备机,主备服务器不需要依赖 Keepalived、pacemaker 等应用高可用组件。 D. 负载均衡支持 4 层一致性 hash、轮询(RR),加权轮询(WRR)和最小连接数(WLC)等调度算法,在上述每种调度算法 4 层支持 TCP 源地址会话保持,7 层支持 HTTP Cookie 会话保持。 E. 负载均衡支持公网和私网类型实例。支持私网实例绑定公网 IP 地址,提供同一个实例同时支持公网和私网客户端访问的功能。支持 ping 私网负载均衡的 IP 地址用于 VIP 探活。 F. 负载均衡支持配置性能保障型实例,针对不同的业务类型配置不同的规格,其中规格涉及并发连接数、每秒新建连接数、每秒查询请求数。支持单实例监听带宽配置,针对同一个 VIP 内不同的监听端口配置不同的带宽限制值。 G. 支持配置多种实例规格,不同规格实例限定最大支持连接数,可以变更实例规格。(如有系统功能界面截图等相关证明材料,请在投标文件中提供)	
9	云虚拟化平台安全服务	A. 提供流量安全监控、态势感知、Web 应用防火墙、云安全管理中心、敏感数据包含、数据库审计、数据梳理及脱敏系统、云堡垒机、漏	

序号	模块名称	具体功能要求	备注
		<p>洞扫描。主机安全防护、密钥管理服务、伪装欺骗系统等安全功能服务。</p> <p>B. 支持动态脱敏功能，可通过调用 ExecDatamask 接口对数据进行动态脱敏。（如有系统功能界面截图等相关证明材料，请在投标文件中提供）</p> <p>C. 支持端口扫描欺骗策略，可添加需要防护的 IP 和端口，对恶意端口扫描行为进行欺骗。（如有系统功能界面截图等相关证明材料，请在投标文件中提供）</p>	
10	裸机管理服务软件基础版	<p>整体要求：对物理机执行节点级别的管理。按纳管的服务器台数计费。</p> <p>功能要求：裸机管理服务可纳管物理服务器，支持裸机自动装机、加入 VPC 网络、机器运维、监报告警等功能</p> <p>支持托管模式，使用客户原有操作系统，不需要重新装机，通过运维控制台录入 IP、账户、密码注册到裸机资源池，之后在运营控制台，对裸机进行开关机、重启、监控、查询操作日志等</p> <p>支持裸机实例加入 VPC，相同 VPC 内网络互通，不同 VPC 之间网络隔离，并且提供网络 ACL 配置，保证裸机实例的安全性。</p> <p>支持用户自定义镜像，镜像文件格式支持 .tgz、.qcow2。</p> <p>支持带外管理，支持服务器上下电；</p> <p>镜像中心提供业界常用操作系统镜像，提供用户自定义镜像上传功能</p>	
11	云接入网关	<p>整体要求：云接入网关提供通用裸机接入 VPC、混合云网络，单个云接入网关实例支持 48 台裸机 2x10/25GE 网络接入</p> <p>功能要求：支持多种接入方式，包括硬件设备、软件客户端和虚拟设备</p> <p>支持双机热备和负载均衡，确保网络连接的高可用性</p> <p>支持云服务访问，裸机可通过 anytunnel，singletunnel vip 访问云服务的能力</p> <p>支持 IPsec VPN 和 SSL VPN，保障数据传输的安全性。</p> <p>支持用户自定义镜像，镜像文件格式支持 .tgz、.qcow2。</p> <p>支持带外管理，支持服务器上下电；</p> <p>支持云服务访问，裸机可通过 anytunnel，singletunnel vip 访问云服务的能力</p>	

## 11 质量标准和验收方案

### 11.1 质量标准

11.1.1 中标人所交付的信息系统应满足本项目合同文件明确的功能性、使用性要求。信息系统的质量标准按照国家标准和招标需求确定，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招标目的的特定标准确定。

11.1.2 中标人所交付的信息系统还应符合国家和上海市有关系统运行安全之规定。

## 11.2 验收方案

11.2.1 本项目验收将由采购人组织进行，采购人也可委托第三方组织验收。

11.2.2 非国产化政务云平台和国产化政务云平台应满足 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》三级要求，并由中标人分别提供网络安全等级保护三级测评报告。

11.2.3 国产化政务云平台应满足 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，并由中标人提供商用密码应用安全性评估报告。

## 12 人员及设备配备要求

### 12.1 人员要求

(1) 中标人应为本项目单独建立运维管理组织，配置相应团队。

(2) 包 1 岗位要求详见人员岗位配置表：

人员岗位配置表

序号	岗位名称	具体要求	数量要求	备注
1	项目经理	具有高级工程师或同等级别证书，承担过同类项目经验。如具有 PMP 项目管理的能力证书请提供相关证明文件。	1	
2	实施工程师	其中 1 人为实施工程师负责人。 其中 5 人具备中级工程师及以上能力证书，其余 5 人如有 PMP、网络、云平台、安全专业能力证书请提供相关证明文件。	10	
3	核心运维工程师	具有同类项目维护经验，负责项目整体运维。 其中 5 人具备中级工程师及以上能力证书，其余 5 人如有信息安全、云相关专业能力证书请提供相关证明文件。 明确 1 人为运维工程师负责人。	10	
4	运维工程师	具有同类项目运维经验，负责项目运维支撑服务。运营人员 12 人（其中云设备服务原厂工程师 7 人，备份设备服务原厂工程师 1 人）。 如有云相关专业认证证书，请在投标文件中提供。	12	
	合计		33	

投标文件请附有相关证明资料（包括但不限于资格证书、在职证明材料等）。

(3) 包 2 岗位要求详见人员岗位配置表：

人员岗位配置表

序号	岗位名称	具体要求	数量要求	备注
1	项目经理	具有高级工程师或同等级别证书，承担过同类项目经验。如有云计算架构师证书、PMP 等相关能力证明请提供证明资料。	1	

序号	岗位名称	具体要求	数量要求	备注
2	实施工程师	具有同类项目实施经验，负责项目实施。 明确 1 人为技术负责人。 如有信息安全、云相关专业认证证书，请在投标文件中提供。	5	
3	核心运维工程师	具有同类项目维护经验，负责项目整体运维。 明确 1 人为运维负责人。 如有信息安全、云相关专业认证证书，请在投标文件中提供。	7	
4	运维工程师	具有同类项目维护经验，负责项目运维。 如有信息安全、云相关专业认证证书，请在投标文件中提供。	20	
	合计		33	

投标文件请附有相关证明资料（包括但不限于资格证书、在职证明材料等）。

**（4）包 3 岗位要求详见人员岗位配置表：**

**人员岗位配置表**

序号	岗位名称	具体要求	数量要求	备注
1	项目经理	具有高级工程师或同等级别证书，承担过同类项目经验。请提供相关证明资料。	1	
2	运维工程师	具有同类项目维护经验，负责项目整体运维。如有信息安全、云相关专业认证证书，请在投标文件中提供。 密码服务提供 1 人及以上的专职支持人员驻场服务。	8	
3	运营工程师	具有同类项目运营经验，负责项目整体运营。如有云相关专业认证证书，请在投标文件中提供。	2	
	合计		11	

投标文件请附有相关证明资料（包括但不限于资格证书、在职证明材料等）。

**12.2 设备要求**

中标人在实施本项目时，配备能完成本项目的相关材料、制品、设备、车辆等，相关费用包含在报价中。

**13 安全生产、文明施工（安装）与环境保护要求**

13.1 投标人应具备上海市或有关行业管理部门规定的在本市进行相关安装、调试服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由投标人自行负责。

13.2 在项目安装、调试实施期间为确保安装作业区域及周围环境的整洁和不影响其他活动正常进行，中标人应严格执行国家与上海市有关安全文明施工（安装）管理的法律、法规和政策，积极主动加强和落实安全文明施工（安装）及环境保护等有关管理工作，并按规定承担相应的费用。中标人若

违反规定野蛮施工、违章作业等原因造成的一切损失和责任由中标人承担。

13.3 中标人在项目供货、安装实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

13.4 中标人现场设备安装负责人应具有专业证书，安装人员必须持证上岗。中标人应对设备安装、调试期间自身和第三方安全与财产负责。

13.5 中标人在组织项目实施时必须按安装施工计划协调好现场施工（安装）工作，在项目验收合格移交前对到场货物承担保管责任。中标人在项目实施期间必须保护好施工区域内的环境和原有建筑、装饰与设施，保证环境和原有建筑、装饰与设施完好。

13.6 各投标人在投标文件中要结合本项目的特点和采购人上述的具体要求制定相应的安全文明施工（安装）和安全生产管理措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价措施费中列支必须的费用清单。

## **14 售后服务要求（包括延伸服务要求）**

### **14.1 具体服务承诺**

云平台运维提供热线电话、电子邮件等技术支持方式，提供每周 7 天×24 小时电话响应服务。投标人提供每周 7 天×24 小时的运维服务保障。

#### **（1）日常监控：**

对云平台进行日常监控，包括监控告警的处理等。

#### **（2）故障处理：**

处理发生的云平台软硬件、通信线路等故障，确保云平台能够正常稳定运行；其中故障处理流程需要规定处理时限及当前处理环节的责任部门和责任人。

#### **（3）安全服务：**

提供政务云平台各个基础组件进行安全策略配置、安全扫描和系统漏洞的安全加固服务。提供政务云常规安全保障和监控预警工作。

#### **（4）节假日保障：**

重大节假日期间进行政务云平台运行和信息安全的重点保障工作。中标人如具备本市重大事件运营保障能力和经验，请在投标文件中提供相关证明文件。

### **14.2 具体制度要求**

中标人应建立完善的政务云运维和安全管理制度的，建立的制度包括但不限于：

（1）政务云日常运行维护管理制度。例如：故障处理、配置变更、安全策略优化、运行监控等。

（2）运维人员管理制度。如：运维团队人员服务管理、机房进出人员管理等。

## **15 项目的保密和知识产权**

15.1 中标人保证对其提供的服务及出售的标的物享有合法的权利，应保证在其出售的标的物上不存在任何未曾向采购人透露的担保物权，如抵押权、质押权、留置权等。

15.2 采购人委托开发软件的知识产权归采购人所有。中标人向采购人交付使用的信息系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。

15.3 在本合同项下的任何权利和义务不因中标人发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则中标人的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对采购人承担连带责任。

15.4 中标人应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。

15.5 采购人具有源代码修改权和永久使用权。采购人对本次开发的软件拥有产权，具有软件开发平台的永久使用权，中标人在售后维护期内（包括续签的售后服务期）应提供软件开发平台的后续升级及因开发平台升级导致的应用软件升级服务。

15.6 如采购人使用该标的物构成上述侵权的，则中标人承担全部责任。

## 16 技术培训

### 16.1 技术文件

中标人提供本系统的详细技术文件。

### 16.2 技术服务

投标人应在投标文件中详细说明技术指导和技术支持的范围和程度。

## 四、投标报价须知

### 17 投标报价依据

17.1 投标报价计算依据包括本项目的招标文件（包括提供的附件）、招标文件答疑或修改的补充文书、工作量清单、项目现场条件等。

17.2 招标文件明确的项目范围、实施内容、实施期限、质量要求、售后服务、管理要求与标准及考核要求等。

#### 17.3 工作量清单说明

17.3.1 工作量清单应与投标人须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

17.3.2 采购人提供的工作量清单是依照采购需求测算出的主要工作内容，允许投标人对工作量清单内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各投标人应认真了解招标需求，如发现核心工作内容和实际采购需求不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件或补充文件予以更正，否则，应以工作量清单为准。

### 18 投标报价内容

18.1 本项目报价为全费用报价，是履行合同的最终价格，除投标需求中另有说明外，投标报价（即投标总价）应包括项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。

18.2 投标报价中投标人应考虑本项目可能存在的风险因素。投标报价应将所有工作内容考虑在内，如有漏项或缺项，均属于投标人的风险，其费用视作已分配在报价明细表内单价或总价之中。投标人应逐项计算并填写单价、合计价和总价。

18.3 在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，投标人应自行考虑，在合同履约期内中标价不作调整。

18.4 投标人按照投标文件格式中所附的表式完整地填写《开标一览表》及各类投标报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

### 19 投标报价控制性条款

19.1 投标报价不得超过公布的预算金额或最高限价，其中各分项报价（如有要求）均不得超过对应的预算金额或最高限价。

19.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

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

★19.4 经评标委员会审定，投标报价存在下列情形之一的，该投标文件作无效标处理：

19.4.1 减少工作量清单中主要工作内容数量；

19.4.2 投标报价和技术方案明显不相符的。

## 五、政府采购政策

### 20 节能产品政府采购

20.1 按照《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“节能产品品目清单”中的，在技术、服务等指标同等条件下，应当优先采购节能产品。采购人需购买的材料产品属于政府强制采购节能产品品目的，投标人必须选用节能产品。

20.2 投标人如选用节能产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的节能产品的认证证书；反之，该产品在评标时不被认定为节能产品。

### 21 环境标志产品政府采购

21.1 按照《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“环境标志产品品目清单”中的，在性能、技术、服务等指标同等条件下，应当优先采购环境标志产品。

21.2 投标人如选用环境标志产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书；反之，该产品在评标时不被认定为环境标志产品。

### 22 促进中小企业发展

22.1 中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业〔2011〕300号）执行，参加投标的中小企业应当提供《中小企业声明函》（具体格式见“投标文件格式”），反之，视作非中小企业，不享受相应的扶持政策。如项目允许联合体参与竞争的，则联合体中的中小企业均应按本款要求提供《中小企业声明函》。

22.2 依据市财政局 2015 年 9 月发布的《关于执行促进中小企业发展政策相关事宜的通知》，事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

22.3 如项目允许联合体参与竞争的，组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

22.4 对于小型、微型企业，按照《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）和《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）规定，其报价给予 **10%** 的扣除，用扣除后的价格参与评审。

22.5 如项目允许联合体参与竞争的，且联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，其报价给予 **10%** 的扣除，用扣除后的价格参与评审。反之，依照联合体协议约定，小型、微型企业的协议合同金额占到联合体协议合同总金额 30% 以上的，给予联合体 **4%** 的价格扣除，用扣

除后的价格参与评审。

22.6 供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

### 23 实施本国产品标准 （本项目不适用）

23.1 按照《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，供应商提供的产品符合本国产品标准的，应提供《关于符合本国产品标准的声明函》（具体格式见“投标文件格式”）或财政部会同有关部门规定的有关证明文件，出具材料符合要求的，视为本国产品，反之，则视为非本国产品。

23.2 政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对本国产品给予价格评审优惠，对本国产品的报价给予 20% 的价格扣除，用扣除后的价格参与评审。

当采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到 80% 以上时，依法对该供应商提供的全部产品给予价格评审优惠，即对该供应商提供的全部产品的总报价给予 20% 的价格扣除，用扣除后的价格参与评审。全部产品是指本项目或本包件中包含的全部货物、服务产品，产品成本以相关会计核算数据、采购合同、进货记录等为基础进行计算。

23.3 供应商提供虚假《关于符合本国产品标准的声明函》、虚假证明文件谋取中标、成交的，依照《中华人民共和国政府采购法》等法律法规规定追究相应责任。

### 24 促进残疾人就业（注：仅残疾人福利单位适用）

24.1 符合财库〔2017〕141 号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

24.2 残疾人福利性单位在参加政府采购活动时，应当按财库〔2017〕141 号规定的《残疾人福利性单位声明函》（具体格式详见“投标文件格式”），并对声明的真实性负责。

## 第三章 采购合同

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]

法定代表人：[合同中心-供应商法人姓名]

（[合同中心-供应商法人性别]）

地址：[合同中心-采购单位所在地]

地址：[合同中心-供应商所在地]

邮政编码：[合同中心-采购单位邮编]

邮政编码：[合同中心-供应商单位邮编]

电话：[合同中心-采购单位联系人电话]

电话：[合同中心-供应商联系人电话]

传真：[合同中心-采购单位传真]

传真：[合同中心-供应商单位传真]

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》及其他有关法律法规之规定，本合同当事人遵循平等、自愿、公平和诚实信用原则，在本项目经过政府采购的基础上，经协商一致，同意按下述条款和条件签署本合同：

### 一、合同主要要素：

1、乙方根据本合同的规定执行及完成合同文件所说明的本信息系统项目集成设计、设备、材料供货、安装、系统调试、技术支撑、售后服务等工作。

乙方所提供的信息系统及其各部分组成来源应符合国家的有关规定，信息系统的配置、功能、规格、等级、版本、数量、价格和交付日期等详见合同文件。

2、合同金额：本合同金额为人民币[合同中心-合同总价]元整，大写：[合同中心-合同总价大写]，与交付的信息系统及履行本合同项下其他义务等涉及的所有费用均包含在该合同金额中，买方不再另行支付任何费用。

3、服务期限：[合同中心-合同有效期]

4、服务地点：上海市浦东新区迎春路 520 号（采购人指定地址）。

5、交付状态：安装、调试、经试运行并验收合格后交付。

6、质量保证期：质量保证期要求按照合同文件规定执行。整体质量保证期从项目验收通过并交付之日后起计。

7、付款方式：分期付款

8、履约保证金：无

9、其它：无

### 二、合同文件的组成和解释顺序如下：

1、本合同执行中双方共同签署的补充与修正文件及双方确认的明确双方权利、义务的会谈纪要；

2、本合同书

3、本项目中标或成交通知书

4、乙方的本项目投标文件或响应文件

5、本项目招标文件或采购文件中的合同条款

6、本项目招标文件或采购文件中的采购需求

7、其他合同文件（需列明）

上述文件互相补充和解释，如有不明确或不一致之处，按照上述文件次序在先者为准。同一层次合同文件有矛盾的，以时间较后的为准。

### 三、合同条款：

## 1 质量标准和要求

1.1 乙方所交付信息系统的质量标准按照国家标准、行业标准或制造厂商企业标准确定，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。

1.2 乙方所交付的信息系统还应符合国家和上海市有关安全、环保、卫生之规定。

## 2 权利瑕疵担保

2.1 乙方保证对其交付的信息系统享有合法的权利，并且就交付的信息系统不做任何的权利保留。

2.2 乙方保证在其交付的信息系统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，不存在会造成甲方任何合同外义务的负担。

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

2.4 如甲方使用该信息系统构成上述侵权的，则由乙方承担全部责任。

## 3 系统集成实施、试运行与验收

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

3.2 乙方应负责系统及系统设备在实施现场就位安装和调试、操作培训等的全部工作，按照合同文件工作与管理要求负责对项目进度的安排、现场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患。由于乙方管理与安全措施不力造成事故的责任和因此发生的费用，由乙方承担。

3.3 系统具备隐蔽条件或达到中间验收部位，乙方进行自检，并在隐蔽或中间验收前 48 小时以书面形式通知甲方、监理验收。通知包括隐蔽和中间验收的内容、验收时间和地点。乙方准备验收记录，验收合格，监理工程师在验收记录上签字后，乙方可进行隐蔽和继续施工。验收不合格，乙方在工程师限定的时间内修改后重新验收。

3.4 乙方应在进行系统交付前 5 个工作日内，以书面方式通知甲方并向甲方提供完整的竣工资料、竣工验收报告及竣工图。甲方应当在接到通知与资料的 5 个工作日内安排交付验收。乙方在交付前应当根据合同文件中的检测标准对本项目进行功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

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

3.6 甲方在本项目交付后，应当在 5 个工作日内向乙方出具书面文件，以确认其初步达到符合本合同所约定信息系统的任务、需求和功能。如有缺陷，应向乙方陈述需要改进的缺陷。乙方应立即改进此项缺陷，并再次进行检测和评估。期间乙方需承担由自身原因造成修改的费用。甲、乙双方将重复 3.4、3.6 项程序直至甲方领受或甲方依法或依约终止本合同为止。

3.7 自系统功能检测通过之日起，甲方拥有（/）天的系统试运行权利。系统验收通过的日期为实际竣工日期。

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

3.9 如果由于甲方原因，导致系统在试运行期间出现故障或问题，乙方应及时配合排除该方面的

故障或问题。以上行为产生的相关费用均由甲方承担。

3.10 系统试运行完成后，甲方应及时进行系统验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 5 个工作日内，确定具体日期，由双方按照本合同的规定完成系统验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

3.11 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时延长试运行期（/）个工作日，直至系统完全符合验收标准。

3.12 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。

3.13 甲方根据信息系统的技术规格要求和质量标准，对信息系统验收合格，签署验收意见。

#### 4 知识产权和保密

4.1 甲方委托开发软件的知识产权归甲方所有。乙方向甲方交付使用的信息系统已享有知识产权的，甲方可在合同文件明确的范围内自主使用。

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

4.3 乙方应遵守合同文件约定内容的保密要求。如果甲方提供的内容涉及保密事项的，应签订保密协议，甲乙双方均有保密义务。

#### 5 付款

5.1 本合同以人民币付款（单位：元）。

5.2 本合同款项按照以下方式支付。

5.2.1 付款方式：本合同付款按照下表付款内容和付款次序分期付款。

5.2.2 付款条件：

（1）第一笔付款-交付付款（80%）：合同签订后，甲方收到乙方关于系统交付报告和发票，经甲方审核均符合要求后 30 日内，向乙方支付合同金额 80%。

（2）第二笔付款-最终验收付款（20%）：项目验收通过，且甲方收到乙方发票后 30 日内，按照验收通过并审定的价格向乙方支付合同尾款。

#### 6 辅助服务

6.1 乙方应提交所提供硬件设备的技术文件，包括相应的每一套设备和仪器的中文技术文件，例如：产品目录、图纸、操作手册、使用说明、维护手册和/或服务指南。这些文件应包装好随同设备一起发运。

6.2 乙方还应提供下列服务：

（1）硬件设备的现场移动、安装、调试及技术支持；

（2）提供系统集成和维修所需的专用工具和辅助材料；

（3）在质量保证期内对交付的信息系统实施运行监督、维护、维修；

（4）乙方应根据项目实施的计划、进度和甲方的合理要求，及时安排对甲方的相关人员进行培训。培训目标为使受训者能够独立、熟练地完成操作，实现依据本合同所规定的信息系统的目标和功能。

6.3 辅助服务的费用应包含在合同价中，甲方不再另行支付。

#### 7 系统保证和维护

7.1 在乙方所交付的信息系统中，不得含有未经甲方许可的自动终止或妨碍系统运作的软件

和硬件，否则，乙方应承担赔偿责任；

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

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

7.4 乙方自各项目交付验收通过之日起（）内向甲方提供免费的保修和维护服务并对由于设计、功能、工艺或材料的缺陷而产生的故障负责。如果厂商对系统产品中的相应部分的保修期超过上述期限的，则按厂商规定进行免费保修。在此期间如发生系统运作故障，或出现瑕疵，乙方将按照售后服务的承诺（见合同附件）提供保修和维护服务。

7.5 乙方应保证所供信息系统是全新的、未使用过的。在质量保证期内，如果信息系统的质量或规格与合同不符，或证实信息系统是有缺陷的，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 8 条规定以书面形式向乙方提出补救措施或索赔。

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

7.7 在保修期内如由于乙方的责任而需要对本信息系统中的部件（包括软件和硬件）予以更换或升级，则该部件的保修期应相应延长。

## 8 补救措施和索赔

8.1 甲方有权根据合同文件要求或质量检测部门出具的检验证书向乙方提出索赔。

8.2 在质量保证期内，如果乙方对缺陷产品负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）乙方同意退货并将货款退还给甲方，由此发生的一切费用和损失由乙方承担。

（2）根据信息系统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信息系统的价格。

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

8.3 如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付货款中扣除索赔金额或者没收**履约保证金**，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

## 9 履约延误

9.1 乙方应按照合同规定的时间、地点、质量标准完成本系统集成和提供相关服务。

9.2 如乙方无正当理由而拖延交货，甲方有权没收乙方提供的履约保证金，并解除合同并追究乙方的违约责任。

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

## 10 误期赔偿

10.1 除合同第 11 条规定外，如果乙方没有按照合同规定的时间交货和提供服务，甲方应从货款

中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（周）赔偿迟交货物的交货价或延期服务的服务费用的百分之零点五（0.5%）计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

## 11 不可抗力

11.1 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。

11.2 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：战争、洪水、六级及以上地震、国家政策的重大变化，以及双方商定的其他事件。

11.3 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。

## 12 履约保证金（不适用）

12.1 为保证乙方按合同约定的服务质量履行合同，乙方需向甲方提交履约保证金。乙方在收到成交通知书后三十日内，并在签订合同协议书之前，按合同总价%的金额向甲方提交履约保证金。合同存续期间，履约保证金不得撤回。

12.2 履约保证金可以采用支票、汇票、本票、保函等非现金形式。前述票据及保函的期限应覆盖自出具之日起至完成服务且验收合格之日止的期间，如未覆盖需重新按合同规定提交。乙方提交履约保证金所需费用均由乙方负担。

12.3 乙方不履行与甲方订立的合同或者履行合同不符合约定，致使不能实现合同目的的，履约保证金不予退还，给甲方造成的损失超过履约保证金数额的，还应当对超过部分予以赔偿；乙方未按约定提交履约保证金的，应当对甲方的损失承担赔偿责任。除本款所列情形外，甲方不得以其他理由拒绝退还履约保证金。

12.4 按合同约定考核验收合格后 15 日内，甲方通过支票、汇票、本票、保函等非现金形式一次性将履约保证金（全额或扣减后剩余金额部分）无息退还乙方。无正当理由逾期不退的，甲方应以应退还履约保证金数额按人民银行同期存款基准利率按日向乙方承担利息损失，直至上述履约保证金退还乙方。

## 13 争端的解决

13.1 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。

13.2 如合同各方协商解决不成，可以向有关部门申请调解，或就争议事项向浦东新区人民法院提起诉讼。

13.3 在诉讼期间，除正在进行诉讼的部分外，本合同的其它部分应继续履行。败诉一方应当承担包括但不限于诉讼费用、律师费用、公证费用等。

## 14 违约终止合同

14.1 因一方违约使合同不能履行，另一方欲终止或解除全部合同，应提前十天通知违约方后，方可按正常途径终止或解除合同，由违约方承担违约责任。

14.2 甲方不能按合同履行自己的各项义务、支付款项及发生其他使合同无法履行的行为，应赔偿因其违约造成的直接经济损失。

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

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

(2) 如果乙方未能履行合同规定的其它义务。

14.4 如果甲方根据上述 14.3 款的规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买未交付的信息系统，乙方应对购买类似的信息系统所超出的那部分费用负责，并赔偿因其违约造成的直接经济损失。但是，乙方应继续执行合同中未终止的部分。

### 15 破产终止合同

15.1 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。

### 16 合同转让和分包

16.1 乙方应全面、适当履行本合同项下义务，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。

16.2 若甲方事先书面同意分包，乙方应书面通知甲方本合同项下所授予的所有分包合同。乙方与分包单位签订分包合同前，应将副本送甲方认可。分包合同签订后，应将副本留存甲方处备案。若分包合同与本合同发生抵触，则以本合同为准。

16.3 分包合同必须符合本合同的规定，接受分包的单位应当具备招标文件及本合同规定的资质(资格)条件。

16.4 分包合同不能解除乙方在本合同中应承担的任何义务和责任。乙方应对分包项目派驻相应监督管理人员，保证合同的履行。分包单位的任何违约或疏忽，均视为乙方的违约或疏忽。

### 17 合同生效

17.1 本合同在合同各方签字盖章后生效。

17.2 本合同一式 3 份，以中文书写，签字各方各执 1 份，另有一份报财政部门备案。

17.3 本合同中双方的地址、传真等联系方式为各自文书、信息送达地址。以专人传送的，受送达人签收即构成送达；以邮件或快递形式送达的，对方签收、拒签、退回之日视为送达；甲乙双方可以采用能够确认对方收悉的电子方式送达文书，电子送达可以采用传真、电子邮件等即时收悉的特定系统作为送达媒介，以送达信息到达受送达人特定系统的日期为送达日期。前述地址同时也作为双方争议发生时的各自法律文书送达地址（包括原审、二审、再审、执行及仲裁等），变更须提前书面通知对方，原送达地址在收到变更通知之前仍为有效送达地址。

### 18 合同附件

18.1 本合同附件包括：招标文件、投标文件等。

18.2 本合同附件与合同具有同等效力。

18.3 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。

### 19 合同修改

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

**[合同中心-补充条款列表]**

**[合同文档模版-其他补充事宜]**

签约各方：

甲方（盖章）：

乙方（盖章）：

法定代表人或授权委托人（签章）：

法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]**

日期：**[合同中心-签订时间\_1]**

合同签订点：网上签约

包 2 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]**

法定代表人：**[合同中心-供应商法人姓名]**

**([合同中心-供应商法人性别])**

地址：**[合同中心-采购单位所在地]**

地址：**[合同中心-供应商所在地]**

邮政编码：**[合同中心-采购单位邮编]**

邮政编码：**[合同中心-供应商单位邮编]**

电话：**[合同中心-采购单位联系人电话]**

电话：**[合同中心-供应商联系人电话]**

传真：**[合同中心-采购单位传真]**

传真：**[合同中心-供应商单位传真]**

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》及其他有关法律法规之规定，本合同当事人遵循平等、自愿、公平和诚实信用原则，在本项目经过政府采购的基础上，经协商一致，同意按下述条款和条件签署本合同：

**一、合同主要要素：**

- 1、乙方根据本合同的规定执行及完成合同文件所说明的本信息系统项目集成设计、设备、材料

供货、安装、系统调试、技术支撑、售后服务等工作。

乙方所提供的信息系统及其各部分组成来源应符合国家的有关规定，信息系统的配置、功能、规格、等级、版本、数量、价格和交付日期等详见合同文件。

2、合同金额：本合同金额为人民币**[合同中心-合同总价]**元整，大写：**[合同中心-合同总价大写]**，与交付的信息系统及履行本合同项下其他义务等涉及的所有费用均包含在该合同金额中，买方不再另行支付任何费用。

3、服务期限：**[合同中心-合同有效期]**

4、服务地点：上海市浦东新区迎春路 520 号（采购人指定地址）。

5、交付状态：安装、调试、经试运行并验收合格后交付。

6、质量保证期：质量保证期要求按照合同文件规定执行。整体质量保证期从项目验收通过并交付之日后起计。

7、付款方式：分期付款

8、履约保证金：无

9、其它：无

## 二、合同文件的组成和解释顺序如下：

- 1、本合同执行中双方共同签署的补充与修正文件及双方确认的明确双方权利、义务的会谈纪要；
- 2、本合同书
- 3、本项目中标或成交通知书
- 4、乙方的本项目投标文件或响应文件
- 5、本项目招标文件或采购文件中的合同条款
- 6、本项目招标文件或采购文件中的采购需求
- 7、其他合同文件（需列明）

上述文件互相补充和解释，如有不明确或不一致之处，按照上述文件次序在先者为准。同一层次合同文件有矛盾的，以时间较后的为准。

## 三、合同条款：

### 1 质量标准和要求

1.1 乙方所交付信息系统的质量标准按照国家标准、行业标准或制造厂商企业标准确定，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。

1.2 乙方所交付的信息系统还应符合国家和上海市有关安全、环保、卫生之规定。

### 2 权利瑕疵担保

2.1 乙方保证对其交付的信息系统享有合法的权利，并且就交付的信息系统不做任何的权利保留。

2.2 乙方保证在其交付的信息系统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，不存在会造成甲方任何合同外义务的负担。

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

2.4 如甲方使用该信息系统构成上述侵权的，则由乙方承担全部责任。

### 3 系统集成实施、试运行与验收

3.1 甲方应依据信息系统项目工程的条件和性质，按照合同文件明确的要求向乙方提供信息系统的施工、安装和集成环境。如甲方未能在该时间内提供该施工和安装环境，乙方可相应顺延交付日期。

如对乙方造成经济损失，甲方还应依本合同规定承担违约责任。

3.2 乙方应负责系统及系统设备在实施现场就位安装和调试、操作培训等的全部工作，按照合同文件工作与管理要求负责对项目进度的安排、现场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患。由于乙方管理与安全措施不力造成事故的责任和因此发生的费用，由乙方承担。

3.3 系统具备隐蔽条件或达到中间验收部位，乙方进行自检，并在隐蔽或中间验收前 48 小时以书面形式通知甲方、监理验收。通知包括隐蔽和中间验收的内容、验收时间和地点。乙方准备验收记录，验收合格，监理工程师在验收记录上签字后，乙方可进行隐蔽和继续施工。验收不合格，乙方在工程师限定的时间内修改后重新验收。

3.4 乙方应在进行系统交付前 5 个工作日内，以书面方式通知甲方并向甲方提供完整的竣工资料、竣工验收报告及竣工图。甲方应当在接到通知与资料的 5 个工作日内安排交付验收。乙方在交付前应当根据合同文件中的检测标准对本项目进行功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

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

3.6 甲方在本项目交付后，应当在 5 个工作日内向乙方出具书面文件，以确认其初步达到符合本合同所约定信息系统的任务、需求和功能。如有缺陷，应向乙方陈述需要改进的缺陷。乙方应立即改进此项缺陷，并再次进行检测和评估。期间乙方需承担由自身原因造成修改的费用。甲、乙双方将重复 3.4、3.6 项程序直至甲方领受或甲方依法或依约终止本合同为止。

3.7 自系统功能检测通过之日起，甲方拥有（/）天的系统试运行权利。系统验收通过的日期为实际竣工日期。

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

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

3.10 系统试运行完成后，甲方应及时进行系统验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 5 个工作日内，确定具体日期，由双方按照本合同的规定完成系统验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

3.11 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时延长试运行期（/）个工作日，直至系统完全符合验收标准。

3.12 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。

3.13 甲方根据信息系统的技术规格要求和质量标准，对信息系统验收合格，签署验收意见。

#### **4 知识产权和保密**

4.1 甲方委托开发软件的知识产权归甲方所有。乙方向甲方交付使用的信息系统已享有知识产权的，甲方可在合同文件明确的范围内自主使用。

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

4.3 乙方应遵守合同文件约定内容的保密要求。如果甲方提供的内容涉及保密事项的，应签订保密协议，甲乙双方均有保密义务。

## 5 付款

5.1 本合同以人民币付款（单位：元）。

5.2 本合同款项按照以下方式支付。

5.2.1 付款方式：本合同付款按照下表付款内容和付款次序分期付款。

5.2.2 付款条件：

（1）第一笔付款-交付付款（80%）：合同签订后，甲方收到乙方关于系统交付报告和发票，经甲方审核均符合要求后 30 日内，向乙方支付合同金额 80%。

（2）第二笔付款-最终验收付款（20%）：项目验收通过，且甲方收到乙方发票后 30 日内，按照验收通过并审定的价格向乙方支付合同尾款。

## 6 辅助服务

6.1 乙方应提交所提供硬件设备的技术文件，包括相应的每一套设备和仪器的中文技术文件，例如：产品目录、图纸、操作手册、使用说明、维护手册和/或服务指南。这些文件应包装好随同设备一起发运。

6.2 乙方还应提供下列服务：

（1）硬件设备的现场移动、安装、调试及技术支持；

（2）提供系统集成和维修所需的专用工具和辅助材料；

（3）在质量保证期内对交付的信息系统实施运行监督、维护、维修；

（4）乙方应根据项目实施的计划、进度和甲方的合理要求，及时安排对甲方的相关人员进行培训。培训目标为使受训者能够独立、熟练地完成操作，实现依据本合同所规定的信息系统的目标和功能。

6.3 辅助服务的费用应包含在合同价中，甲方不再另行支付。

## 7 系统保证和维护

7.1 在乙方所交付的信息系统中，不得含有未经甲方许可的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；

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

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

7.4 乙方自各项目交付验收通过之日起（ ）内向甲方提供免费的保修和维护服务并对由于设计、功能、工艺或材料的缺陷而产生的故障负责。如果厂商对系统产品中的相应部分的保修期超过上述期限的，则按厂商规定进行免费保修。在此期间如发生系统运作故障，或出现瑕疵，乙方将按照售后服务的承诺（见合同附件）提供保修和维护服务。

7.5 乙方应保证所供信息系统是全新的、未使用过的。在质量保证期内，如果信息系统的质量或规格与合同不符，或证实信息系统是有缺陷的，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 8 条规定以书面形式向乙方提出补救措施或索赔。

7.6 乙方在约定的时间内未能弥补缺陷，甲方可以采取必要的补救措施，但其风险和费用将由乙方

承担，甲方根据合同规定对乙方行使的其他权利不受影响。

7.7 在保修期内如由于乙方的责任而需要对本信息系统中的部件（包括软件和硬件）予以更换或升级，则该部件的保修期应相应延长。

## 8 补救措施和索赔

8.1 甲方有权根据合同文件要求或质量检测部门出具的检验证书向乙方提出索赔。

8.2 在质量保证期内，如果乙方对缺陷产品负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）乙方同意退货并将货款退还给甲方，由此发生的一切费用和损失由乙方承担。

（2）根据信息系统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信息系统的价格。

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

8.3 如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付货款中扣除索赔金额或者没收**履约保证金**，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

## 9 履约延误

9.1 乙方应按照合同规定的时间、地点、质量标准完成本系统集成和提供相关服务。

9.2 如乙方无正当理由而拖延交货，甲方有权没收乙方提供的履约保证金，并解除合同并追究乙方的违约责任。

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

## 10 误期赔偿

10.1 除合同第 11 条规定外，如果乙方没有按照合同规定的时间交货和提供服务，甲方应从货款中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（周）赔偿迟交货物的交货价或延期服务的服务费用的百分之零点五（0.5%）计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（**一周按七天计算，不足七天按一周计算。**）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

## 11 不可抗力

11.1 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。

11.2 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：战争、洪水、六级及以上地震、国家政策的重大变化，以及双方商定的其他事件。

11.3 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。

## 12 履约保证金（不适用）

12.1 为保证乙方按合同约定的服务质量履行合同，乙方需向甲方提交履约保证金。乙方在收到成交通知书后三十日内，并在签订合同协议书之前，按合同总价%的金额向甲方提交履约保证金。合同存续期间，履约保证金不得撤回。

12.2 履约保证金可以采用支票、汇票、本票、保函等非现金形式。前述票据及保函的期限应覆盖自出具之日起至完成服务且验收合格之日止的期间，如未覆盖需重新按合同规定提交。乙方提交履约保证金所需费用均由乙方负担。

12.3 乙方不履行与甲方订立的合同或者履行合同不符合约定，致使不能实现合同目的的，履约保证金不予退还，给甲方造成的损失超过履约保证金数额的，还应当对超过部分予以赔偿；乙方未按约定提交履约保证金的，应当对甲方的损失承担赔偿责任。除本款所列情形外，甲方不得以其他理由拒绝退还履约保证金。

12.4 按合同约定考核验收合格后 15 日内，甲方通过支票、汇票、本票、保函等非现金形式一次性将履约保证金（全额或扣减后剩余金额部分）无息退还乙方。无正当理由逾期不退的，甲方应以应退还履约保证金数额按人民银行同期存款基准利率按日向乙方承担利息损失，直至上述履约保证金退还乙方。

### **13 争端的解决**

13.1 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。

13.2 如合同各方协商解决不成，可以向有关部门申请调解，或就争议事项向浦东新区人民法院提起诉讼。

13.3 在诉讼期间，除正在进行诉讼的部分外，本合同的其它部分应继续履行。败诉一方应当承担包括但不限于诉讼费用、律师费用、公证费用等。

### **14 违约终止合同**

14.1 因一方违约使合同不能履行，另一方欲终止或解除全部合同，应提前十天通知违约方后，方可按正常途径终止或解除合同，由违约方承担违约责任。

14.2 甲方不能按合同履行自己的各项义务、支付款项及发生其他使合同无法履行的行为，应赔偿因其违约造成的直接经济损失。

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

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

（2）如果乙方未能履行合同规定的其它义务。

14.4 如果甲方根据上述 14.3 款的规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买未交付的信息系统，乙方应对购买类似的信息系统所超出的那部分费用负责，并赔偿因其违约造成的直接经济损失。但是，乙方应继续执行合同中未终止的部分。

### **15 破产终止合同**

15.1 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。

### **16 合同转让和分包**

16.1 乙方应全面、适当履行本合同项下义务，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。

16.2 若甲方事先书面同意分包，乙方应书面通知甲方本合同项下所授予的所有分包合同。乙方与

分包单位签订分包合同前，应将副本送甲方认可。分包合同签订后，应将副本留存甲方处备案。若分包合同与本合同发生抵触，则以本合同为准。

16.3 分包合同必须符合本合同的规定，接受分包的单位应当具备招标文件及本合同规定的资质(资格)条件。

16.4 分包合同不能解除乙方在本合同中应承担的任何义务和责任。乙方应对分包项目派驻相应监督管理人员，保证合同的履行。分包单位的任何违约或疏忽，均视为乙方的违约或疏忽。

## 17 合同生效

17.1 本合同在合同各方签字盖章后生效。

17.2 本合同一式 3 份，以中文书写，签字各方各执 1 份，另有一份报财政部门备案。

17.3 本合同中双方的地址、传真等联系方式为各自文书、信息送达地址。以专人传送的，受送达人签收即构成送达；以邮件或快递形式送达的，对方签收、拒签、退回之日视为送达；甲乙双方可以采用能够确认对方收悉的电子方式送达文书，电子送达可以采用传真、电子邮件等即时收悉的特定系统作为送达媒介，以送达信息到达受送达人特定系统的日期为送达日期。前述地址同时也作为双方争议发生时的各自法律文书送达地址（包括原审、二审、再审、执行及仲裁等），变更须提前书面通知对方，原送达地址在收到变更通知之前仍为有效送达地址。

## 18 合同附件

18.1 本合同附件包括：招标文件、投标文件等。

18.2 本合同附件与合同具有同等效力。

18.3 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。

## 19 合同修改

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

### [合同中心-补充条款列表]

### [合同文档模版-其他补充事宜]

签约各方：

甲方（盖章）：

乙方（盖章）：

法定代表人或授权委托人（签章）：

法定代表人或授权委托人（签章）：

日期：[合同中心-签订时间]

日期：[合同中心-签订时间\_1]

合同签订点：网上签约

包 3 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]

法定代表人： [合同中心-供应商法人姓名]

（ [合同中心-供应商法人性别] ）

地址： [合同中心-采购单位所在地]

地址： [合同中心-供应商所在地]

邮政编码： [合同中心-采购单位邮编]

邮政编码： [合同中心-供应商单位邮编]

电话： [合同中心-采购单位联系人电话]

电话： [合同中心-供应商联系人电话]

传真： [合同中心-采购单位传真]

传真： [合同中心-供应商单位传真]

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》及其他有关法律法规之规定，本合同当事人遵循平等、自愿、公平和诚实信用原则，在本项目经过政府采购的基础上，经协商一致，同意按下述条款和条件签署本合同：

## 一、合同主要要素：

1、乙方根据本合同的规定执行及完成合同文件所说明的本信息系统项目集成设计、设备、材料供货、安装、系统调试、技术支撑、售后服务等工作。

乙方所提供的信息系统及其各部分组成来源应符合国家的有关规定，信息系统的配置、功能、规格、等级、版本、数量、价格和交付日期等详见合同文件。

2、合同金额：本合同金额为人民币 [合同中心-合同总价] 元整，大写： [合同中心-合同总价大写]，与交付的信息系统及履行本合同项下其他义务等涉及的所有费用均包含在该合同金额中，买方不再另行支付任何费用。

3、服务期限： [合同中心-合同有效期]

4、服务地点：上海市浦东新区迎春路 520 号（采购人指定地址）。

5、交付状态：安装、调试、经试运行并验收合格后交付。

6、质量保证期：质量保证期要求按照合同文件规定执行。整体质量保证期从项目验收通过并交付之日后起计。

7、付款方式：分期付款

8、履约保证金：无

9、其它：无

## 二、合同文件的组成和解释顺序如下：

- 1、本合同执行中双方共同签署的补充与修正文件及双方确认的明确双方权利、义务的会谈纪要；
- 2、本合同书
- 3、本项目中标或成交通知书
- 4、乙方的本项目投标文件或响应文件
- 5、本项目招标文件或采购文件中的合同条款
- 6、本项目招标文件或采购文件中的采购需求
- 7、其他合同文件（需列明）

上述文件互相补充和解释，如有不明确或不一致之处，按照上述文件次序在先者为准。同一层次合同文件有矛盾的，以时间较后的为准。

## 三、合同条款：

### 1 质量标准和要求

1.1 乙方所交付信息系统的质量标准按照国家标准、行业标准或制造厂商企业标准确定，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。

1.2 乙方所交付的信息系统还应符合国家和上海市有关安全、环保、卫生之规定。

### 2 权利瑕疵担保

2.1 乙方保证对其交付的信息系统享有合法的权利，并且就交付的信息系统不做任何的权利保留。

2.2 乙方保证在其交付的信息系统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，不存在会造成甲方任何合同外义务负担。

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

2.4 如甲方使用该信息系统构成上述侵权的，则由乙方承担全部责任。

### 3 系统集成实施、试运行与验收

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

3.2 乙方应负责系统及系统设备在实施现场就位安装和调试、操作培训等的全部工作，按照合同文件工作与管理要求负责对项目进度的安排、现场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患。由于乙方管理与安全措施不力造成事故的责任和因此发生的费用，由乙方承担。

3.3 系统具备隐蔽条件或达到中间验收部位，乙方进行自检，并在隐蔽或中间验收前 48 小时以书面形式通知甲方、监理验收。通知包括隐蔽和中间验收的内容、验收时间和地点。乙方准备验收记录，验收合格，监理工程师在验收记录上签字后，乙方可进行隐蔽和继续施工。验收不合格，乙方在工程师限定的时间内修改后重新验收。

3.4 乙方应在进行系统交付前 5 个工作日内，以书面方式通知甲方并向甲方提供完整的竣工资料、竣工验收报告及竣工图。甲方应当在接到通知与资料的 5 个工作日内安排交付验收。乙方在交付前应当根据合同文件中的检测标准对本项目进行功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

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

3.6 甲方在本项目交付后，应当在 5 个工作日内向乙方出具书面文件，以确认其初步达到符合本合同所约定信息系统的任务、需求和功能。如有缺陷，应向乙方陈述需要改进的缺陷。乙方应立即改进此项缺陷，并再次进行检测和评估。期间乙方需承担由自身原因造成修改的费用。甲、乙双方将重复 3.4、3.6 项程序直至甲方领受或甲方依法或依约终止本合同为止。

3.7 自系统功能检测通过之日起，甲方拥有（/）天的系统试运行权利。系统验收通过的日期为实际竣工日期。

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

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

3.10 系统试运行完成后，甲方应及时进行系统验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 5 个工作日内，确定具体日期，由双方按照本合同的规定完成系统验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

3.11 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时延长试运行期（/）个工作日，直至系统完全符合验收标准。

3.12 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。

3.13 甲方根据信息系统的技术规格要求和质量标准，对信息系统验收合格，签署验收意见。

#### **4 知识产权和保密**

4.1 甲方委托开发软件的知识产权归甲方所有。乙方向甲方交付使用的信息系统已享有知识产权的，甲方可在合同文件明确的范围内自主使用。

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

4.3 乙方应遵守合同文件约定内容的保密要求。如果甲方提供的内容涉及保密事项的，应签订保密协议，甲乙双方均有保密义务。

#### **5 付款**

5.1 本合同以人民币付款（单位：元）。

5.2 本合同款项按照以下方式支付。

5.2.1 付款方式：本合同付款按照下表付款内容和付款次序分期付款。

5.2.2 付款条件：

（1）第一笔付款-交付付款（80%）：合同签订后，甲方收到乙方关于系统交付报告和发票，经甲方审核均符合要求后 30 日内，向乙方支付合同金额 80%。

（2）第二笔付款-最终验收付款（20%）：项目验收通过，且甲方收到乙方发票后 30 日内，按照验收通过并审定的价格向乙方支付合同尾款。

#### **6 辅助服务**

6.1 乙方应提交所提供硬件设备的技术文件，包括相应的每一套设备和仪器的中文技术文件，例

如：产品目录、图纸、操作手册、使用说明、维护手册和/或服务指南。这些文件应包装好随同设备一起发运。

6.2 乙方还应提供下列服务：

- (1) 硬件设备的现场移动、安装、调试及技术支持；
- (2) 提供系统集成和维修所需的专用工具和辅助材料；
- (3) 在质量保证期内对交付的信息系统实施运行监督、维护、维修；
- (4) 乙方应根据项目实施的计划、进度和甲方的合理要求，及时安排对甲方的相关人员进行培训。培训目标为使受训者能够独立、熟练地完成操作，实现依据本合同所规定的信息系统的目标和功能。

6.3 辅助服务的费用应包含在合同价中，甲方不再另行支付。

## 7 系统保证和维护

7.1 在乙方所交付的信息系统中，不得含有未经甲方许可的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；

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

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

7.4 乙方自各项目交付验收通过之日起（ ）内向甲方提供免费的保修和维护服务并对由于设计、功能、工艺或材料的缺陷而产生的故障负责。如果厂商对系统产品中的相应部分的保修期超过上述期限的，则按厂商规定进行免费保修。在此期间如发生系统运作故障，或出现瑕疵，乙方将按照售后服务的承诺（见合同附件）提供保修和维护服务。

7.5 乙方应保证所供信息系统是全新的、未使用过的。在质量保证期内，如果信息系统的质量或规格与合同不符，或证实信息系统是有缺陷的，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 8 条规定以书面形式向乙方提出补救措施或索赔。

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

7.7 在保修期内如由于乙方的责任而需要对本信息系统中的部件（包括软件和硬件）予以更换或升级，则该部件的保修期应相应延长。

## 8 补救措施和索赔

8.1 甲方有权根据合同文件要求或质量检测部门出具的检验证书向乙方提出索赔。

8.2 在质量保证期内，如果乙方对缺陷产品负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

- (1) 乙方同意退货并将货款退还给甲方，由此发生的一切费用和损失由乙方承担。
- (2) 根据信息系统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信息系统的价格。
- (3) 乙方应在接到甲方通知后七天内负责采用符合合同规定的规格、质量和性能要求的措施和设备来更换有缺陷的部分或修补缺陷部分，其费用由乙方负担。同时，乙方应在约定的质量保证期基础上重新计算修补和/或更换件的质量保证期。

8.3 如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方

未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付货款中扣除索赔金额或者没收**履约保证金**，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

## 9 履约延误

9.1 乙方应按照合同规定的时间、地点、质量标准完成本系统集成和提供相关服务。

9.2 如乙方无正当理由而拖延交货，甲方有权没收乙方提供的履约保证金，并解除合同并追究乙方的违约责任。

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

## 10 误期赔偿

10.1 除合同第 11 条规定外，如果乙方没有按照合同规定的时间交货和提供服务，甲方应从货款中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（周）赔偿迟交货物的交货价或延期服务的服务费用的百分之零点五（0.5%）计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（**一周按七天计算，不足七天按一周计算。**）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

## 11 不可抗力

11.1 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。

11.2 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：战争、洪水、六级及以上地震、国家政策的重大变化，以及双方商定的其他事件。

11.3 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。

## 12 履约保证金（不适用）

12.1 为保证乙方按合同约定的服务质量履行合同，乙方需向甲方提交履约保证金。乙方在收到成交通知书后三十日内，并在签订合同协议书之前，按合同总价%的金额向甲方提交履约保证金。合同存续期间，履约保证金不得撤回。

12.2 履约保证金可以采用支票、汇票、本票、保函等非现金形式。前述票据及保函的期限应覆盖自出具之日起至完成服务且验收合格之日止的期间，如未覆盖需重新按合同规定提交。乙方提交履约保证金所需费用均由乙方负担。

12.3 乙方不履行与甲方订立的合同或者履行合同不符合约定，致使不能实现合同目的的，履约保证金不予退还，给甲方造成的损失超过履约保证金数额的，还应当对超过部分予以赔偿；乙方未按约定提交履约保证金的，应当对甲方的损失承担赔偿责任。除本款所列情形外，甲方不得以其他理由拒绝退还履约保证金。

12.4 按合同约定考核验收合格后 15 日内，甲方通过支票、汇票、本票、保函等非现金形式一次性将履约保证金（全额或扣减后剩余金额部分）无息退还乙方。无正当理由逾期不退的，甲方应以退还履约保证金数额按人民银行同期存款基准利率按日向乙方承担利息损失，直至上述履约保证金退

还乙方。

### 13 争端的解决

13.1 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。

13.2 如合同各方协商解决不成，可以向有关部门申请调解，或就争议事项向浦东新区人民法院提起诉讼。

13.3 在诉讼期间，除正在进行诉讼的部分外，本合同的其它部分应继续履行。败诉一方应当承担包括但不限于诉讼费用、律师费用、公证费用等。

### 14 违约终止合同

14.1 因一方违约使合同不能履行，另一方欲终止或解除全部合同，应提前十天通知违约方后，方可按正常途径终止或解除合同，由违约方承担违约责任。

14.2 甲方不能按合同履行自己的各项义务、支付款项及发生其他使合同无法履行的行为，应赔偿因其违约造成的直接经济损失。

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

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

(2) 如果乙方未能履行合同规定的其它义务。

14.4 如果甲方根据上述 14.3 款的规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买未交付的信息系统，乙方应对购买类似的信息系统所超出的那部分费用负责，并赔偿因其违约造成的直接经济损失。但是，乙方应继续执行合同中未终止的部分。

### 15 破产终止合同

15.1 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。

### 16 合同转让和分包

16.1 乙方应全面、适当履行本合同项下义务，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。

16.2 若甲方事先书面同意分包，乙方应书面通知甲方本合同项下所授予的所有分包合同。乙方与分包单位签订分包合同前，应将副本送甲方认可。分包合同签订后，应将副本留存甲方处备案。若分包合同与本合同发生抵触，则以本合同为准。

16.3 分包合同必须符合本合同的规定，接受分包的单位应当具备招标文件及本合同规定的资质(资格)条件。

16.4 分包合同不能解除乙方在本合同中应承担的任何义务和责任。乙方应对分包项目派驻相应监督管理人员，保证合同的履行。分包单位的任何违约或疏忽，均视为乙方的违约或疏忽。

### 17 合同生效

17.1 本合同在合同各方签字盖章后生效。

17.2 本合同一式 3 份，以中文书写，签字各方各执 1 份，另有一份报财政部门备案。

17.3 本合同中双方的地址、传真等联系方式为各自文书、信息送达地址。以专人传送的，受送达人签收即构成送达；以邮件或快递形式送达的，对方签收、拒签、退回之日视为送达；甲乙双方可以采用能够确认对方收悉的电子方式送达文书，电子送达可以采用传真、电子邮件等即时收悉的特定系统作为送达媒介，以送达信息到达受送达人特定系统的日期为送达日期。前述地址同时也作为双方争

议发生时的各自法律文书送达地址（包括原审、二审、再审、执行及仲裁等），变更须提前书面通知对方，原送达地址在收到变更通知之前仍为有效送达地址。

**18 合同附件**

18.1 本合同附件包括：招标文件、投标文件等。

18.2 本合同附件与合同具有同等效力。

18.3 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。

**19 合同修改**

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

**[合同中心-补充条款列表]**

**[合同文档模版-其他补充事宜]**

签约各方：

甲方（盖章）：

乙方（盖章）：

法定代表人或授权委托人（签章）：

法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]**

日期：**[合同中心-签订时间\_1]**

合同签订点：网上签约

## 第四章投标文件格式

**说明：1、投标人未按本投标文件格式填写的，或相关证书与证明材料提供不完整的，投标人需承担其投标文件在评标时被扣分甚至被评标委员会否决的风险。2、相关表式不够，可另附页填写。**

### 与评审相关的投标文件内容索引表

（此表置于投标文件首页）

项目名称或包件号：\_\_\_\_\_

序号	招标文件内容说明	是否提供/ 满足	对应 投标 文件 起始 页码	备注
<b>一、商务部分</b>				
1	投标承诺书			<u>经投标人盖章、法定代表人或授权代理人签字或盖章</u>
2	投标函			<u>经投标人盖章、法定代表人或授权代理人签字或盖章</u>
3	法定代表人身份证明及授权委托书			<u>经投标人盖章和法定代表人签字或盖章</u>
4	投标保证金 <u>（本项目不适用）</u>			投标保证金（ <b>支票、汇票、本票、保函等非现金形式</b> ） 投标文件中提供原件扫描件加盖公章（注：原件在投标截止时间之前提交集中采购机构）
5	投标人基本情况表			
6	投标人应提交的资格证明材料			财务状况及税收、社会保障资金缴纳情况声明函；资格（资质）证书
7	开标一览表			<u>经投标人盖章、法定代表人或授权代理人签字或盖章</u>
8	投标报价明细表			此表的价格总计须与“开标一览表”总报价保持一致
9	根据招标文件要求，投标人提供以下证明材料： ① <u>国家强制认证的产品承诺书</u> 。			
10	拟分包项目一览表 <u>（本项目不适用）</u>			
11	投标人可提交的商务部分其他证明材料			中小企业声明函； 近三年承揽的类似项目情况表；残疾人福利性单位声明函；（注：仅残疾人福利单位须提供）

序号	招标文件内容说明	是否提供/满足	对应投标文件起始页码	备注
				制造商授权书等证明文件（如果有）；《关于符合本国产品标准的声明函》或财政部会同有关部门规定的有关证明文件（本项目不适用）；关于符合本国产品标准的成本占比的承诺函（本项目不适用）；供应商认为可以证明其能力、信誉和信用的其他材料等
<b>二、技术部分</b>				
1	技术方案			总体方案、分项实施方案等
2	拟投入本项目的人员组成情况			《拟派人员汇总表》、《项目主要人员基本情况表》、《项目其他工作人员基本情况表》）
3	项目服务质量保证措施			《项目实施进度计划表》、《风险管理表》等
4	拟投所有产品清单、偏离表			《拟投所有产品清单》、《技术偏离表》等（如果有）
5	拟投入本项目的设备材料情况			《拟配设备、材料情况一览表》（如果有）
6	售后服务			质保期内的服务方案、
7	其他需说明的问题或需采取的技术措施。			

## 一、投标人提交的商务部分相关内容格式

### 1 投标承诺书格式

#### 投标承诺书

本公司郑重承诺：

将遵循公开、公平、公正和诚实守信的原则，参加项目的投标。

一、不提供有违真实的材料。

二、不与采购人或其他投标人串通投标，损害国家利益、社会利益或他人的合法权益。

三、不向采购人或评标委员会成员行贿，以谋取中标。

四、不以他人名义投标或者其他方式弄虚作假，骗取中标。

五、不进行缺乏事实根据或者法律依据的质疑或投诉。

六、不在投标中哄抬价格或恶意压价。

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

八、已对照“投标人须知”第 3 条要求进行了自查，承诺满足招标文件对投标人的资格要求，且在参加此次采购活动前 3 年内，在经营活动中无重大违法记录。

九、满足招标文件关于不接受整体进口产品的要求。

十、我方承诺投标文件中提供的相关资料均真实有效。

十一、保证中标之后，按照投标文件承诺履约、实施项目。

十二、接受招标文件规定的结算原则和支付方式。

十三、按照招标文件和相关规范性管理文件要求，按时足额发放员工的工资，且**员工工资、社会保障、福利等各类费用符合国家、地方相关管理部门的规定**，我方将积极配合采购人和第三方履约过程中的员工工资支付情况的监督。

十四、已按《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》相关法律法规的规定，充分行使了对招标文件（含补充文件）提出质疑的权利，已完全理解和接受招标文件（含补充文件）的所有内容及要求，无需做进一步解释和修正。

**十五、我方承诺严格按照《上海市电子政府采购管理暂行办法》、《上海市数字证书使用管理办法》等有关规定和要求参加本次投标。**

十六、本公司若违反本投标承诺，愿承担相应的法律责任。

投标人（盖章）：

法定代表人或授权代理人（签字或盖章）：

年月日

提示：投标人未按要求提供本承诺书的，经评标委员会审定后，作为非实质性响应投标而不纳入详细评审。

## 2 投标函格式

### 投标函

项目名称：

致：（采购人全称）

上海市浦东新区政府采购中心

1、我方已详细审查全部招标文件（包括答疑文件）以及全部参考资料和附件，我方已完全理解和确认招标文件对本项目的一切内容与要求，已不需要作出任何其它解释，我方同意放弃对这方面有不明及误解的权利。

2、我方同意所递交的投标文件在招标文件规定的投标有效期内有效，并遵守在此期限内，本投标文件对我方一直具有约束力，随时可接受中标。

3、如果我方的投标文件被接受，我方将提供履约担保（如果有）。我方保证在投标文件承诺的服务期限内完成合同范围内的全部内容，保证本项目服务质量全部达到投标文件承诺的标准和要求。

4、除非并直到制定并实施正式协议书，本投标文件及你方书面中标通知，应构成你我双方间有约束力的合同文件。

5、我方提供人民币\*\*\*元整的投标保证金（**支票、汇票、本票、保函等非现金形式**）（如果有）**（本项目不适用）**，若我方在投标有效期内撤回我方的投标，或在收到贵方的书面中标通知书后不在规定的期限内签订承包合同，则我方同意贵方没收我方的投标保证金，并对我方参与政府采购项目予以不良诚信记录。

6、我方已按照本项目招标文件中所附的《资格性及符合性检查表》进行了自查，对评标委员会根据《资格性及符合性检查表》判定的非实质性响应投标无任何异议。

7、我方同意按照《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》及相关法律法规的规定提出询问或质疑。我方已经充分行使了对招标要求提出质疑和澄清的权利，因此我方承诺不再对招标要求提出质疑。

8、投标人同意提供按照贵方可能要求的与其投标有关的一切数据或资料，完全理解贵方不一定要接受最低价的投标或收到的任何投标。

投标人（盖章）：

法定代表人或授权代理人（签字或盖章）：

### 3 法定代表人身份证明及授权委托书格式

#### 3.1 法定代表人身份证明

投标人：

单位性质：

请选择以下一项：1) 国家行政企业、公私合作企业、中外合资企业、社会组织机构、国际组织机构、外资企业、私营企业、集体企业、国防军事企业、其他（请填写）

地址：

成立时间：年月日

营业期限：

姓名：性别：

年龄：职务：

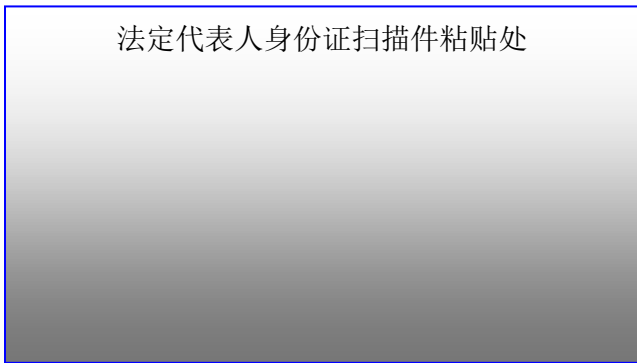
系（投标人名称）的法定代表人。

特此证明。

投标人（盖章）：

法定代表人（签字或盖章）：

时间：年月日



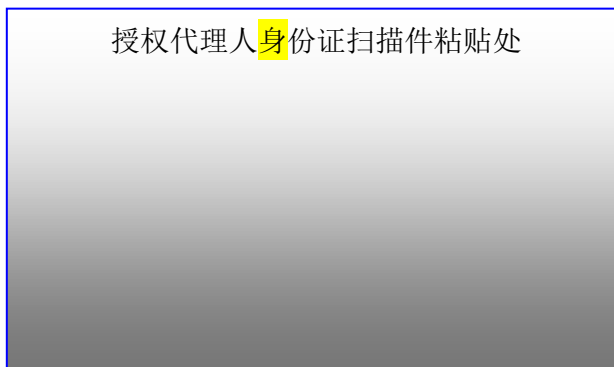
### 3.2 授权委托书

本授权书声明：注册于（公司注册地点）的（公司名称）法定代表人（姓名）代表本公司授权：（公司名称）（职务）（姓名）为正式的合法代理人，参加（项目名称、包件）的投标工作，以投标人的名义签署投标书、进行投标、签署合同并处理与此有关的一切事务，本授权书不得转委托。

投标人（盖章）：

法定代表人（签字或盖章）：

时间：年月日



备注：

请授权代理人如实填写以下联系方式，以便在有需要时能够及时与您取得联系。

授权代理人联系电话（手机）：\_\_\_\_\_

授权代理人邮箱：\_\_\_\_\_

4 投标保证金（银行保函）格式 （本项目不适用）

投标保证金（银行保函）

致：\_\_\_\_\_（采购人全称）

上海市浦东新区政府采购中心

本保函作为（投标人名称、地址）（以下简称投标人）参加贵方（项目名称和招标编号）项目投标的投标保证金。

（银行名称）不可撤销地保证并约束本行及其继承人和受让人，一旦收到贵方提出下列**任何一种情况**（如以联合体形式投标的，则联合体各方均适用）的书面通知后，不管投标人如何反对，立即无条件、无追索权地向贵方支付总额为\*\*\*\*元人民币。

（1）投标人在开标后至投标有效期期满前撤回投标；

（2）投标人不接受贵方按照招标文件规定对其投标文件错误所作的修正；

（3）投标人在收到中标通知书后三十天（30）内，未能和贵方签订合同或提交可接受的履约保证金；

（4）投标人有招标文件规定的腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序行为。

除贵方提前终止或解除本保函外，本保函自开标之日起到投标有效期期满后三十（30）天（即至\*\*年\*\*月\*\*日）有效，以及贵方和投标人同意延长的并通知本行的有效期内继续有效。

出证行名称：\_\_\_\_\_

出证行地址：\_\_\_\_\_

经正式授权代表本行的代表的姓名和职务（打印和签字）：\_\_\_\_\_

银行公章：\_\_\_\_\_

出证日期：\_\_\_\_\_

说明：

- 1、本保函应由商业银行的总行或者分行出具，分行以下机构出具的保函恕不接受。
- 2、如以联合体形式投标的，银行保函可由联合体中任意一方提供。
- 3、投标人如同时参加同一项目多个包件投标的，各包件的投标保函应独立开具。

## 5 投标人基本情况表格式

投标人基本情况表

项目		内容及说明	
<b>一、营业基本情况</b>			
单位名称		经营场所地址	
注册编号		注册日期/有效期限	
企业类型及单位性质		经营范围	
法定代表人		电话/传真	
<b>二、基本经济指标（截止到上一年度 12 月 31 日止）</b>			
实收资本		资产总额	
负债总额		营业收入	
净利润		上缴税收	
上一年度资产负债率		上一年度主营业务利润率	
<b>三、人员情况（以报名的时间为时点统计并填写）</b>			
技术负责人		联系电话	
在册人数			
其中职称等级		其中执业资格	
职称名称	级别 (如：高级、中级、 初级、技工、其 他)	人数	执业资格名称  人数
<b>四、其他</b>			
开户银行名称 (供应商是法人的，填 写基本存款账户信息)		开户银行地址 (供应商是法人的，填 写基本存款账户信息)	
开户银行账号 (供应商是法人的，填 写基本存款账户信息)		所属集团公司（如有）	
企业资格（资质） (如有，需提供彩色扫 描件加盖公章)		质量体系认证 (如有，需提供彩色扫 描件加盖公章)	
近三年内因违法违规受 到行业及相关机构通报 批评以上处理的情况			

项目	内容及说明
其他需要说明的情况	

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

## 6 投标人应提交的资格证明材料

**说明：以下扫描件均应为 A4 纸大小**

### 6.1 财务状况及税收、社会保障资金缴纳情况声明函

#### 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：

### 6.2 法人或其他组织的资格（资质）证书

#### 资质（资格）证书

法人或其他组织的资格（资质）证书扫描件粘贴处



7 开标一览表格式

开标一览表

项目名称或包件号:

单位: 元(人民币)

**中国（上海）自贸区基础云平台 2026 年建设项目包 1**

项目编号	包号	包名称	服务期限	备注	金额(总价、元)

**中国（上海）自贸区基础云平台 2026 年建设项目包 2**

项目编号	包号	包名称	服务期限	备注	金额(总价、元)

**中国（上海）自贸区基础云平台 2026 年建设项目包 3**

项目编号	包号	包名称	服务期限	备注	金额(总价、元)

**说明:**

- 1、所有价格均系用人民币表示，单位为元。
- 2、投标人应按照《项目招标需求》和《投标人须知》的要求报价。
- 3、如果投标人投多个包件，则每个包件的《开标一览表》须分开单独填制。
- 4、各包件投标报价未超过招标文件中规定的【预算金额】；
- 5、最后一栏“金额”即填写投标总价；包号填写所投项目对应包件号；工期填写最终完成本包件的时间。
- 6、如此表中的内容与投标文件其它部分内容不一致的，以此表内容为准。
- 7、此表必须与上海市政府采购信息管理平台投标工具投标客户端《开标一览表》中的内容保持一致。

投标人（盖章）:

法定代表人或授权代理人（签字或盖章）:

日期: \*\*\*\*年\*\*月\*\*日

**8 投标报价明细表格式****8.1 投标报价分类明细表格式（按子项目报价）****8.1.1 包 1 投标报价分类明细表（按子项目报价）****包 1 投标报价分类明细表（按子项目报价）**

中国（上海）自贸区基础云平台 2026 年建设项目区域一

单位：元(人民币)

序号	子项目名称		服务期	投标报价	备注
1	服务 1	云平台资源	十二个月		
2		GPU 资源			
3		国产化资源			
4		网络服务			
5		安全服务			
6		运维服务			
7	服务 2	云平台资源（国产化）			
8		网络服务			
9		安全服务			
10		密码服务			
11	服务 3	云平台资源（国产化）			
12		GPU 资源（国产化）			
13		运维服务			
...					
投标总价					

说明：

- 1、所有价格均系用人民币表示，单位为元。
- 2、此表中的“子项目名称”应与“工作量清单”中的名称保持一致。
- 3、此表中的服务期从实际交付时间开始计算，如实填写。
- 4、投标人可根据本项目实际情况对以上内容进行扩充（不仅限于以上类别）。
- 5、此表中的投标总价应与《开标一览表》中的投标总价保持一致。

**8.1.2 包 2 投标报价分类明细表（按子项目报价）****包 2 投标报价分类明细表（按子项目报价）**

中国（上海）自贸区基础云平台 2026 年建设项目区域二

单位：元(人民币)

序号	子项目名称	服务期	投标报价	备注
----	-------	-----	------	----

1	服务 1	计算资源服务（非国产化）	十二个月		
2		计算资源服务（国产化）			
3		计算资源服务（推理服务器）			
4		计算资源服务（训练服务器）			
5		网络资源服务			
6		密码服务			
7		运维服务			
8	服务 2	计算资源服务（国产化）			
9		计算资源服务（推理服务器）			
10		计算资源服务（训练服务器）			
11		机房机柜服务			
12		信息安全技术服务			
13		密码服务			
14	服务 3	计算资源服务（推理服务器）			
15		计算资源服务（渲染服务器）			
16		计算资源服务（训练服务器）			
17		运维服务			
投标总价					

说明：

- 1、所有价格均系用人民币表示，单位为元。
- 2、此表中的“子项目名称”应与“工作量清单”中的名称保持一致。
- 3、此表中的服务期从实际交付时间开始计算，如实填写。
- 4、投标人可根据本项目实际情况对以上内容进行扩充（不仅限于以上类别）。
- 5、此表中的投标总价应与《开标一览表》中的投标总价保持一致。

**8.1.3 包 3 投标报价分类明细表（按子项目报价）**

**包 3 投标报价分类明细表（按子项目报价）**

中国（上海）自贸区基础云平台 2026 年建设项目区域三

单位：元(人民币)

序号	子项目名称		服务期	投标报价	备注
1	服务 1	物理托管	十二个月		

2		网络资源服务			
3		计算资源服务			
4		存储资源服务			
5		安全服务			
6		密码服务			
7		计算资源服务			
8	服务 2	密码服务			
9		网络资源服务			
投标总价					

说明：

- 1、所有价格均系用人民币表示，单位为元。
- 2、此表中的“子项目名称”应与“工作量清单”中的名称保持一致。
- 3、此表中的工期按完成各子项目的总工期如实填写。
- 4、投标人可根据本项目实际情况对以上内容进行扩充（不仅限于以上类别）。
- 5、此表中的投标总价应与《开标一览表》中的投标总价保持一致。

**8.2 投标报价分类明细表格式表（按工作量清单报价）**

**8.2.1 包 1 投标报价分类明细表格式**

**包 1 投标报价明细表**

中国（上海）自贸区基础云平台 2026 年建设项目区域一

单位：元(人民币)

序号	具体内容		单位	资源总量	备注	报价
1	服务 1	云平台资源	CPU	核	5960	
2			内存	GB	55698	
3			应用存储空间	TB	6615	
4			数据库存储	TB	1638	
5			数据备份服务	TB	1500	
6			整机柜租用	个	2	
7		GPU 资源	CPU	核	120	
8			GPU（训练）	块	10	
9			内存	GB	1920	
10		国产化资源	CPU	核	640	
11			内存	GB	10240	
12			数据库存储	TB	208	
13			应用存储空间	TB	399	
14		网络服务	应用负载均衡服务	IP	97	
15			网络资源	Gps	1	
16			互联网带宽（骨干级）	Gps	1	
17			安全交换区（网闸）	IP	100	
18			网管服务	套	1	
19		安全服务	网络访问控制服务	套	6	
20			入侵防御服务	套	6	
21			常规安全漏洞扫描	次	100	
22			用户管理服务	套	6	
23			用户身份	套	6	

序号	具体内容		单位	资源总量	备注	报价	
		认证服务					
24		在线防护 WAF	套	6			
25		运维服务	套	1			
26	服务 2	云平台资源 (国产化)	CPU	核	2944		
27			内存	GB	47104		
28			应用存储 空间	TB	300		
29			数据库存 储	TB	200		
30			数据备份 服务	TB	400		
31			网络服务	应用负载 均衡服务	IP	45	
32		安全交换 区(网闸)		IP	45		
33		安全服务	网络访问 控制服务	套	19		
34			入侵防御 服务	套	19		
35			常规安全 漏洞扫描	次	988		
36			用户管理 服务	套	19		
37			用户身份 认证服务	套	19		
38			在线防护 WAF	套	19		
39		密码服务	安全认证 网关服务	套	15		
40	时间戳服 务		套	15			
41	签名验签 服务		套	15			
42	可信密码 服务		套	15			
43	服务 3	云平台资源 (国产化)	CPU	核	576		
44			内存	GB	6144		
45			数据库存 储	TB	74		
46		GPU 资源 (国产化)	CPU	核	1536		
47			GPU (推 块)	块	64		

序号	具体内容		单位	资源总量	备注	报价
		理)				
48		内存	GB	8192		
49	运维服务	运维服务	套	1	保障算力等创新业务	
投标总价						

说明：

1、所有价格均系用人民币表示，单位为元。

2、以上提供的报价应当包含项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。

3、此表中的内容应与“工作量清单”保持一致。

4、投标人可根据本项目实际情况对以上内容进行扩充（不限于以上类别）。

5、此表中的投标总价应与《开标一览表》中的投标总价保持一致。

### 8.2.2 包 2 投标报价分类明细表格式

#### 包 2 投标报价明细表

中国（上海）自贸区基础云平台 2026 年建设项目区域二

单位：元(人民币)

序号	具体内容		单位	资源总量	备注	报价
1	服务 1	计算资源服务（非国产化）	CPU	核	4892	
2			内存	GB	34513.17	
3			应用存储空间（HDD）	TB	2219.72	
4			数据库存储（SSD）	TB	103.66	
5		计算资源服务（国产化）	CPU	核	582	
6			内存	GB	3641.34	
7		计算资源服务（推理服务器）	CPU	核	392	
8			内存	GB	7168	
9			GPU（推理）	块	56	
10		计算资源服务（训练服务器）	CPU	核	240	
11			内存	GB	3072	
12			数据库存储（SSD）	TB	23.04	
13			GPU（训练）	块	24	
14		网络资源服务	互联网带宽	Gbps	2	
15			互联网公有 IP 服务	个	512	
16			政务外网链路	条	2	
17			应用负载均衡服务	每 IP	42	

序号	具体内容		单位	资源总量	备注	报价	
18	信息安全技术服务	安全交换区 (网闸)	每 IP	214			
19		入侵防御服务	套	40			
20		用户管理服务	套	40			
21		常规安全漏洞 扫描	次	2080			
22		网络访问控制 服务	套	8			
23		数据库审计服 务	套	8			
24		日志审计服务	套	8			
25		用户身份认证 服务	套	8			
26		在线防护 WAF	套	8			
27		网页防篡服务	套	8			
28		密码服务	安全认证网关 服务	套	8		
29			可信密码服务	套	8		
30			文件加密存储 /签名验签服 务	套	8		
31			时间戳服务	套	4		
32	运维服务	运维服务	人	4			
33	计算资源服务（国 产化）	CPU	核	3293			
34		内存	GB	26214.4			
35		应用存储空间 (HDD)	TB	300			
36		数据库存储 (SSD)	TB	100			
37	计算资源服务（推 理服务器）	CPU	核	896			
38		内存	GB	17408			
39		数据库存储 (SSD)	TB	264.04			
40		GPU（推理）	块	112			
41	计算资源服务（训 练服务器）	CPU	核	896			
42		内存	GB	11264			
43		数据库存储 (SSD)	TB	122.88			
44		GPU（训练）	块	64			
45	机房机柜服务	整机柜租用	个	9			
46	信息安全技术 服务	网络访问控制 服务	套	15			

序号	具体内容		单位	资源总量	备注	报价	
47			数据库审计服务	套	15		
48			日志审计服务	套	15		
49			用户身份认证服务	套	15		
50			在线防护 WAF	套	15		
51			网页防篡服务	套	15		
52			密码服务	安全认证网关服务	套	15	
53		可信密码服务		套	15		
54		文件加密存储/签名验签服务		套	15		
55		时间戳服务		套	8		
56		服务 3		计算资源服务（推理服务器）	CPU	核	1792
57			内存		GB	14336	
58	应用存储空间（HDD）		TB		1536		
59	数据库存储（SSD）		TB		174.08		
60	GPU（推理）		块		128		
61	计算资源服务（渲染服务器）		CPU	核	192		
62			内存	GB	3072		
63			数据库存储（SSD）	TB	23.04		
64			GPU（渲染）	块	24		
65	计算资源服务（训练服务器）		CPU	核	1088		
66			内存	GB	13824		
67			数据库存储（SSD）	TB	93.44		
68			GPU（训练）	块	72		
69	运维服务		运维服务	人	2		
投标总价							

说明：

- 1、所有价格均系用人民币表示，单位为元。
- 2、以上提供的报价应当包含项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。
- 3、此表中的内容应与“工作量清单”保持一致。
- 4、投标人可根据本项目实际情况对以上内容进行扩充（不仅限于以上类别）。
- 5、此表中的投标总价应与《开标一览表》中的投标总价保持一致。

## 包 3 投标报价明细表

中国（上海）自贸区基础云平台 2026 年建设项目区域三

单位：元(人民币)

序号	具体内容		单位	资源总量	备注	报价
1	服务 1	物理托管	机房机柜服务	个	5	
2		网络资源 服务	互联网公有 IP 服务	个	254	
3			互联网带宽（骨干级）	GB	4	
4			政务专线	10GB/条	4	
5			应用负载均衡服务	每 IP	103	
6			安全交换区	每 IP	254	
7			计算资源 服务	CPU	核	10984
8		内存		G	67660	
9		存储资源 服务	应用存储空间	TB	3373.7	
10			高性能数据库存储	TB	523	
11		安全服务	网络访问控制服务	租户	130	
12			入侵防御服务	租户	130	
13			用户管理服务	租户	130	
14			用户身份认证服务	租户	130	
15			数据库审计服务	实例	100	
16			常规安全漏洞扫描	次	2400	
17			在线防护 WAF	套	148	
18			网页防篡服务	套	148	
19		密码服务	安全认证网关服务	套	10	
20	时间戳服务		套	1		
21	服务 2	计算资源 服务	CPU	核	2515	
22			内存	G	20700	
23			GPU 算力服务器 CPU	核	1536	
24			GPU 算力服务器 内存	G	10240	
25			GPU 算力服务器 存储	TB	19.88	
26			GPU（推理）	块	48	
27			GPU（训练）	块	32	

序号	具体内容		单位	资源总量	备注	报价
28	密码服务	安全认证网关服务	套	15		
29		签名验签服务	套	15		
30		可信密码服务	套	15		
31		时间戳服务	套	15		
32	网络资源服务	政务专线	条	1		
投标总价						

## 说明：

- 1、所有价格均系用人民币表示，单位为元。
- 2、以上提供的报价应当包含项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。
- 3、此表中的内容应与“工作量清单”保持一致。
- 4、投标人可根据本项目实际情况对以上内容进行扩充（不仅限于以上类别）。
- 5、此表中的投标总价应与《开标一览表》中的投标总价保持一致。

## 9 投标人提供的其他证明材料

### ①国家强制认证的产品承诺书。

**提示：投标人应按招标文件“前附表”第10.1.1（9）要求提供相应证明材料**

#### 1、国家强制认证的产品承诺书

**致：招标人、招标代理机构**

我方参加（项目名称）（包件号及包件名称）投标所投入的产品皆符合国家强制性标准。本项目中若涉及国家强制认证产品，我方承诺提供的产品皆满足相关强制认证要求。

投标人（盖章）：

法定代表人或授权代理人（签字或盖章）：

日期：\*\*\*\*年\*\*月\*\*日

**10 拟分包项目一览表格式（本项目不适用）**

**拟分包项目一览表**

项目名称或包件号: \_\_\_\_\_

序号	分包内容	价格	分包人名称	分包人资格（资质）	以往做过的类似项目的经历
1					
.....					

**说明：**

1、各分包内容附分包意向协议书，格式自拟。

**分包意向协议书（参考格式）**

为参加 （采购人单位名称） 的 （项目名称） 采购项目，（甲方：投标人）与（乙方：承担分包供应商）通过友好协商，就分包事宜达成以下协议：

一、在本次投标有效期内，乙方同意甲方代理上述投标事宜。若中标，各方按照本协议中约定的分工事项，完成各方对应的工作。

二、各方分工：

- 1、本项目投标工作由甲方负责。
- 2、本项目由甲方授权人员负责与采购人联系。
- 3、甲方拟承担的工作和责任: \_\_\_\_\_。
- 4、乙方拟承担的工作和责任: \_\_\_\_\_。

（注：本项目采购需求明确的非主体、非关键性工作允许投标单位分包。乙方不得承担本项目主体、关键性工作，不得再次分包。）

5、乙方承担的合同份额为合同总额的 \_\_\_\_\_ %

6、分包承担主体应具备承担分包合同的专业资格（资质）或经营范围，并具备履约所必须的设备和专业技术能力。但中小企业享受中小企业扶持政策获取政府采购合同后，小型、微型企业不得分包或转包给大型、中型企业，中型企业不得分包或者转包给大型企业。

7、如中标，各方应按照招标文件的各项要求和内部职责的划分，承担自身所负的责任和风险。

三、本协议自签署之日起生效，投标有效期内有效，如获中标资格，协议有效期延续至合同履行完毕之日。

四、本协议一式肆份，随投标文件装订壹份，送采购人壹份，分包意向协议成员各壹份。

甲方（盖章）：

乙方（盖章）：

日期： 年 月 日

## 11 投标人可提交的商务部分其他证明材料格式

### 11.1 中小企业声明函的格式（仅中型/小型/微型企业需提供）

#### 中小企业声明函

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

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

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

说明：（1）本声明函适用于所有在中国境内依法设立各类所有制和各种组织形式的企业。事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

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

注：各行业划型标准：

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

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

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

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

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

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

员 20 人以下或营业收入 200 万元以下的为微型企业。

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

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

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

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

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

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

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

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

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

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

**11.2 近三年类似项目承接及履约情况一览表格式**

近三年类似项目承接及履约情况一览表

包件号: \_\_\_\_\_

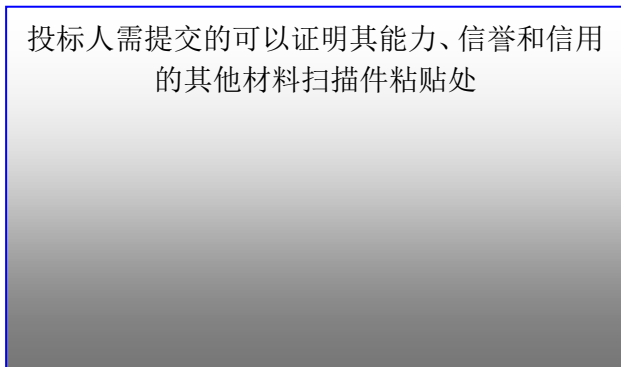
序号	项目名称	采购人	合同价	履约评价	备注
1					
2					
3					
...					
合计数量				合计 金额	

说明：

- 1、近三年指：从投标截止之日起倒推 36 个月以内。
- 2、本表中所涉项目均须附项目**中标通知书**或**承包合同协议书**（二选一），相应资料提供不完整的，该项目在分项评审时不予考虑。
- 3、履约评价可以提供**业主评价**或**项目验收报告**（二选一）的复印件，相应资料提供不完整的，该项目在分项评审时不予考虑。
- 4、投标人还可提供项目履约情况的其他证明材料，例如**项目取得的奖项荣誉证书**。
- 5、评标委员会认为必要时可要求投标人在规定时间内提供原件备查。

### 11.3 投标人认为可以证明其能力、信誉和信用的其他材料

**说明：扫描件应为 A4 纸大小**



### 11.4 残疾人福利性单位声明函格式（仅残疾人福利性单位需提供）

#### 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：

### 11.5 制造商授权书（如果有）

**说明：扫描件应为 A4 纸大小**



**11.6 关于符合本国产品标准的声明函格式（如果有）（本项目不适用）**

（提示：

①本国产品标准适用于货物，包括政府采购货物项目和服务项目中涉及的货物。适用本国产品标准的货物具体是指《政府采购品目分类目录》中的货物类产品，但不包括其中的房屋和构筑物，文物和陈列品，图书和档案，特种动植物，农林牧渔业产品，矿与矿物，电力、城市燃气、蒸汽和热水、水，食品、饮料和烟草原料，无形资产。

②根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）的规定，本国产品应当符合以下条件：

（一）在中国境内生产

产品应当在中国境内生产，即在中华人民共和国关境内实现从原材料、组件到产品的属性改变。

属性改变是指经过制造、加工或者组装等工序，产生完全不同于原材料、组件的新产品，并具有新的名称和特征（用途）。属性改变不包括以下细微操作：

1. 为确保产品在运输或者储存期间保持某种状态而进行的操作；
2. 为产品运输或者销售进行的包装或者展示；
3. 在产品或者其包装上粘贴或者印刷品牌、标志、标识以及其他用于区别的标记；
4. 简单的上漆、磨光和分装；
5. 其他不属于属性改变的情形。

（二）在中国境内生产的组件成本占比达到规定比例（暂未实施）

（三）特定产品的关键组件、关键工序符合相关要求（暂未实施）

③投标人应依据声明函格式，对本项目中涉及的货物进行声明，填写信息与投标文件中的所投产品保持一致。）

### 关于符合本国产品标准的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，本公司（单位）提供的以下产品属于本国产品。具体情况如下：

1. (产品名称 1)<sup>1</sup>，生产厂为 (厂名)<sup>2</sup>，厂址为 (生产厂址)。(产品名称 1) 的中国境内生产的组件成本占比≥ (规定比例)<sup>3</sup>。(产品名称 1) 的 (关键组件)<sup>4</sup> 在中国境内生产。(产品名称 1) 的 (关键工序)<sup>5</sup> 在中国境内完成。

2. (产品名称 2)，生产厂为 (厂名)，厂址为 (生产厂址)。(产品名称 2) 的中国境内生产的组件成本占比≥ (规定比例)。(产品名称 2) 的 (关键组件) 在中国境内生产。(产品名称 2) 的 (关键工序) 在中国境内完成。

.....

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：

日期： 年 月 日

#### 说明：

- 1、产品如有型号，请在“产品名称”栏一并填写。
- 2、生产厂名与厂址应与生产厂营业执照载明的相关信息保持一致。
- 3、该产品的中国境内生产的组件成本占比相关要求实施前，“规定比例”栏可不填，下同。
- 4、该产品的关键组件要求实施前，“关键组件”栏可不填，下同。
- 5、该产品的关键工序要求实施前，“关键工序”栏可不填，下同。

**11.7 关于符合本国产品标准的成本占比的承诺函**（采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到 80% 以上时提供，未达到上述比例要求、或未按照上述要求提供《关于符合本国产品标准的成本占比的承诺函》的，不享受本国产品的支持政策。）**（本项目不适用）**

#### 关于符合本国产品标准的成本占比的承诺函

本公司（单位）郑重承诺，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，本公司（单位）为 本项目/包件\*\*（多包件时请填写包件号） 提供的符合本国产品标准的产品成本之和占提供的全部产品成本之和的比例达到 80% 以上。

本公司（单位）对上述承诺内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：

日期： 年 月 日

#### 说明：

- 1、全部产品是指本项目或本包件中包含的全部货物、服务产品；
- 2、产品成本以相关会计核算数据、采购合同、进货记录等为基础进行计算。

## 二、投标人提交的技术部分相关内容格式

### 1 技术方案

【包括：总体方案、分项实施方案等】；

说明：具体组成内容和编写要求详见“前附表”

### 2拟投入本项目的人员组成情况

#### 2.1 拟派人员汇总表格式

拟派人员汇总表

项目名称或包件号: \_\_\_\_\_

序号	岗位类别及职务	姓名	性别	年龄	学历	职称（或从业资格或执业资格）	相关工作年限	备注
1								
2								
3								
4								
5								
6								
7								
8								
9								

说明：

- 1、请按岗位类别及职务详细罗列参与本项目的人员名单及其基本情况。
- 2、除招标文件另有规定外，上述人员必须为本单位在职人员，不得是兼职人员和退休人员。
- 3、上表如若行数不够，可自行扩充。

**2.2 项目主要人员基本情况表格式**

**项目主要人员基本情况表**

姓名		性别		年龄		从事本专业 工作年限	
毕业院校和专业		**年**月毕业于*****学校*****系（科），学制**年					
职称（或执业资格）			拟在本项目中担任的职务				
<b>主要工作经历</b>							
年~ 年	参加过的项目			担任何职		备注	

**说明：**

- 1、主要人员需每人填写一份此表。“主要人员”是指实际参与本项目的项目经理、专业技术负责人等。
- 2、表后需附相关证书（包括职称/职业资格、执业资格、学历等）和在职证明材料等，所附证书和证明材料均为原件扫描件。  
在职证明材料是指：投标人单位提供相关人员在职承诺书（格式自拟）。
- 3、如果表格填写不准确，或证书（证明材料）提供不完整的，投标人需承担其投标文件在评标时被扣分甚至被认定为无效标。
- 4、表式不够，可另附页填写。

**2.3 项目其他工作人员表基本情况表格式****拟派项目其他工作人员表基本情况表**

项目名称或包件号: \_\_\_\_\_

序号	姓名	性别	年龄	学历	主要分工	资格水平证书	相关工作年限	其他

### 3 项目服务质量保证措施

#### 3.1 项目实施进度计划表格式

项目实施进度计划表

项目名称或包件号: \_\_\_\_\_

序号	时间	工作内容	阶段成果/完成进度

#### 3.2 风险管理表格式

风险管理表

项目名称或包件号: \_\_\_\_\_

序号	预期风险	应对方案
1		
2		
3		

**4拟投所有产品清单、偏离表（如果有）**

**4.1 拟投硬件产品清单**

拟投硬件产品清单（如需）

项目名称或包件号:\_\_\_\_\_

序号	产品名称	数量	品牌、型号	规格参数	制造商名称	产地	质保期	是否为优先采购品目	是否为国家强制认证产品	备注
1										
2										
3										
4										
5										

说明：

- 1、此表中“规格参数”这一项请详细描述，如遇篇幅过长，另制表描述；
- 2、投标人应如实填写产品信息。
- 3、如本项目所采购的产品属于优先采购品目【包括属于节能产品品目、环境标志产品品目、或其他国家强制认证产品的，须填写以下分项表。

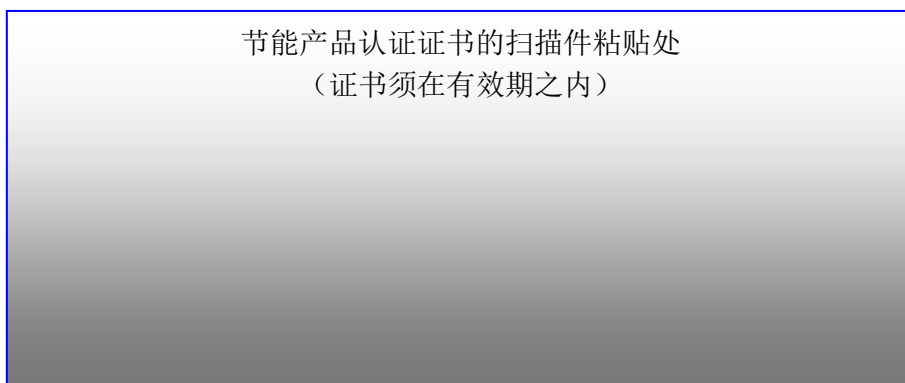
**4.1.1 节能产品格式（如需）**

节能产品一览表

项目名称或包件号:\_\_\_\_\_

序号	节能产品名称	型号	制造商名称	是否属于强制节能	备注
1					
2					
3					

说明：若本项目涉及节能产品采购，投标人应选用节能产品品目清单中的产品，并如实填写上表，同时提供国家确定的认证机构出具的、处于有效期之内的节能产品的认证证书。



**4.1.2 环境标志产品格式（如需）**

环境标志产品一览表

项目名称或包件号: \_\_\_\_\_

序号	环境标志产品名称	型号	制造商名称	备注
1				
2				
3				

说明：若本项目涉及环境标志产品采购，投标人应选用环境标志品目清单中的产品，并如实填写上表，同时提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书。

环境标志产品认证证书的扫描件粘贴处  
(证书须在有效期之内)

**4.1.3 强制认证产品证书（如需）**

说明：若本项目涉及国家强制认证产品（信息安全产品、3C 认证产品、电信设备进网许可证等），投标人应提供该产品按国家标准认证颁发的有效认证证书复印件。

投标人需提交的本项目涉及国家强制认证产品，如信息安全产品、3C 认证产品、电信设备进网许可证等材料的扫描件粘贴处

#### 4.2 拟投软件产品清单

项目名称或包件号: \_\_\_\_\_

序号	产品名称或模块名称	详细技术参数或模块功能描述	开发商	开发地点	数量	备注

**4.3 拟投主要产品技术规格偏离表**

项目名称或包件号: \_\_\_\_\_

序号	产品名称	招标要求	投标参数	偏离情况 (正/无/负)	对应 投标文件页码	说明

说明:

- 1、上表中所列参数为该项目核心指标，投标人应根据实际投标货物的参数指标对照填写。
- 2、除上述所列指标以外，如投标人另有偏离（包括正偏离和负偏离）的指标，请一并如实填写。
- 3、如投标货物实际技术规格与技术需求无偏差，在“是否有偏差”一列填写“无”。
- 4、投标货物的规格、技术参数和性能与招标文件的要求如不完全一致，请注明是“正偏离”还是“负偏离”。

**5拟投入本项目的设备材料情况**

拟配设备、材料情况一览表

项目名称或包件号: \_\_\_\_\_

序号	设备、材料名称	数量	单价	品牌	产地	规格型号	额定功率 或容量	备注(如使用 区域等)

## 6 售后服务

### 6.1 质保期内的服务方案

## 7 其他需说明的问题或需采取的技术措施

## 第五章项目评审

## 一、资格及符合性检查表

序号	检查内容	检查结果
	<b>一、资格性检查</b>	
1	投标人满足招标文件“投标人须知”第 3 条规定的投标人应具备资格条件的	
2	投标人按“投标人须知前附表”第 10.1.1（6）条款提交资格证明材料	
	<b>二、符合性检查</b>	
1	投标文件中的下列内容按招标文件要求签署、盖章的（具体详见“投标文件格式”要求）： ▲ 投标承诺书 ▲ 投标函 ▲ 授权委托书 ▲ 开标一览表	
2	未发现投标人递交两份或多份内容不同的投标文件，或在一份投标文件中对同一招标项目报有两个或多个报价，且未声明哪一个有效；（注：招标文件另有规定除外）	
3	接受招标文件规定的投标有效期	
4	接受招标文件规定的项目实施和服务期限	
5	未出现投标报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的；	
6	各包件投标报价未超过招标文件中规定的【预算金额】；	
7	未发现投标报价存在“第二章”第 19.4 条款所列情形之一的	
8	按规定交纳投标保证金 <u>（本项目不适用）</u>	
9	根据招标文件要求，投标人提供以下证明材料的： ① <u>国家强制认证的产品承诺书</u> ；	
10	按“投标人须知”第 21.4 条款规定，对投标报价算术性错误修正予以确认的	
11	接受招标文件规定的结算原则和支付方式	
12	未出现《政府采购货物和服务招标投标管理办法》第三十七条所列的串通投标情形之一的	
13	未出现提供虚假材料、行贿等违法行为	
14	未发现因电子文档本身的计算机病毒、或电子文档损坏等原因造成投标文件无法打开或打开后无法完整读取的	
15	满足招标文件规定的以下要求： ① <u>接受并满足招标文件的实质性响应要求和条件</u> ；	
16	未发现投标人违反《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》规定的	

**注意：**

1、以上符合性检查内容由评标委员会负责最终审定，未通过资格性及符合性检查的投标将被作为非实质性响应投标而不纳入详细评审范围。

2、集中采购机构详细列出资格性及符合性检查的目的在于方便投标人进行自查，请投标人对照招标文件（包括答疑和补充文件）的内容进行自查，以避免投标文件出现非实质性响应的情况。本表中所列实质性检查内容判断标准与“前附表”中所列要求有矛盾之处，以“前附表”中所列要求为准。

## 二、评委评审

### 【中国（上海）自贸区基础云平台 2026 年建设项目】评标办法

#### （一）评标原则

1、本评标办法作为本项目择优选定中标人的依据，在评标全过程中应遵照执行，违反本评标办法的打分无效。

2、评标委员会负责对符合资格的投标人的投标文件进行符合性审查。对通过符合性审查的投标文件按此评标办法进行详细评审，未通过符合性审查的投标文件将被作为无效标而不纳入详细评审范围。

3、本次评标采用“综合评分法”，分值保留小数点后两位，第三位四舍五入。

4、评标委员会根据招标文件（包括答疑和补充文件）的规定，对各投标人商务标的完整性、合理性、准确性进行评审，确认商务标的有效性和评标价，以此为基础计算各投标人的商务标得分。

5、如果评标委员会认定投标人的报价存在异常低价情形的，应当要求其在评标现场合理的时间提供书面说明及必要的证明材料，对投标价格作出解释。评标委员会应当按照《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2号）的规定对报价合理性进行判断，投标人不能在规定时间内提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，应当将其作为无效投标处理。审查相关情况应当在评审报告中记录。

6、对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人做出必要的澄清、说明或者补正。

7、按照《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）和《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号），对于非专门面向中小企业采购的项目，小型和微型企业参加投标的，享受以下扶持政策，用扣除后的价格参与评审：

（1）小型、微型企业的最终报价给予 **10%** 的扣除；（包 1：10；包 2：10；包 3：10；）

（2）如项目允许联合体参与竞争的，且联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，其报价给予 **10%** 的扣除。反之，依照联合体协议约定，小型、微型企业的协议合同金额占到联合体协议合同总金额 30% 以上的，给予联合体 **4%** 的价格扣除。

8、残疾人福利性单位视同小型、微型企业，其投标价格享受小型和微型企业同等的价格扣除政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

9、按照《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号），政府采购活动中既有本国产品又有非本国产品参与竞争的，对本国产品给予价格评审优惠，用扣除后的价格参与评审。评标委员会应当按照《关于贯彻落实《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》的意见》（财库〔2025〕30号）的规定对投标人所出具的《关于符合本国产品标准的声明函》进行审查。（本项目不适用）

10、评标委员会成员对投标人的投标文件进行仔细审阅、评定后各自独立打分，评委应并提出技术标的详细评审意见（方案的优缺点均加以评述），打分可在规定幅度内允许打小数

11、本项目技术标评审项中标有“\*”内容属于客观评审因素，根据《政府采购货物和服务招标投标管理办法》要求，评标委员会成员对客观评审因素评分应一致。

12、技术标、商务标两者之和为投标人的最终得分，评标委员会按照各有效投标人最终得分由高到低顺序排列，推荐得分最高者为第一中标候选人，依此类推。如得分相同的，按投标报价由低到高

顺序排列，得分且投标报价相同的，按技术标得分由高到低顺序排列。依照上述排序方法后仍出现得分相同时，由评委记名投票表决，得票多者排名靠前。

13、本项目包含 3 个包件，同一投标人允许最多中标 2 个包件。若同一中标人在多个（即大于允许中标包件数）包件中排名均为第一的，由电子采购平台按以下选择顺序和原则确定投标人中标包件：按包件号顺序号确定中标包件。

## （二）评审内容及打分原则

类别	分值	项目		权重	评分办法	评定分
商务	20	价格	投标报价得分	20	投标报价得分=（评标基准价 / 投标报价）×20 注：评标基准价为通过资格性及符合性检查的所有投标中的最低投标报价。	
技术	80	技术及服务水平	整体方案设计	10	一、评审内容： 整体架构方案、云虚拟化平台方案、资源池架构设计方案等完整性、先进性、合理性，包括： 1、总体设计思路及技术架构合理性； 2、功能结构及描述详细、简洁、完整。 二、评审标准： 1、方案完整合理，针对性和可操作性强，得 8~10 分； 2、方案合理，针对性和可操作性一般，得 7~8（不含 8）分； 3、方案基本合理，针对性和可操作性弱，得 6~7（不含 7）分。	
			技术参数	15	一、评审内容： 1、软硬件产品技术参数与招标需求的偏离情况。 二、评审标准： 1、参数指标高于招标要求的，得 12~15 分； 2、参数指标与招标要求契合的，得 10~12（不含 12）分； 3、参数指标与招标要求存在负偏离的，得 9~10（不含 10）分。	
			资源及安全保障方案	20	一、评审内容： 1、机房环境管理及链路配置情况； 2、信息安全技术服务方案。 二、评审标准： 1、方案完整合理，针对性和可操作性强，得 17~20 分； 2、方案合理，针对性和可操作性一般，得 14~17（不含 17）分； 3、方案基本合理，针对性和可操作性弱，得 12~14	

类别	分值	项目	权重	评分办法	评定分
				(不含 14) 分。	
		整体方案及实施	12	<p>一、评审内容：</p> <p>1、拟投入人力资源（包括项目主要人员资质及以往类似业绩、项目组人员资质，在职证明材料等）；</p> <p>2、详细进度安排；</p> <p>3、项目管理方案是否详细完整；</p> <p>4、项目验收方案是否详细完整；</p> <p>5、项目支撑及培训方案是否详细完整。</p> <p>二、评审标准：</p> <p>1、交付优于要求时限，方案完善、科学合理，实施操作性高，验收标准与方案详细，项目投入人员充分，项目主要人员资质材料完整提供，得 9~12 分；</p> <p>2、交付满足要求时限，方案合理性一般，实施操作性一般，验收标准与方案一般，项目投入人员较合理，项目主要人员资质材料提供基本完整，得 6~9（不含 9）分；</p> <p>3、交付不满足要求时限，方案合理性较差，实施操作性弱，验收标准与方案不完善，项目投入人员缺乏，项目主要人员资质材料提供缺失，得 4~6（不含 6）分。</p>	
		售后服务	15	<p>一、评审内容：</p> <p>1、服务体系与标准情况是否详细完整；</p> <p>2、运营运维制度与规范是否详细完整；</p> <p>3、运营运维服务内容及方案是否详细完整。</p> <p>二、评审标准：</p> <p>1、响应情况良好，得 11~15 分；</p> <p>2、响应情况一般，得 7~11（不含 11）分；</p> <p>3、响应情况较差，得 5~7（不含 7）分；</p> <p>4、未响应不得分。</p>	
		投标人履约能力	8	<p>一、评审内容：</p> <p>1、近三年有效类似项目的承接情况；</p> <p>2、投标人的综合履约能力。</p> <p>二、评审标准：</p> <p>1、是否属于近三年有效类似项目由评标委员会根据投标人提供的项目承接情况在业务内容、技术特点等方面与本项目类似程度进行认定。有一个得 2 分，在此基础上每增加一个加 2 分，最高得分为 6 分，没有得 0 分；</p>	

类别	分值	项目	权重	评分办法	评定分
				2、近三年承接的有效类似项目获得的用户或第三方评价情况、与本项目相关的第三方技术认可情况，得 0~2 分。	
合计			100		

采购人：上海市浦东新区大数据中心  
集中采购机构：上海市浦东新区政府采购中心

2026 年 5 月