**公开招标文件**

项目名称：北京市怀柔区政务云项目云计算服务采购项目

项目编号：HCZX-2025-C0007/11011625210200013549-XM001-01

采购人：北京市怀柔区政务服务和数据管理局

采购代理机构：北京市怀柔区公共资源交易中心（北京市怀柔区政府采购中心）

2025年8月

**目录**

[第一章投标邀请 1](#_Toc25448)

[第二章投标人须知 5](#_Toc12229)

[第三章资格审查 1](#_Toc8999)9

[第四章评标程序、评标方法和评标标准 2](#_Toc8999)2

[第五章采购需求 3](#_Toc5904)2

[第六章拟签订的合同文本 9](#_Toc5904)9

[第七章投标文件格式](#_Toc25364) 108

**第一章投标邀请**

1. **项目基本情况**

项目编号：HCZX-2025-C0007/11011625210200013549-XM001-01

项目名称：北京市怀柔区政务云项目云计算服务采购项目

采购方式：公开招标

项目预算金额：3764.679万元；

服务期限：以甲方需求为准。

采购需求：具体采购需求详见招标文件。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 包号 | 标的名称 | 采购包预算金额  （元） | 数量 | 简要技术需求或服务要求 |
| 01 | 北京市怀柔区政务云项目 | 37646790.00 | 1项 | 要求将全区分散在不同数据中心和云平台的75个系统逐步迁移至怀柔区政务服务怀柔区政务云，为全区政务系统建设提供一站式的计算、存储、网络、安全、密码、运维、迁移和增值等政务云服务和数据管理。政务云应满足未来三年全区政务业务持续上云需求，确保全区政务云业务集约性和稳定性。本项目服务期限为3年，服务期间需按要求完成三级等保测评和密码安全测评相关工作。 |

合同履行期限：3年。

本项目是否接受联合体投标：■是 □否。

## 申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求:

2.1中小企业政策

■本项目不专门面向中小企业预留采购份额。

□本项目专门面向 □中小 □小微企业采购。即：提供的货物全部由符合政策要求的小微企业制造、服务全部由符合政策要求的小微企业承接。

□本项目预留部分采购项目预算专门面向中小企业采购。对于预留份额，提供的货物由符合政策要求的中小企业制造、服务由符合政策要求的中小企业承接。预留份额通过以下措施进行：/。

2.2其它落实政府采购政策的资格要求（如有）： / 。

3.本项目的特定资格要求：

3.1本项目是否属于政府购买服务：

□否

■是，公益一类事业单位、使用事业编制且由财政拨款保障的群团组织，不得作为承接主体；

3.2其他特定资格要求：

3.2.1单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加同一合同项下的政府采购活动；

3.2.2除单一来源采购项目外，为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，不得再参加该采购项目的其他采购活动；

3.2.3根据财政部财库〔2016〕125号《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》文件相关规定，投标人不得为“信用中国”网站（www.creditchina.gov.cn）中列入失信被执行人和重大税收违法案件当事人名单的投标人，不得为中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的投标人。

## 三、获取招标文件

时间：2025年8月11日至2025年8月18日，每天09:00至16:00（北京时间，法定节假日除外）

地点：北京市政府采购电子交易平台

方式：供应商使用CA数字证书或电子营业执照登录北京市政府采购电子交易平台（http://zbcg-bjzc.zhongcy.com/bjczj-portal-site/index.html#/home）获取电子版招标文件。

## 四、提交投标文件截止时间、开标时间和地点

2025年9月1日上午9时00分(北京时间)

## 地点：采用远程电子开标方式，投标人使用CA认证证书登录北京市政府采购电子交易平台参与电子开标。投标人自行对电子投标文件进行解密，不接受纸质文件，无须投标人到达现场。

## 五、公告期限

自本公告发布之日起5个工作日。

1. **其他补充事宜**

1.本项目需要落实的政府采购政策:

1.1.《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46号；

1.2.《北京市人民政府关于进一步支持小型微型企业发展的意见》-京政发〔2012〕40号；

1.3.《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》-财库〔2014〕68号；

1.4.《关于促进残疾人就业政府采购政策的通知》-财库〔2017〕141号；

1.5.《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）；

1.6.《关于开展政府采购信用担保试点工作的通知》（财库【2011】124号）。

2.本项目采用全流程电子化采购方式，请供应商认真学习北京市政府采购电子交易平台发布的相关操作手册（供应商可在交易平台下载相关手册）办理CA数字证书或电子营业执照、进行北京市政府采购电子交易平台注册绑定，并认真核实CA数字证书或电子营业执照情况确认是否符合本项目电子化采购流程要求。

CA数字证书服务热线010-58511086

电子营业执照服务热线400-699-7000

技术支持服务热线010-86483801

2.1办理CA数字证书或电子营业执照

供应商登录北京市政府采购电子交易平台查阅“用户指南”—“操作指南”—“市场主体CA办理操作流程指引”/“电子营业执照使用指南”，按照程序要求办理。

2.2注册

供应商登录北京市政府采购电子交易平台“用户指南”—“操作指南”—“市场主体注册入库操作流程指引”进行自助注册绑定。

2.3驱动、客户端下载

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“招标采购系统文件驱动安装包”下载相关驱动。

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“投标文件编制工具”下载相关客户端。

2.4获取电子招标文件

供应商使用CA数字证书或电子营业执照登录北京市政府采购电子交易平台获取电子招标文件。

供应商如计划参与多个采购包的投标，应在登录北京市政府采购电子交易平台后，在【我的项目】栏目依次选择对应采购包，进入项目工作台招标/采购文件环节分别按采购包下载招标文件电子版。未在规定期限内按上述操作获取文件的采购包，供应商无法提交相应包的电子投标文件。

2.5编制电子投标文件

供应商应使用电子投标客户端编制电子投标文件并进行线上投标，供应商电子投标文件需要加密并加盖电子签章，如无法按照要求在电子投标文件中加盖电子签章和加密，请及时通过技术支持服务热线联系技术人员。

2.6提交电子投标文件

供应商应于投标截止时间前在北京市政府采购电子交易平台提交电子投标文件，上传电子投标文件过程中请保持与互联网的连接畅通。

2.7电子开标

供应商在开标地点使用CA数字证书或电子营业执照登录北京市政府采购电子交易平台进行电子开标。

1. **对本次招标提出询问，请按以下方式联系。**

1.采购人信息

名称：北京市怀柔区政务服务和数据管理局

地址：北京市怀柔区府开放路33号

联系方式：010-69685930

2.采购代理机构信息

名称：北京市怀柔区公共资源交易中心（北京市怀柔区政府采购中心）

地　址：北京市怀柔区雁栖大街53号

联系方式：卢月010-60680843

3.项目联系方式

项目联系人：卢月

电　话：010-60680843

**第二章投标人须知**

## 投标人须知资料表

本表是对投标人须知的具体补充和修改，如有矛盾，均以本资料表为准。标记“**■**”的选项意为适用于本项目，标记“□”的选项意为不适用于本项目。

| **条款号** | **条目** | **内容** |
| --- | --- | --- |
| 2.2 | 项目属性 | 项目属性：  **■**服务  □货物 |
| 2.3 | 科研仪器设备 | 是否属于科研仪器设备采购项目：  □是  **■**否 |
| 2.4 | 核心产品 | ■关于核心产品本项目不适用。  □本项目\_\_包为单一产品采购项目。  □本项目\_\_包为非单一产品采购项目，核心产品为：\_\_\_\_。 |
| 3.1 | 现场考察 | **■**不组织  □组织，考察时间：\_\_年\_月\_日\_点\_分  考察地点：\_\_\_\_\_\_\_\_\_\_\_\_。 |
| 开标前答疑会 | **■**不召开  □召开，召开时间：\_\_年\_月\_日\_点\_分  召开地点：\_\_\_\_\_\_\_\_\_\_\_\_。 |
| 4.1 | 样品 | 投标样品递交：  **■**不需要  □需要，具体要求如下：  （1）样品制作的标准和要求：\_\_\_\_\_\_\_\_\_；  （2）是否需要随样品提交相关检测报告：  □不需要  □需要  （3）样品递交要求：\_\_\_\_\_\_\_\_\_；  （4）未中标人样品退还：\_\_\_\_\_\_\_\_\_；  （5）中标人样品保管、封存及退还：\_\_\_\_\_\_\_\_\_；  （6）其他要求（如有）：\_\_\_\_\_\_\_\_\_。 |
| 5.2.5 | 标的所属行业 | 本项目采购标的对应的中小企业划分标准所属行业：   |  |  | | --- | --- | | 标的名称 | 中小企业划分标准所属行业 | | 北京市怀柔区政务云项目云计算服务采购项目 | 软件和信息技术服务业 | | 说明：本项目中小企业划分标准所属行业，其划型标准如下: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。 | | |
| 11.2 | 投标报价 | 投标报价的特殊规定：  **■**无  □有，具体情形：\_\_\_\_\_。 |
| 13.1 | 投标有效期 | 自提交投标文件的截止之日起算90日历天。 |
| 18.2 | 解密时间 | 解密时间：30分钟 |
| 22.1 | 确定中标人 | 中标候选人并列的，采购人是否委托评标委员会确定中标人：  ■否  □是  中标候选人并列的，按照以下方式确定中标人：  ■得分且投标报价均相同的，以技术部分得分高者为中标人  □随机抽取 |
| 25.5 | 分包 | 本项目的非主体、非关键性工作是否允许分包：  ■不允许  □允许，具体要求：  （1）可以分包履行的具体内容：\_\_\_\_\_；  （2）允许分包的金额或者比例：\_\_\_\_\_；  （3）其他要求：\_\_\_\_\_。 |
| 25.6 | 政采贷 | 为更大力度激发市场活力和社会创造力，增强发展动力，按照《北京市全面优化营商环境助力企业高质量发展实施方案》（京政办发〔2023〕8号）部署，进一步加强政府采购合同线上融资“一站式”服务（以下简称“政采贷”），北京市财政局、中国人民银行营业管理部联合发布《关于推进政府采购合同线上融资有关工作的通知》（京财采购〔2023〕637号）。有需求的供应商，可按上述通知要求办理“政采贷”。 |
| 26.1.1 | 询问 | 询问送达形式：  口头询问：请致电010-60680843  书面询问：请将书面文件递交至：北京市怀柔区公共资源交易中心（北京市怀柔区政府采购中心）  递交地址：北京市怀柔区雁栖大街53号217室。 |
| 26.3 | 联系方式 | 接收询问和质疑的联系方式  联系部门：北京市怀柔区公共资源交易中心（北京市怀柔区政府采购中心）；  联系电话：010-60680843；  通讯地址：北京市怀柔区雁栖大街53号217室。 |

**投标人须知**

## 一说明

1. 采购人、采购代理机构、投标人、联合体
   1. 采购人、采购代理机构：指依法进行采购的国家机关、事业单位、团体组织，及其委托的采购代理机构。本项目采购人、采购代理机构见第一章《投标邀请》。
   2. 投标人（也称“投标人”、“申请人”）：指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。
   3. 联合体：指两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身份共同参加采购。
2. 资金来源、项目属性、科研仪器设备采购、核心产品
   1. 资金来源为财政性资金和/或本项目采购中无法与财政性资金分割的非财政性资金。
   2. 项目属性见《投标人须知资料表》。
   3. 是否属于科研仪器设备采购见《投标人须知资料表》。
   4. 核心产品见《投标人须知资料表》。
3. 现场考察、开标前答疑会
   1. 若《投标人须知资料表》中规定了组织现场考察、召开开标前答疑会，则投标人应按要求在规定的时间和地点参加。
   2. 由于未参加现场考察或开标前答疑会而导致对项目实际情况不了解，影响投标文件编制、投标报价准确性、综合因素响应不全面等问题的，由投标人自行承担不利评审后果。
4. 样品
   1. 本项目是否要求投标人提供样品，以及样品制作的标准和要求、是否需要随样品提交相关检测报告、样品的递交与退还等要求见《投标人须知资料表》。
   2. 样品的评审方法以及评审标准等内容见《评标程序、评标方法和评标标准》。
5. 采购政策（包括但不限于下列具体政策要求）
   1. 采购本国货物、工程和服务
      1. 政府采购应当采购本国货物、工程和服务。但有《**中华人民共和国政府采购法**》第十条规定情形的除外。
      2. 本项目如接受非本国货物、工程、服务参与投标，则具体要求见第五章《采购需求》。
      3. 进口产品指通过中国海关报关验放进入中国境内且产自关境外的产品，包括已经进入中国境内的进口产品。关于进口产品的相关规定依据《政府采购进口产品管理办法》（财库〔2007〕119号文）、《关于政府采购进口产品管理有关问题的通知》（财办库〔2008〕248号文）。
   2. 中小企业、监狱企业及残疾人福利性单位
      1. 中小企业定义：
         1. 中小企业是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。关于中小企业的判定依据《中华人民共和国中小企业促进法》、《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）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）、《金融业企业划型标准规定》（〔2015〕309号）等国务院批准的中小企业划分标准执行。
         2. 投标人提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

* + - 1. 在货物采购项目中，投标人提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。
      2. 以联合体形式参加采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。
    1. 在政府采购活动中，监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。监狱企业定义：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。
    2. 在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。残疾人福利性单位定义：享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：
       1. 安置的残疾人占本单位在职职工人数的比例不低于25%（含25%），并且安置的残疾人人数不少于10人（含10人）；
       2. 依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；
       3. 为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；
       4. 通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；
       5. 提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）；
       6. 前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1至8级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或服务协议的雇员人数。
    3. 本项目是否专门面向中小企业预留采购份额见《投标邀请》。
    4. 采购标的对应的中小企业划分标准所属行业见《投标人须知资料表》。
    5. 小微企业价格评审优惠的政策调整：见《评标程序、评标方法和评标标准》。
  1. 采购节能产品、环境标志产品
     1. 采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门根据产品节能环保性能、技术水平和市场成熟程度等因素，确定实施政府优先采购和强制采购的产品类别及所依据的相关标准规范，以品目清单的形式发布并适时调整。依据品目清单和认证证书实施政府优先采购和强制采购。
     2. 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。关于采购节能产品、环境标志产品的相关规定依据《关于调整优化节能产品、环境标志产品采购执行机制的通知》（财库〔2019〕9号）。
     3. 如本项目采购产品属于实施政府强制采购品目清单范围的节能产品，则投标人所报产品必须获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则**投标无效**；
     4. 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定见《评标程序、评标方法和评标标准》（如涉及）。
  2. 正版软件
     1. 各级政府部门在购置计算机办公设备时，必须采购预装正版操作系统软件的计算机产品，相关规定依据《国家版权局、信息产业部、财政部、国务院机关事务管理局关于政府部门购置计算机办公设备必须采购已预装正版操作系统软件产品的通知》（国权联〔2006〕1号）、《国务院办公厅关于进一步做好政府机关使用正版软件工作的通知》（国办发〔2010〕47号）、《财政部关于进一步做好政府机关使用正版软件工作的通知》（财预〔2010〕536号）。
  3. 网络安全专用产品
     1. 根据《关于调整网络安全专用产品安全管理有关事项的公告》（2023年第1号），所提供产品属于列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品时，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。
  4. 推广使用低挥发性有机化合物（VOCs）
     1. 为全面推进本市挥发性有机物（VOCs）治理，贯彻落实挥发性有机物污染治理专项行动有关要求，相关规定依据《北京市财政局北京市生态环境局关于采购推广使用低挥发性有机化合物（VOCs）有关事项的通知》（京财采购〔2020〕2381号）。本项目中涉及涂料、胶黏剂、油墨、清洗剂等挥发性有机物产品的，属于强制性标准的，投标人应执行符合本市和国家的VOCs含量限制标准（具体标准见《采购需求》），否则**投标无效**；属于推荐性标准的，优先采购，具体见《评标程序、评标方法和评标标准》。
  5. 采购需求标准
     1. 商品包装、快递包装政府采购需求标准（试行）

为助力打好污染防治攻坚战，推广使用绿色包装，根据财政部关于印发《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》的通知（财办库〔2020〕123号），本项目如涉及商品包装和快递包装的，则其具体要求见第五章《采购需求》。

* + 1. 其他政府采购需求标准

为贯彻落实《深化政府采购制度改革方案》有关要求，推动政府采购需求标准建设，财政部门会同有关部门制定发布的其他政府采购需求标准，本项目如涉及，则具体要求见第五章《采购需求》。

1. 投标费用

6.1投标人应自行承担所有与准备和参加投标有关的费用，无论投标的结果如何，

采购人或采购代理机构在任何情况下均无承担这些费用的义务和责任。

## 二招标文件

1. 招标文件构成
   1. 招标文件包括以下部分：
2. 投标邀请
3. 投标人须知
4. 资格审查
5. 评标程序、评标方法和评标标准
6. 采购需求
7. 拟签订的合同文本
8. 投标文件格式
   1. 投标人应认真阅读招标文件的全部内容。投标人应按照招标文件要求提交投标文件并保证所提供的全部资料的真实性，并对招标文件做出实质性响应，否则**投标无效**。
9. 对招标文件的澄清或修改
   1. 采购人或采购代理机构对已发出的招标文件进行必要澄清或者修改的，将在原公告发布媒体上发布更正公告，并以书面形式通知所有获取招标文件的潜在投标人。
   2. 上述书面通知，按照获取招标文件的潜在投标人提供的联系方式发出，因提供的信息有误导致通知延迟或无法通知的，采购人或采购代理机构不承担责任。
   3. 澄清或者修改的内容为招标文件的组成部分，并对所有获取招标文件的潜在投标人具有约束力。澄清或者修改的内容可能影响投标文件编制的，将在投标截止时间至少15日前，以书面形式通知所有获取招标文件的潜在投标人；不足15日的，将顺延提交投标文件的截止时间和开标时间。

## 三投标文件的编制

1. 投标范围、投标文件中计量单位的使用及投标语言
   1. 本项目如划分采购包，投标人可以对本项目的其中一个采购包进行投标，也可同时对多个采购包进行投标。投标人应当对所投采购包对应第五章《采购需求》所列的全部内容进行投标，不得将一个采购包中的内容拆开投标，否则其对该采购包的投标将被认定为**无效投标**。
   2. 除招标文件有特殊要求外，本项目投标所使用的计量单位，应采用中华人民共和国法定计量单位。
   3. 除专用术语外，投标文件及来往函电均应使用中文书写。必要时专用术语应附有中文解释。投标人提交的支持资料和已印制的文献可以用外文，但相应内容应附有中文翻译本，在解释投标文件时以中文翻译本为准。未附中文翻译本或翻译本中文内容明显与外文内容不一致的，其不利后果由投标人自行承担。
2. 投标文件构成
   1. 投标人应当按照招标文件的要求编制投标文件。投标文件应由《资格证明文件》、《商务技术文件》两部分构成。投标文件的部分格式要求，见第七章《投标文件格式》。
   2. 对于招标文件中标记了“实质性格式”文件的，投标人不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，否则**投标无效**。未标记“实质性格式”的文件和招标文件未提供格式的内容，可由投标人自行编写。
   3. 第四章《评标程序、评标方法和评标标准》中涉及的证明文件。
   4. 对照第五章《采购需求》，说明所提供货物和服务已对第五章《采购需求》做出了响应，或申明与第五章《采购需求》的偏差和例外。如第五章《采购需求》中要求提供证明文件的，投标人应当按具体要求提供证明文件。
   5. 投标人认为应附的其他材料。
3. 投标报价
   1. 所有投标均以人民币为计价货币。
   2. 投标人的报价应包括为完成本项目所发生的一切费用和税费，采购人将不再支付报价以外的任何费用。投标人的报价应包括但不限于下列内容，《投标人须知资料表》中有特殊规定的，从其规定。
      1. 投标货物及标准附件、备品备件、专用工具等的出厂价（包括已在中国国内的进口货物完税后的仓库交货价、展室交货价或货架交货价）和运至最终目的地的运输费和保险费，安装调试、检验、技术服务、培训、质量保证、售后服务、税费等；
      2. 按照招标文件要求完成本项目的全部相关费用。
   3. 采购人不得向投标人索要或者接受其给予的赠品、回扣或者与采购无关的其他商品、服务。
   4. 投标人不能提供任何有选择性或可调整的报价（招标文件另有规定的除外），否则其**投标无效**。
4. 投标保证金（不涉及）
   1. 投标人应按《投标人须知资料表》中规定的金额及要求交纳投标保证金。投标人自愿超额缴纳投标保证金的，投标文件不做无效处理。
   2. 交纳投标保证金可采用的形式：政府采购法律法规接受的支票、汇票、本票、网上银行支付或者金融机构、担保机构出具的保函等非现金形式。
   3. 投标保证金到账（保函提交）截止时间同投标截止时间。以支票、汇票、本票、网上银行支付等形式提交投标保证金的，应在投标截止时间前到账；以金融机构、担保机构出具的纸质保函等形式提交投标保证金的，应在投标截止时间前将原件提交至采购代理机构；以电子保函形式提交投标保证金的，应在投标截止时间前通过北京市政府采购电子交易平台完成电子保函在线办理。未按上述要求缴纳投标保证金的，其投标无效。
   4. 投标人除需在投标文件中提供“投标保证金凭证/交款单据电子件”，还需在投标截止时间前，通过电子交易平台上传“投标保证金凭证/交款单据电子件”。
   5. 投标保证金有效期同投标有效期。
   6. 投标人为联合体的，可以由联合体中的一方或者多方共同交纳投标保证金，其交纳的投标保证金对联合体各方均具有约束力。
   7. 采购人、采购代理机构将及时退还投标人的投标保证金，采用银行保函、担保机构担保函等形式递交的投标保证金，经投标人同意后采购人、采购代理机构可以不再退还，但因投标人自身原因导致无法及时退还的除外：
      1. 投标人在投标截止时间前撤回已提交的投标文件的，自收到投标人书面撤回通知之日起5个工作日内退还已收取的投标保证金；
      2. 中标人的投标保证金，自采购合同签订之日起5个工作日内退还中标人；
      3. 未中标投标人的投标保证金，自中标通知书发出之日起5个工作日内退还未中标人；
      4. 终止招标项目已经收取投标保证金的，自终止采购活动后5个工作日内退还已收取的投标保证金及其在银行产生的孳息。
   8. 有下列情形之一的，采购人或采购代理机构可以不予退还投标保证金：
      1. 投标有效期内投标人撤销投标文件的；
      2. 《投标人须知资料表》中规定的其他情形。
5. 投标有效期
   1. 投标文件应在本招标文件《投标人须知资料表》中规定的投标有效期内保持有效，投标有效期少于招标文件规定期限的，其**投标无效**。
6. 投标文件的签署、盖章
   1. 招标文件要求签字的内容（如授权委托书等），可以使用电子签章或使用原件的电子件（电子件指扫描件、照片等形式电子文件）；要求第三方出具的盖章件原件（如联合协议、分包意向协议、制造商授权书等），投标文件中应使用原件的电子件。
   2. 招标文件要求盖章的内容，一般通过投标文件编制工具加盖电子签章。

## 四投标文件的提交

1. 投标文件的提交
   1. 本项目使用北京市政府采购电子交易平台。投标人根据招标文件及电子交易平台供应商操作手册要求编制、生成并提交电子投标文件。
   2. 采购人及采购代理机构拒绝接受通过电子交易平台以外任何形式提交的投标文件，投标保证金除外。
2. 投标截止时间
   1. 投标人应在招标文件要求提交投标文件截止时间前，将投标文件提交至电子交易平台。
3. 投标文件的修改与撤回
   1. 投标截止时间前，投标人可以通过电子交易平台对所提交的投标文件进行补充、修改或者撤回。投标保证金的补充、修改或者撤回无需通过电子交易平台，但应就其补充、修改或者撤回通知采购人或采购代理机构。
   2. 投标人对投标文件的补充、修改的内容应当按照招标文件要求签署、盖章，作为投标文件的组成部分。

## 五开标、资格审查及评标

1. 开标
   1. 采购人或采购代理机构将按招标文件的规定，在投标截止时间的同一时间和招标文件预先确定的地点组织开标。
   2. 本项目开标使用北京市政府采购电子交易平台。投标人应在《投标人须知资料表》规定的时间内对投标文件进行解密，因非系统原因导致的解密失败，视为**投标无效**。
   3. 开标过程将使用电子交易平台宣布投标人名称、投标价格和招标文件规定的需要宣布的其他内容并进行记录，并由参加开标的各投标人确认。投标人未在规定时间内提出疑义或确认一览表的，视同认可开标结果。
   4. 投标人对开标过程和开标记录有疑异，以及认为采购人、采购代理机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请。采购人、采购代理机构对投标人提出的询问或者回避申请将及时处理。
   5. 投标人不足3家的，不予开标。
2. 资格审查
   1. 见第三章《资格审查》。
3. 评标委员会
   1. 评标委员会根据采购有关规定和本次招标采购项目的特点进行组建，并负责具体评标事务，独立履行职责。
   2. 评审专家须符合《财政部关于在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）的规定。依法自行选定评审专家的，采购人和采购代理机构将查询有关信用记录，对具有行贿、受贿、欺诈等不良信用记录的人员，拒绝其参与政府采购活动。
4. 评标程序、评标方法和评标标准
   1. 见第四章《评标程序、评标方法和评标标准》。

## 六确定中标

1. 确定中标人
   1. 采购人将在评标报告确定的中标候选人名单中按顺序确定中标人，中标候选人并列的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定中标人；招标文件未规定的，采取随机抽取的方式确定。采购人是否委托评标委员会直接确定中标人，见《投标人须知资料表》。中标候选人并列的，按照《投标人须知资料表》要求确定中标人。
2. 中标公告与中标通知书
   1. 采购人或采购代理机构自中标人确定之日起2个工作日内，在北京市政府采购网公告中标结果，同时向中标人发出中标通知书，中标公告期限为1个工作日。
   2. 中标通知书对采购人和中标投标人均具有法律效力。中标通知书发出后，采购人改变中标结果的，或者中标投标人放弃中标项目的，应当依法承担法律责任。
3. 废标
   1. 在招标采购中，出现下列情形之一的，应予废标：
      1. 符合专业条件的投标人或者对招标文件作实质响应的投标人不足三家的；
      2. 出现影响采购公正的违法、违规行为的；
      3. 投标人的报价均超过了采购预算，采购人不能支付的；
      4. 因重大变故，采购任务取消的。
   2. 废标后，采购人将废标理由通知所有投标人。
4. 签订合同
   1. 中标人、采购人应当自中标通知书发出之日起30日历日内，按照招标文件和中标人投标文件的规定签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。
   2. 中标人拒绝与采购人签订合同的，采购人可以按照评标报告推荐的中标候选人名单排序，确定下一候选人为中标人，也可以重新开展采购活动。
   3. 联合体中标的，联合体各方应当共同与采购人签订合同，就中标项目向采购人承担连带责任。
   4. 政府采购合同不能转包。
   5. 采购人允许采用分包方式履行合同的，中标人可以依法在中标后将中标项目的非主体、非关键性工作采取分包方式履行合同。本项目的非主体、非关键性工作是否允许分包，见《投标人须知资料表》。采购合同分包履行的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包**，**否则**投标无效**。中标人就采购项目和分包项目向采购人负责，分包投标人就分包项目承担责任。
   6. “政采贷”融资指引：详见《投标人须知资料表》。
5. 询问与质疑
   1. 询问
      1. 投标人对政府采购活动事项有疑问的，可依法向采购人或采购代理机构提出询问，提出形式见《投标人须知资料表》。
      2. 采购人或采购代理机构对供应商依法提出的询问，在3个工作日内作出答复，但答复的内容不得涉及商业秘密。
   2. 质疑
      1. 投标人认为采购文件、采购过程、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7个工作日内，由投标人派授权代表以书面形式向采购人、采购代理机构提出质疑。采购人、采购代理机构在收到质疑函后7个工作日内作出答复。
      2. 质疑函须使用财政部制定的范本文件。投标人为自然人的，质疑函应当由本人签字；投标人为法人或者其他组织的，质疑函应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。
      3. 投标人委托代理人进行质疑的，应当随质疑函同时提交投标人签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。
      4. 投标人应在法定质疑期内一次性提出针对同一采购程序环节的质疑，法定质疑期内针对同一采购程序环节再次提出的质疑，采购人、采购代理机构有权不予答复。
   3. 接收询问和质疑的联系部门、联系电话和通讯地址见《投标人须知资料表》。

**第三章****资格审查**

**一、资格审查程序**

1. 开标结束后，评标委员会将根据《资格审查要求》中的规定，对投标人进行资格审查，并形成资格审查结果。
2. 《资格审查要求》中对格式有要求的，除招标文件另有规定外，均为“实质性格式”文件。
3. 投标人的投标文件中有任何一项不符合《资格审查要求》的，资格审查不合格，其**投标无效**。
4. 资格审查合格的投标人不足3家的，不进行评标。

**二、资格审查要求**

| **序号** | **审查因素** | **审查内容** | **格式要求** |
| --- | --- | --- | --- |
| 1 | 满足《中华人民共和国采购法》第二十二条规定及法律法规的其他规定 | 具体规定见第一章《投标邀请》 |  |
| 1-1 | 营业执照等证明文件 | 投标人为企业（包括合伙企业）的，应提供有效的“营业执照”；  投标人为事业单位的，应提供有效的“事业单位法人证书”；  投标人是非企业机构的，应提供有效的“执业许可证”、“登记证书”等证明文件；  投标人是个体工商户的，应提供有效的“个体工商户营业执照”；  投标人是自然人的，应提供有效的自然人身份证明。  分支机构参加投标的，应提供该分支机构或其所属法人/其他组织的相应证明文件；同时还应提供其所属法人/其他组织出具的授权其参与本项目的授权书（格式自拟，须加盖其所属法人/其他组织的公章）；对于银行、保险、石油石化、电力、电信等行业的分支机构，可以提供上述授权，也可以提供其所属法人/其他组织的有关文件或制度等能够证明授权其独立开展业务的证明材料。 | 提供证明文件的复印件加盖投标人公章 |
| 1-2 | 投标人资格声明书 | 提供了符合招标文件要求的《投标人资格声明书》。 | 格式见《投标文件格式》 |
| 1-3 | 投标人信用记录 | 查询渠道：信用中国网站和中国采购网（www.creditchina.gov.cn、www.ccgp.gov.cn）；  截止时点：投标截止时间以后、资格审查阶段采购人或采购代理机构的实际查询时间；  信用信息查询记录和证据留存具体方式：查询结果网页打印页作为查询记录和证据，与其他采购文件一并保存；  信用信息的使用原则：经认定的被列入失信被执行人、重大税收违法案件当事人名单、采购严重违法失信行为记录名单的投标人，其**投标无效**。联合体形式投标的，联合体成员存在不良信用记录，视同联合体存在不良信用记录。 | 无须投标人提供，由采购人或采购代理机构查询。 |
| 1-4 | 法律、行政法规规定的其他条件 | 法律、行政法规规定的其他条件 | / |
| 2 | 落实采购政策需满足的资格要求 | 具体要求见第一章《投标邀请》 |  |
| 2-1 | 中小企业政策 | 具体要求见第一章《投标邀请》 |  |
| 2-1-1 | 中小企业声明函 | 当本项目（包）涉及预留份额专门面向中小企业采购，此时建议在《资格证明文件》中提供。  1、投标人单独投标的，应提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。  2、如招标文件要求以联合体形式参加或者要求合同分包的，且投标人为联合体或拟进行合同分包的，则联合体中的中小企业、签订分包意向协议的中小企业具体情况须在《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件中如实填报，且满足招标文件关于预留份额的要求。 | 格式见《投标文件格式》 |
| 2-1-2 | 拟分包情况说明及分包意向协议 | 如本项目（包）要求通过分包措施预留部分采购份额面向中小企业采购、且投标人因落实政府采购政策拟进行分包的，必须提供；  否则无须提供。  对于预留份额专门面向中小企业采购的项目（包），组成联合体或者接受分包合同的中小企业与联合体内其他企业、分包企业之间不得存在直接控股、管理关系。 | 格式见《投标文件格式》 |
| 2-2 | 其它落实政府采购政策的资格要求 | 如有，见第一章《投标邀请》 | 提供证明文件的电子件或电子证照并加盖电子印章 |
| 3 | 本项目的特定资格要求 | 如有，见第一章《投标邀请》 |  |
| 3-1 | 是否接受联合体投标 | 1、如本项目接受联合体投标，且投标人为联合体时必须提供《联合协议》，明确各方拟承担的工作和责任，并指定联合体牵头人，授权其代表所有联合体成员负责本项目投标和合同实施阶段的牵头、协调工作。该联合协议应当作为投标文件的组成部分，与投标文件其他内容同时递交。  2、联合体各成员单位均须提供本表中序号1-1、1-2的证明文件。联合体各成员单位均应满足本表3-2及3-3项规定。  3、本表序号3-4项规定的其他特定资格要求中的每一小项要求，联合体各方中至少应当有一方符合本表中其他资格要求并提供证明文件。  4、联合体中有同类资质的投标人按照联合体分工承担相同工作的，应当按照资质等级较低的投标人确定资质等级。  5、以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他投标人另外组成联合体参加同一合同项下的政府采购活动。  6、若联合体中任一成员单位中途退出，则该联合体的**投标无效**。  7、**联合体各方应明确在本项目中的不同专业分工，且按照在本项目中负责的专业分工提供相应的技术应答、企业资质和人员资质。**  8、本项目不接受联合体投标时，投标人不得为联合体。 | 提供《联合协  议》原件的电  子件格式见《投标文件格式》 |
| 3-2 | 政府购买服务承接主体的要求 | 如本项目属于政府购买服务，投标人不属于公益一类事业单位、使用事业编制且由财政拨款保障的群团组织。 | 格式见《投标文件格式》“1-2投标人资格声明书” |
| 3-3 | 承诺书 | 供应商近三年无行贿犯罪行为承诺书 | 格式自拟 |
| 3-4 | 其他特定资格要求 | 如有，见第一章《投标邀请》 | 提供证明文件的电子件或电子证照并加盖电子印章 |
| 4 | 投标费用承诺函 | 投标人应自行承担所有与准备和参加投标有关的费用，无论投标的结果如何，采购人或采购代理机构在任何情况下均无承担这些费用的义务和责任（详见附件） | 提供证明文件的复印件加盖投标人公章 |

**第四章评标程序、评标方法和评标标准**

**一、评标方法**

1. 投标文件的符合性审查
   1. 评标委员会对资格审查合格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。
   2. 评标委员会根据《符合性审查要求》中规定的审查因素和审查内容，对投标人的投标文件是否实质上响应招标文件进行符合性审查，并形成符合性审查评审结果。投标人的投标文件中有任何一项不符合《符合性审查要求》要求的，**投标无效**。

**符合性审查要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **审查因素** | **审查内容** |
| 1 | 授权委托书 | 按招标文件要求提供授权委托书； |
| 2 | 投标完整性 | 未将一个采购包中的内容拆开投标； |
| 3 | 投标报价 | 投标报价未超过招标文件中规定的项目/采购包预算金额或者项目/采购包最高限价； |
| 4 | 报价唯一性 | 投标文件未出现可选择性或可调整的报价（招标文件另有规定的除外）； |
| 5 | 投标有效期 | 投标文件中承诺的投标有效期满足招标文件中载明的投标有效期的； |
| 6 | 实质性格式 | 标记为“实质性格式”的文件均按招标文件要求提供且签署、盖章的； |
| 7 | ★号条款响应 | 投标文件满足招标文件第五章《采购需求》中★号条款要求的。 |
| 8 | 拟分包情况说明（如有） | 如本项目（包）非因“落实政府采购政策”亦允许分包，且供应商拟进行分包时，必须提供；否则无须提供； |
| 9 | 分包其他要求（如有） | 分包履行的内容、金额或者比例未超出《投标人须知资料表》中的规定；  分包承担主体具备《投标人须知资料表》载明的资质条件且提供了资质证书电子件（如有）； |
| 10 | 报价的修正（如有） | 不涉及报价修正，或投标文件报价出现前后不一致时，投标人对修正后的报价予以确认；（如有） |
| 11 | 报价合理性 | 报价合理，或投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，能够应评标委员会要求在规定时间内证明其报价合理性的； |
| 12 | 进口产品（如有） | 招标文件不接受进口产品投标的内容时，投标人所投产品不含进口产品； |
| 13 | 国家有关部门对投标人的投标产品有强制性规定或要求的 | 国家有关部门对投标人的投标产品有强制性规定或要求的（如相应技术、安全、节能和环保等），投标人的投标产品应符合相应规定或要求，并提供证明文件电子件：  1）采购的产品若属于《节能产品政府采购品目清单》范围中政府强制采购产品，则投标人所报产品必须获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书；  2）所投产品属于列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品时，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求；（如该产品已经获得公安部颁发的计算机信息系统安全专用产品销售许可证，且在有效期内，亦视为符合要求）  3）项目中涉及涂料、胶黏剂、油墨、清洗剂等挥发性有机物产品，且属于强制性标准的，供应商应执行符合本市和国家的VOCs含量限制标准。 |
| 14 | 公平竞争 | 投标人遵循公平竞争的原则，不存在恶意串通，妨碍其他投标人的竞争行为，不存在损害采购人或者其他投标人的合法权益情形的； |
| 15 | 串通投标 | 不存在《采购货物和服务招标投标管理办法》视为投标人串通投标的情形：（一）不同投标人的投标文件由同一单位或者个人编制；（二）不同投标人委托同一单位或者个人办理投标事宜；（三）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；（四）不同投标人的投标文件异常一致或者投标报价呈规律性差异；（五）不同投标人的投标文件相互混装；（六）不同投标人的投标保证金从同一单位或者个人的账户转出； |
| 16 | 附加条件 | 投标文件未含有采购人不能接受的附加条件的； |
| 17 | 其他无效情形 | 投标人、投标文件不存在不符合法律、法规和招标文件规定的其他无效情形。 |

1. 投标文件有关事项的澄清或者说明
   1. 评标过程中，评标委员会将以书面形式要求投标人对其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，作出必要的澄清、说明或者补正。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。澄清文件将作为投标文件内容的一部分。如需投标人进行澄清的内容，投标人需在2个小时内予以反馈。
   2. 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，有权要求该投标人在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；若投标人不能证明其报价合理性，评标委员会将其作为**无效投标处理**。
   3. 投标报价须包含招标文件全部内容，如分项报价表有缺漏视为已含在其他各项报价中，将不对投标总价进行调整。评标委员会有权要求投标人在评标现场合理的时间内对此进行书面确认，投标人不确认的，视为将一个采购包中的内容拆开投标，其**投标无效**。
   4. 投标文件报价出现前后不一致的，按照下列规定修正：
      1. 招标文件对于报价修正是否另有规定：

□有，具体规定为：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

■无，按下述2.4.2-2.4.8项规定修正。

* + 1. 单独递交的开标一览表（报价表）与投标文件中开标一览表（报价表）内容不一致的，以单独递交的开标一览表（报价表）为准；
    2. 投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
    3. 大写金额和小写金额不一致的，以大写金额为准；
    4. 单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；
    5. 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。
    6. 同时出现两种以上不一致的，按照前款规定的顺序修正。
    7. 修正后的报价经投标人书面确认后产生约束力，投标人不确认的，其**投标无效**。
  1. 落实采购政策的价格调整：只有符合第二章《投标人须知》5.2条规定情形的，可以享受中小企业扶持政策，用扣除后的价格参加评审；否则，评标时价格不予扣除。
     1. 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对小微企业报价给予10%的扣除，用扣除后的价格参加评审。
     2. 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，且接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的联合体或者大中型企业的报价给予10%的扣除，用扣除后的价格参加评审。
     3. 组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。
     4. 价格扣除比例对小型企业和微型企业同等对待，不作区分。
     5. 中小企业参加采购活动，应当按照招标文件给定的格式出具《中小企业声明函》，否则不得享受相关中小企业扶持政策。
     6. 监狱企业提供了由省级以上监狱管理局（北京市含教育矫治局）、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的，视同小微企业。
     7. 残疾人福利性单位按招标文件要求提供了《残疾人福利性单位声明函》（见附件）的，视同小微企业。
     8. 若投标人同时属于小型或微型企业、监狱企业、残疾人福利性单位中的两种及以上，将不重复享受小微企业价格扣减的优惠政策。

1. 投标文件的比较和评价
   1. 评标委员会将按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价；未通过符合性审查的投标文件不得进入比较与评价。
   2. 评标方法和评标标准
      1. 本项目采用的评标方法为：

■综合评分法，指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法，见《评标标准》，招标文件中没有规定的评标标准不得作为评审的依据。

□最低评标价法，指投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人的评标方法。

* + 1. 采用最低评标价法时，提供相同品牌产品（单一产品或核心产品品牌相同）的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照下述方法确定一个参加评标的投标人，其他**投标无效**。

□随机抽取

□其他方式，具体要求：\_\_\_\_\_

* + 1. 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定（如涉及）在评分表中加分。

1. 确定中标候选人名单
   1. 采用综合评分法时，提供相同品牌产品（单一产品或核心产品品牌相同）且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，评标委员会按照下述规定确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。

□随机抽取

■其他方式，具体要求：评审得分相同的则投标报价最低优先，如报价相同则按照评审因素的量化指标评审得分最高优先。如报价相同且量化指标评审得分也相同的，由评标委员会现场采取随机抽取方式确定。其他同品牌投标人不作为中标候选人。

* 1. 采用综合评分法时，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。评分分值计算保留小数点后两位，第三位四舍五入。
  2. 采用最低评标价法时，评标结果按本章2.4、2.5调整后的投标报价由低到高顺序排列。投标报价相同的并列。投标文件满足招标文件全部实质性要求且投标报价最低的投标人为排名第一的中标候选人。
  3. 评标委员会要对评分汇总情况进行复核，特别是对排名第一的、报价最低的、投标或响应文件被认定为无效的情形进行重点复核。
  4. 评标委员会将根据各投标人的评标排序，依次推荐本项目（各采购包）的中标候选人，起草并签署评标报告。本项目（各采购包）评标委员会共（各）推荐三名中标候选人。

1. 报告违法行为
   1. 评标委员会在评标过程中发现投标人有行贿、提供虚假材料或者串通等违法行为时，应当及时向财政部门报告。
2. **评标标准**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评审因素** | **分值** | **评审标准** |
| **报价部分（满分10分）** | | | |
| 1 | 投标报价 | 10 | 满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：  投标报价得分＝（评标基准价/投标报价）×分值。  说明：此处投标报价指经过报价修正，及因落实政府采购政策进行价格调整后的报价，详见第四章《评标程序、评标方法和评标标准》2.4及2.5。 |
| **技术部分（满分73分）** | | | |
| 2 | 技术指标响应情况 | 30 | 根据投标人针对采购需求的响应情况，进行综合评分。  全部满足招标文件采购需求的得满分30分，如投标人参数或所投产品技术参数不满足招标文件中采购需求的条款要求，标▲项每一项负偏离扣1分，扣完为止。  注：1、投标人需在采购需求偏离表中对采购需求的条款进行逐条响应。  2、以投标文件中提供的采购需求偏离表及招标文件采购需求中要求提供的证明材料作为评审依据。  (根据具体参数的要求提供相关证明材料，包括产品功能截图、或官网文档材料、或相应权威机构检测报告，并加盖投标人公章，投标人需对提供的相关证明材料的真实性负完全责任。) |
| 3 | 云平台建设方案 | 10 | 综合考虑投标人提供的计算服务方案的先进性、科学性、合理性和可行性。完全满足要求，技术路线清晰，实施路径明确，可得2分；部分满足要求可得1分，未提供方案或不满足得0分。 |
| 综合考虑投标人提供的存储服务方案的先进性、科学性、合理性和可行性。完全满足要求，技术路线清晰，实施路径明确，可得2分；部分满足要求可得1分，未提供方案或不满足得0分。 |
| 综合考虑投标人提供的网络服务方案的先进性、科学性、合理性和可行性。完全满足要求，技术路线清晰，实施路径明确，可得2分；部分满足要求可得1分，未提供方案或不满足得0分。 |
| 综合考虑投标人提供的云管理平台服务方案的先进性、科学性、合理性和可行性。完全满足要求，技术路线清晰，实施路径明确，可得2分；部分满足要求可得1分，未提供方案或不满足得0分。 |
| 综合考虑投标人提供的运维监控平台服务方案的先进性、科学性、合理性和可行性。完全满足要求，技术路线清晰，实施路径明确，可得2分；部分满足要求可得1分，未提供方案或不满足得0分。 |
| 4 | 业务部署迁移服务 | 3 | 投标人提供的应用系统云迁移方案需重点考察以下能力：   1. 具备完善的业务迁移服务能力，方案需体现通用性、可操作性和规范性，确保迁移风险最小化； 2. 提供云主机迁移服务，提供支持主流数据库的数据迁移服务； 3. 需针对迁移的业务系统提供详实可行的迁移方案。   评审将根据上述三个方面综合评定：完全满足要求得3分，部分满足要求可得1分，未提供方案或不满足得0分。 |
| 5 | 安全防护服务 | 3 | 投标人提供的安全防护方案需明确涵盖物理安全、网络安全、主机安全等关键领域的安全服务内容。  评审将重点考察安全防护体系的可靠性、全面性及可行性。  完全满足要求、方案设计科学合理且防护措施到位的得3分；  基本满足要求、方案存在部分不足但整体可行的得1分；  方案存在重大缺陷或未提供的得0分。 |
| 6 | 业务连续保障方案 | 3 | 投标人需提供完整的业务连续性保障方案，方案应包含确保云上业务7×24小时连续运行的技术保障措施、运维管理机制及应急处理预案，重点保障已在政务云底座运行的业务系统持续稳定运行，避免非应用自身原因导致的计划外服务中断。  评审将从方案的完整性、针对性和可行性三个维度进行综合评估：  方案设计完善、保障措施具体可行、具有较强的可操作性得3分；  方案内容基本完整、保障措施基本可行得1分；  方案存在重大缺陷或未提供的得0分。 |
| 7 | 服务和质量保障 | 3 | 投标人须提供基于云平台完整的服务保障方案，方案内容应包括交付能力保障措施、服务组织架构、进度管控机制及验收标准等核心要素。  方案内容全面、设计科学合理、保障措施完善且可操作性强得3分；  方案基本完整但部分内容有待完善得1分；  方案存在明显缺陷或未提供得0分。 |
| 8 | 专业培训服务方案 | 2 | 投标人应提供针对采购方及使用单位的项目管理人员、系统运维人员、云平台最终用户及开发人员提供对应的培训、培训方案及手册等；  完全满足得2分，部分满足得1分，未提供方案或不满足得0分。 |
| 9 | 运行维护服务方案 | 3 | 投标人须提供项目整体运维服务方案，包含但不限于以下内容：   1. 现场日常运维服务方案的科学性、合理性及可行性综合评分。 2. 现场重保运维服务方案的科学性、合理性及可行性综合评分。 3. 现场运维服务组织机构明晰，职责范围明确。 4. 现场运维服务制度、规范、流程、表单完整度。 5. 服务应急处置方案的细致程度。 6. 对采购人运维服务使用提出有利于用户的合理化建议。   完全满足得3分，部分满足得1分，未提供方案或不满足得0分。 |
| 10 | 数据中心要求 | 2 | 满足国家数据局“原始数据不出域”的要求及运维检査便利性，投标人须在北京市怀柔区内拥有自有产权数据中心，需提供数据中心房屋所有权证或国有土地使用证，提供材料且满足上述要求得2分，未提供材料或不满足得0分。 |
| 4 | 投标人提供的数据中心须提供独立物理区域供政务云平台使用，且所有功能模块的机柜在同一楼层，可为本项目提供不少于50个机柜空间，并可以根据区政府要求按需在同一楼层扩容至不少于100个机柜。 在响应文件中，投标人应对上述要求做出专项承诺，同时提供平面布置图以及现场机房照片并加盖公章。提供材料同时满足上述两项要求得4分，未提供材料或任一项不满足得0分。 |
| 3 | 投标人提供的数据中心须满足如下电力系统要求： 1）总供电能力：投标机房供电等级10KV及以上，并提供双路市电。投标人需提供电力公司的供电方案报装批复手续并加盖公章。 2）UPS：配备UPS和蓄电池组，续航时间不少于15分钟。投标人需提供三方设计院盖章的电力专业设计方案和UPS电池组照片并加盖公章。 3）备用电源：投标机房配备燃油发电机，在市电异常断电后，发电机组须在15分钟内提供备用电力，确保业务不间断运行。投标人需提供承诺函及发电机组照片并加盖公章。 提供材料且同时满足上述三项要求得3分，未提供材料或任一项不满足得0分。 |
| 2 | 投标人提供的数据中心须满足如下节能要求：  采用氟泵自然冷却或循环水冷技术，机房按冷热通道布局。符合北京地方标准《数据中心能源效率限额》DB11/T1139-2023（PUE≤1.35）。 投标人需提供三方设计院盖章的机房设计方案（明确PUE≤1.35）和现场空调系统照片并加盖公章；  提供材料同时满足上述两项要求得2分，未提供材料或任一项不满足得0分。 |
| 2 | 投标人提供的数据中心须满足如下安防系统要求：  机房配有监控和门禁系统,要求对机房出入口及热通道进行门禁管理，且要求机房及机柜列间均配备门禁系统，门禁系统需要与视频监控系统集成到同平台上管理，以满足数据中心安全要求。  投标人需提供机房安防系统照片并加盖公章，提供材料同时满足上述要求得2分，未提供材料或不满足得0分。 |
| 2 | 投标人提供的数据中心须满足如下消防系统要求：  机房配有专业的气体灭火系统，并带泄压及事故排风系统。 投标人需提供三方设计院盖章的机房消防设计方案和现场消防系统照片并加盖公章，提供材料同时满足上述要求得2分，未提供材料或不满足得0分。 |
| 1 | 为满足未来政务云业务双活及容灾备份需要，投标人需具备与主投的数据中心直线距离大于40公里的扩展灾备数据中心能力，需提供灾备数据中心所在建筑房屋所有权证或国有土地使用证，并提供灾备数据中心的详细地址及地图测距截图。  满足得1分，未提供证明或不符合要求不得分。 |
| **商务部分（满分17分）** | | | |
| 11 | 企业资质 | 2 | 投标人或所投云平台厂商须提供有效的CMMI软件能力成熟度证书五级。  符合要求的得2分，未提供或无效的不得分。 |
| 3 | 投标人或所投云平台厂商须提供有效质量管理体系认证证书、环境管理体系证书、个人身份信息保护管理体系认证证书、隐私信息管理体系认证证书、数据存储安全管理体系认证证书、云服务信息安全管理体系认证证书；  提供以上所有证书扫描件并加盖公章，每提供一个得0.5分，全部提供得3分，未提供或无效的不得分。 |
| 1 | 投标人或所投云平台厂商具有ITSS颁发的信息技术服务标准符合性证书-IaaS私有云服务能力证书，提供证书扫描件并加盖公章。  二级及以上得1分，三级及以下得0.5分，未提供不得分。 |
| 1 | 投标人或所投云平台厂商具有ITSS颁发的信息技术服务标准符合性证书-SaaS云能力证书，提供证书扫描件并加盖公章。  二级及以上得1分，三级及以下得0.5分，未提供不得分。 |
| 12 | 投标人业绩 | 2 | 投标人近三年（自2022年8月1日至今）承担云平台建设、或服务、或租用、或运营相关项目及相关证明文件（如：首页、服务内容信息页、合同金额页、签字盖章页等）。复印件加盖公章，时间以合同签订日期为准。合同签订方必须是投标人自身，存在控股、管理关系投标人之间签订的合同无效，不符合上述要求或未按要求提供有效证明文件的业绩在评审时将不予承认。每提供1个案例得1分，此项最多可得2分。 |
| 13 | 项目团队 | 2 | 投标人拟任项目经理须具备良好的项目管理能力，须具有信息系统项目管理师，并提供相关证书复印件（加盖投标人公章），提供投标人为其缴纳的近6个月的社保证明文件。满足全部要求得2分，未提供或不符合要求得0分。 |
| 2 | 投标人拟任项目技术负责人（与项目经理不得为同一人）须具备良好的项目技术服务能力，具有正高级工程师，并提供相关证书复印件（加盖投标人公章），提供投标人为其缴纳的近6个月的社保证明文件。满足全部要求得2分，未提供或不符合要求得0分。 |
| 4 | （1）投标人承诺为本项目组建交付以及在政务云机房所在位置组建项目团队（需在合同签订后一个月内组建完毕），团队人员30人或以上的得2分，10-29人的得1分，10人及以下不得分；  （2）团队人员中持有信息系统项目管理师、PMP、数据库系统工程师、注册信息安全工程师等相关专业证书的人员（1人持有多个证书以1人计算），每有1人得0.2分，本项最高得2分。  注：投标人自行提供服务团队人员表、人员学历、人员简历、人员身份证（正反）、提供投标人为其缴纳的近6个月的社保证明文件。以及相关专业证书等证明材料。 |

**第五章采购需求**

**一、项目背景**

1.1项目名称：北京市怀柔区政务云项目云计算服务采购项目

1.2采购人：北京市怀柔区政务服务和数据管理局

1.3项目最高限价：人民币37646790.00元，其中业务系统迁移最高限价：人民币3449250.00元。最终项目结算金额不超过项目预算金额。

1.4资金来源：财政性资金。

1.5服务期限：3年。

1.6项目概况：

根据怀柔区数字经济发展需要和“十四五”智慧城市建设要求，以及数字政府治理提升目标，按照“统筹规划、适度超前、分级管理、资源共享”的原则建设和管理怀柔区政务云。未来三年，以采购服务的方式，建设安全、可靠、高效的政务云，具备“一云多芯”、“多元算力”能力，兼容鲲鹏、海光等主流国产信创芯片，能提供通用算力，通过打造怀柔区安全自主可控的政务云平台，不断优化服务能力，提升服务水平，为怀柔区建设全球数字经济标杆城市提供坚实的数字底座。怀柔区政务云应具备拓展智能算力服务的能力，具备支持云原生、AI等技术的能力满足日益增长的政务云服务需求。

**二、总体要求**

要求将全区分散在不同数据中心和云平台的75个系统逐步迁移至怀柔区政务服务怀柔区政务云，为全区政务系统建设提供一站式的计算、存储、网络、安全、密码、运维、迁移和增值等政务云服务和数据管理。政务云应满足未来三年全区政务业务持续上云需求，确保全区政务云业务集约性和稳定性。本项目服务期限为3年，服务期间需按要求完成三级等保测评和密码安全测评相关工作。

2.1基础设施即服务（IaaS）服务

包括计算资源、存储资源、网络资源等服务。

计算资源服务：包括x86虚拟机、信创海光虚拟化、信创鲲鹏虚拟化服务等。

存储资源服务：包括块存储服务、对象存储服务服务等。

网络资源服务：涵盖互联网链路、VPN网关、负载均衡等服务，具备接入2家以上运营商的能力，提供稳定、高效、安全的网络支持。

2.2平台即服务（PaaS）服务

包括开源数据库、中间件服务。

按照规范提供标准接口，具备开放性，可移植。

数据库服务：提供满足各部门关系型数据库、非关系型数据库以及分布式数据库使用需求。在数据库层面上实现统一建设、统一管理、统一服务。包括MySQL分布式数据库服务、PostgreSQL分布式关系数据库集群服务、Redis数据库服务、MongoDB数据库服务等。

中间件服务：提供消息中间件及其他中间件服务。

2.3本地备份服务

为各类应用数据提供不同等级的备份服务，实时/定时备份与恢复、海量文件备份、操作系统备份、数据库备份以及虚拟化平台备份等，满足各种类型的结构化、非结构化数据以及半结构化数据的备份需求。

2.4云安全服务

为云上租户提供多种安全服务，能够满足云上用户业务二级等保、三级等保测评合规。用户可以通过调用密码服务平台提供的服务满足应用系统密码应用合规要求。

2.5租户密码服务

为云上租户提供合规的密码资源能力，建设统一的密码资源池，为全区政务云云上租户业务系统提供合规、高效、灵活的租户密码服务支撑，可以为怀柔区政务云租户密码测评提供虚拟加解密服务、通信链路加密服务、租户身份认证服务、密码资源统一管理服务、可信时间戳服务、客户端身份认证服务、可信设备证书服务、可信个人数字证书服务。

2.6深度监控服务

中标单位需提供7\*24小时云主机深度监控服务并提供报告，以保障云环境稳定、安全运行。

2.7迁移服务

需提供整体的业务上云迁移服务，包括迁移评估与分析、迁移方案设计、云平台环境准备、迁移测试验证、业务系统迁移、迁移业务切割等服务。业务系统在向云平台迁移的过程中要做到无缝迁移，确保业务连续不中断。迁移后的数据需通过目标系统的业务验证，所有数据必须符合业务规则，核心业务数据迁移准确率需达到99.99%以上。

2.8运维服务：包括中标单位提供的基础设施运行维护服务、网络专线运维服务和云平台软件运维服务。运维团队包含不少于8人的驻场运维，其中1人需为云平台原厂运维。

运维响应SLA需满足以下要求：

一级故障（重大）：系统全面宕机、核心业务中断或大量数据异常，需5分钟内响应，30分钟内提供解决方案，4小时内恢复服务。

二级故障（严重）：部分功能模块失效、非核心业务中断，需30分钟内响应，4小时内提供解决方案，8小时内恢复服务。

三级故障（一般）：单个用户操作异常、数据查询延迟等不影响整体业务的问题，需2小时内响应，8小时内提供解决方案，24小时内解决。

四级故障（轻微）：界面显示异常、非关键功能优化建议等，需4小时内响应，48小时内处理完毕。

（1）基础设施运行维护服务

中标单位对云平台的设备硬件提供维护保障服务。包括服务器、存储、网络设备、安全设备、备份设备及信息化系统相关的配套设备进行设备外观检查、维修保养、设备软硬件配置检查、设备除尘、清洁、线路整理、设备和线路标识检查、网络线路通信质量测试等运维服务。

（2）网络专线运维服务

中标单位对云平台的网络提供维护保障服务。包括网络的日常维护、故障处理、网络变更、设备配置管理、网络分析诊断、网络监控、网络定期巡查、日志分析、网络优化等运维服务。

（3）云平台软件运维服务

中标单位承担云平台软件的建设和运行维护。

2.9增值服务要求

（1）基础软件栈全生命周期保障维护服务要求

1、操作系统支持服务：需提供商用操作系统、开源操作系统支持服务。

2、中间件支持服务：需提供国产商用应用中间件、开源中间件支持服务。

3、数据库支持服务：需提供商用、开源数据库支持服务。

每种服务均有对应的套餐租用、安装及维保服务。

（2）安全重保服务要求

中标单位需提供日常安全运维驻场服务、中级安全服务、高级安全服务，以保障信息系统在不同阶段和场景下的安全稳定运行。

（3）IDC服务要求

需提供IDC机柜扩增服务，以满足后续业务扩容需求，包含新增机柜及相关配套设施和对应服务。

按需求点位提供裸纤接入服务，裸纤采用单模光纤传输，光衰符合两端设备要求，保证业务使用。按使用需求，提供对应带宽的数传专线，保证专线安全性、稳定性和时延符合要求，并提供两端设备兼容的端口。

（4）CDN服务要求

需要提供不同速度的内容加速及视频加速服务。

（5）扩展网络维保支持服务要求

需提供不同规模的网关维保支持服务，包括小型、中型、大型、超大型，每种规模都有对应的维保服务。

2.10机房服务要求

提供政务云所需的机房环境，具有符合北京市数据中心要求的机房空间和环境、机柜配置、电力配套、能效要求、安防和消防系统。机房物理设施满足等保3级要求，且具有自主产权和灾备能力。

投标人需承诺投标机房配备燃油发电机，在市电异常断电后，发电机组须在15分钟内提供备用电力，确保业务不间断运行。

2.11团队人员要求

中标单位须根据项目要求安排具备相应资质和经验的项目经理、技术负责人、交付团队以及运维团队从事本项目工作。其中，项目经理和技术负责人不得随意更换，如更换需征求甲方同意，需确保项目实施队伍的稳定。

2.12运营要求

中标单位需满足区内系统对云资源的使用量，在现有调研基础上，如出现变更、新建系统需求（以正式需求函为准），中标单位应在承诺建设总量内，通过调整配置、资源类别优化等工作，满足需求。

在项目运营过程中，如出现需求总量超过建设资源量的情况下，将提前以正式需求函的形式，通知中标人。中标人应在接到正式需求函后，4个月内完成新增资源建设。

**三、政务云平台要求**

3.1建设要求

1．建设符合工信部《基于云计算的电子政务公共平台顶层设计指南》、《信息安全技术云计算服务安全指南》和《信息安全技术云计算服务安全能力要求》等国家及行业标准、规范的政务云平台。

2.为保证政务云达到招标人对相关服务的要求，投标人须承诺建设的云平台在投入使用前必须对提供服务项的功能和性能进行验证，并通过三级等保测评和密码安全测评相关工作。

3.2服务要求

怀柔区政务云采用购买服务方式，由投标人在北京市怀柔区政数局指定的时间内完成政务云平台的建设部署。

1.采用购买服务方式在数据中心搭建政务云平台，机房和其他组成政务云平台所必需的软硬件设备均由中标单位提供，并承担相关建设和运行维护成本。

2.中标单位完成政务云平台区本身的网络搭建和部署，政务外网由采购人提供（带宽足够满足需求），互联网及带宽由中标单位保障，可自行接入组网。

3.中标单位应构建完整的政务云服务体系。

**四、云服务要求**

4.1服务目录及预估需要服务资源数量

★投标人须承诺在合同签署后60个工作日内完成怀柔区政务云平台建设工作，具备下列可用资源，并提供承诺函。

|  |  |  |  |
| --- | --- | --- | --- |
| **服务类别** | **服务子类** | **服务项单位** | **可用资源总数** |
| 计算服务 | x86平台云主机服务 | vCPU（1vCPU） | 4100 |
| x86平台云主机服务 | 内存（1GB） | 14640 |
| C86平台云主机服务 | vCPU（1vCPU） | 4136 |
| C86平台云主机服务 | 内存（1GB） | 13856 |
| ARM平台云主机服务 | vCPU（1vCPU） | 448 |
| ARM平台云主机服务 | 内存（1GB） | 3904 |
| 存储服务 | 高性能存储 | 1GB | 171212 |
| 普通性能存储 | 1GB | 318504 |
| 对象存储 | 1TB | 311 |
| 本地备份服务 | 1GB | 163840 |
| 网络服务 | 互联网链路服务 | 互联网链路带宽（Mb） | 3072 |
| 互联网IP地址租用服务、并提供备案服务（IP） | 75 |
| 主机负载均衡服务 | 主机负载均衡服务（IP） | 75 |
| VPN服务 | SSLVPN接入（1账号） | 75 |
| IPSecVPN接入（1Mb带宽） | 75 |
| 安全服务 | 等保二租户安全 | | |
| 云安全中心服务（主机杀毒服务、漏洞扫描、主机防护、主机安全加固） | 1个租户 | 20 |
| 云防火墙 | 1个租户,1G防护能力 | 20 |
| web应用防火墙（web应用防火墙、网页防篡改） | 1个租户,1G防护能力 | 20 |
| 云堡垒机 | 1个租户，20个资产 | 20 |
| 数据库审计 | 1个租户，3个数据库资产 | 20 |
| 多云安全管理服务（云安全统一运维平台、综合日志审计） | 1个租户 | 20 |
| 等保三租户安全 | | |
| 云安全中心服务（主机杀毒服务、漏洞扫描、主机防护、主机安全加固） | 1个租户 | 22 |
| 云防火墙 | 1个租户 | 22 |
| web应用防火墙（web应用防火墙、网页防篡改） | 1个租户,1G防护能力 | 22 |
| 多云安全管理服务（云安全统一运维平台、综合日志审计） | 1个租户 | 22 |
| 高级网络威胁检测服务（入侵攻击防护、攻击威胁检测防护） | 1个租户 | 22 |
| 云堡垒机 | 1个租户，20个资产 | 22 |
| 数据库审计 | 1个租户，3个数据库资产 | 22 |
| 密码服务 | 虚拟加解密服务 | 1个业务系统，云服务器密码机 | 22 |
| 通信链路加密服务 | 1个业务系统，综合安全网关 | 22 |
| 租户身份认证服务 | 1个业务系统，云服务器密码机 | 22 |
| 密码资源统一管理服务 | 1个业务系统，密码服务管理平台 | 22 |
| 可信时间戳服务 | 1个业务系统，时间戳服务器 | 22 |
| 客户端身份认证服务 | 1个业务系统，智能密码钥匙 | 22 |
| 可信设备证书服务 | 1个业务系统，设备证书 | 22 |
| 可信个人数字证书服务 | 1个业务系统，个人数字证书 | 22 |
| 深度监控服务 | 特定云主机深度监控及运维保障服务（7\*24小时值守） | 一主机 | 300 |
| 迁移服务 | 为业务系统提供迁移评估与分析服务、迁移方案设计服务、迁移云平台环境准备服务、迁移测试验证服务、迁移业务迁移服务以及迁移业务切割服务 | 人月 | 240 |

考虑本项目中迁移及信创改造等因素，本项目的服务资源总数见下表，并需提供以下四类服务，包括基础服务、扩展服务、迁移服务和增值服务，服务目录如下。各资源量以实际发生数量核准后，按量付费。

4.1.1基础服务目录

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 基础 服务 目录 | **编号** | **服务类别** | **服务子类** | **计价单位** | **报价单位** | **最高限制单价（元/每月）** | **服务资源总数** |
| 1 | 计算服务 | x86平台云主机服务 | vCPU（1vCPU） | 元/月 | 10.8 | 3500 |
| 2 | 内存（1GB） | 元/月 | 30.56 | 12618 |
| 3 | C86平台云主机服务 | vCPU（1vCPU） | 元/月 | 10.8 | 1197 |
| 4 | 内存（1GB） | 元/月 | 30.56 | 1708 |
| 5 | ARM平台云主机服务 | vCPU（1vCPU） | 元/月 | 10.8 | 269 |
| 6 | 内存（1GB） | 元/月 | 30.56 | 2342 |
| 7 | 存储服务 | 高性能存储 | 1GB | 元/月 | 0.22 | 171212 |
| 8 | 普通性能存储 | 1GB | 元/月 | 0.16 | 318504 |
| 9 | 对象存储 | 1TB | 元/月 | 36 | 187 |
| 10 | 本地备份服务 | 1GB | 元/月 | 0.32 | 98019 |
| 11 | 网络服务 | 互联网链路服务 | 互联网链路带宽（Mb） | 元/月 | 38.5 | 3072 |
| 12 | 互联网IP地址租用服务、并提供备案服务（IP） | 元/月 | 36 | 75 |
| 13 | 主机负载均衡服务 | 主机负载均衡服务（IP） | 元/月 | 2.6 | 75 |
| 14 | VPN服务 | SSLVPN接入（1账号） | 元/月 | 55.9 | 75 |
| 15 | IPSecVPN接入（1Mb带宽） | 元/月 | 48.6 | 75 |

4.1.2扩展服务目录

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 扩展 服务 目录 | **编号** | **服务类别** | **服务子类** | **计价单位** | **报价单位** | **最高限制单价（元/每月）** | **服务资源总数** |
|  | 安全服务 | **等保二租户安全** |  |  |  |  |
| 1 | 云安全中心服务（主机杀毒服务、漏洞扫描、主机防护、主机安全加固） | 1个租户 | 元/月 | 320 | 20 |
| 2 | 云防火墙 | 1个租户 | 元/月 | 356 | 20 |
| 3 | web应用防火墙（web应用防火墙、网页防篡改） | 1个租户 | 元/月 | 206 | 20 |
| 4 | 云堡垒机 | 1个租户，20个资产 | 元/月 | 121.6 | 20 |
| 5 | 数据库审计 | 1个租户，3个数据库资产 | 元/月 | 206 | 20 |
| 6 | 多云安全管理服务（云安全统一运维平台、综合日志审计） | 1个租户 | 元/月 | 356 | 20 |
|  | **等保三租户安全** |  |  |  |  |
| 7 | 云安全中心服务（主机杀毒服务、漏洞扫描、主机防护、主机安全加固） | 1个租户 | 元/月 | 320 | 22 |
| 8 | 云防火墙 | 1个租户 | 元/月 | 356 | 22 |
| 9 | web应用防火墙（web应用防火墙、网页防篡改） | 1个租户 | 元/月 | 206 | 22 |
| 10 | 多云安全管理服务（云安全统一运维平台、综合日志审计） | 1个租户 | 元/月 | 323 | 22 |
| 11 | 高级网络威胁检测服务（入侵攻击防护、攻击威胁检测防护） | 1个租户 | 元/月 | 356 | 22 |
| 12 | 云堡垒机 | 1个租户，20个资产 | 元/月 | 121.6 | 22 |
| 13 | 数据库审计 | 1个租户，3个数据库资产 | 元/月 | 206 | 22 |
| 14 | 密码服务 | 虚拟加解密服务 | 1个业务系统 | 元/月 | 569.334 | 22 |
| 15 | 通信链路加密服务 | 1个业务系统 | 元/月 | 253.6 | 22 |
| 16 | 租户身份认证服务 | 1个业务系统 | 元/月 | 223.6 | 22 |
| 17 | 密码资源统一管理服务 | 1个业务系统 | 元/月 | 424.668 | 22 |
| 18 | 可信时间戳服务 | 1个业务系统 | 元/月 | 317.778 | 22 |
| 19 | 客户端身份认证服务 | 1个业务系统 | 元/月 | 14.304 | 22 |
| 20 | 可信设备证书服务 | 1个业务系统 | 元/月 | 14.406 | 22 |
| 21 | 可信个人数字证书服务 | 1个业务系统 | 元/月 | 15.66 | 22 |
| 22 | 深度监控服务 | 特定云主机深度监控及运维保障服务（7\*24小时值守） | 一主机 | 元/月 | 60 | 300 |

4.1.3迁移服务目录

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 迁移服务 | **编号** | **服务类别** | **服务子类** | **计价单位** | **报价单位** | **最高限制单价（元/每月）** | **服务资源总数** |
| 1 | 迁移服务 | 为业务系统提供迁移评估与分析服务、迁移方案设计服务、迁移云平台环境准备服务、迁移测试验证服务、迁移业务迁移服务以及迁移业务切割服务 | 人月 | 元/月 | 14372 | 240 |

4.1.4增值服务目录

★增值服务目录如下，客户根据实际需求按需订购，本部分价格不计入招标总价；投标人需承诺后续提供本部分增值服务的各项单价不高于中标的各项单价。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 增值服务目录 | **编号** | **服务类别** | **服务子类** | **计价单位** | **报价单位** |
| 1 | 基础软件栈全生命周期保障维护服务 | WindowsServer系统租用、安装及维护服务 | 月 | 元/月 |
| 2 | 国产Linux操作系统租用、安装及维护服务 | 月 | 元/月 |
| 3 | 提供开源操作系统安装及维护服务 | 月 | 元/月 |
| 4 | 国产商用应用中间件租用、安装及维护服务 | 月 | 元/月 |
| 5 | 主流开源应用中间件安装及维护服务（覆盖3种以上） | 月 | 元/月 |
| 6 | 国产商用数据库租用、安装及维护服务（支持至少3种主流国产库） | 月 | 元/月 |
| 7 | 开源数据库安装及维护服务 | 月 | 元/月 |
| 8 | 安全重保服务 | 日常安全运维驻场服务（中级） | 人天 | 元/天 |
| 9 | 中级安全服务（Web失陷检测、等保咨询等） | 人天 | 元/天 |
| 10 | 高级安全服务（重保服务、攻防演习服务、渗透测试、代码审计、应急响应、安全事件检查服务等） | 人天 | 元/天 |
| 11 | IDC服务 | 机柜扩增 | 1架 | 元/月 |
| 12 | 裸光纤 | 点位 | 元/月 |
| 13 | 数传专线(6M) | 条 | 元/月 |
| 14 | 数传专线(10M) | 条 | 元/月 |
| 15 | 数传专线(20M) | 条 | 元/月 |
| 16 | 数传专线(32M) | 条 | 元/月 |
| 17 | 数传专线(56M) | 条 | 元/月 |
| 18 | CDN加速服务 | 提供内容加速及视频加速服务（1MB） | Mbps | 元/月 |
| 19 | 提供内容加速及视频加速服务（1GB） | Mbps | 元/月 |
| 20 | 提供内容加速及视频加速服务（100GB） | Mbps | 元/月 |
| 21 | 扩展网络维保支持服务 | 小型网关维保支持服务 | 月 | 元/月 |
| 22 | 中型网关维保支持服务 | 月 | 元/月 |
| 23 | 大型网关维保支持服务 | 月 | 元/月 |
| 24 | 超大型网关维保支持服务 | 月 | 元/月 |

本次项目需迁移上云业务系统共计75个（最终以北京市怀柔区政务服务和数据管理局确认的迁移系统为准），具体系统如下：

| **序号** | **单位** | **系统名称** |
| --- | --- | --- |
| 1 | 区政数局 | 办好一件事主题服务区级支撑系统 |
| 2 | 政务区块链场景应用 |
| 3 | 怀柔政务-金钥匙专员企业管家服务及京策服务管理平台建设项目 |
| 4 | 怀柔区政府网站 |
| 5 | 怀柔区OA系统 |
| 6 | 区教委 | 怀柔区教育资源公共服务平台系统 |
| 7 | 怀柔区适龄幼儿入园服务平台 |
| 8 | 怀柔区智慧融合管理平台 |
| 9 | 怀柔区智慧教育平台 |
| 10 | 协同办公系统 |
| 11 | 教育大数据采集平台 |
| 12 | 教育大数据分析平台 |
| 13 | 怀柔区医院 | 临床数据发布中心平台系统 |
| 14 | 区中医院 | 怀柔中医院网站 |
| 15 | 区卫健委 | 怀柔区人口健康信息平台 |
| 16 | 区水务局 | 怀柔区村级供水站智能远传计量系统（智慧水务服务平台） |
| 17 | 北京市怀柔区取用水监控管理系统 |
| 18 | 怀柔区自备井水量监控系统 |
| 19 | 怀柔区农业灌溉机井智能计量管理系统 |
| 20 | 怀柔区水务局防汛指挥系统 |
| 21 | 怀柔区村镇污水处理设施远程监测系统 |
| 22 | 区园林绿化局 | 生物多样性智慧感知与监测系统 |
| 23 | 区财政局 | 行业电子票据云服务平台 |
| 24 | 怀柔区财源建设企业服务平台 |
| 25 | 怀柔区财政局OA办公自动化系统 |
| 26 | 怀柔区财政局OA门户网站 |
| 27 | 信创智能档案管理系统 |
| 28 | 区应急局 | 怀柔区韧性城市技术迭代平台 |
| 29 | 区文旅局 | 全域旅游数字地图小程序 |
| 30 | 长城保护巡检系统 |
| 31 | 区博物馆 | 网上博物馆系统 |
| 32 | 文物综合展示系统 |
| 33 | 馆藏文物数字化管理系统 |
| 34 | 区融媒体中心 | 手机客户端系统 |
| 35 | 区城管委 | 燃气一期-燃气安全运行监测系统 |
| 36 | 燃气二期-城镇燃气行业安全综合监管系统（一网统管平台） |
| 37 | 怀柔区生活垃圾精细化管理平台系统 |
| 38 | 区经信局 | 怀柔地理空间信息系统 |
| 39 | 怀柔社会信用信息服务平台 |
| 40 | 区生态环境局 | 大气环境精细化管控服务平台 |
| 41 | 大气VOCs监测预警系统 |
| 42 | 怀柔区生态环境监测综合业务管理平台 |
| 43 | 怀柔区水环境智慧监管平台 |
| 44 | 噪声检测系统 |
| 45 | 区人保局 | 自动化办公系统 |
| 46 | 文书档案系统 |
| 47 | 机关事业单位人事工资管理系统 |
| 48 | 区医保局 | 智慧医保服务信用结算平台 |
| 49 | 区发改委 | 怀柔区经济运行监测平台评估调研表 |
| 50 | 区司法局 | 怀柔区领导干部学法考法平台V2.0 |
| 51 | 区城指中心 | 怀柔区接诉既办一体化系统平台 |
| 52 | 科学城管委会 | 怀柔科学城智慧督查管理平台 |
| 53 | 区政府办 | 北京市怀柔区人民政府办公室项目管理督查系统 |
| 54 | 雁栖湖公司 | OA办公系统 |
| 55 | 网站系统 |
| 56 | 票务系统 |
| 57 | 区政协 | 怀柔政协官网 |
| 58 | 区疾控中心 | 疾控慢病管理系统 |
| 59 | 怀胜公司 | 北京怀胜协同OA系统 |
| 60 | 电子档案系统、固定资产管理系统 |
| 61 | 区人大办 | 怀柔区人民代表大会常务委员会网站系统 |
| 62 | 区公共资源交易中心 | 怀柔区公共资源交易平台 |
| 63 | 区国资公司 | 怀柔国资公司OA协同办公系统 |
| 64 | 京北职业学院 | 北京京北职业技术学院官方网站、北京京北职业技术学院教务系统 |
| 65 | 长城伟业 | OA办公系统 |
| 66 | 区总工会 | 怀柔区总工会综合服务平台 |
| 67 | 区气象局 | 信息发布预警系统 |
| 68 | 区民政局 | 怀柔区养老服务信息综合平台 |
| 69 | 区残联 | 档案管理系统 |
| 70 | 怀源供水公司 | 怀源供水智能管理系统 |
| 71 | 区投促中心 | 怀柔区企业集中办公区信息化管理服务平台 |
| 72 | 区纪委区监委机关 | 怀柔区纪检监察网 |
| 73 | 区委办公室 | 怀柔区区委办公室档案管理系统 |
| 74 | 区委宣传部 | 怀柔区新时代文明实践中心网络平台 |
| 75 | 区科委 | 苗圃计划项目管理系统 |

4.2规格参数要求

| **序号** | **指标类别** | **指标名称** | **规格要求** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 云管平台 | 云管理平台软件 | 一、访问控制 1、登录：支持用户端主账号或子用户登录云平台用户端，子用户可SSO登录至用户端。 2、账户中心：支持通过密码强度检测、超时登出等选项保护用户账号安全；支持为每个用户提供多因子认证能力，登录时开启二次验证，保护用户的安全。 3、用户管理：支持子用户的生命周期管理，包含创建子用户、搜索和删除运维用户、修改基本信息、重置密码等；支持子用户的权限管理，支持管理子用户的策略配置、用户组关联配置，支持子用户的登录配置管理，支持配置是否允许控制台登录。 4、用户组管理：支持用户组的生命周期管理，包含创建用户组、搜索和删除用户组；支持为用户组配置策略和配置关联用户、项目用户组管理。 5、项目管理：支持项目的生命周期管理，包含创建项目、创建子项目、编辑项目、查看项目列表、查看项目项目详情、搜索项目、查看项目资源；支持项目用户关联管理，包含项目用户关联与用户授权；支持项目用户组关联管理，包含项目用户组关联与用户组授权。 6、▲身份映射：支持第三方来源用户在平台的身份与权限映射管理（提供产品对应功能界面截图并加盖原厂盖章证明材料）。 7、策略管理：支持策略的生命周期管理，包含创建、搜索、编辑、删除策略。支持基于条件的鉴权，如资源标签；支持为策略配置关联用户组、配置关联用户、项目策略管理。 8、角色管理：支持角色的生命周期管理，包含创建、搜索、编辑和删除角色；支持角色的信任关系和策略管理。 9、密钥管理：支持密钥的生命周期管理，创建、查看和删除密钥，启用及禁用密钥。 二、组织管理 1、部门管理：支持部门组织中管理成员的单位节点，最多包含五个层级。支持部门的创建、编辑、删除等。 2、成员管理：支持组织中除管理员账号外的其他账号为成员账号，支持其他主账号添加至企业组织中，以部门为单位进行管理。 3、管控策略：支持基于企业组织的组织架构划定各层级、各账号最大权限范围，满足企业中成员账号权限控制、确保操作安全合规和维护可控企业成本的需求。 三、配额管理 1、支持主账号的配额管理，包含查看产品列表、查看产品配额详情、搜索产品配额参数、申请产品配额、查看产品配额申请历史。支持设置配额告警。 2、支持用户查看和搜索配额申请历史。 四、操作审计 1、支持操作审计的查看与检索，支持通过事件名称、事件别名、项目名称、用户名、事件源、请求ID、AccessKeyID、地域、IP地址、结果和身份筛选事件记录。 五、费用中心 1、订单管理：支持查看主账号的预付费和后付费订单、订单详情，支持通过订单号检索订单信息。 2、账单管理：支持查看主账号的账单明细信息、账单汇聚信息、导出账单，支持通过账单明细号、实例名称、实例ID检索账单信息，支持在控制台获取计费项明细的标签信息和项目归属。提供后付费资源账单的费用预警能力。 3、费用标签：支持根据自身企业内部成本管理分析维度，按需定义标签键值来对云资源进行分类或分账，启用费用标签后可在账单明细查看标签信息。 六、消息中心 1、站内信管理：支持云平台管理员发布的站内信的查看、标记已读。 2、消息接收管理：支持主账号管理员可以根据消息类型配置接收方式和接收人。 六、工单管理 1、支持创建工单、查看已提起工单、在线补充信息、流转工单状态等。 七、多云纳管 1、▲支持第三方虚拟机实例的创建、开机、关机、释放、远程连接、冷迁移、热迁移、虚拟机克隆、虚拟机重置密码。支持关联云盘的查看、修改规格、删除（提供产品对应功能界面截图并加盖原厂盖章证明材料）。 八、在线文档： 1、支持在文档中心中查看产品文档、检索文档信息。在平台可访问公网的前提下，支持基于大模型的智能搜索。 九、包含三年软件平台更新与支持 十、提供云平台的交付部署实施服务，包括项目管理服务、实施工勘、实施方案规划、硬件布线、云平台部署及测试验收等； | 政务外网区、互联网区各一套 |
| 2 | 云平台计算软件 | 一、实例管理 1、支持创建/删除云服务器，能够选择地域与可用区、实例规格、实例数量、镜像信息、存储信息（系统盘、数据盘大小及容量）、配置主网卡网络信息（具体子网、IP）、配置公网信息（IP、带宽）、配置辅助网卡信息、配置安全组等，可兼容X86和ARM架构。 2、支持主机名注入功能，对已创建的实例支持重置密码、更改实例规格、重装系统的操作。 3、支持实例生命周期管理，包含创建、启动、停止/强制停止、重启/强制重启、暂停、恢复、删除等操作。 4、▲支持批量创建云服务器时，可以设置在云服务器名称设置有序主机名和实例名称，并可以自定义起始标识数字。（提供产品对应功能界面截图并加盖原厂盖章证明材料） 5、支持获取实例系统日志和实例屏幕截屏，可获取运行中状态手里的系统日志和屏幕截图。 6、实例列表支持名称、ID、状态、可用区、公网/私网IP地址、标签/标签键、镜像名称、镜像ID、IPv6等搜索，支持状态和可用区列表字段筛选；实例列表支持字段的列宽动态调整；实例列表支持自定义列，支持导出列表，支持筛选后列表导出；实例列表批量操作支持启动、停止/强制停止、重启、删除。 7、支持停机状态下，更换私有网络。 8、支持更改实例规格：支持停机状态下对通用型/计算型/内存型/大数据型/GPU型支持同规格族下变更实例规格；支持开机状态下，对通用型/计算型/内存型在同规格族下变更实例规格。 9、支持重置密码，重启实例后密码生效。 10、支持实例删除保护，防止通过控制台或API误删除。 11、支持自定义数据，自定义数据可以让实例首次启动时进行数据传输、安装服务器、软件升级等。 12、支持整机镜像，导出自定义镜像支持包含实例已挂载的所有数据盘，可以按照整机镜像创建实例。 13、支持VNC登录，Terminal，挂载/卸载云盘、辅助网卡和公网IP。 14、支持通过查看实例监控指标获取监控信息。 15、支持标签能力，通过标签为资源进行分类，便于资源统一管理、使用和查找。 16、支持预付费和后付费两种计费模式，支持按量计费转包年包月。 17、支持配额，可在vcpu、规格可创建实例数、实例数量、内存等维度设置ECS配额。 18、支持创建、删除、绑定、解绑密钥对，支持查看密钥对详情，在详情中支持修改密钥对描述、查看已绑定实例。 19、支持查看事件监控的能力。 20、支持实例回收站，在删除实例时，可将实例放入回收站保留一段时间，并根据当前的清除策略一定周期后自动释放；对于进入回收站的实例，在未彻底删除前，可将该实例恢复至原环境；保留在回收站的实例，支持手动彻底删除，以释放存储空间。 二、高性能计算集群 1、支持高性能计算集群默认支持RDMA网络规格。 2、支持高性能计算集群与实例的VPC解绑，同一高性能计算集群可扩容不同VPC的实例。 3、支持高性能计算集群维度的诊断能力。 三、部署集 1、支持创建部署集支持强制高可用、非强制高可用策略。 2、支持修改部署集名称，描述，删除部署集，支持添加实例、移除实例。 四、镜像 1、支持公共镜像和自定义镜像。支持自定义镜像生命周期管理，包含导入镜像、创建镜像、共享或取消共享镜像、对象存储/本地镜像、删除镜像、导出镜像、复制镜像、修改镜像名称/描述等。 2、▲支持用户粒度设置规格、镜像白名单开放能力。（提供产品对应功能界面截图并加盖原厂盖章证明材料） 五、弹性伸缩 1、支持伸缩组、伸缩配置来源、实例管理、伸缩规则、伸缩日志、项目和标签能力。 2、目标追踪规则、报警任务支持同时设置多个监控指标。 六、一云多芯 1、支持同一管理平台纳管x86、c86、arm等不同架构硬件系统，同步支持裸机纳管国产、非国产GPU系统； 2、▲能够提供一云多算融合相关的第三方权威检测机构检测检验的相关证明文件，多算融合检验项至少包含多种算力、高速存储、高速网络、数据协同等能力的检验； 3、▲能够提供一云多算协同调度相关的第三方权威检测机构检测检验的相关证明文件，多算协同调度检验项至少包含多算资源管理、多算资源调度等能力的检验； 4、▲能够提供一云统管相关的第三方权威检测机构检测检验的相关证明文件，一云统管检验项至少包含统一运营、统一运维的能力检验； 七、包含三年软件平台更新与支持 八、云平台重保演练 1、重保故障演练可视化：包括演练活动观测、演练统计分析两个模块，演练活动观测包括演练活动看板、状态验证、观测感知、数据展示、监控接入管理等功能，实现执行过程的可视化。演练统计分析，包括应用稳定性分析应用稳定性分析、演练活动量统计、应用风险统计、演练活动概览等功能。 2、重保故障演练执行引擎：包含演练场景编排、演练活动执行、演练过程防护和演练结果报告四个模块，演练场景编排实现将不同故障场景组合成演练任务计划，并分配至相应执行人实施，实现演练活动参数化配置。演练活动执行实现人员管理、申请/审批、流程编辑、串/并/循环实验、动态可编辑、能力开放等；演练过程防护实现演练过程中控制爆炸半径，包括手动终止、超时终止、阈值终止、智能终止；演练结果报告负责生成故障演练报告，包含演练任务概要、稳态指标、故障分析诊断、问题反馈记录、系统抵御故障的通过率、整体总结、风险反馈等。 3、故障演练管理引擎：包含演练活动管理、演练资源管理两个模块，实现演练活动的编辑、复制、迁移、查询等功能，对演练活动的状态进行管理，通过活动的“上线/下线”决定演练活动是否可用。演练活动管理包括演练任务、演练反馈、风险事项跟踪、生产事件库等功能。演练资源管理模块，包括故障流程管理、系统关联管理、告警通知、压力测试场景库等功能。 4、平台基础管理引擎：包含原子故障库、探针管理、应用管理、系统管理四个模块，原子故障库实现对主机、各版本分布式容器、数据库、中间件等多环境的原子故障场景库创建，开箱即用。探针管理实现探针一键安装、卸载、启停，实现探针列表管理功能。应用管理实现应用资源管理、应用信息同步，历史演练记录查询等功能；系统管理实现角色管理、部门管理、操作审计、白名单管理等功能。 | 政务外网区、互联网区各一套 |
| 3 | 云平台网络软件 | 一、私有网络 1、支持创建VPC，创建VPC时支持同时添加多个子网。 2、支持删除已创建的VPC，可查看VPC详情，支持修改VPC名称、描述信息，修改DNS地址，支持VPC跨账号授权给云企业网。 3、支持创建子网（支持同时添加多个子网），删除子网，为子网更换路由表，修改子网名称、描述信息。 4、支持自定义子网网关。 5、支持创建网卡，可手动/自动分配主私网IP以及手动/自动分配辅助私网IP。 6、支持为网卡关联安全组，解关联安全组，支持删除网卡。辅助网卡可开启随云服务器实例删除，当云服务器释放时，随其一同释放。 7、支持修改网卡名称、描述信息，将网卡挂载到云服务器实例、从云服务器实例卸载网卡。 8、支持托管弹性网卡和安全组，即服务创建的网卡作为托管网卡不允许用户操作。 9、支持管理网卡IP地址，包括增加辅助私网IP地址、释放辅助私网IP地址、私网IP绑定EIP、私网IP解绑EIP。 10、支持创建高可用虚拟IP，修改高可用虚拟IP信息和删除高可用虚拟IP；支持为高可用虚拟IP绑定/解绑公网IP，为高可用虚拟IP绑定/解绑云服务器实例或网卡。 11、支持修改路由表关联的子网，可创建自定义路由表、删除自定义路由表，在路由表中添加路由条目、删除路由条目。 12、支持创建新的安全组，删除安全组，修改安全组名称描述，为安全组关联网卡，取消关联网卡；支持查看安全组关联的网卡，支持创建、修改、复制、删除安全组规则。支持批量删除安全组规则，openAPI支持批量创建；支持安全组批量导入导出和克隆。 13、支持创建网络ACL、修改网络ACL、删除网络ACL，为关联子网以及取消网络ACL关联的子网；支持添加网络ACL规则、修改网络ACL规则、修改网络ACL规则优先级、删除网络ACL规则；支持五元组ACL。 14、支持流量镜像能力，通过流量镜像，可以按需复制指定网卡的流量，并私网转发到目标网卡或负载均衡进行监控分析。 二、NAT网关 1、支持创建NAT网关，为NAT网关绑定/解绑公网IP，支持删除NAT网关，修改NAT网关名称、描述，查看NAT网关监控指标并配置告警。 2、NAT网关支持全通模式，即为NAT网关自动配置一条私有网络粒度的SNAT规则，使私有网络内所有未绑定公网IP的云服务器实例均可通过NAT网关访问公网。 3、支持私网NAT网关，单VPC支持多NAT网关。 4、支持查看ECS实例维度的流量监控。当使用NAT网关的ECS实例流量异常时，可查看IP流量监控，快速定位到流量异常的ECS实例。 三、公网IP 1、支持创建公网IP、释放公网IP（支持强制释放）、修改公网IP名称描述、修改公网IP带宽上限、支持查看公网IP监控指标并配置告警规则。包月的服务器绑定按需计费的公网IP，退订时支持捆绑释放。 2、支持自定义公网线路名称。 3、支持指定地址创建。 4、支持为公网IP绑定云资源（云服务器/负载均衡/NAT网关/辅助网卡IP地址），从云资源（云服务器/负载均衡/NAT网关/辅助网卡）上解绑公网IP。 5、支持公网IP绑定高可用虚拟IP（白名单功能）、解绑高可用虚拟IP，支持配额管理能力，支持计量计费（按量付费-按带宽计费）。 四、负载均衡 1、支持创建负载均衡实例、修改负载均衡实例名称描述、变更规格、删除负载均衡实例。 2、创建公网负载均衡时指定已有公网IP。 3、支持为负载均衡实例添加监听器、删除监听器、启动监听器、停止监听器和编辑监听器；四层监听支持用户启用ProxyProtocolv2协议携带源IP、源端口、VIP、VPORT信息至后端服务器。 4、支持创建后端服务器组、编辑后端服务器名称、编辑服务器端口/权重、移除服务器、删除后端服务器组。 5、支持添加服务器，控制台添加辅助网卡的多个IP作为RS。 6、支持为监听器配置黑白名单访问控制，创建访问控制策略组，编辑访问控制策略组及删除访问控制策略组，支持IPv6条目。 7、支持开启/配置健康检查、关闭健康检查，UDP支持指定字符串。 8、支持创建、删除证书的能力。 五、应用负载均衡 1、支持创建公网/私网应用负载均衡实例。 2、支持查看实例详情信息，包含实例名称、实例描述、地域、子网、公私网IP等基本信息。 3、支持更改实例名称、实例描述等实例基本信息；支持实例删除保护；支持查看实例列表，通过实例id、公网IP、实例名称等搜索实例。 4、支持创建HTTP、HTTPS监听器，支持为HTTPS监听器开启证书双向认证功能；支持为同一个HTTPS监听器配置多本证书；支持查看监听器详情信息、监听器列表，并通过监听器id搜索监听器。 5、支持创建服务器组；支持添加ECS或ENI作为服务组内后端；支持基于Cookie的会话保持；支持加权轮询、最小连接数、IP哈希等负载均衡算法。 6、支持创建个性化配置并关联至监听器，包括：长连接保持时间、客户端上传body最大值、TLS协议版本等。 六、专线连接 1、支持展示物理专线列表、创建专线网关、支持创建虚拟接口、BFD联动BGP、虚拟接口开启BFD联动静态路由、支持负载冗余、主备冗余的线路冗余能力、NQA检测、支持主备与负载。 七、包含三年软件平台更新与支持 | 政务外网区、互联网区各一套 |
| 4 | 云平台存储软件 | 一、弹性块存储 1、具备完整云盘生命周期管理功能，支持创建、挂载、卸载、删除、扩容云盘。 2、支持批量扩容。 3、支持修改云盘属性信息，支持查询云盘信息，允许筛选云盘状态，支持导出云盘信息。 4、支持PL0等类型云盘。 5、支持云盘规格变配。 6、支持创建快照、查看快照创建的进度、查看快照（查看快照列表，查看快照链）、回滚快照、复制快照、删除快照、编辑快照信息、通过快照创建自定义镜像，创建实例时，支持通过快照创建新数据盘；支持设置自动快照策略，支持按天或按周为备份周期设置自动快照策略，为云盘定期创建快照备份数据；支持手动快照设置保留策略；支持查看快照链，查看同一云盘的快照。 7、支持创建快照一致性组，保证数据写入云盘的时序一致性，并保证其崩溃一致性。 二、对象存储 1、支持创建桶、查看桶列表、删除桶、搜索桶、桶概览、导出桶信息、用量统计、查看S3各类endpoint。 2、生命周期功能可实现整桶生效、前缀生效，过期天数、过期日期，策略状态启用、禁用，文件历史版本过期策略配置，分片过期策略配置，设置生命周期规则生效的文件大小、创建前缀重合的生命周期规则。生命周期规则列表支持tag和前缀。 3、支持版本控制功能，保留存储桶数据的历史版本，避免存储桶内的数据被误删除。 4、支持Project管理，用户管理一组具有相同功能或功能强关联的资源。 5、支持browser、自签名工具。 6、可通过文件列表上传文件、创建文件夹、分片管理、删除文件、下载文件、修改文件访问权限、查看文件详情、管理文件元数据、删除文件夹、搜索文件、重命名文件、复制文件、移动文件、管理文件标签、RenameObject。 7、支持图片缩放、图片水印、自定义裁剪、内切圆、索引切割、圆角矩形、质量变换、格式转换、获取信息、获取图片主色调、自适应方向、图片模糊、图片旋转、渐进显示、图片亮度、图片锐化、对比度、图片高级压缩、图片处理持久化。 8、权限管理功能可实现存储桶授权策略管理、桶ACL、跨域访问设置、访问控制IAM。 三、日志服务 1、支持日志项目、日志主题、机器组的增删改查；支持分区的信息查看与自动分裂；支持为日志项目和日志主题添加标签进行云资源归类。 2、支持采集器LogCollector的安装与升级、LogCollector服务日志的采集与管理。支持通过LogCollector采集文本日志与容器日志。支持使用webTracking、Kafka协议等方式采集并上传日志。支持导入从Kafka、对象存储、Elasticsearch等渠道导入数据。 3、▲支持以API或者SDK采集日志，SDK支持golangSDK、Node.jsSDK、java、pythonSDK。（提供产品对应功能界面截图并加盖原厂盖章证明材料） 4、支持配置全文索引或字段索引。支持JSON等多种字段类型索引，支持丰富的检索语法与SQL函数、语法。支持上下文查询和下载日志数据。 5、支持表格、折线图、柱状图等多种分析图表，支持将分析图表保存到仪表盘。支持仪表盘的创建、修改与删除等管理操作。支持将检索分析页面、仪表盘页面嵌入到外部系统的自建Web页面中。 6、支持通知组的增删改查等管理操作，支持告警策略的创建与管理，支持告警历史等数据的查看。支持通过内容语法、内容函数和内容变量设计自定义的通知内容。 7、支持通过日志服务控制台或云监控服务实时监控日志服务的资源用量；支持以日志方式记录日志服务各个功能运行过程中的状态信息、业务运行的行为数据等信息。 四、包含三年软件平台更新与支持 | 政务外网区、互联网区各一套 |
| 5 | 云平台数据库 | 一、数据库MySQL 1、支持实例管理，包括创建实例（共享型和通用型）、查看实例拓扑、变更配置、变更同步方式、增加只读节点、重启实例或只读节点、删除实例、创建相同配置实例、导出实例列表、手动主备切换、迁移可用区。支持为批量实例进行续费、变更配置和重启。 2、支持账号管理，包括创建高权限/普通账号、查看账号列表、重置密码、修改权限、删除账号。支持在高权限账号名称中使用root和admin。 3、MySQL支持开启全局只读的方式。 4、▲支持创建数据库、删除数据库。支持在创建数据库时为数据库添加描述信息。支持在删除实例的时候为了防止误删需要用户输入实例ID进行确认。（提供产品对应功能界面截图并加盖原厂盖章证明材料） 5、支持连接管理，包括命令行等方式连接实例、管理连接终端、查看连接信息、开启全局只读，切换连接池模式、开启公网访问、关闭公网访问、管理私网访问地址和端口、修改私有网络、开启或关闭数据库代理、修改公网端口号。 6、支持数据备份和数据恢复，包括查看数据备份列表、设置备份策略、手动备份数据库和Binlog、下载数据和binlog备份文件、按备份文件恢复、按时间点恢复、按备份集恢复、按时间段导出数据备份信息、跨地域备份和恢复、删除手动备份。 7、支持白名单管理，即查看白名单列表、创建白名单、绑定/解绑实例白名单、删除白名单、检索白名单。 8、支持查看和下载主备切换日志日志/慢日志/错误日志、设置审计日志。 9、支持修改参数、查看修改历史、创建参数模板、应用参数模板、将参数导出为模板、导出参数配置、修改最大连接数、异步删除大表。支持为批量实例进行修改参数、应用参数模板、下载Binglog备份。 10、支持监控告警和事件告警，包括资源监控、部署监控、代理监控、引擎监控，支持使用预置的告警模板。 二、文档数据库MongoDB 1、支持创建4.0、4.2、4.4、5.0、6.0版本实例、查看实例列表、查看实例详情、变更配置、重启实例、删除实例、查看节点信息、支持TAG标签管理、切换主从节点。 2、支持连接管理，包括查看连接信息、申请公网地址、释放公网地址、修改端口号。 3、支持备份恢复，可查看备份列表、设置备份策略、批量设置备份策略、手动数据备份、按备份文件恢复、按时间点恢复、获取并下载备份文件、支持库表恢复、恢复已删除实例。 4、支持参数管理功能，可查看参数列表、修改参数、批量修改参数、查看参数修改历史。 5、支持监控告警功能，可对资源进行监控，设置告警规则、支持预配置告警功能。 6、支持查看已删除实例，重建实例；支持查看历史事件列表，查看历史事件详情。 三、缓存数据库Redis 1、支持创建实例，包括设置实例名称、设置数据库版本、设置分片集群、设置分片数、设置每分片节点数、设置节点规格、设置可用区、设置访问方式、设置端口；实例列表支持批量搜索、标签管理、project项目管理、调整最大连接数、调整单分片带宽、购买相同配置实例、支持单节点缓存型实例、单分片最大连接数上限调整至10000。 2、支持变更实例配置，支持重启实例、删除按量计费实例、设置可维护时间段、导出实例列表、已删除实例备份（恢复已删除实例和管理已删除实例备份）。 3、支持更换子网、连接实例、申请直连地址、释放直连地址、修改端口号、免密访问、更新CA证书、修改TLS版本、修改连接地址、开启公网访问、关闭公网访问、手动主备切换、修改私有网络。 4、支持查看白名单设置，创建白名单、编辑白名单、删除白名单、绑定实例和白名单、解绑实例和白名单，设置SSL加密和清除数据，创建实例时支持直接绑定白名单。 5、支持设置自动备份，包括设置备份保留天数、设置备份周期、设置备份开始时间。支持手动备份、按备份集恢复（恢复到新实例、恢复到原实例）、按时间点恢复（恢复到新实例、恢复到原实例）、开启数据闪回。 6、支持查询慢日志、导出慢日志，包括数据节点慢日志和代理节点慢日志列表。 7、支持调整Redis定期任务的执行频率，设置内存碎片整理、禁止命令、选用使用ziplist编码、Redis后台任务每秒执行次数、基于lazyfree的功能（驱逐、过期键删除、DEL）、key的过期驱逐策略、读写分离、一个Lua脚本的最长执行时间、缓存写满后Redis删除键的策略。 8、支持调整慢日志参数，设置Redis的读写请求策略、设置就近访问、主从复制Backlog容量大小、选用Intset作为内部编码、客户端空闲连接超时时间、查看参数修改记录、参数模板。 四、数据库传输 1、支持迁移任务的创建、查询、任务调整、删除。 2、支持通过专有网络实现数据迁移、Project项目管理、标签管理。 3、支持数据订阅任务的创建、查询、任务调整、删除。支持消费组的创建、查询、删除、配置。 4、支持通过调用API接口实现数据传输。 5、支持通过Pythonsdk实现数据传输。 五、数据库PostgreSQL 1、实例管理：支持实例管理，包括创建实例、查看实例列表、查看实例详情、变更配置、创建只读节点、重启实例、重启只读节点、删除实例。支持通过项目管理实例资源。 2、账号与访问授权：支持账号管理，包括创建和管理账号、支持创建只读账号、重置账号密码、修改账号权限。 3、数据库管理：支持数据库管理，包括创建数据库、查看数据库列表、修改Owner、删除数据库。 4、Schema管理：支持Schema管理，包括创建Schema、查看Schema列表、修改Owner、删除Schema。 5、连接管理：支持连接管理，包括命令行等方式连接实例、查看私网访问地址和端口、修改私网访问端口、开启全局只读、开启读写分离. 6、备份恢复：支持备份恢复能力、查看备份进度、在备份列表中按备份方式筛选查看备份、在通过备份恢复到新实例时变更实例主节点的可用区，不再强制要求与原实例一致、复制槽，包括查看复制槽，删除复制槽。 7、数据安全管理：支持数据安全，包括添加IP白名单分组。支持白名单管理，即查看白名单列表、创建白名单、绑定/解绑实例白名单、删除白名单、合并生成白名单。 8、支持日志管理、参数管理、监控告警、历史事件、插件管理、观测诊断、计费等 六、包含三年软件平台更新与支持 | 政务外网区、互联网区各一套 |
| 6 | 云平台中间件 | 一、云搜索服务 1、支持创建实例、查看实例信息、重启实例或节点、重置实例密码、修改实例信息、设置可维护时间段、变更实例配置（横向扩容、纵向扩容）、删除实例。 2、支持手动备份和自动备份功能；支持内置参数的修改。 3、支持插件列表查看、ik分词插件配置。 4、支持数据自动备份功能。 5、支持根据业务需要切换实例的传输协议，通过启用和禁用HTTPS实现协议的切换。 6、支持同义词配置和参数配置。 二、消息队列RocketMQ版 1、支持接入点管理、实例规格配置、支持VPC访问、支持自定义数据保存时间、支持在线调试。 2、支持Group订阅关系展示、partition列表（消费位点展示）、重置消费位点功能、批量导入或导出Topic。 3、支持Topic订阅关系展示、客户端连接列表、重置消费位点功能。 4、支持多种消息类型，包括定时消息、延时消息、事务消息、顺序消息、全局顺序消息、分区顺序消息。 5、支持消息查询（通过时间范围、消息Key或消息ID）、消息轨迹查询、消息重试（无序消息重试、顺序消息重试、批量重试）。 6、支持展示死信消息列表，可展示死信消息，搜索/查询符合条件的死信消息。支持导出死信消息、逐条或批量重新发送死信消息。 7、支持实例级、Topic级、Group、死信队列级的监控和告警，支持预置的告警策略。 8、支持系统内置策略、用户自定义策略和用户账号密钥（AccessKey）鉴权。 9、支持AccessKey的创建、删除、查看，支持密钥细粒度权限管理。 10、具备OpenAPI调用能力，提供相关OpenAPI文档，SDK兼容ApacheRocketMQ（TCP）。 三、消息队列Kafka 1、支持接入点管理、实例规格配置、支持私有网络VPC访问、升级实例配置、变更消息配置、配置白名单、修改子网、在线调试、标签管理、重启实例。 2、支持Topic参数配置、关联Group管理、partition列表（消费位点展示）、导入导出Topic列表功能。 3、支持查看ConsumerGroup订阅的Topic、客户端连接列表、开启自动创建ConsumerGroup、重置消费位点。 4、支持消息查询、配置消息存储时长。 5、支持实例级、Topic级、Group级的监控和告警，支持使用预置的告警策略。支持通过Kakfa控制台查看云监控指标。 6、支持查看后台任务执行状态。 7、支持系统内置策略、用户自定义策略、用户账号密钥（AccessKey）鉴权。 8、支持用户创建、删除、查看。支持用户细粒度权限管理。 9、具备OpenAPI调用能力，提供相关OpenAPI文档；SDK支持ApacheKafka2.2.2、2.8.2。 四、包含三年软件平台更新与支持 | 政务外网区、互联网区各一套 |
| 7 | 数据备份云平台 | 一、备份策略 1、备份规则支持设置备份任务优先级，优先级高的任务优先执行。 2、支持多种备份规则策略类型，如一次性任务、按分钟、按小时、按天、按周、按月、按季度、按年计划执行备份作业。 3、支持选择排除日期，排除日期内的备份任务将自动跳过不执行。 4、支持设定备份时间窗口，非备份时间窗口内不允许备份传输；支持设定执行时间窗口，非执行时间窗口内不允许触发执行备份任务。 5、支持备份规则关联备份集复制规则，备份任务完成后触发执行备份集复制任务； 6、支持IPv4、IPv6、IPSAN、FCSAN网络环境备份和恢复。 7、备份规则提供多种传输链路选择，支持自动优先选择SAN网络作为备份传输链路，例如客户端和备份服务器之间满足SAN传输条件则优先SAN网络备份传输，若不符合条件则通过TCP/IP网络备份传输。 8、LANFREE备份传输时无需在生产客户端挂载磁盘，且生产客户端系统的SCSI设备名不能使用默认设备名例如/dev/sdX，以避免生产系统设备误操作，提高生产系统安全性。 9、支持设置备份集多种保留期限，如按天、按周、按月、按年以及永久保留等，超过保留期限的备份集数据自动过期删除。 10、支持备份/恢复前置后置脚本。 11、支持传输压缩，提供多种压缩级别。 12、支持传输加密，提供AES、SM4标准加密算法。 13、支持备份数据压缩加密，支持源端或目标端压缩加密处理，提供多种压缩级别，提供AES-128、AES-256、SM4、RC5标准加密算法。 14、备份规则支持按时间策略设定带宽控制，避免备份流量对生产带宽的影响；备份任务提供数据流量图展示。 15、备份规则支持手动备份、克隆、启用/禁用、授权、删除等操作。 16、备份规则支持查看历史版本，便于审计。 二、任务监控 1、支持备份系统业务相关任务的统一调度，例如备份、恢复、过期/无效数据清理、备份集复制、备份集验证、磁带清点、磁带擦除等相关任务的统一调度管理。 2、支持实时查看任务状态、任务进度、任务详情，任务日志，如关键事件输出、日志以及数据流量等信息；方便备份运维和排错处理。 3、支持在Web图形管理界面直接查看后台日志，方便运维管理。 4、支持失败或停止任务一键重启，重新启动任务继续进行。 5、支持按指定条件搜素过滤任务执行情况。 6、支持任务批量停止、删除等操作。 7、支持任务批量导出，可导出成.csv和.xslx两种格式。 8、支持任务保留期限设置，默认7天，可自定义，超过保留期限的任务将自动归档到数据库中，不再任务监控页面显示。 9、支持查看总任务、运行中、等待、完成、停止、失败、跳过、超时等状态总任务数量汇总。 三、备份集管理 1、支持查看备份集相关信息，如备份集ID、备份客户端、备份内容、备份时间、过期时间等信息。 2、支持根据客户端、备份规则名称、备份时间范围、备份规则类型、备份服务器、目标存储单元（组）等条件进行相关备份集的搜素。 3、支持备份集多副本管理，可查看多种维度的备份集视图，如查看全副本视图、仅主副本视图。 4、支持备份链智能选择恢复策略，数据恢复时无需关心备份集数据所在服务器或存储设备位置。 5、支持备份集验证，提供简单验证方式验证备份集是否可访问，可正常访问，则将备份集状态置为“正常/过期”等实际状态。 6、支持备份集手动延长期限，立即过期操作。 7、支持选择指定的备份集进行恢复。 8、支持已过期备份集的搜素、导出、删除、刷新等操作。 9、支持备份集手动将源备份集通过复制或归档技术复制到目标存储单元（组）。 10、支持异构存储介质类型之间的备份集复制。 11、备份集复制规则支持指定下一级备份集复制规则，支持备份集级联复制。 12、备份集复制支持并行流传输和流数设置，提供动态或固定设定并行流数。 13、备份集复制规则支持设置目标存储单元（组）的保留期限。 14、备份集复制规则支持设置任务优先级，优先级高的复制任务优先执行。 15、备份集复制规则支持设置传输压缩、传输加密。 16、支持备份数据压缩加密，无关数据源，启用此功能后，备份任务可根据备份服务器创建的密钥名称及选择的加密算法等对备份数据进行压缩加密处理。 17、备份集复制规则支持设定带宽控制，实现对备份集复制流量的精准控制。 18、备份集复制失败支持重试功能，允许用户在备份时间窗口内对失败的复制任务自动重试，支持自定义重试次数和重试间隔时间，提高备份集复制的成功率，确保数据备份的完整性和可靠性。 19、备份集复制规则提供多种传输链路选择，支持自动优先选择SAN网络作为传输链路，例如源备份服务器和目标备份服务器之间满足SAN传输条件则优先SAN网络传输，若不符合条件则通过TCP/IP网络传输。 20、备份集复制规则支持设置备份时间窗口，即备份时间窗口内完成备份集复制任务。 21、备份集复制规则支持设置源、目标备份集保留等级，允许自定义保留等级期限，备份规则直接引用即可。 22、支持备份集发现特性，可扫描指定的存储单元以获取其备份集列表清单，用于后续备份集导入。 23、支持备份集导入特性，可针对已发现的备份集，选择部分或全部备份集进行导入，备份集导入后可实现正常的备份集数据管理。 24、备份集管理页面提供主副本视图和全副本视图两种展示模式，用户可灵活切换视图，分类查看备份集信息。主副本视图仅展示主备份集，全副本视图展示所有备份集（包括主副本和非主副本），帮助用户更高效地管理和定位备份数据。 25、支持备份集跨域复制特性，可实现不同备份域之间的备份集复制，确保数据在多域环境下的高可用性和灾难恢复能力。 | 政务外网区、互联网区各一套 |
| 8 | 服务器硬件 | 云平台管控服务器 | 1、CPU：Hygon7360，配置≥2颗CPU，每颗CPU核数≥24，频率≥2.2GHz； 2、内存：容量≥1024GB，配置DDR43200MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥1块7.68TNVMeSSD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX5)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，支持Raid0,1,5,6,10和60； | 政务外网区4台，互联网区4台 |
| 9 | 云平台网关服务器 | 1、CPU：Hygon5480，配置≥2颗CPU处理器，每颗CPU核数≥32，频率≥2.5GHz； 2、内存：容量≥1024GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥1块7.68TNVMeSSD硬盘； 4、网卡：提供≥2块25Gb双口网卡； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区2台，互联网区2台 |
| 10 | 云安全管控服务器 | 1、CPU：Hygon7360，配置≥2颗CPU，每颗CPU核数≥24，频率≥2.2GHz； 2、内存：容量≥1024GB，配置DDR43200MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥1块7.68TNVMeSSD硬盘； 4、网卡：提供≥2块25Gb双口网卡； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，支持Raid0,1,5,6,10和60； | 政务外网区3台，互联网区3台 |
| 11 | 云安全数据服务器 | 1、CPU：Hygon5480，配置≥2颗CPU，每颗CPU核数≥32，频率≥2.5GHz； 2、内存：容量≥1024GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥1块7.68TNVMeSSD硬盘； 4、网卡：提供≥2块25Gb双口网卡； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区3台，互联网区3台 |
| 12 | intel计算服务器 | 1、CPU：IntelXeonGold6330，配置≥2颗CPU，每颗CPU核数≥28，频率≥2.0GHz； 2、内存：容量≥1024GB，配置DDR43200MHz及以上； 3、硬盘：配置≥1块1.92TNVMeSSD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)，网口前置； 5、管理网络：配置1个前置1000MbpsRJ45独立管理网口 6、电源：配置1+1冗余电源； | 政务外网区11台（计算10台，安全带外1台），互联网区4台（计算3台，安全带外1台） |
| 13 | 海光计算服务器 | 1、CPU：Hygon7490，配置≥2颗CPU，每颗CPU核数≥64，频率≥2.7GHz； 2、内存：容量≥1536GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区6台，互联网区2台 |
| 14 | 鲲鹏计算服务器 | 1、CPU：Kunpeng920，配置≥2颗CPU，每颗CPU核数≥64，频率≥2.6GHz； 2、内存：容量≥1024GB，配置DDR43200MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区2台，互联网区2台 |
| 15 | 全闪高性能云盘块存储服务器 | 1、CPU：Hygon5480，配置≥2颗CPU，每颗CPU核数≥32，频率≥2.5GHz； 2、内存：容量≥256GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥8块3.84TNVMeSSD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区8台，互联网区6台 |
| 16 | 混闪普通性能云盘块存储服务器 | 1、CPU：Hygon5480，配置≥2颗CPU，每颗CPU核数≥32，频率≥2.5GHz； 2、内存：容量≥512GB，配置DDR55600MHz及以上； 3、硬盘：配置≥1块1.92TNVMeSSD硬盘，≥2块6.4T（可由7.68T做OP实现）NVMeSSD硬盘，≥10块20THDD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； | 政务外网区4台，互联网区4台 |
| 17 | 对象存储服务器 | 1、CPU：Hygon5480，配置≥2颗CPU，每颗CPU核数≥32，频率≥2.5GHz； 2、内存：容量≥256GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥2块1.92TNVMeSSD硬盘，≥10块20THDD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区4台，互联网区4台 |
| 18 | 日志服务器 | 1、CPU：Hygon5480，配置≥2颗CPU，每颗CPU核数≥32，频率≥2.5GHz； 2、内存：容量≥256GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥2块1.92TNVMeSSD硬盘，≥10块20THDD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区4台，互联网区4台 |
| 19 | 数据库&中间件服务器 | 1、CPU：Hygon5480，配置≥2颗CPU，每颗CPU核数≥32，频率≥2.5GHz； 2、内存：容量≥1024GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘，≥8块3.84TNVMeSSD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区4台，互联网区4台 |
| 20 | 数据备份服务器 | 1、CPU：IntelXeonSilver4314，配置≥2颗CPU，每颗CPU核数≥16，频率≥2.4GHz； 2、内存：容量≥256GB，配置DDR43200MHz及以上； 3、硬盘：配置≥3块1.92TNVMeSSD硬盘，≥12块20THDD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)，网口前置； 5、管理网络：配置1个前置1000MbpsRJ45独立管理网口 6、电源：配置1+1冗余电源； | 政务外网区1台，互联网区1台 |
| 21 | VPC防火墙服务器 | 1、CPU：Hygon7490，配置≥2颗CPU，每颗CPU核数≥64，频率≥2.7GHz； 2、内存：容量≥1536GB，配置DDR55600MHz及以上； 3、硬盘：配置≥2块960GSATASSD硬盘； 4、网卡：提供≥2块25Gb双口网卡(CX6)； 5、电源：配置1+1冗余电源； 6、RAID卡：配置1张RAID卡，缓存≥4GB，支持Raid0,1,5,6,10和60； | 政务外网区2台，互联网区2台 |
| 22 | 交换机硬件 | BMC交换机 | 1、主机：配置L3以太网交换机主机； 2、端口：配置≥48个10/100/1000BASE-T接口模块，≥4个10G/1GBASE-XSFP+端口，≥1个带外管理以太网口； 3、电源：配置双模块化电源； 4、风扇：配置冗余风扇模块； 5、二层功能:支持STP/RSTP/MSTP；支持基于PPS/bps的风暴抑制；支持设置端口MAC地址学习最大个数 6、三层功能：支持静态路由；支持RIP，RIPng；支持OSPFv2，OSPFv3；支持BGP4，BGP4+forIPv6；支持等价路由 7、网络管理：支持命令行接口（CLI），Telnet，Console口进行配置；支持SNMPv2/v3 | 政务外网区4台，互联网区3台 |
| 23 | 专线网络交换机 | 1、主机：配置L3以太网交换机主机； 2、端口：配置≥24端口10GMACSEC以太网光接口，≥2端口40G以太网光接口，≥8端口100GMACSEC以太网光接口； 3、电源：配置4个冗余电源； 4、风扇：配置冗余可热插拔风扇模块； 5、网络性能：交换容量≥6.4Tbps；包转发率≥2030Mpps； 6、数据中心特性：支持AIECN；ECN支持VxlanOverlay场景；支持DLB:动态负载均衡 7、三层功能：支持静态路由和默认路由；支持RIP、OSPF、BGP、ISIS等IPv4动态路由协议；支持RIPng、OSPFv3、BGP4+、ISISv6等IPv6动态路由协议；支持等价路由、策略路由 8、管理功能：支持Telemetry可视化功能；支持全网路径探测；支持缓存微突发检测；支持零配置Auto-config和配置回滚；支持ZTP | 政务外网区2台，互联网区2台 |
| 24 | 汇聚交换机 | 1、主机：配置L3以太网交换机主机； 2、端口：配置≥1个24端口10GMACSEC以太网光接口，≥1个2端口40G以太网光接口，≥3个8端口100GMACSEC以太网光接口，≥1个带外管理以太网口； 3、电源：配置4个冗余电源 4、风扇：配置冗余可热插拔风扇模块； 5、网络性能：交换容量≥6.4Tbps；包转发率≥2030Mpps 6、数据中心特性：支持AIECN；ECN支持VxlanOverlay场景；支持DLB:动态负载均衡 7、三层功能：支持静态路由和默认路由；支持RIP、OSPF、BGP、ISIS等IPv4动态路由协议；支持RIPng、OSPFv3、BGP4+、ISISv6等IPv6动态路由协议；支持等价路由、策略路由 8、管理功能：支持Telemetry可视化功能；支持全网路径探测；支持缓存微突发检测；支持零配置Auto-config和配置回滚；支持ZTP | 政务外网区2台，互联网区2台 |
| 25 | 核心交换机 | 1、主机：配置L3框式以太网交换机主机； 2、端口：配置≥4个32端口100G以太网光接口； 3、电源：配置冗余交流电源模块 4、风扇：配置冗余以太网交换机风扇模块 5、网络性能：交换容量≥25.6Tbps；包转发率≥8000Mpps 6、二层功能：支持JumboFrame；支持STP/RSTP/MSTP协议； 7、三层功能：支持IPv4、IPv6静态路由;支持策略路由；支持RIPv1/2、支持等价路由、VRRP、OSPFv2、OSPFv3、BGP、ISIS等增强三层路由协议；支持VRRPv6 8、网络管理：支持INT；支持Netconf；支持SNMPv1/v2c/v3；支持ZTP功能 9、数据中心特性：支持PFC、ECN等数据中心特性、支持M-LAG特性 | 政务外网区2台，互联网区2台 |
| 26 | 25G接入交换机 | 1、主机：配置L3以太网交换机主机； 2、端口：配置≥48个10GE/25GESFP28以太网光接口，≥8个40GE/100GEQSFP28以太网光接口，≥1个带外管理以太网口； 3、电源：配置双模块化电源； 4、风扇：配置冗余可热插拔风扇模块； 5、网络性能：交换容量≥4.8Tbps；包转发率≥2000Mpps 6、二层功能：支持JumboFrame；支持STP/RSTP/MSTP协议； 7、三层功能：支持静态路由和默认路由；支持RIP、OSPF、BGP、ISIS等IPv4动态路由协议；支持RIPng、OSPFv3、BGP4+、等IPv6动态路由协议；支持等价路由、策略路由； 8、网络管理：支持Telemetry功能；支持Netconf和Python；支持SNMPv1/v2c/v3 | 政务外网区13台，互联网区13台 |
| 28 | 云安全 | 云防火墙 | 1、云原生： （1）云防火墙基于云平台内生安全和云原生安全服务，云防火墙产品实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号； （2）云防火墙与云平台共用同一套网络架构，无需在网络对接过程中配置策略路由或进行额外定制开发工作。 （3）云防火墙基于云平台进行部署运行，云防火墙可以主动获取云内的资产，并且可以根据云内资产变化做到实时更新资产信息。无需像传统安全产品需要配置IP范围，被动识别流量中资产，同步不及时，而导致资产信息遗漏； （4）云防火墙访问控制是基于云平台网络架构实现东西向的访问控制，云防火墙可支持下发策略到安全组进行主机访问控制。 2、防火墙开关-互联网边界防火墙： （1）支持互联网通信协议的入方向和出方向流量进行访问控制（南北向）； （2）支持对公网资产进行开关防护，包括ECS、NAT网关、CLB等公网IP资产类型； （3）互联网边界防火墙支持主备容灾防护措施。 3、防火墙开关-VPC边界防火墙： （1）支持对VPC间流量、云上云下间流量进行访问控制（东西向）； （2）支持VPC间流量引流设置，包括手动引流、自动引流两种方式； （3）▲支持VPC间流量引流场景选择，包括点到点、点到多点、多点互联三种引流场景模式选择。（提供产品对应功能界面截图并加盖原厂盖章材料）； （4）VPC边界防火墙支持主备容灾防护措施。 4、防护分析： （1）主动外联分析：提供主机的主动外联数据，帮助用户及时发现可疑主机，支持展示外联域名统计分析、外联IP统计分析等内容。 （2）拦截分析：提供当前防火墙已经拦截的所有流量数据，包括已拦截的外联IPTOP5、意图外放IPTOP5、拦截趋势图等内容。 （3）资产暴露分析：提供展示资产入方向流量的概览信息，帮助用户发现暴露在互联网的风险端口，包括访问源IPTOP5、开放端口TOP5、资产、开放端口、开放协议、访问源等内容。 （4）VPC互访分析：支持展示VPC间的流量访问关系，包括VPC流量速率趋势图、IP流量大小TOP10、开放端口TOP5等内容。 5、访问控制： （1）互联网边界防火墙：互联网边界防火墙支持对公网IP资产的出、入互联网流量进行访问控制；支持域名访问控制，支持输入多级域名参数配置；支持地理位置访问控制，包括国内省份，国际区域的选择。 （2）▲VPC边界防火墙：支持VPC间东西向流量的访问控制。（提供产品对应功能界面截图并加盖原厂盖章材料）。 （3）主机边界防火墙：主机边界防火墙可以对ECS实例间的入流量和出流量进行访问控制，限制ECS实例间的未授权访问。 （4）地址簿：支持配置地址簿，包括IP地址簿、端口地址簿，一条访问控制策略最多可配置20个地址簿，10万个IP地址。 | 政务外网区1套，互联网区1套 |
| 28 | 高级网络威胁检测系统 | 1、云原生： （1）高级网络威胁检测系统基于云平台内生安全和云原生安全服务，高级网络威胁检测系统实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号； （2）高级网络威胁检测系统与云平台共用同一套网络架构，无需在网络对接过程中配置策略路由或进行额外定制开发工作； （3）高级网络威胁检测系统基于云平台进行部署运行，可以主动获取云内的资产，并且可以根据云内资产变化做到实时更新资产信息。无需像传统安全产品需要配置IP范围，被动识别流量中资产，同步不及时，而导致资产信息遗漏。 2、数据流量采集： 协议解析支持HTTP、HTTPS、TCP、UDP、ICMP、DNS、SNMP、SSH、Telnet、RDP、IPsec、GRE、VXLAN、FTP、SMB等20+种协议解析检测。 3、威胁检测： （1）Web攻击检测：支持SQL注入、跨站脚本、请求伪造、命令注入、代码注入、路径穿越、文件包含、web后门、敏感文件、LDAP注入、XML外部实体注入等Web攻击检测。 （2）漏洞利用攻击检测：支持反序列化漏洞、系统漏洞、RDP漏洞、软件漏洞、Shellcode、SMB漏洞、拒绝服务漏洞、未授权漏洞、远程命令执行漏洞等漏洞利用攻击检测。 （3）▲行为分析：支持挖矿行为、隐蔽隧道、安全基线模型、C&C模行为、网络扫描、暴力破解等行为分析检测能力。（提供产品对应功能界面截图并加盖原厂盖章材料） 4、威胁感知： （1）▲威胁专项：威胁专项展示了当前网络主机异常行为的整体趋势情况，弱口令、隐蔽隧道、文件威胁、邮件数据。（提供产品对应功能界面截图并加盖原厂盖章材料）。 （2）挖矿行为：支持挖矿行为检测分析，能够展示网络中所有的挖矿告警，并呈现告警时间、攻击结果、风险等级等信息。 （3）代理穿透：支持代理穿透检测分析，包括多种工具的代理穿透场景检测分析。 （4）隐蔽隧道：支持隐蔽隧道专项分析，包括不限于gre隐蔽隧道、icmp隐蔽隧道、ipsec隐蔽隧道等隐蔽隧道场景检测分析。 （5）文件威胁：支持文件威胁检测专项，能够检测网络传输中的恶意文件，并呈现文件名称、文件MD5值、病毒类型、资产IP、外部IP等内容。 （6）数据邮件：支持邮件数据检测，能够检测网络传输中的恶意邮件，并呈现发件人邮箱、收件人邮箱、邮件标题、邮件附件、邮件类型等内容。 5、分析中心： （1）流量分析：支持展示所有资产暴露在互联网上的风险端口以及被攻击利用过的高危端口，展示内容包括端口、资产IP、影响资产、修复建议、协议、端口服务、是否被利用等内容；支持按照外联流量大小，展示资产外联访问关系。支持展示外联资产TOP5、流量趋势图，并展示访问源、访问目的、访问次数、访问流量大小、访问时间、访问协议等内容。 （2）日志分析：支持告警日志存储，包括威胁类型、攻击结果、风险等级、访问源IP、访问目的iP、端口、协议等内容，并支持用户下载数据包；支持网络流量审计，包括访问时间、访问源、源端口、协议、访问目的、目的端口、域名、访问方向、访问流量大小、访问报文数等内容。 6、响应中心： ▲检测防御配置：支持基础防御、虚拟补丁、智能防御、文件威胁检测、邮件威胁检测等检测能力。（提供产品对应功能界面截图并加盖原厂盖章材料）。 | 政务外网区1套，互联网区1套 |
| 29 | Web应用防火墙 | 1、云原生： （1）web防火墙基于云平台内生安全和云原生安全服务，web防火墙产品实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号； （2）web防火墙与云平台共用同一套网络架构，无需在网络对接过程中配置策略路由或进行额外定制开发工作。 2、漏洞防护： （1）Web漏洞检测及防护：OWASPTop10漏洞，SQL注入，命令注入，webshell、表达式注入，XPath注入，LDAP注入，任意文件读&目录遍历，LFI，SSTI，SSRF，XSS等漏洞检测及防护。 （2）逻辑漏洞：对部分中间件存在越权、表单绕过漏洞进行检测与拦截。 （3）Web后门：通过对以asp、php、jsp或者cgi等网页文件形式存在的Web命令进行检测，拦截网页木马。 （4）请求加白：对特定请求进行加白，加白的请求不会送入漏洞检测引擎。 3、CC攻击防护：支持基于对源IP、自定义header等的访问频次统计，对指定目标进行记录、限速或拦截。 4、访问管控： （1）访问白名单：对来源于特定ip、ip段的请求流量进行放过，不受所有检测拦截规则的影响。 （2）访问黑名单：对来源于特定ip、ip段的请求流量进行拦截。 （3）自定义拦截响应：当满足条件的请求被WAF拦截(CC拦截除外)时返回，返回自定义的响应码和响应页面。 5、BOT管理： （1）托管Bot分类规则管理：可识别公开类型Bot并进行分类，支持按IP情报进行Bot识别和分类，可以对识别出的Bot进行告警、拦截或放过。 （2）自定义Bot分类规则管理：支持按自定义Bot特征进行识别和分类，对识别出的Bot进行告警、拦截或放过。 6、敏感信息防泄漏：支持对内容信息如身份证、银行卡、手机号进行检测，支持响应码检测，检测出敏感信息后支持进行观察和拦截操作。 | 政务外网区1套，互联网区1套 |
| 30 | 云安全中心 | 1、云原生： （1）云安全中心基于云平台内生安全和云原生安全服务，云安全中心产品服务实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建云安全中心实例时，无需在云平台来回切换账号； （2）云安全中心与云平台共用同一套网络架构，无需在网络对接过程中配置策略路由或进行额外定制开发工作； （3）云安全中心基于云平台进行部署运行，云安全中心可以主动获取云内的资产，并且可以根据云内资产变化做到实时更新资产信息。无需像传统安全产品需要配置IP范围，被动识别流量中资产，同步不及时，而导致资产信息遗漏。 2、入侵防御： （1）病毒查杀：支持结合复合病毒检测引擎、实时威胁情报，快速精确地识别和清除主机中的恶意文件。 （2）告警处置：1）支持告警处置能力，包括终止进程与隔离文件等操作；2）支持自定义多维度白名单，包括进程二进制、命令行、MD5、IP等。 （3）告警调查：1）支持对疑似入侵检测行为进行自动化上下文关联，并通过安全攻击图谱可视化展示。2支持对疑似入侵检测行为前后一个小时内的行为进行关联。3）支持至少以下几种行为的关联：同一进程组的进程创建行为，同一进程组的进程网络连接行为，同一进程组的进程DNS请求行为，同一进程组的进程文件创建行为。4）支持展示进程、文件创建、DNS解析、网络连接、SSH登录等原始数据直观展示。 （4）主动防御：支持实时监控主机的多种活动，如网络访问、文件操作和进程运行，对高置信度攻击进行实时拦截。 3、漏洞检测： （1）Linux软件漏洞：通过与漏洞库的对比分析，检测Linux操作系统官方维护软件中的漏洞。 （2）Windows系统漏洞：通过匹配微软官方的更新通告，检测Windows操作系统中的安全漏洞。 （3）Web-CMS漏洞：通过监控网站目录与建站软件，检测对建站软件中存在的安全漏洞。 （4）应用漏洞：通过监控运行应用，检测应用中存在的漏洞。 （5）高可利用性漏洞：支持根据漏洞的影响面、紧迫性等，展示高可利用性漏洞。 4、基线检查： （1）弱口令：检测系统弱口令风险，检测多项应用弱口令风险。 （2）等保合规：支持等保二/三级基线检查所需检查项，帮助用户信息安全等级达到国家标准，满足合规要求。 （3）CIS标准：支持CIS标准检查项。 （4）最佳实践：提供大型用户最佳实践。 | 政务外网区1套，互联网区1套 |
| 31 | 云堡垒机 | 1、云原生：云堡垒机基于云平台内生安全和云原生安全服务，云堡垒机产品服务实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建云堡垒机实例时，无需在云平台来回切换账号。 2、多网域：云堡垒机提供多网域管理功能，支持通过网络域代理方式连通多个VPC、异构云等不同网络环境中的服务器资产，实现多网域运维。 3、主机管理：（1）支持导入同品牌公共云主机；（2）支持新建、编辑、删除主机资源，支持修改主机的服务端口；（3）支持新建、编辑和删除主机账户；（4）支持新建、修改、删除主机组，支持添加、移除主机组成员；（5）堡垒机提供密钥管理功能，用户可以创建密钥并将密钥批量关联到主机账户中，提高管理主机账户的效率。 4、数据库管理： （1）将数据库资源纳管到云堡垒机统一管理。提供数据库资源的全生命周期管理，包括：新建数据库、编辑、删除等； （2）手动同步数据库中指定的账号，实现账号粒度的运维权限接管。并提供数据库账号的全生命周期管理，包括：添加、编辑、删除，验证密码等。 5、用户管理： （1）支持导入同公有云的IAM用户，支持编辑和删除用户，支持启停用户； （2）支持新建、编辑、删除用户组，支持添加、移除用户组成员； （3）支持用户的公钥管理； （4）支持用户授权主机，用户组授权主机、用户授权主机组、用户组授权主机组。 6、策略管理： （1）支持命令控制策略，控制用户命令的输入，支持命令审批； （2）支持访问控制策略，控制用户登录、文件管理等权限； （3）支持批量修改主机的密码。 7、运维审计：支持查看实时会话、历史会话，支持阻断对话。支持堡垒机的登录日志和操作日志。 8、系统管理： （1）双因子认证功能在本地用户登录时发送短信口令，二次认证用户身份，可以有效降低账户泄露等情况带来的安全风险； （2）为了保障系统的安全，防止用户密码被暴力破解，用户可以在安全配置中设置用户锁定配置。包括密码尝试次数、锁定时长、重置计数器。 | 政务外网区1套，互联网区1套 |
| 32 | 数据库审计 | 1、云原生： 数据库审计基于云平台内生安全和云原生安全服务，数据库审计服务实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建数据库审计服务实例时，无需在云平台来回切换账号。 2、数据库兼容性： （1）支持关系型数据库：Oracle、SQLserver、MySQL、DB2、Sybase、Informix、Postgresql、Gbase、Teradata、Cache、CacheWeb、tibero； （2）国产化关系型数据库：DM7、人大金仓（KingbaseES）、神通、浪潮KDB、湖南上容、HighGo（瀚高）； （3）非关系型数据库：MongoDB、Hive、HDFS文件系统、Hana、HWMPP、Hbase、ES、Solr、Redis、SSDB、KingbaseAnalyticsDB。 3、审计能力： （1）数据库访问记录应至少包括发生时间、业务用户名、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、响应时间、返回结果等关键信息； （2）支持变量绑定值的记录：很多基于数据库的查询是通过BindVariable完成的。这就要求审计系统不光要记录查询中BindVariable的变量的名字，还要记录BindVariable的数值； （3）支持定义事件类型，每种事件类型可以对应多个事件策略，不同策略命中的事件可以有高、中、低等多个风险级别支持定义所有SQL的相应威胁程度，至少包括高、中、低、提醒等告警级别； 4、审计策略与规则： （1）系统必须自带默认审计策略，支持用户自定义策略和规则，系统必须支持配置操作行为的黑名单、白名单、入侵检测策略、Oracle风险策略、运维定义策略，方便用户灵活配置审计规则； （2）支持以操作类型、时间、IP地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间、返回码、关键字、敏感数据、等作为事件识别规则及审计规则。 5、审计告警： （1）内置自动告警设置，允许用户设定威胁自动告警，告警必须提供级别设定，至少提供致命、高风险、中风险、低风险4种告警级别； （2）支持SysLog、邮件、短信、FTP、Snmp、KAFKA等多种事件告警和提示方式。 6、监控扫描： （1）提供对数据库漏洞、不安全配置、弱口令、补丁等深层薄弱环节的安全检测及准确评估； （2）▲支持服务扫描和发现功能，通过扫描网络中的开放端口以及确定监听这些端口的服务。如主机IP、端口、主机操作系统、服务的类型等。并实现自动或手动将这些服务添加到数据库引擎。（提供产品对应功能界面截图并加盖原厂盖章材料）； （3）支持对数据库服务器的扫描，实现对数据库的表、字段等敏感信息的自动识别； （4）▲支持对敏感数据分布的服务器进行统计，并以图表的形式展示，可导出为报表。（提供产品对应功能界面截图和原厂盖章材料）。 7、数据库状态监控： （1）系统界面可以显示数据库状态、缓冲区击中率、库缓存大小等变化趋势图； （2）系统界面可以显示数据库的会话明细、查询缓冲击中率等信息。 | 政务外网区1套，互联网区1套 |
| 33 | 多云安全管理 | 1、云原生： （1）多云安全管理基于云平台内生安全和云原生安全服务能力，多云安全管理产品实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号； （2）多云安全管理基于云平台进行部署运行，多云安全管理可以主动获取云内的资产，并且可以根据云内资产变化做到实时更新资产信息。无需像传统安全产品需要配置IP范围，被动识别流量中资产，同步不及时，而导致资产信息遗漏。 2、多云安全全景： （1）看已接入云环境的资源数量统计、类型分布、脆弱性风险检测通过占比。查看已接入云环境的资源整体风险分布； （2）查看已接入云环境的风险态势评分，等级评定。查看已接入云环境的待修复风险清单，包含风险等级、风险名称、修复状态。 3、多云开放集成 （1）云账号添加与管理 1）支持至少3家主流云厂商的子账号添加，支持手动配置子账号添加以及子账号自动化生成模版； 2）支持已添加的云账号删除、关闭/启用、搜索与筛选功能。。 （2）主机安全数据接入 ▲支持至少3家主流云厂商主机安全产品的告警、漏洞、基线扫描结果，以及waf安全产品的告警结果数据接入。（提供产品对应功能界面截图并加盖原厂盖章材料）； 4、多云资产管理： （1）计算类资产数据采集，支持多云厂商的计算类资产的数据采集，包括： 1）虚拟机：支持虚拟机类型资产的基本信息、配置的采集； 2）容器：支持容器类型资产（含集群、pod、容器）的基本信息、配置的采集。 （2）存储类资数据采集： 支持多云厂商的存储类资产的数据采集，包括：支持对象存储类型资产的基本信息、配置的采集。 （3）网络类资产数据采集：支持多云厂商的网络类资产的数据采集，包括：EIP、安全组、ACL、VPC、NAT、LB基本信息、配置的采集。 （4）数据库类资产数据采集：支持多云厂商的数据库类资产的数据采集，包括：MySQL、PostgreSQL、Redis、MongoDB基本信息、配置的采集。 （5）数据归一化管理：支持不同格式的资产数据归一化、范式化，支持将不同云的同类型的字段归一化统一展现。 5、云安全风险分析与评估： 支持云上计算、存储、网络资产的云控制台错误配置检测，评估配置所引入的多云实际安全风险，包括：1）计算：虚拟机、容器、集群资产错误配置检测；2）网络：EIP、安全组、ACL、VPC、NAT、LB错误配置检测；3）存储：对象存储、MySQL、PostgreSQL、Redis、MongoDB错误配置检测。 | 政务外网区1套，互联网区1套 |
| 34 | 密钥管理系统 | 1、云原生： （1）密钥管理系统是基于云平台部署的，与云平台共用同一套网络架构，无需在网络对接过程中进行额外定制开发工作； （2）密钥管理系统基于云平台内生安全和云原生安全服务能力，密钥管理系统产品实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号。 2、用户主密钥管理： （1）提供对用户主密钥生命周期的管理能力，主要包括增删改查的能力； （2）提供自动化的用户密钥轮转能力； （3）对无须使用的密钥进行归档处理，轻松满足合规需求； （4）提供多种加密方式：1）提供在线的加解密运算能力，直接调用密钥管理服务的接口对数据加密。2）提供加密的SDK，帮助用户轻松实现信封加密。 3、凭据管理： 凭据管理服务用于加密存储用户敏感数据在凭据管理服务侧，用户可以动态、安全地从凭据管理获取凭据的明文数据。凭据管理服务可以使用用户自管理的KMS密钥来加密敏感数据，采用了信封加密机制。 | 政务外网区1套，互联网区1套 |
| 35 | 云工作负载保护平台CWPP | 1、资产管理： （1）资产清点 1）支持主机常见的端口、进程、软件、系统服务、定时任务、系统软件、内核模块、硬件网卡、常见中间件、web站点等指纹信息采集和展示，并支持自定义扫描时间与频率； 2）支持采集容器集群的工作负载、容器组、容器信息； 3）支持批量导入主机资产。 （32）资产风险： 1）支持对主机上的文件完整性进行校验，展示变更文件的哈希和MD5； 2）支持基于风险维度展示资产，例如是否存在系统完整性分析、是否为常见进程、是否为容器进程等； 3）支持SSH、RDP暴力破解识别，其中SSH支持自动封禁； 4）▲支持对容器集群暴露面进行分析，并可视化展示暴露路径。（提供产品对应功能界面截图并加盖原厂盖章材料）。 2、风险防范： （1）基线检查 1）支持大型互联网企业用户的最佳实践、系统弱口令、应用弱口令、未授权访问、等级保护2/3基线检查； 2）支持用户手动/自动下发基线检查任务，并且可以实时获取检查进度； 3）支持基线定时扫描，可为不同主机配置不同的扫描策略； 4）支持主机视角和检查项视角的基线检查，支持对k8s节点进行CIS标准基线扫描，持对k8s节点进行应用巡检。 （2）漏洞管理 1）支持对Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞进行检测； 2）支持用户手动/自动下发漏洞巡检任务，并且可以实时获取检查进度； 3）支持漏洞库在线/离线升级，支持根据CVSS评分，漏洞类型，是否存在EXP等关键条件进行筛选与管理； 4）支持漏洞定时扫描，可为不同主机配置不同的扫描策略； 5）支持根据漏洞的影响面、紧迫性等，为用户展示高可利用性漏洞。 3、入侵检测： （1）主机和容器检测 1）支持检测主机和容器内发生的入侵行为； 2）支持可疑文件落盘行为检测； 3）支持检测常见的反弹shell，后门驻留，恶意信息收集，权限提升，横向移动，暴力破解等恶意动态行为； 4）支持检测常见的内核态后门。 （2）应用运行时检测 1）支持应用层反入侵，包括Java，Golang语言； 2）支持配置RASP进程注入白名单，命中白名单的进程不会被注入； 3）支持勒索诱饵投放，检出攻击后进行告警。 4、威胁溯源： （1）▲支持对疑似入侵检测行为进行自动化上下文关联，并通过安全攻击图谱可视化展示。（提供产品对应功能界面截图并加盖原厂盖章材料）； （2）支持对疑似入侵检测行为前后一个小时内的行为进行关联； （3）▲支持展示进程、文件创建、DNS解析、网络连接、SSH登录等原始数据直观展示。（提供产品对应功能界面截图并加盖原厂盖章材料）。 5、病毒查杀： （1）支持检测常见的Webshell，木马，后门，挖矿程序等恶意二进制静态文件； （2）支持对扫描出的病毒文件一键隔离至文件隔离箱，并且支持一键恢复。 6、攻击诱捕：支持主机蜜罐攻击诱捕，包括SSH、Redis、Mysql、Web等服务，展示捕获的攻击行为 | 政务外网区1套，互联网区1套 |
| 36 | 密码安全 | 服务器密码机 | 1、总体要求： （1）支持与密钥管理系统KMS的集成对接，提供密钥管理系统KMS的密钥生成与存储等功能。提供产品相关功能证明材料。 （2）▲产品具有产品认证证书，符合GM/T0028安全等级第二级要求；提供产品相关资质证明材料。 （3）产品具有国家强制性产品认证证书；提供产品相关资质证明材料。 （4）采用厂商自有知识产权的密码卡；提供产品相关资质证明材料。 （5）产品具有公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品，提供产品相关资质证明材料。 （6）产品具有IPV6ReadyLogo认证证书；提供产品相关资质证明材料。 （7）产品具有信息技术产品安全测试证书。提供产品相关资质证明材料。 （8）产品具备国产化cpu、国产化操作系统厂商联合出具的兼容性证明。 （9）至少具备和5家主流云厂商云管平台的兼容性证明。提供产品相关资质证明材料。 2、硬件要求： （1）至少提供4个网络端口,2个千兆电口，2个万兆光口；提供产品截图证明。 （2）2U标准机箱，为了防止数据窃听，设备不得存在USB接口；提供产品相关功能证明材料。 （3）支持设备状态灯显示运行状态，包括不限于电源状态灯、运行状态灯、告警灯等；提供产品相关功能证明材料。 （4）支持应急状态下，物理密钥销毁按钮对密钥进行销毁；提供产品相关功能证明材料。 3、密码算法： （1）集成国密认证的二级信创密码卡实现各类密码算法，保证算法的高安全性； （2）对称算法：支持国产SM1/SM4算法、以用国际通用算法DES、TDES、AES； （3）摘要算法：支持国产SM3和通用SHA1/SHA256/SHA384/SHA512等算法； （4）非对称算法：支持SM2、SM9、RSA、ECC等算法； 4、密钥管理： （1）采用多级密钥管理体系，逐层保护； （2）密钥产生，密码机支持产生高质量的随机密钥； （3）密钥存储，密码机支持安全存储对称密钥、RSA密钥和SM2密钥，任何时候密钥不以明文形式出现在密码机外； （4）密钥备份恢复，密码机支持内部密钥的安全备份和恢复，可用于实现互备或负载的多台设备间的密钥同步； （5）提供紧急情况下的密钥销毁手段； 5、安全控制： （1）物理分割的工作服务端口和设备管理端口； （2）使用多片国家密码管理局批准芯片并行生成随机数，产生的随机数符合国家密码管理局颁布的《随机数检测规范》，在部分随机数芯片出现问题时仍然可以保证随机数的生成质量； （3）支持通过管理串口获取和配置密码机管理网络功能，支持重置密码机恢复出厂设置等功能。提供产品相关功能证明材料。 （4）业务调用加密机支持SSL安全协议，保证通讯数据安全，支持自签发SSL证书； 6、性能要求： （1）SM2密钥生成≥10000对/秒 （2）SM2签名≥9000次/秒 （3）SM2验签名≥5000次/秒 （4）SM3摘要≥800Mbps （5）SM4加解密≥800Mbps | 政务外网区2套，互联网区2套 |
| 37 | 国密堡垒机 | 1、产品形态 （1）软硬件一体化产品，2U标准机架设备； （2）32G内存/硬盘2T/2个1000M自适应电口/双电源； （3）最大可扩展至6电口4光口，（提供产品照片）。 2、产品资质 （1）▲具有公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品（增强级）。提供相关资质证明材料。 （2）具有计算机软件著作权登记证书。提供相关资质证明材料。 （3）具备国家强制认证产品资质：信息安全服务资质认证(CCRC)。提供相关资质证明材料。 （4）▲具备符合GM/T0028《密码模块安全技术要求》第三级要求《商用密码产品认证证书》。提供相关资质证明材料。 3、用户管理 （1）灵活划分角色权限，可根据业务模块自定义角色权限，控制可操作的业务模块范围； （2）一个用户可同时拥有多个角色。提供产品相关功能证明材料。 （3）内置角色需包括：系统管理员、权限管理员、操作员与审计员。提供产品相关功能证明材料。 （4）投标产品支持静态口令、动态口令、AD域、LDAP、Radius、国密ukey、短信、指纹等多种认证方式。提供产品相关功能证明材料。 （5）支持静态口令、动态口令、AD域、LDAP、Radius、国密ukey、短信、指纹任意两种组合的双因子认证。 （6）认证因素含静态口令时，静态口令有有效期限制和使用次数限制，口令到期前会有到期提醒； （7）口令到期或用户成功登录次数达上限时会强制要求改密； （8）管理员注册用户时指定了用户口令，用户首次登录成功后强制要求改密。提供产品相关功能证明材料。 （9）设备自身集成一次性口令认证服务器模块，或能对接专用的OTP动态口令认证系统； （10）支持手机软件程序APP。提供产品相关功能证明材料。 4、帐户管理 （1）支持纳管Unix/Linux/Windows操作系统帐户； （2）支持纳管AD域、LDAP帐户； （3）支持纳管MySQL、Oracle、SqlServer、DaMeng、DB2、PG等常见数据库帐户； 5、资源访问、帐户领用 （1）支持SSH/TELNET文本协议资源访问代理； （2）支持web方式、web调用CS客户端、客户端直连方式运维目标资源。提供产品相关功能证明材料。 （3）支持RDP/VNC/X11图形协议资源访问代理； （4）支持web方式、web调用CS客户端方式运维目标资源。提供产品相关功能证明材料。 （5）支持基于windows平台的浏览器、C/S客户端软件应用发布运维访问。提供产品相关功能证明材料。 （6）支持基于linux平台的B/S、数据库客户端(dbeaver)应用发布运维访问。提供产品相关功能证明材料。 （7）支持调用本地浏览器、数据库客户端(dbeaver)实现应用发布运维访问。 （8）基于windows的应用发布，全面支持微软Windows2008r2/2012r2/2016的RemoteAPP功能，所有发布应用程序均可本地化展示。提供产品相关功能证明材料。 （9）支持纯web方式进行各类文本、文件、图形、应用发布类协议资源的运维访问。提供产品相关功能证明材料。 6、审计管理 （1）支持各类协议的全流程会话审计； （2）会话基本信息包含用户、客户端IP、服务器IP、协议类型、开始及结束时间，使用的帐户，会话日志大小，告警，复核基本信息； （3）支持对活动会话的实时监控； （4）支持会话日志下载，使用会话日志进行会话回放。提供产品相关功能证明材料。 （5）支持通过用户、客户端IP、设备/设备组、协议类型、会话状态、会话时间、会话中的操作命令等组合信息执行过滤查询。提供产品相关功能证明材料。 （6）支持对活动会话执行中止操作。提供产品相关功能证明材料。 （7）支持SSH/TELNET文类协议运维过程中全部命令与执行结果审计； （8）支持SFTP/FTP文件类协议运维过程中的全部命令与执行结果审计； （9）支持RDP图形协议运维过程中的文字识别； 7、安全要求/国密要求 （1）提供初始化国密计算服务功能，可灵活选择国密计算服务，可以通过内置密码卡、外部密码机、密码服务平台作为安全计算源。提供产品相关功能证明材料。 （2）提供成熟的合规模板供选择，覆盖密评设备与计算环节对堡垒机的相关要求。 （3）提供合规模板的灵活调整功能，可对启用的合规模板基线按企业自身需要进行灵活调整。 （4）对用户登录堡垒机的认证凭据等敏感信息加密存储。 （5）对访问目标资源的帐户口令等认证凭据加密存储。提供产品相关功能证明材料。。 （6）堡垒机自身访问数据库的用户名、认证口令加密存储。 （7）采用国密Ukey或者动态令牌满足身份鉴别国密的要求。提供产品相关功能证明材料。 （8）通过https访问，同时兼容国密和国际链路SSL，自适应国密和国际浏览器。提供产品相关功能证明材料。 （9）一键生成合规报告并可导出，针对密评可按密评DAK量化评估框架对密评实现状况进行量化评估。 8、性能参数 （1）可管理不低于1000个用户； （2）可管理不少于2000个设备资源； （3）可管理不低于10000个帐户。 （4）可支持3000文本协议运维访问并发。 （5）可支持1000RDP图形协议运维访问并发。 | 政务外网区2套，互联网区2套 |
| 38 | SSLVPN安全网关 | 1、总体要求： （1)▲产品具有产品认证证书，符合GM/T0028安全等级第二级要求；提供相关资质证明材料。 （2)产品符合GM/T0024、GM/T0025规范要求，支持国密标准SSLv1.1协议；提供相关证明材料。 （3)支持国际算法SSLv3/TLS1.0/1.1/1.2/1.3认证模式； （4)采用厂商自有知识产权的信创密码卡；提供产品相关功能证明材料。 （5)采用厂商自有知识产权的符合GM/T0028安全等级第二级要求信创密码卡；提供产品相关功能证明材料。 （6)产品具有公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品；提供相关资质证明材料。 （7)产品具有IPV6ReadyLogo认证证书；提供相关资质证明材料。 （8)产品具有信息技术产品安全测试证书。提供相关资质证明材料。 （9)产品具备电信入网许可证。提供相关资质证明材料。 2、硬件要求： （1)至少提供4个网络端口,2个千兆电口，2个万兆光口； （2)2U标准机箱，为了防止数据窃听，设备不得存在USB接口； （3)支持设备状态灯显示运行状态，包括不限于电源状态灯、运行状态灯、告警灯等；提供产品相关功能证明材料。 （4)支持应急状态下，物理密钥销毁按钮对密钥进行销毁。提供产品相关功能证明材料。 3、密码算法： （1)集成国密认证的二级信创密码卡实现各类密码算法，保证算法的高安全性； （2)对称算法：支持国产SM1/SM4算法、以用国际通用算法DES、TDES、AES； （3)摘要算法：支持国产SM3和通用SHA1/SHA256/SHA384/SHA512等算法； （4)非对称算法：支持SM2、RSA、ECC等算法； 4、SSL网关功能 （1)符合GM/T0024规范要求 （2)支持国密SSL卸载 （3)支持国际算法SSLv3/TLS1.0/1.1/1.2/1.3认证模式 （4)支持国密双证双向HTTPS应用交付功能 （5)支持一个地址端口上RSA与SM2同时自适应 （6)支持正向SSL加载安全代理模式，将HTTP协议转换为HTTPS协议 （7)支持SSL协议转换（如将RSA算法SSL转换为SM2国密SSL） （8)支持内部产生密钥、生成CSR证书请求、支持GSMA组织指定多根多曲线协议 （9)支持国密X509数字双证书、支持国际标准的X509数字证书 5、SSLVPN功能 （1)符合GM/T0024规范要求 （2)支持国际算法SSLv3/TLS1.0/1.1/1.2/1.3认证模式 （3)支持IP协议与TCP/UDP/ICMP协议的加密传输 （4)SSLVPN隧道支持使用UDP传输协议进行加速、 （5)支持国密X509数字双证书、支持国际标准的X509数字证书、 （6)支持导入密钥、证书和PKCS12格式文件 （7)支持一个服务中可同时配置多条证书链，验证不同CA的用户证书 6、性能要求 （1)RSA2048并发用户数≥10000； （2)RSA2048新建连接数≥3000； （3)RSA2048吞吐量≥300Mbps； （4)SM2并发用户数≥10000； （5)SM2新建连接数≥3000； （6)SM2吞吐量≥300Mbps； | 政务外网区2套，互联网区2套 |
| 39 | 动态令牌认证系统 | 1、系统部署要求 （1)系统环境：支持windows、Linux等系统部署； （2)支持X86、ARM等服务器架构，支持国产CPU和操作系统； （3)数据库：支持Mysql、达梦等数据库； （4)密码机：支持符合GMT0030-2014《服务器密码机技术规范》的物理密码机和虚拟密码机；采用负载均衡模式调用多台密码机资源，支持对密码资源的动态调整； 2、系统服务功能指标： （1)认证服务协议：提供标准RADIUS协议的认证服务，支持对接第三方RADIUS客户端；提供HTTPSRESTfulAPI风格的认证服务接口，支持JSON格式的请求和响应数据； （2)动态口令认证：支持时间型动态口令的生成和验证，符合GM/T0021规范；支持用户ID+口令、令牌ID+口令的认证方式；支持时间飘移调节机制，认证窗口和同步窗口可配置； （3)通讯安全：管理服务支持双算法加密套件的https通讯协议，能够自适应客户端浏览器的加密套件；业务服务支持https加密通道，并支持白名单和访问密钥两种方式认证应用客户端的身份； （4)敏感安全参数安全：采用多级密钥管理体系，确保种子密钥全生命周期的安全管理和使用；采用密码机保证密钥和密码运算的安全； （5)访问控制：具备严格的访问控制机制，仅允许授权用户/业务系统进行权限范围内的访问； （6)多应用管理：支持多应用管理，可配置应用的服务模式和认证方式； （7)应用用户管理：支持管理业务系统的应用用户，将用户与令牌绑定； （8)令牌管理功能：支持硬件令牌、手机令牌；支持完善的令牌生命周期管理，包括激活、挂起、解挂、锁定、废止、查询等功能；支持对令牌的自动锁定/解锁和手动锁定/解锁；支持设置令牌的临时静态密码功能； 3、认证服务性能指标： （1）最大并发数：>10000用户 （2）认证响应性能：>1000TPS 4、手机令牌指标 （1）APP安装：支持android（从5.0至最新版本）和IOS（从10.0至最新版本）；支持从手机的应用市场直接下载安装； （2）启动保护：手机令牌应具有令牌保护密码管理功能，令牌保护密码管理功能包括修改令牌保护密码、静态密码、手势密码和指纹； （3）令牌类型：手机令牌应支持时间型动态口令的生成； （4）扫码激活：同一个手机令牌应用扫码添加多个不同的令牌二维码生成不同的动态口令；不同的手机令牌应用扫码添加同一个令牌二维码生成相同的动态口令； 5、产品资质 （1）▲商密认证：动态令牌认证服务具备商用密码产品型号证书，符合GM/T0021《动态口令密码应用技术规范》。提供相关资质证明材料。 （2）软著：国家版权局颁发的软件著作权登记证书。提供相关资质证书证明材料。 | 政务外网区2套，互联网区2套 |
| 40 | 国密浏览器 | 1、资质要求： （1）▲具备符合GM/T0028《密码模块安全技术要求》第二级要求《商用密码产品认证证书》。 （2）支持国密算法SM2、SM3、SM4，支持国密SSL协议，符合GM/T0024-2014《SSLVPN技术规范》； （3）提供由国家版权局颁发的《计算机软件著作权登记证书》。提供相关资质证明材料。； 2、产品要求： （1）支持HTML和CSS解析，支持JavaScrip引擎，可以正确的渲染显示页面，支持基本的浏览器操作功能； （2）支持国密算法SM2、SM3、SM4。在Chrome内核下均支持国密SSL协议； （3）Chrome内核版本要求不低于86，该版本Chrome内核需要同时支持NPAPI、PPAPI； | 政务外网区10套，互联网区10套 |
| 41 | SSL站点证书 | 1、基础要求：经由第三方CA机构颁发的SSL证书 2、兼容性要求：需要与SSL网关国密浏览器兼容 | 政务外网区2套，互联网区2套 |
| 42 | 安全硬件 | 万兆应用防火墙 | 1、网络层吞吐量≥50G，应用层吞吐量≥30G，防病毒吞吐量≥6G，IPS吞吐量≥6G，全威胁吞吐量≥3G，并发连接数≥800万，HTTP新建连接数≥20万。 2、规格≥2U，内存大小≥32G，硬盘容量≥256G，电源：冗余电源，接口≥4千兆电口+4千兆光口SFP+4万兆光口SFP+。 3、支持虚拟防火墙功能，支持虚拟防火墙的创建和删除。 4、支持路由类型、协议类型、网络对象等条件进行自动选路的策略路由，至少包括带宽比例、加权流量、线路优先等。 5、支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 6、支持对不少于6000种应用的识别和控制。 7、支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。 8、内置不低于11000种漏洞规则，同时支持在控制台界面通过漏洞名称、漏洞CVE标识等条件查询漏洞特征信息，支持用户自定义IPS规则。 | 政务外网区2台，互联网区2台 |
| 43 | 网闸 | 1、系统采用2+1架构设计，包括内端机、外端机和独立的硬件隔离信息交换区,内外网主机系统与交换模块之间采用隔离板卡连接。 2、支持对系统各类业务流量及任务状态进行实时监控，监控范围包括隔离映射、文件交换、数据库交换以及视频互联模块。 3、支持以趋势图形式实时监控设备cpu、内存、负载状态以及会话连接数，并提供近7天历史状态查询。 4、▲提供同步业务链路实时拓扑监控，可实时监测源端、目标端以及系统服务状态。（提供产品对应功能界面截图并加盖原厂盖章材料）。 5、▲API管理接口支持访问密钥数字签名验证，确保访问请求身份认证以及数据未被非法篡改。（提供产品对应功能界面截图并加盖原厂盖章材料）。 6、▲API管理接口支持访问密钥授权管理，可针对访问请求进行访问权限控制，访问资源权限包括：运行状态、网络、对象、设备管理、设备信息、规则策略、版本升级、日志审计以及工业协议权限。（提供产品对应功能界面截图并加盖原厂盖章材料）。 7、支持反向远程管理，系统本地管理服务主动注册到远程管理服务器，并将本地管理服务端口与远程管理服务端口绑定，实现远程管理服务器通过本地管理服务对系统进行反向远程管理。提供产品对应功能界面截图并加盖原厂盖章材料。 8、文件标识客户端支持Windows和国产银河麒麟操作系统，可针对文件数据进行打标和除标操作。 9、支持高斯（GaussDB）分布式数据库同步，兼容分布式主键数据库同步。 10、分解UPDATE同步，检测目标数据库无update数据主键则转换为insert操作进行同步，处理数据冲突，保证数据一致性。 | 政务外网区1台，互联网区1台 |
| 44 | 入侵防护系统 | 1、支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像。 2、支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP。 3、聚合接口支持非负载均衡模式（Roundrobin/Activebackup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。 4、漏洞扫描支持产品内置的默认模板以及自定义模板进行漏洞扫描，可扫描出漏洞名称、漏洞级别、漏洞描述、CVE-ID、CNNVD-ID等信息；支持查看资产关联的漏洞信息，并跳转到详情。提供产品对应功能界面截图并加盖原厂盖章材料。 5、支持对SSH、FTP等协议的弱密码扫描，扫描使用的密码表支持系统预置的完整表，常用表以及自定义表，可扫描IP地址、端口、服务、用户名、弱密码、风险等级等信息。提供产品对应功能界面截图并加盖原厂盖章材料。 6、支持HTTP、FTP、POP3、SMTP、IMAP协议的110多种预定义文件类型过滤，支持上传下载的方向选择；并支持自定义文件类型过滤。提供产品对应功能界面截图并加盖原厂盖章材料。 7、支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。 | 政务外网区2台，互联网区2台 |
| 45 | 网络行为审计系统 | 1、网络层吞吐量（大包）≥50Gb，带宽性能≥10Gb，最大并发连接数≥8000000。 2、规格≥2U，内存大小≥32G，硬盘容量≥1024G，电源：冗余电源，接口≥4千兆电口+4千兆光口SFP+4万兆光口SFP+。 3、支持首页显示在线用户、流量分析、行为日志分析、用户流量排名。 4、支持IPV6双栈。 5、设备内置应用识别规则库，支持超过7000种以上应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制。 6、支持针对搜索引擎、HTTP、网页内容进行关键字过滤并实时生成日志记录，日志级别包括但不限于紧急、告警、严重、通知、信息、调试、不记录。 7、可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（ZIP、RAR、GZ、BZ2、Z、TGZ、TBZ、7Z、CAB、BZ等）、应用程序、Office系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。 8、支持对FTP、Telnet、DNS等协议的相关操作命令进行过滤控制。 9、支持自定义URL过滤，包括恶意URL白名单、恶意URL黑名单、URL白名单等，并支持URL的模糊匹配。 10、支持WEB/FTP/SMB类型业务的行为和内容审计。 | 政务外网区1台，互联网区1台 |
| 46 | SSLVPN安全网关（商密） | 1、加密最大流量（Mbps）≥120，理论并发隧道数（Tunnel）≥300；SSL性能参数≥最大理论加密流量（Mbps）≥600，最大理论建议并发用户数≥1200。 2、硬件规格要求：规机架式设备≥1U，内存大小≥16G，硬盘容量≥480GSSD，电源：冗余电源，接口≥6千兆电口+4千兆光口SFP。 3、支持多因素认证，至少包括：账号密码认证、短信认证、证书认证、动态令牌认证、扫码认证，以及对接统一认证平台实现单点登录等认证方式。账号密码认证应支持设备自带账号密码认证，或通过LDAP/Radius/HTTPS协议对接第三方认证服务器。扫码认证应至少支持零信任客户端、企微、钉钉、飞书扫码认证。单点登录应支持标准的CAS、OAuth2.0、OIDC协议对接。为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：账号首次登录、账号在该终端首次登录、闲置账号登录、弱密码登录、异常时间登录、非常用地点登录等。 4、持针对发布的WEB应用开启WEB水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用。应支持对WEB应用禁止复制、禁止打印、禁止下载、禁止鼠标右键、禁止浏览器调试功能，以保护应用的数据安全与应用安全。 5、客户端应兼容主流操作系统和芯片，操作系统至少包括Windows、macOS、Ubuntu、Android、iOS、UOS、Kylin、NFS、Harmonynext，芯片至少包括兆芯、海光、飞腾、鲲鹏、海思麒麟、龙芯（含MIPS和Loongarch）。 6、支持UDP+TCP组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口。安全码支持共享码和一人一码及一次一码三种模式，可通过短信分发安全码。一人一码模式下，当实际登录用户跟分发SPA安全码绑定的用户不一致时，零信任系统可以产生安全告警。一次一码模式下激活码被用户使用并正常登录零信任系统后转换为安全码加密存储，换码成功后激活码失效，控制台日志须体现用户首次登录后的换码过程。 7、支持用户登录日志（登录、注销，含MAC地址、终端类型、浏览器类型等）支持管理员操作日志（含管理员、接入IP、时间、管理行为、对象）。 | 政务外网区2台，互联网区2台 |
| 47 | 集中日志系统 | 1、独立完成审计日志采集，不依赖于设备或系统自身的日志系统。 2、采用解决方案包上传对产品进行功能扩展，无需代码开发。 3、支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能。Kafka收发支持SSL加密。 4、日志转发与存储支持数字签名与加密，数字签名支持SM3和SHA256，加密模式支持AES和SM4，日志接收支持解密 5、支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。 6、支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息。 7、支持关联规则性能以界面列表形式显示，可了解触发次数、最近一周监控状态等信息。 8、▲具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。（提供产品对应功能界面截图并加盖原厂盖章材料）。 9、▲三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。（提供产品对应功能界面截图并加盖原厂盖章材料）。 10、用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户。 | 政务外网区1台，互联网区1台 |
| 48 | 漏洞扫描 | 1、设备硬件参数要求：标准机架式硬件，1U，交流单电源，4T硬盘，千兆电口≥4个，千兆光口≥4个，万兆SFPP插槽≥2个，USB口≥2个，1\*串口，默认提供1路扫描端口授权，最大并发主机数60个，最大并发任务数10个。 2、▲支持检测的漏洞数大于340000条，兼容CVE、CNCVE、CNNVD、CNVD等主流标准，并提供CVECompatible证书。（提供相关证书证明材料并加盖厂商公章）。 3、支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态， 4、支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义。 5、内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术。 6、▲支持系统漏洞库和Web漏洞库通过多种维度对漏洞进行检索，包括：漏洞名称、漏洞ID，CVEID、BUGTRAQID、CNCVEID、CNVDID、CNNVDID、MS编号、风险等级、是否使用危险插件、是否支持漏洞验证，漏洞发布日期、漏洞分类信息。（提供产品对应功能界面截图并加盖原厂盖章材料）。 | 政务外网区1台，互联网区1台 |
| 49 | 安全态势感知平台 | 1、性能要求：带宽性能≥1Gbps时存储时长≥900天/1Gbps。 2、硬件参数要求：规格≥2U，CPU≥16C，内存≥128GB，系统盘≥256GB，电源：冗余电源，接口≥4千兆电口+2万兆光口SFP+。 3、支持资产自动识别和资产扫描功能。 4、支持整体展示服务器脆弱性风险分析、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码）等安全风险信息。 5、支持工单下发闭环，针对检测出来的安全事件，下发给下级管理员，通过工单系统可以跟进事件处置状态，完成闭环。支持向下级管理员推送预警。支持向其它管理员推送公告。 6、平台支持攻击告警功能，攻击告警可结合ATT&CK技术栈进行关联分析。 7、平台支持安全态势可视化的展示，能够以图表/柱形/动画等形式展示实施安全威胁态势。 | 政务外网区1套，互联网区1套 |
| 50 | 态势感知探针 | 1、性能参数要求：网络层吞吐量≥10Gbps，应用层吞吐量≥3.4Gbps。 2、硬件参数要求：设备规格≥2U，内存大小≥16G，硬盘容量≥480G，电源：冗余电源，接口≥4千兆电口+4千兆光口SFP+2万兆光口SFP+。 3、支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 4、系统使用资源状态、吞吐量、接口状态等信息展示。 5、支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞、等网站攻击检测。 6、支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、php反序列化检测等自定义配置启用。 7、提供三权分立的用户管理能力：系统管理员、审计管理员、安全管理员、普通管理员四个角色相互独立；同时支持IP绑定的登录安全设置。普通管理员角色的权限可自定义模块页面的编辑和查看权限。 8、支持基于IP和域名的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断。 9、支持敏感信息检测功能，内置身份证、手机号码、银行卡号。 10、支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Media漏洞攻击、NetworkDevice、Shellcode漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测。 | 政务外网区1台，互联网区1台 |
| 51 | 密码服务 | 虚拟加解密服务 | 1、提供虚拟加解密服务的性能：SM2密钥对生成≥100000对/秒、SM2签名≥180000次/秒、SM2验签≥60000次/秒、SM2加密≥40000次/秒、SM2解密≥70000次/秒、SM3≥9Gbps、SM4≥9Gbps。 2、支持SM2、SM3、SM4、RSA、AES等国内国际密码算法，对称算法模式支持ECB/CBC； 3、支持通过VXLAN等方式与租户VPC打通、支持各虚拟化密码机之间的基于SR-IOV的硬件级安全隔离。 4、提供虚拟密码机数量≥32。 5、支持“一机多用”：包括服务器密码机，金融数据密码机，签名验签服务器，数字证书系统，密钥管理系统，手机盾、SSLVPN安全网关等产品，且实现密码功能池化融合。 6、支持IPV4/IPV6双栈网络协议。（提供云服务器密码机IPV6证书） 7、虚拟密码机支持设置基于源IP访问白名单功能，实现应用访问控制。 8、提供服务能力的云服务器密码机支持虚拟密码机管理能力，支持虚拟密码机的创建/启动/停止/删除/克隆/token配置/VNC连接/强制关机。 9、支持VSM的手动/自动迁移功能,既支持同一宿主机内部，也支持不同宿主机之间的两虚拟机手动/自动迁移，可以查看虚拟机迁移历史记录，记录中需能显示出迁移结果、迁移时间以及迁移类型（手动或自动）。 10、提供服务的云服务器密码机设备具备有效期内的《商用密码产品认证证书》,满足GM/T0028《密码模块安全技术要求》安全等级第二级及以上相关要求。 11、提供服务的云服务器密码机设备内由同品牌密码卡提供密钥管理能力充分保证兼容性和稳定性，密码卡具有《商用密码产品认证证书》，并符合GM/T0028《密码模块安全技术要求》第二级要求。 12、提供服务的云服务器密码机产品具有《网络安全专用产品安全检测证书》。 13、提供服务的云服务器密码机产品具有《信息技术产品安全测试证书》。 | - |
| 52 | 通信链路加密服务 | 1、提供通信链路加密服务性能：密文速率≥900Mbps，密文吞吐率≥900Mbps，每秒新建连接数（SSL）≥5000，每秒新建隧道数（IPSec）≥3000，转发延时＜1ms，会话恢复时间＜2s，并发连接：最大并发连接数≥20万，最大并发用户数（隧道）≥3000 2、支持国密SM2/SM3/SM4算法，支持DES、3DES、AES对称算法，支持SHA-256散列算法，支持2048位RSA非对称算法。 3、支持通过WEB、CLI管理，支持反向代理、SSLVPN隧道、IPSecVPN隧道工作模式，支持智能终端、应用APP、PC、手机等设备接入，支持用户终端安全检查(通过操作系统版本、IE浏览器版本、进程、开放端口、杀毒软件和安全补丁安装等情况进行检查，对于不符合要求的终端禁止接入网关)。 4、支持FTP代理、SMTP/SMTPS代理、POP3/POP3S代理，可实现支持基于VPN隧道的应用代理，实现深层次的通信数据过滤；支持设置证书过滤规则，可通过对用户证书C、ST、O、CN、L、OU、Email等字段进行过滤，实现对接入用户的登入控制。（提供产品功能截图） 5、支持抗非法报文攻击：包括land、Smurf、Pingofdeath、Winnuke、Tcp\_sscan、Ip\_option、Teardrop、Targa3、Ipspoof等、支持通用非法报文、非法TCP报文、非法ICMP报文的检测、支持抗系统扫描，包括Syn半开扫描、FIN、ACK扫描、圣诞树扫描、NULL扫描、UDP扫描等、支持抗洪泛攻击，包括DOS、DDOS、SYNFLOOD、UDPFLOOD、PINGFLOOD等。 6、支持IPV4/IPV6双栈。 7、支持IPSecVPN多隧道策略，可与对端建立两条通信策略完全相同的隧道，并通过权重实现隧道备份和隧道负载均衡功能。 8、提供服务的综合安全网关密码设备具备有效期内的《商用密码产品认证证书》,满足GM/T0028《密码模块安全技术要求》安全等级第二级及以上相关要求。 9、提供服务的综合安全网关产品具有《网络安全专用产品安全检测证书》 10、提供服务的综合安全网关产品具有中国质量认证中心颁发的节能产品认证证书以及具有环境标志认证资质的机构颁发的中国环境标志产品认证证书。 11、提供服务的综合安全网关产品具有《信息技术产品安全测试证书》。 | - |
| 53 | 租户身份认证服务 | 1、提供租户身份认证服务的性能：SM2签名≥18000次/秒，SM2验签≥9400次/秒，SM2制作信封≥9400次/秒，SM2解密信封≥11600次/秒，SM1加解密≥850Mbps，SM4加解密≥850Mbps，SM3≥850Mbps，RSA(2048)签名≥5600次/秒，RSA(2048)验签≥35000次/秒 2、对称算法：SM1、SM4，非对称算法：SM2，摘要算法：SM3，MAC算法：HMAC、CMAC。 3、支持对数据块和文件进行支持SM2算法的签名和验签服务，支持内部/外部密钥运算，支持PKCS#1格式的数字签名与验证能力，支持PKCS#7格式的数字签名与验证能力，支持Detach与Attach模式。支持对数据块和文件的摘要进行支持SM2算法的签名和验签服务。解决数据或文件在过大时，传输缓慢的问题。减小网络流量开销，提高运算效率，支持基于SM2密码算法的数字信封加解密服务。 4、满足用户数据签名、XML封皮签名、XML封内签名、PDF签名、CMS签名、APK签名、可执行文件签名等多种签名/验签业务。 5、支持生成对国密SM2双证书和RSA证书进行管理，支持证书申请、导入、删除、更新，支持导入多个CA根证书或证书链，并对其进行管理，支持多CA证书同步验证，证书链管理可对数字证书进行验证，查询证书有效性，证书验证支持不验证、CRL验证、OCSP验证。 6、支持应用新增、编辑、删除，支持应用绑定SM2证书、RSA证书。 7、提供服务的签名验签服务器密码设备具备有效期内的《商用密码产品认证证书》,满足GM/T0028《密码模块安全技术要求》安全等级第二级及以上相关要求。 8、提供服务的签名验签服务器产品具有《网络安全专用产品安全检测证书》 9、提供服务的签名验签服务器产品具有中国质量认证中心颁发的节能产品认证证书以及具有环境标志认证资质的机构颁发的中国环境标志产品认证证书。 10、提供服务的签名验签服务器产品具有《信息技术产品安全测试证书》。 | - |
| 54 | 密码资源统一管理服务 | 1、提供密码资源统一管理服务的性能：应用系统接入数≥100，并发连接数≥2000。 2、支持国密和国际通用算法，对称算法：SM4、3DES、AES，非对称算法：SM2、RSA1024/RSA2048；摘要算法：SM3、SHA-256，MAC算法：HMAC、CMAC。 3、支持通用的密码服务，支持SM4国密算法和3DES、AES国际算法的数据加解密，支持SM2、RSA算法的数据加密和解密运算服务，满足用户数据传输或存储过程中的机密性保护，支持内部存储的SM2/RSA私钥或外部SM2/RSA私钥进行数字签名、验签服务，提供基于SM3、SHA256杂凑算法服务，提供支持基于SM3算法、SM4算法的MAC产生及验证服务，采用由国家密码管理局批准的双物理噪声源生成随机数。可提供256位SM2密钥对和1024/2048/3072/4096位RSA密钥对，或直接为用户提供随机数服务。 4、对密码资源分组管理，支持对密码资源进行管理，包含资源注册、资源分组等管理，密码资源至少包含服务器密码机、签名验签服务器、云服务器密码机等；支持对密码设备和虚拟密码设备进行管理；支持密码资源与密码服务进行绑定和解绑。 5、支持对接入的应用系统进行管理，支持对应用系统的注册、授权和冻结管理，应用注册支持管理员和租户两种方式；支持对应用系统进行访问控制及身份认证；身份认证支持AK/SK方式，至少支持IP白名单和应用授权码方式进行访问控制，IP白名单支持IP地址或IP段两种访问控制策略；用信息隔离控制，每个租户只能对本账户的应用进行管理；支持为应用系统分配密码资源组及密码服务。 6、▲提供大屏显示能力，支持显示密码资源实时调用情况统计、系统信息的统计信息（包含服务量、运行时间、保护应用数量以及接入设备数量等）、以及分中心的地理位置的地图展示、应用的资源用量（含TOP10统计）以及告警信息的展示（提供产品对应功能界面截图并加盖原厂盖章材料） 7、支持多种调用方式，有Linux调用接口，支持Java接口，提供标准SDK接口，支持Restful接口调用方式，满足各类语言的调用，支持统一的自定义接口，满足密码服务能力的接口扩展。 8、支持云服务器密码机的管理，可通过页面进行设备注册，支持云服务器密码机重启、注销、备份与恢复、升级、网络配置、DNS配置、NTP配置、影像上传地址配置、日志上传地址配置，详情查看等。 9、对所有密码设备信息进行统计管理，可快速了解所有设备的设备情况，包含不限于：设备标识、设备名称、厂商名称、设备型号等内容。 10、对密钥基础策略、模板、密钥生成、密钥分发等进行策略管理：对密钥通用性的策略进行统一化管理，避免重复操作、支持创建对称密钥模板和非对称密钥模板，支持对密钥模板进行增加、修改、删除、支持密钥生成策略的增删改查、支持生成对称密钥和非对称密钥生成策略、支持密钥分发策略的增删改查，策略可以根据实际修改 11、支持密码资源加密导出：支持通过第三方证书进行加密导出密码资源，密码资源包括密钥、证书等，满足向第三方平台或设备密码资源的迁移需求，导出的密码资源通过智能密码钥匙硬件介质进行加密保存。 12、支持为应用系统和密码设备下发密钥，支持应用系统的凭据的安全管理、对凭据密钥的全生命周期管理，支持多凭据管理。 13、▲具备密码服务功能，以图形化方式展示密码资源情况、应用密码实时用量、应用密码使用情况、租户服务统计等。具备设备管理服务功能，以GIS地图配合文字描述方式显示设备实时信息。具备密钥管理服务功能，以图形化方式展示备用对称/非对称密钥、在用对称/非对称密钥使用情况等多种密钥使用情况（提供产品对应功能界面截图并加盖原厂盖章材料） 14、▲具备认证管理服务功能，具体显示系统基本信息，并且以图形化方式展示证书统计和证书有效期统计。支持系统配置凭据密钥能力。提供凭据管理功能，为应用添加一条或多条关键凭据，可以自定义凭据有效期。（提供产品对应功能界面截图并加盖原厂盖章材料） 15、为租户提供独立的自助管理系统，租户登录支持账号、数字证书、双因子等方式；通过图形化方式对租户应用及密码服务使用情况进行大屏展示，至少包含应用数、服务数、服务使用量、服务余量等信息，支持系统告警消息和未读消息数量展示；支持租户应用、服务、账户信息等变化通知，可对消息详情进行查看。具备应用申请功能和服务订阅功能。 16、支持租户工具包管理。对租户提供密码服务工具包管理，至少包含工具包版本、开发语言、上传时间、工具包描述等信息。支持默认工具包，支持工具包更新。工具包至少包含接口手册、SDK开发包、用户手册等内容。 17、▲密码服务管理平台包含密钥管理及设备管理系统，密钥管理系统需提供《商用密码产品认证证书》。同时设备管理系统需提供《商用密码产品认证证书》，并符合GM/T0028《密码模块安全技术要求》第二级要求。（提供产品对应功能界面截图并加盖原厂盖章材料） 18、提供服务的密码服务管理平台密码设备具备有效期内的《商用密码产品认证证书》,满足GM/T0028《密码模块安全技术要求》安全等级第二级及以上相关要求。 19、提供服务的密码服务管理平台产品具有《网络安全专用产品安全检测证书》。 20、提供服务的密码服务管理平台产品具有《信息技术产品安全测试证书》。 21、提供服务的密码服务管理平台产品具有中国质量认证中心颁发的节能产品认证证书以及具有环境标志认证资质的机构颁发的中国环境标志产品认证证书。 | - |
| 55 | 可信时间戳服务 | 1、提供可信时间戳服务的性能：SM2生成时间戳请求≥13000tps、SM2验证时间戳≥9200tps、RSA生成时间戳请求≥4000tps、RSA验证时间戳≥20000tps 2、对称算法：SM1、SM4，非对称算法：SM2，摘要算法：SM3，MAC算法：HMAC、CMAC。 3、支持SM2、RSA算法时间戳，为应用系统提供时间戳签发、验证时间戳核心功能，实现对数据、消息等多种格式原文数据的时间戳服务。 4、时间戳服务器支持为PDF、微软SignCode工具提供时间戳服务。 5、支持对时间戳的保存、备份、检索、删除和销毁；支持时间戳的查看和验证。 6、支持对数字证书的全生命周期管理，支持生成对国密SM2双证书和RSA证书进行管理，支持证书申请、导入、删除、更新。 7、提供服务的时间戳服务器密码设备具备有效期内的《商用密码产品认证证书》,满足GM/T0028《密码模块安全技术要求》安全等级第二级及以上相关要求。 8、提供服务的时间戳服务器产品具有《网络安全专用产品安全检测证书》。 9、提供服务的时间戳服务器产品具有《信息技术产品安全测试证书》 10、提供服务的时间戳服务器产品具有中国质量认证中心颁发的节能产品认证证书以及具有环境标志认证资质的机构颁发的中国环境标志产品认证证书。 | - |
| 56 | 客户端身份认证服务 | 1、提供客户端身份认证服务的性能：SM4加解密≥2Mbps，SM2密钥对生成≥4次/秒，SM2解密≥90次/秒，SM2签名≥120次/秒。 2、算法支持SM1、SM2、SM3、SM4。 3、提供服务的智能密码钥匙产品支持USB2.0接口。 4、支持CSP/PKCS#11，SKF国密标准，X.509证书格式； | - |
| 57 | 证书服务 | 1、可信设备证书服务：为设备颁发的唯一证书文件，标识设备唯一网络身份。 2、可信个人数字证书服务：提供个人身份认证服务。 | - |
| 58 | 网络服务 | 网络分区 | 网络采用基于VXLAN技术的Overlay网络架构，按照服务类型及安全等级，把整个网络分成不同的业务区块：根据政务网络安全管理、信息安全等级保护等要求，在政务云中明确部署和划分互联网区和政务外网区，两个区域之间应按照要求进行安全隔离并提供必要的安全保障，分别承载政务外网和互联网应用，政务外网应用与互联网应用实现安全隔离和数据交换。 | - |
| 59 | 网络带宽 | 政务云互联网出口满足3G带宽要求，且具备接入2家以上运营商的能力。平台核心骨干设备、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≥40G带宽，服务器业务≥10G带宽。 云平台需满足基于SDN、VxLAN技术提供相关网络服务，SDN可以与云平台能实现自动化动态的网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接。本次采用SDN解决方案，实现云网络的搭建，需要实现云网络对网络的需求、弹性计算业务对网络的需求、云存储对网络的要求、云安全业务对网络的需求、云数据库对网络的需求、管理与监控对网络的需求，以及网络本身的规格要求。 | - |
| 60 | 网络隔离 | 迁移上云的电子政务系统，不能因为部署虚拟化技术而改变原有的安全区域划分和互访规则，委办局之间应实现VPC逻辑隔离，单委办局内的业务通过安全组逻辑隔离。 | - |
| 61 | 机房产权 | 在北京市怀柔区内拥有自有产权数据中心，需提供数据中心房屋所有权证或国有土地使用证。 |  |
| 62 | 等级保护 | 提供的机房物理环境满足信息系统安全等级保护3级要求。 |  |
| 63 | 机房供电 | 支持两路市电供电，具备独立的UPS和发电机组，不间断电源保障在紧急状况下的平台运行，切换过程不影响业务正常运行。 |  |
| 64 | 能效 | 符合北京市《数据中心能源效率限额》DB11/T 1139-2023 （PUE≤1.35）。 |  |
| 65 | 安防系统 | 机房配有监控和门禁系统,要求对机房出入口及热通道进行门禁管理，且要求机房及机柜列间均配备门禁系统，门禁系统需要与视频监控系统集成到同平台上管理，以满足数据中心安全要求。 |  |
| 66 | 消防系统 | 机房配有专业的气体灭火系统，并带泄压及事故排风系统。 |  |
| 67 | 机柜 | 提供的数据中心须提供独立物理区域供政务云平台使用，且所有功能模块的机柜在同一楼层，可为本项目提供不少于50个机柜空间，并可以根据区政府要求按需在同一楼层扩容至不少于100个机柜。 |  |
| 68 | 基础软件栈全生命周期保障维护服务 | 商用操作系统维保服务 | 1、提供全面的操作系统支持服务，涵盖以下方面：技术支持、部署支持及售后支持。系统覆盖范围至少包括主流的WindowsServer系列视窗操作系统，同时可根据具体需求，提供其他同系列商用产品的支持服务。 2、提供兼容并支持在政务云平台环境中运行的操作系统支持服务。 |  |
| 69 | 1、提供全面的操作系统支持服务，涵盖以下方面：技术支持、部署支持及售后支持。服务范围广泛，系统覆盖至少包括麒麟、统信、RedHat等主流国产商业化Linux操作系统。此外，根据具体需求，还可提供其他商用产品的支持服务。 2、提供兼容并支持在政务云平台环境中运行的操作系统支持服务。 |  |
| 70 | 开源操作系统维保服务 | 1、提供全面的操作系统支持服务，涵盖技术支持、部署支持及售后支持。系统覆盖范围至少包括Ubuntu、CentOS等主流开源Linux操作系统，并可根据具体需求，扩展至其他开源产品的支持服务。 2、提供兼容并支持在政务云平台环境中运行的操作系统支持服务。 |  |
| 71 | 国产商用应用中间件维保服务 | 1、提供全面的中间件支持服务，涵盖以下方面：技术支持、部署支持及售后支持。中间件产品覆盖范围至少包括TongWeb、Primesoft等三类主流商用产品，同时可根据具体需求，扩展支持其他商用产品。 2、提供兼容并支持在政务云平台环境中运行的中间件支持服务。 |  |
| 72 | 开源应用中间件维保服务 | 1、提供全面的中间件支持服务，涵盖以下方面：技术支持、部署支持以及售后支持。所涉及的中间件范围至少包括Nginx、Apache、Tomcat等三种主流开源中间件，并且能够根据特定需求，灵活提供对其他开源产品的支持服务。 2、提供兼容并支持在政务云平台环境中运行的中间件支持服务。 |  |
| 73 | 商用数据库维保服务 | 1、提供全面的数据库支持服务，涵盖以下方面：技术支持、部署支持及售后支持。支持的数据库产品至少包括GaussDB、达梦数据库、KingBase等三种主流国产商用产品，且可根据具体需求，扩展提供其他国产商用产品的支持服务。 2、提供兼容并支持在政务云平台环境中运行的数据库支持服务。 |  |
| 74 | 开源数据库维保服务 | 1、提供全面的数据库支持服务，涵盖技术支持、部署支持及售后支持。所支持的数据库类型至少包括Mysql、openGauss、PostgreSQL等三种主流开源数据库，并且可根据具体需求，扩展支持其他开源产品。 2、提供兼容并支持在政务云平台环境中运行的数据库支持服务。 |  |
| 75 | 扩展网络维保支持服务 | 小型支持服务 | 1、提供最大1万连接数和每秒1千新建连接数的SNAT能力。 |  |
| 76 | 中型支持服务 | 1、提供最大5万连接数和每秒5千新建连接数的SNAT能力。 |  |
| 77 | 大型支持服务 | 1、提供最大20万连接数和每秒1万新建连接数的SNAT能力。 |  |
| 78 | 超大型支持服务 | 1、提供最大100万连接数和每秒3万新建连接数的SNAT能力。 |  |
| 79 | 其他支持要求 | 通用要求： 1、提供网络地址转换服务，支持私有网络内的多个云服务器通过共享一个弹性IP访问外部网络。 2、支持SNAT（源网络地址转换）功能，使私有网络内的云服务器能够通过NAT网关共享一个弹性IP的方式访问外部网络。 3、具备高可用能力； 4、通过政务云平台提供扩展网络服务NAT网关服务； |  |
| 80 | CDN加速服务 | CDN服务 | 提供内容加速及视频加速服务1MB/1GB/100GB，需支持对静态页面、静态图片、流媒体点播直播、动态内容等各类内容资源进行处理，由CDN核心节点从源站获取分发资源后，分级分发至相应边缘节点，确保用户能够从最近且响应最优的节点访问到对应的资源。 |  |
| 81 | IDC服务 | 机柜扩增 | 提供IDC机柜扩增服务，以满足后续业务扩容需求，包含新增机柜及相关配套设施和对应服务。机柜应满足机柜规格600×1200×2200mm，机柜功率5kW等标准 |  |
| 82 | 裸光纤 | 提供裸纤接入服务，单模光纤传输，光衰符合两端设备要求。施工材料采用国家标准（B1.3）、ITU—TG.652单模光纤，符合工业和信息化部颁布的《通信行业服务质量标准》及其他国家有关标准和规定。光纤维护依照电信行业相关标准的服务级别要求。 |  |
| 83 | 数传专线 | 提供数据传输专线接入服务，可按需求开通对应带宽，保证专线安全性、稳定性和时延符合要求，并提供两端设备兼容的端口。 |  |
| 84 | 安全重保服务 | 日常安全运维驻场服务 | 重保期全方位防护，监控流量与状态，拦截攻击。有应急预案，定时汇报安全状况。 |  |
| 85 | 中级安全服务 | 开展Web失陷检测，发现并处置异常。提供等保咨询，助系统达等保要求。 |  |
| 86 | 高级安全服务 | 组织攻防演习，提改进建议。熟练渗透测试，出修复方案。会代码审计，给优化建议。应急响应高效，减事件损失。定期查安全事件，防患未然。 |  |
| 87 | 运维服务 | 高级云平台服务 | 需提供一名（5\*8）高级驻场（兼项目经理，高级云运维）。包括项目统筹、应用维护、数据库中间件维护等业务运维支撑服务。负责云平台故障、网络管理、日常维护及资源管理。 |  |
| 88 | 机房云运维运维服务 | 需提供4名7×24小时驻场运维，负责机房驻守、基础维护、拨测支持、云平台的日常运行维护与故障处理等运维服务，包括但不限于：系统及业务监控，其它工作如遇紧急突发情况也需提供7×24小时服务支撑，随时根据动态进行服务保障。负责对租户、客户经理发起的问题、投诉进行响应，记录，跟踪，协调组织排查，负责软硬件资产管理，硬件巡检，备品备件管理、机房出入管理。日常线上巡检作业，周检，月检。 |  |
| 89 | 高级网络服务 | 需提供一名（5\*8）高级驻场运维（兼项目经理，高级网络和系统运维）。包括设备配置定期备份、网络设备巡检、IP地址分配、网络基础数据维护。按照流程进行网络配置变更，主要涉及网络配置调整、防火墙策略变更。设备故障处理及网络故障排查。与第三方厂商一起完成网络调整、割接。网络咨询、相关网络项目配合、相关网络文档编写等。 |  |
| 90 | 中级售后服务 | 需提供一名（5\*8）中级驻场运维（兼项目经理，中级网络和系统运维）。项目规划、实施、管理、支撑服务；售后阶段的客户上云支持，同售中-业务交付；制定售后管理流程与基本要求、根据客户需求输出优化建议及方案；对云和网络的资源管理，包括云的计算、存储、网络资源和云平台网络的物理端口、IP地址资源、备件等资源的分配、变更、回收、统计分析等工作。 |  |
| 91 | 原厂运维服务 | 需提供一名（5\*8）原厂专属服务经理，进行云平台驻场运维。 |  |
| 92 | 深度监控服务 | 云主机深度监控 | 提供云主机7\*24小时深度监控服务，并提供相应报告。 |  |
| 93 | 迁移服务 | 技术要求 | 1、迁移评估与分析。系统评估与分析需明确迁移范围和目标，确定评估形式，并形成规范的调研分析报告。  2、迁移方案设计。方案设计需涵盖云化适用性分析、迁移场景梳理及迁移技术方案规划。  3、云平台环境准备。云平台环境准备合相关资源的配置项的准备。  4、迁移测试验证。需针对性地实施涵盖功能性测试、性能测试及稳定性测试的完整方案，确保应用系统在云平台环境中稳定可靠地运行。  5、业务系统迁移。需包含迁移实施方案、迁移工具等。  6、迁移业务割接。需制定完善的割接方案，割接完成后即进入割接后观察期，待系统稳定运行1个月后，需出具专项性能分析报告。 |  |
| 94 | 迁移时间 | 在政务云平台具备提供系统生产环境运行资源后，每一个业务系统获甲方书面确认系统迁移工作后30日内完成业务迁移（在甲方书面确认的业务维护窗口期内），180日内完成《迁移系统服务系统清单》中的业务系统迁移至政务云平台运行的工作。 |  |
| 95 | 迁移范围 | 完成75套业务系统迁移上云。 |  |
| 96 | 售后服务与要求 | 1、在系统迁移上云后，一旦出现故障或性能问题，乙方应在接到通知后迅速响应，进行远程或现场的故障排查。  2、乙方需提供专业的技术支持，能够快速定位问题原因，并提出有效的解决方案。 |  |

**注：**

**1.★条款为必须响应条款，不满足将无法通过资格评审；**

**2.▲为重要技术条款，作为技术评分依据**

**3.所有证书需在有效期内，若证书处于延期办理中，需提供相关部门出具的证明文件，否则该证书不予认可。**

**第六章拟签订的合同文本**

**政府采购合同（服务类）**

合同编号：【 】

本合同由以下双方根据平等自愿原则，协商一致在北京市怀柔区签订：

**甲方：北京市怀柔区政务服务和数据管理局**

地址：北京市怀柔区开放路33号

授权代表人：

邮编：

联系电话：

传真：

**乙方：**

营业执照注册号：

地址：

法定代表人：

联系电话：

账户名称：

开户银行：

公司账号：

本《服务合同》（以下简称**本合同**）经甲、乙双方友好协商签订，双方达成以下合同内容。

1. **服务内容与服务标准**

1.故障响应定位服务：乙方需提供技术咨询与故障定位服务，提供7\*24响应；

2.远程巡检服务：乙方需提供服务巡检，对云服务的状态进行远程巡检，以确保云平台正常提供服务；

3.技术文档支持服务：乙方需开放本项目全量文档和知识库，可随时获取技术文档及相关素材；

4.API与SDK支持服务：乙方需提供本项目全量产品的OpenAPI/SDK接口及工具，方便调用和集成开发；

5.缺陷修复服务：乙方需提供已交付版本产品软件的缺陷修复服务。乙方在征得甲方同意后，在与甲方约定变更时间窗口内完成修复工作；

6.本合同所涵盖的各项服务内容与服务标准详细内容见附件一《投标文件技术应答部分》。

1. **服务期限**

服务期限自【年月日至年月日】止，期限需与政府采购备案有效期匹配，若因业务特殊需要调整，双方应提前协商，通过补充协议明确。

1. **工作检查**

1.测试验收

（1）乙方需完成功能测试、性能测试等必要测试工作，提交测试报告等相关材料，甲方在合理期限内组织审核。​

（2）测试未通过的，甲方向乙方出具书面整改意见，乙方应及时整改并重测，相关事宜双方协商处理；若因特殊情况需延长整改时间，乙方可提前与甲方沟通，经同意后适当顺延。​

2.日常考核与追溯

（1）甲方可每月从“可用性、响应时效、安全合规”等维度进行考核，考核结果作为双方沟通改进的依据，若存在明显不足，乙方应积极整改。​

（2）乙方每季度提交系统运行状况，甲方在合理时间内给出审核意见，乙方根据意见进行完善，具体优化事项双方协商确定。

3.交付管控

（1）上云需求确认：乙方负责复核本项目涉及的上云需求、负责一系统一方案制定上云方案、负责资源容量确认、负责上云可行性分析。配合甲方进行整体规划，进行建设、交维指导等。

（2）资源开通：乙方需依据本项目需求在云管平台上开通基础服务及安全资源、管理并移交项目账号、操作手册等。

（3）网络策略配置：乙方需根据业务系统提交的网络资源申请表进行云内与云外的网络及安全策略配置。

（4）上云业务迁移支持：乙方需对涉及迁移上云系统跟进其交付部署进展，并提供技术支持。

（5）流程规范化管理：乙方需对建立规范化管理流程，需向甲方提供符合验收标准要求的依据、配合开展试运行相关工作，监控运行状态、配合整改。

（6）甲方有权按本合同第一条约定的服务内容和标准对乙方工作进行工作检查，经甲方工作检查不合格的，甲方有权要求乙方在指定期限内采取弥补措施，乙方采取弥补措施之后再次提交甲方进行检查。经乙方【三】次弥补仍未能经甲方检查合格的，甲方有权单方解除合同，按照实际发生服务项目数量支付合同价款。

1. 服务费支付方式及发票

本合同总金额为【】万元，最终实际支付价款以实际发生服务项数量为结算依据，且总支付价款不超过合同总金额。本项目按照实际需求量下订单，按月对账。乙方每月5日前通过电子邮件方式向甲方发送上月账单，甲方收到邮件后5日内进行审核，甲方如有异议应该前述期限内向乙方提出，甲方在前述期限内未提出异议的，视为甲方对账单无异议。

1.支付周期与结算流程

自合同签订之日起，甲方按半年度向乙方支付服务费，每6个月为一个结算周期。每个结算周期届满前10个工作日内，乙方应向甲方提交验收报告申请以及相应服务费用详细证明材料。甲方应在5个工作日内确认验收报告，逾期未确认的，视为验收合格，并在结算周期后20个工作日内完成支付。

2.发票开具要求

乙方应在甲方付款前向甲方开具增值税普通发票，否则甲方有权暂不付款且不承担逾期付款的违约责任。

3.特殊计费周期调整

如因项目实际需求或政策调整等原因，需变更结算周期，应由一方提出书面申请，并说明调整理由。经双方协商一致后，可签订补充协议调整支付周期，补充协议与本合同具有同等法律效力。

4.财政免责条款

因财政预算调整、资金拨付延迟等不可归责于甲方的原因导致支付延迟的，甲方应积极履行资金申请、协调义务，在合理范围内尽最大努力推进款项落实，除因法定不可抗力外，须在具备支付条件后15个工作日内完成款项支付，乙方不得降低服务质量、中断服务，乙方不因此追究任何甲方责任。

5.乙方收款账户信息

银行账户名称：

银行账号：。

1. **乙方义务**

1.乙方需按照投标文件响应内容，安排专人负责与甲方对接本合同约定的相关工作，确保乙方按时保质完成工作，乙方安排人员未经甲方书面同意，不得随意更换。

2.乙方保证所有项目符合国家标准以及行业标准。

3.乙方严格遵守中华人民共和国法律、法规及合同对有关技术资料及技术的要求。

4.乙方确保其提供的本合同项下的所有服务所涉及的产品、技术、资料不会侵犯第三方的知识产权或所有权，否则由此造成的损失，由乙方承担全部责任。乙方派出人员在甲方服务期间，因故意或过失给甲方造成相应损失的，乙方应承担相应的赔偿责任。

5.乙方应按照本合同约定完成相关建设和提供云服务，确保服务质量符合本合同约定或甲方合理要求。

6.部署在政务云平台上的各部门业务系统、所有数据的所有权及使用权均属于政府，乙方无权对其进行支配，若发现乙方未经许可对业务系统和数据进行采集和使用，政务云管理单位将对其采取惩罚措施并追究其法律责任。

7.乙方有义务配合甲方根据工作需要，对其提供服务情况及项目服务使用情况进行的监督和检查，出现问题的应及时整改。

8.乙方负责管理甲方提供的IP地址，为政务云使用单位提供IP地址分配和管理服务。

9.乙方应协助甲方建立健全配套制度标准，包括：政务云管理办法、运维制度、应急预案、安全保障制度、运行监管办法等。

10.乙方应具备为政务云使用单位提供优质及定制化服务的能力，满足云使用单位方了解、使用、监控自身采购云资源的情况等需求。

11.乙方不得在政务云内搭建自身业务系统和非政务业务系统。

1. **知识产权**

1.乙方保证乙方提供的服务不存在任何侵犯第三方知识产权的情形。如果第三方声称乙方向甲方提供的服务侵犯其知识产权，并已就此对甲方或乙方提起（包括威胁提起或很可能提起）法律诉讼程序或知识产权行政执法程序（简称侵权诉讼），则知悉上述事项的一方应立即通知合同对方，甲乙双方协商一致后，甲方有权：（1）暂停履行对侵权诉讼所涉服务的采购或支付义务直至侵权诉讼完全解决，并要求乙方自担费用向甲方提供与该第三方协商、诉讼、和解所需的一切协助（包括但不限于向甲方提供证明侵权不存在的各类证据、派出人员参加协商、诉讼或会谈等）；（2）甲方有权在经得乙方书面同意确认后选择与该第三方达成和解，并由乙方支付和解协议所约定的全部费用以及甲方因侵权诉讼而遭受的全部损失或费用（包括但不限于诉讼/仲裁费、律师费、交通费、通讯费、差旅费、对第三方的损害赔偿金、行政处罚罚款、获取该服务相应使用许可的费用、因停止使用或修改、替换侵权威胁所涉及的服务而遭受的损失等）。如果甲方选择继续参加侵权诉讼法律程序，乙方应当赔偿甲方因侵权诉讼及履行生效法律裁判而需支付的费用或遭受的损失，但生效法律裁判认定乙方服务不存在侵犯第三方知识产权情形的除外。

2.甲方在本项目中自行开发、研制形成的技术成果（包括但不限于程序、文件、资料等）的知识产权归甲方所有。

3.不论本合同是否解除或终止，本合同项下第六条独立适用。

1. **保密义务**

1.任何一方（“接收方“）应对其知晓的甲方的商业、技术、市场、管理、人事、财务等任何方面的信息和资料予以保密，未经另一方事先书面同意，不得披露、使用或以任何方式处置上述信息、资料，并应促使其员工、关联方承担相同保密义务，如果接收方员工、关联方违反上述保密义务，视为接收方违反保密义务并适用本条第2点的约定。

2.任何一方违反保密义务的，应当对另一方因此所遭受的损失承担赔偿责任。如果违约方在本合同有效期内违反保密义务，守约方有权单方提前终止本合同。

3.不论本合同是否解除或终止，本合同项下第七条独立适用。

1. **不可抗力**

1.由于发生不可抗力事件（如战争、暴动、严重火灾、水灾、台风、地震、政府行为和禁令等事件），致使合同任一方不能履行合同义务时，遭受不可抗力事件影响的一方负有在不可抗力事件发生之日起15日内尽快通知合同对方以减轻可能给对方造成的损失，并应当在合理期限内提供证明。

2.遭受不可抗力事件影响的一方在履行前述义务后免除违约责任，但其合同义务不因此免除。经合同双方协商同意，合同履行时间可合理延长，延长时间相当于因事件发生受到影响的时间。

1. **违约责任**

1.一般违约：乙方违反本合同约定义务的，甲方有权要求乙方在指定期限内采取弥补措施，乙方未能弥补的，视为乙方违约，乙方应向甲方支付相当于合同总金额【5%】的违约金。

2.严重违约：乙方服务期间出现安全合规不达标、擅自变更配置，导致甲方重大损失的，支付合同总金额【10%】违约金；

3.根本违约：乙方未按照本合同约定提供专业技术人员团队，经甲方通知后，应及时予以改正，经甲方通知后仍不改正的或上述情况累计发生3次以上的，乙方应向甲方支付该项服务费总额【20%】的违约金。

4.任何一方基于本协议承担的损失赔偿责任上限原则上不超过就引起该责任的部分产品或者服务实际收取的费用；就按照年度收取服务费的产品和服务而言，任何一方基于本协议承担的损失赔偿责任上限不超过自损失确定之日前连续十二（12）个月内、就引起该责任的部分产品和服务收取的相应服务费用的总额。

1. **争议管辖**

本合同项下发生的争议，由双方当事人协商解决；协商不成的，依法向甲方所在地人民法院起诉。

1. 本合同自双方法定代表人或授权代表人签字并加盖公章之日起生效。本合同壹式**肆**份，双方各执**貳**份，具有同等法律效力。本合同的任何变更、补充或修改，应由双方协商一致并签署书面协议。
2. **通知与送达**

任何一方根据本合同规定向另一方发出的通知应以书面形式作出，并以邮寄/快递、传真、专人送达方式发送。如以邮寄/快递方式发送，以邮寄/快递回执上注明的收件日期为送达日期。如以传真方式发送，收到传真机发出的确认信息后，视为送达。如专人送达，被送达人签署后，视为送达。各方联系信息以本合同首部所列为准，一方联系信息变化后，该方应在联系信息变化之前将变化情况书面通知其他方，否则该方应自行承担相应的风险、责任和后果。

1. 本合同中出现的“日”，除非明确写明为工作日，否则为自然日。
2. 本合同附件作为本合同内容的一部分，与本合同具有同等法律效力。
3. 如甲方因为机构调整变更主体，由变更后的主体继续履行本合同项下的内容。

附件一：《投标文件技术应答部分》

附件二：《验收标准》

附件三：《合作伙伴廉政协议》

（本页为签署页）

**甲方：北京市怀柔区政务服务和数据管理局**

（公章）

授权代表人（签字）：

【】年【】月【】日

**乙方：**

（公章）

法定代表人或者授权代表人（签字）：

【】年【】月【】日

附件一：《投标文件技术应答部分》

附件二：《验收标准》

按照要求，乙方提供云服务，并向甲方提供：

1.应急预案及云平台管理规范；

2.每月提供月度报告，内容包括：云平台和云资源使用情况分析报告；

3.每季度提供云平台故障记录、巡检、运维、故障排除记录；

4.年度项目总结报告；

5.其他材料（中标方可根据实际情况提供项目材料）。

附件三：

**合作伙伴廉政协议**

为共同维护商业活动公平竞争秩序，保证双方在业务交往活动中做到诚信、廉洁、高效和共赢，特订本协议如下：

1、双方在合作过程中，自觉遵守国家法律、法规，按照《中华人民共和国反不正当竞争法》、《中华人民共和国招标投标法》、《关于禁止商业贿赂行为的暂行规定》以及其他相关法律规定开展商业交易活动。

2、在供应商资格预审、投标、开标与评标等过程中，做到公平、公正、公开，禁止暗箱操作。甲方监察部门或其授权人员按照规定对招投标项目实施监督，对于乙方有关招投标的投诉和举报，监察部门认真调查，秉公处理，及时回复。

3、双方相关工作人员及其亲属，不得收受对方馈送的现金、贵重物品、有价证券等，不得要求或接受对方为其住房建修、婚丧嫁娶、出国等提供资助，不得介绍亲友从事与双方合作有关的业务活动，不得收受回扣，不得参加影响公正执行公务的高档娱乐、宴请、健身或旅游活动，不得由对方报销应由本人支付的费用。

4、双方相关工作人员不得为谋取私利私下就材料供应、数量变化、材料质量问题处理等进行私下商谈或者达成默契。

5、不做违反商业道德、扰乱正常竞争秩序、有损双方形象的事情，不围标、串标，不泄露双方机密，不排挤其他经营者的公平竞争，不在预决算、招投标和商务报价中弄虚作假或恶意高估冒算。

6、双方人员发现对方人员有受贿或索贿行为以及徇私舞弊、滥用职权、严重渎职等情况时，有义务向对方监察或相应部门举报。

7、乙方若违反廉政协议将被列入廉政黑名单，甲方将视情节轻重，停止该项目或类似项目的合作，一至三年内不再邀请其投标或比选，不再开展新的业务合作。

8、甲方人员若违反廉政协议，造成公司重大损失或恶劣影响的部门和人员，将按照相关规定进行处理，对于涉嫌犯罪的，按照有关程序移送司法机关。

甲方举报渠道乙方举报渠道

电话：

**第七章投标文件格式**

投标人编制文件须知

1、全部声明和问题的回答及所附材料必须是真实的、准确的和完整的。

**一、资格证明文件格式**

**投标文件（资格证明文件）封面**

**投标文件**

**（资格证明文件）**

**项目名称:**

**项目编号/包号：**

**投标人名称：**

**1满足《中华人民共和国采购法》第二十二条规定及法律法规的其他规定**

**1-1营业执照等证明文件**

### 1-2投标人资格声明书

**投标人资格声明书**

致：采购人或采购代理机构

在参与本次项目投标中，我单位承诺：

1. 具有良好的商业信誉和健全的财务会计制度；
2. 具有履行合同所必需的设备和专业技术能力；
3. 有依法缴纳税收和社会保障资金的良好记录；
4. 参加采购活动前三年内，在经营活动中没有重大违法记录（重大违法记录指因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，不包括因违法经营被禁止在一定期限内参加采购活动，但期限已经届满的情形）；
5. 我单位不属于采购法律、行政法规规定的公益一类事业单位、或使用事业编制且由财政拨款保障的群团组织（仅适用于政府购买服务项目）；
6. 我单位不存在为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后，再参加该采购项目的其他采购活动的情形（单一来源采购项目除外）；
7. 与我单位存在“单位负责人为同一人或者存在直接控股、管理关系”的其他法人单位信息如下（如有，不论其是否参加同一合同项下的采购活动均须填写）：

|  |  |  |
| --- | --- | --- |
| 序号 | 单位名称 | 相互关系 |
| 1 |  |  |
| 2 |  |  |
| … |  |  |

上述声明真实有效，否则我方负全部责任。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

说明：投标人承诺不实的，依据《采购法》第七十七条“提供虚假材料谋取中标、成交的”有关规定予以处理。

**2落实采购政策需满足的资格要求（如有）**

**2-1中小企业声明函**

说明：

（1）如本项目（包）不专门面向中小企业预留采购份额，资格证明文件部分无需提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件；供应商如具有上述证明文件，建议在商务技术文件中提供。

（2）如本项目（包）专门面向中小企业采购，投标文件中须提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，且建议在资格证明文件部分提供。

（3）如本项目（包）预留部分采购项目预算专门面向中小企业采购，且要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业的，如供应商因落实政府采购政策拟进行分包的，投标文件中除须提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，还须同时提供《拟分包情况说明》及《分包意向协议》，且建议在资格证明文件部分提供。

（4）如本项目（包）预留部分采购项目预算专门面向中小企业采购，且要求供应商以联合体形式参加采购活动，如供应商为联合体的，投标文件中除须提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，还须同时提供《联合协议》；上述文件建议在资格证明文件部分提供。

（5）中小企业声明函填写注意事项

1）《中小企业声明函》由参加政府采购活动的投标人出具。联合体投标的，《中小企业声明函》可由牵头人出具。

2）对于联合体中由中小企业承担的部分，或者分包给中小企业的部分，必须全部由中小企业制造、承建或者承接。供应商应当在声明函“标的名称”部分标明联合体中中小企业承担的具体内容或者中小企业的具体分包内容。

3）对于多标的采购项目，投标人应充分、准确地了解所提供货物的制造企业、提供服务的承接企业信息。对相关情况了解不清楚的，不建议填报本声明函。

（6）温馨提示：为方便广大中小企业识别企业规模类型，工业和信息化部组织开发了中小企业规模类型自测小程序，在国务院客户端和工业和信息化部网站上均有链接，投标人填写所属的行业和指标数据可自动生成企业规模类型测试结果。本项目中小企业划分标准所属行业详见第二章《投标人须知资料表》，如在该程序中未找到本项目文件规定的中小企业划分标准所属行业，则按照《关于印发中小企业划型标准规定的通知（工信部联企业﹝2011﹞300号）》及《金融业企业划型标准规定》（〔2015〕309号）等国务院批准的中小企业划分标准执行。

### 2-1-1中小企业声明函及残疾人福利性单位声明函格式

**中小企业声明函（服务）格式**

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

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

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_\_\_\_

|  |
| --- |
| 1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。 |

**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采购政策的通知》（财库〔2017〕141号）的规定，本单位**（请进行勾选）**：

**□不属于符合条件的残疾人福利性单位。**

**□属于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：

### 2-1-2拟分包情况说明及分包意向协议

**拟分包情况说明**

致：（采购人或采购代理机构）

我单位参加贵单位组织采购的项目编号为\_\_\_\_\_\_\_的\_\_\_\_\_\_\_\_\_项目（填写采购项目名称）中\_\_\_包（填写包号）的投标。拟签订分包合同的单位情况如下表所示，我单位承诺一旦在该项目中获得采购合同将按下表所列情况进行分包，同时承诺分包承担主体不再次分包。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 分包承担  主体名称 | 分包承担  主体类型  （选择） | 资质等级 | 拟分包  合同内容 | 拟分包  合同金额  （人民币元） | 占  **合同金额的**  比例（%） |
| 1 |  | □中型企业  □小微企业  □其他 |  |  |  |  |
| 2 |  | □中型企业  □小微企业  □其他 |  |  |  |  |
| … |  |  |  |  |  |  |
| 合计： | | | | |  |  |

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

注：

如本招标文件《投标人须知资料表》载明本项目分包承担主体应具备的相应资质条件，则投标人须在本表中列明分包承担主体的资质等级，并后附资质证书电子件，否则**投标无效**。

**分包意向协议**

甲方（投标人）：\_\_\_\_\_\_\_\_

乙方（拟分包单位）：\_\_\_\_\_\_\_\_

甲方承诺，一旦在\_\_\_\_\_\_\_\_\_（采购项目名称）（项目编号/包号为：\_\_\_\_\_\_\_）招标采购项目中获得采购合同，将按照下述约定将合同项下部分内容分包给乙方：

1.分包内容：\_\_\_\_\_。

2.分包金额：\_\_\_\_\_，该金额占该采购包合同金额的比例为\_\_\_%。

乙方承诺将在上述情况下与甲方签订分包合同。

本协议自各方盖章之日起生效，如甲方未在该项目（采购包）中标，本协议自动终止。

甲方（盖章）：\_\_\_\_\_\_\_\_\_乙方（盖章）：\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

注：

本协议仅在投标人“为落实政府采购政策”而向中小企业分包时必须提供，否则**投标无效**；且投标人须与所有拟分包单位分别签订《分包意向协议》，每单位签订一份，并在投标文件中提交全部协议原件的电子件，否则**投标无效**。

**2-2其它落实采购政策的资格要求（如有）**

**3本项目的特定资格要求**

3-1联合协议（如有）

**联合协议**

\_\_\_\_\_\_、\_\_\_\_\_及\_\_\_\_\_就“\_\_\_\_\_\_\_\_（项目名称）”\_\_\_\_包招标项目的投标事宜，经各方充分协商一致，达成如下协议：

1. 由\_\_\_\_\_\_\_\_\_牵头，\_\_\_\_\_\_\_\_\_、\_\_\_\_\_\_\_\_\_\_参加，组成联合体共同进行招标项目的投标工作。
2. 联合体中标后，联合体各方共同与采购人签订合同，就采购合同约定的事项对采购人承担连带责任。
3. 联合体各方均同意由牵头人代表其他联合体成员单位按招标文件要求出具《授权委托书》。
4. 牵头人为项目的总负责单位；组织各参加方进行项目实施工作。
5. \_\_\_\_\_\_负责\_\_\_\_\_，具体工作范围、内容以投标文件及合同为准。
6. \_\_\_\_\_\_负责\_\_\_\_\_，具体工作范围、内容以投标文件及合同为准。
7. \_\_\_\_\_\_负责\_\_\_\_\_（如有），具体工作范围、内容以投标文件及合同为准。
8. 本项目联合协议合同总额为\_\_\_\_\_\_\_\_元，联合体各成员按照如下比例分摊（按联合体成员分别列明）：

## （1）\_\_\_\_\_\_为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为\_\_\_\_\_元；

## （2）\_\_\_\_\_\_为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为\_\_\_\_\_元；

## （…）\_\_\_\_\_\_为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为\_\_\_\_\_元。

1. 以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。
2. 其他约定（如有）：\_\_\_\_\_\_\_。

## 本协议自各方盖章后生效，采购合同履行完毕后自动失效。如未中标，本协议自动终止。

联合体牵头人名称：\_\_\_\_\_\_ 联合体成员名称：\_\_\_\_\_\_

盖章：\_\_\_\_\_\_盖章：\_\_\_\_\_\_

联合体成员名称：\_\_\_\_\_\_

盖章：\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

注：

1.如本项目（包）接受供应商以联合体形式参加采购活动，且供应商以联合体形式参与时，须提供《联合协议》，否则**投标无效**。

2.联合体各方成员需在本协议上共同盖章。

**3-2其他特定资格要求**

## 请提供供应商近三年无行贿犯罪行为承诺书（格式自拟）

**4、投标费用承诺函**

致:北京市怀柔区公共资源交易中心（北京市怀柔区政府采购中心）

我公司应承担所有与准备和参加投标有关的费用。不论投标的结果如何，采购人和采购代理机构均无义务和责任承担这些费用(投标人提供针对本条款的承诺函并加盖公章）

单位名称（盖章）**:**

日期**:**

**二、商务技术文件格式**

**投标文件（商务技术文件）封面**

**投标文件**

**（商务技术文件）**

**项目名称:**

**项目编号/包号：**

**投标人名称**

**1投标书**

**投标书**

致：（采购人或采购代理机构）

我方参加你方就\_\_\_\_\_\_\_\_\_\_\_（项目名称，项目编号）组织的招标活动，并对此项目进行投标。

1.我方已详细审查全部招标文件，自愿参与投标并承诺如下：

（1）本投标有效期为自提交投标文件的截止之日起\_\_\_\_\_个日历日。

（2）除合同条款及采购需求偏离表列出的偏离外，我方响应招标文件的全部要求。

（3）我方已提供的全部文件资料是真实、准确的，并对此承担一切法律后果。

（4）如我方中标，我方将在法律规定的期限内与你方签订合同，按照招标文件要求提交履约保证金，并在合同约定的期限内完成合同规定的全部义务。

2.其他补充条款（如有）：\_\_\_\_\_\_\_\_\_\_\_。

与本投标有关的一切正式往来信函请寄：

地址\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_传真\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

电话\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_电子函件\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

投标人名称（加盖公章）\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日**2授权委托书**

**授权委托书**

本人\_\_\_\_\_\_\_（姓名）系\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（投标人名称）的法定代表人（单位负责人），现委托\_\_\_\_\_\_\_（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（标的名称）响应文件和处理有关事宜，其法律后果由我方承担。

委托期限：自本授权委托书签署之日起至响应有效期届满之日止。

代理人无转委托权。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

法定代表人（单位负责人）（签字或签章或印鉴）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

委托代理人（签字或签章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

附：法定代表人（单位负责人）及委托代理人身份证明文件电子件：

说明：

1.若供应商为事业单位或其他组织或分支机构，则法定代表人（单位负责人）处的签署人可为单位负责人。

2.若投标文件中签字之处均为法定代表人（单位负责人）本人签署，则可不提供本《授权委托书》，但须提供《法定代表人（单位负责人）身份证明》；否则，不需要提供《法定代表人（单位负责人）身份证明》。

3.供应商为自然人的情形，可不提供本《授权委托书》。

4.供应商应随本《授权委托书》同时提供法定代表人（单位负责人）及委托代理人有效的身份证或护照等身份证明文件电子件。提供身份证的，应同时提供身份证**双面**电子件章。

**附：法定代表人（单位负责人）身份证明**

致：（采购人或采购代理机构）

兹证明，

姓名：\_\_\_\_性别：\_\_\_\_年龄：\_\_\_\_职务：\_\_\_\_

系 （投标人名称）的法定代表人（单位负责人）。

附：法定代表人（单位负责人）有效期内的身份证正反面电子件。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

法定代表人（单位负责人）（签字或签章或印鉴）：\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

**3开标一览表**

**开标一览表**

项目编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目名称：\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **投标人名称** | **投标报价** | |
| **大写** | **小写** |
|  |  |  |  |

注：1.此表中，每包的投标报价应和《投标分项报价表》中的总价相一致。

2.本表必须按包分别填写。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

**4投标分项报价表**

**投标分项报价表**

项目编号：\_\_\_\_\_\_\_\_\_\_\_项目名称：\_\_\_\_\_\_\_\_\_\_报价单位：人民币元

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **分项名称** | **单价（元）** | **数量** | **合价（元）** | **备注/说明** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **3** | **…** |  |  |  |  |
| **总价（元）** | | | |  |  |

注：1.本表应按包分别填写。

2.如果不提供分项报价将视为没有实质性响应招标文件。

3.上述各项的详细规格（如有），可另页描述。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

**5合同条款偏离表**

**合同条款偏离表**

项目编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **对本项目合同条款的偏离情况（请进行勾选）：**  **□无偏离**（如无偏离，仅勾选无偏离即可）  **□有偏离**（如有偏离，则应在本表中对偏离项逐一列明） | | | | | |
| 序号 | 招标文件条目号和页码 | 招标文件要求 | 投标文件内容 | 偏离情况 | 说明 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：

1.对合同条款中的所有要求，除本表所列明的所有偏离外，均视作投标人已对之理解和响应。

2.“偏离情况”列应据实填写“正偏离”或“负偏离”。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

**6采购需求偏离表**

**采购需求偏离表**

项目编号/包号：项目名称：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 招标文件条目号(页码) | 招标文件要求 | 投标响应内容 | 偏离情况 | 说明 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：

1. 对招标文件中的所有商务、技术要求，除本表所列明的所有偏离外，均视作供应商已对之理解和响应。若本表为空，则表示应答人“全部满足”招标文件相应要求；
2. 若存在偏离情况，应答人应逐行填写存在偏离的条款并逐列填写对应的响应情况，优于招标文件要求的应在说明处写明“正偏离”，部分满足或不满足的条款应写明“负偏离”，对未提及的条款，视为“无偏离”。
3. “偏离情况”列应据实填写“无偏离”、“正偏离”或“负偏离”。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

**7类似项目业绩**

项目编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 采购人名称 | 项目名称 | 合同签订时间 | 合同金额（万元） | 联系方式 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

应附：

1.有效证明材料：业绩合同关键页（含：首页、服务内容信息页、合同金额页、签字盖章页）。复印件加盖公章，时间以合同签订日期为准。合同签订方必须是投标人自身，存在控股、管理关系投标人之间签订的合同无效，不符合上述要求或未按要求提供有效证明文件的业绩在评审时将不予承认。

2.项目业绩以合同为准，同一项目不同年限不重复计算。

3.投标人提供虚假信息、虚假合同的，按**虚假投标处理**。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

**8招标文件要求提供或投标人认为应附的其他材料**