北京市政府采购项目
公开招标文件

项目名称：北京市规划和自然资源委员会 2026 年政务云租用

采购编号：BGPC-G25316

采 购 人：北京市规划和自然资源委员会

采购代理机构：北京市公共资源交易中心（北京市政府采购中心）

目　　录

注：采购文件条款中以 “✡”形式标记的内容适用于本项目，以“□”形式标记的内容不适用于本项目。

第一章　投标邀请

一、项目基本情况

1.采购编号：BGPC-G25316

2.项目名称：北京市规划和自然资源委员会 2026 年政务云租用

3.项目预算金额：2000 万元

4.采购需求：

包号	标的名称	采购包 预算金额 （万元）	数量	简要技术需求或服务要求
1	北京市规划和自然资源委员会 2026 年政务云租用	2000	1	详见第五章采购需求

5. 服务期限：提供 12 个月的政务云资源租用服务，自 2026 年 1 月 1 日起，至 2026 年 12 月 31 日止。

合同履行期限：2026 年 1 月 1 日起至 2027 年 3 月 31 日止（包含履约验收相关工作）。

6.本项目是否接受联合体投标：□是　☑否。

二、申请人的资格要求（须同时满足）

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中小/小微企业制造、服务全部由符合政策要求的中小/小微企业承接（允许分包的项目，分包承担主体应当同时满足本款对应的中小/小微企业要求）。其中，专门面向中小企业且需预留小微企业份额的（如有），预留份额通过以下措施进行：_____/_____。

□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：

根据工业和信息化部《关于督促互联网网络接入服务企业依法持证经营的通知》工信管函〔2018〕84 号文件精神，投标人应取得互联网资源协作服务业务许可：

投标人须提供《中华人民共和国增值电信业务经营许可证》复印件：

该许可证中的“业务种类（服务项目）及覆盖范围中”须包含第一类增值电信业务中的“互联网数据中心业务”或“互联网数据中心业务（不含互联网资源协作服务）”或“互联网数据中心业务（仅限互联网资源协作服务）”，机房所在地均须包含“北京”；

投标人提供的《中华人民共和国增值电信业务经营许可证》复印件中的表述内容符合上述情形的均合格。

三、获取招标文件

1.时间：2025 年 11 月 19 日至 2025 年 11 月 26 日，每天上午 00:00 至 12:00，下午 12:00 至 24:00（北京时间，法定节假日除外）。

2.地点：北京市政府采购电子交易平台

3.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。

4.售价：0 元。

四、提交投标文件截止时间、开标时间和地点

投标截止时间、开标时间：2025 年 12 月 10 日 9 点 30 分（北京时间）。

地点：北京市政府采购电子交易平台（http://zbcg-bjzc.zhongcy.com/bjczj-portal-site/index.html#/home）。

注意事项：为保证开标解密顺利进行，请投标人务必远程参加并保持联系人电话畅

通，同时确保使用制作上传本项目电子投标文件的计算机设备及自身 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自行进行解密操作。

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

1.本项目需要落实的政府采购政策：如涉及的详见招标文件各章对应条款要求。

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。

七、对本次招标提出询问和质疑，请按以下方式联系。

1.采购人信息

名　　称：北京市规划和自然资源委员会

地　　址：北京市通州区承安路 1 号院

询问和质疑联系人：贺老师

联系方式：010-55594486

2.采购代理机构信息

名　　称：北京市公共资源交易中心

询问联系人：李老师

联系方式：010-83916677

地　　址：北京市丰台区玉林里 45 号腾飞大厦

质疑联系人：魏老师

联系方式：010-83537377

地　　址：北京市西城区广安门南街甲 68 号 407 室（邮编：100054）

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。

<table>
<tr><th>条款号</th><th>条目</th><th>内容</th></tr>
<tr><td>2.2</td><td>项目属性</td><td>项目属性：
☑服务
□货物</td></tr>
<tr><td>2.3</td><td>科研仪器设备</td><td>是否属于科研仪器设备采购项目：
□是
☑否</td></tr>
<tr><td>2.4</td><td>核心产品</td><td>☑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：____。</td></tr>
<tr><td rowspan="2">3.1</td><td>现场考察</td><td>☑不组织
□组织，考察时间：__年_月_日_点_分
考察地点：_____。</td></tr>
<tr><td>开标前答疑会</td><td>☑不召开
□召开，召开时间：__年_月_日_点_分
召开地点：_____。</td></tr>
<tr><td>4.1</td><td>样品</td><td>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）：_____。</td></tr>
<tr><td>5.2.5</td><td>标的所属行业</td><td>本项目采购标的对应的中小企业划分标准所属行业：
<table>
<tr><th>包号</th><th>标的名称</th><th>中小企业划分标准所属行业</th></tr>
<tr><td>1</td><td>北京市规划和自然资源委员会2026年政务云租用</td><td>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</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>条款号</th><th>条目</th><th>内容</th></tr>
<tr><td></td><td></td><td><table>
<tr><td></td><td></td><td>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。</td></tr>
</table></td></tr>
<tr><td>11.2</td><td>投标报价</td><td>投标报价的特殊规定：
☑无
□有，具体情形：_____。</td></tr>
<tr><td>12.1</td><td>投标保证金</td><td>投标保证金金额：无须提交</td></tr>
<tr><td>13.1</td><td>投标有效期</td><td>自提交投标文件的截止之日起算 180 日历天。</td></tr>
<tr><td>18.2</td><td>解密时间</td><td>解密时间：__120__分钟</td></tr>
<tr><td>22.1</td><td>确定中标人</td><td>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，技术部分评审得分相同的，以披露 2023 年度或 2024 年度 ESG 报告的（当且仅当得分相同的中标候选人均已在 2023 年度或 2024 年度运行一个完整自然年度时适用本条款）中标候选人为中标人。（请已经披露 2023 年度或 2024 年度 ESG 报告的投标人提供相应网页截图及网址。）
□随机抽取</td></tr>
<tr><td>25.5</td><td>分包</td><td>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：
①可分包部分特定资格要求：_____；
②可分包部分标的对应的中小企业划分标准所属行业：<table>
<tr><td>包号</td><td>可分包部分标的名称</td><td>中小企业划分标准所属行业</td></tr>
<tr><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>25.6</td><td>政采贷</td><td>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”。</td></tr>
<tr><td>26.1</td><td>询问</td><td>询问形式：电话、北京市政府采购电子交易平台或其他方式</td></tr>
</table>

条款号	条目	内容
		联系方式： 1、采购人：详见招标文件第一章投标邀请“七”。 2、采购代理机构：详见招标文件第一章投标邀请“七”。
26.2	质疑	质疑送达形式：书面形式 具体要求详见 26.2.3-26.2.5
		联系方式： 1、采购人：详见招标文件第一章投标邀请“七”。 2、采购代理机构： ① 联系部门：北京市公共资源交易中心法律事务部（监督服务部） ② 地址：北京市西城区广安门南街甲 68 号 407 室（邮编：100054） ③ 联系人：魏老师 联系方式：010-83537377
27	代理费	无

投标人须知

一　说　明

1　采购人、采购代理机构、投标人、联合体

1.1　采购人、采购代理机构：指依法进行政府采购的国家机关、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》。

1.2　投标人（也称“供应商”、“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。

1.3　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，以一个供应商的身份共同参加政府采购。

2　资金来源、项目属性、科研仪器设备采购、核心产品

2.1　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。

2.2　项目属性见《投标人须知资料表》。

2.3　是否属于科研仪器设备采购见《投标人须知资料表》。

2.4　核心产品见《投标人须知资料表》。

3　现场考察、开标前答疑会

3.1　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。

3.2　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

4.1　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》。

4.2　样品的评审方法以及评审标准等内容见第四章《评标程序、评标方法和评标标准》。

5　政府采购政策（包括但不限于下列具体政策要求）

5.1　采购本国货物、工程和服务

5.1.1 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。

5.1.2 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》。

5.1.3 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）。

5.2 中小企业、监狱企业及残疾人福利性单位

5.2.1 中小企业定义：

5.2.1.1 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。

5.2.1.2 供应商提供的货物、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。

5.2.1.3 在货物采购项目中，供应商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。

5.2.1.4 以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

5.2.2 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。

5.2.3 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：

5.2.3.1 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）；

5.2.3.2 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；

5.2.3.3 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；

5.2.3.4 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；

5.2.3.5 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）；

5.2.3.6 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。

5.2.4 本项目是否专门面向中小企业预留采购份额见第一章《投标邀请》。

5.2.5 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》。

5.2.6 小微企业价格评审优惠的政策调整：见第四章《评标程序、评标方法和评标标准》。

5.3 政府采购节能产品、环境标志产品

5.3.1 政府采购节能产品、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。

5.3.2 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。关于政府采购节能产品、环境标志产品的相关规定依据《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9 号）。

5.3.3 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**；

5.3.4 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第四章《评标程序、评标方法和评标标准》（如涉及）。

5.4 正版软件

5.4.1 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）。

5.5 网络安全专用产品

5.5.1 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。

5.6 推广使用低挥发性有机化合物（VOCs）

5.6.1 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政府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，供应商应执行符合本市和国家的 VOCs 含量限制标准（具体标准见第五章《采购需求》），否则**投标无效**；属于推荐性标准的，优先采购，具体见第四章《评标程序、评标方法和评标标准》。

5.7 采购需求标准

5.7.1 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》。

5.7.2 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》。

5.8 强制性产品认证

5.8.1 如本项目采购产品属于《强制性产品认证目录》的产品，则投标人所报产品必须获得经国家市场监督管理总局指定的认证机构出具的、处于有效期之内的强制性产品认证证书，否则**投标无效**。

6 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

7 招标文件构成

7.1 招标文件包括以下部分：

第一章 投标邀请

第二章 投标人须知

第三章 资格审查

第四章 评标程序、评标方法和评标标准

第五章 采购需求

第六章 拟签订的合同文本

第七章 投标文件格式

7.2 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**。

8 对招标文件的澄清或修改

8.1 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。

8.2 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。

8.3 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

9　投标范围、投标文件中计量单位的使用及投标语言

9.1　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分投标，否则其对该采购包的投标将被认定为**无效投标**。

9.2　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。

9.3　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。

10　投标文件构成

10.1　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》。

10.2　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。

10.3　第四章《评标程序、评标方法和评标标准》中涉及的证明文件。

10.4　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。

10.5 投标人认为应附的其他材料。

11 投标报价

11.1 所有投标均以人民币为计价货币。

11.2 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。

11.2.1 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；

11.2.2 按照招标文件要求完成本项目的全部相关费用。

11.3 采购人不得向供应商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。

11.4 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**。

12 投标保证金（本项目不涉及）

12.1 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。

12.2 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。

12.3 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**。

12.4 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”。

12.5 投标保证金有效期同投标有效期。

12.6 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。

12.7 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：

12.7.1 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；

12.7.2 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；

12.7.3 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；

12.7.4 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。

12.8 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：

12.8.1 投标有效期内投标人撤销投标文件的；

12.8.2 《投标人须知资料表》中规定的其他情形。

13 投标有效期

13.1 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**。

14 投标文件的签署、盖章

14.1 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。

14.2 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

15 投标文件的提交

15.1 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。

15.2 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。

16 投标截止时间

16.1 投标人应在招标文件要求提交投标文件截止时间前，将电子投标文件提交至电子交易平台。

17 投标文件的修改与撤回

17.1 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。

17.2 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

18 开标

18.1 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。

18.2 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**。

18.3 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。

18.4 投标人对开标过程和开标记录有疑义，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。

18.5 投标人不足 3 家的，不予开标。

19 资格审查

19.1 见第三章《资格审查》。

20 评标委员会

20.1 评标委员会根据政府采购有关规定和本次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。

20.2 评审专家须符合《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125 号）的规定。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。

21 评标程序、评标方法和评标标准

21.1 见第四章《评标程序、评标方法和评标标准》。

六 确定中标

22 确定中标人

22.1 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。

23 中标公告与中标通知书

23.1 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。

23.2 中标通知书对采购人和中标供应商均具有法律效力。中标通知书发出后，采购人改变中标结果的，或者中标供应商放弃中标项目的，应当依法承担法律责任。

23.3 中标公告发布后，未中标供应商可在北京市政府采购电子交易平台查询本单位未通过资格性和符合性审查原因、评审得分与排序等相关信息。

24 废标

24.1 在招标采购中，出现下列情形之一的，应予废标：

24.1.1 符合专业条件的供应商或者对招标文件作实质响应的供应商不足三家的；

24.1.2 出现影响采购公正的违法、违规行为的；

24.1.3 投标人的报价均超过了采购预算，采购人不能支付的；

24.1.4　因重大变故，采购任务取消的。

24.2　废标后，采购人将废标理由书面通知所有投标人。

25 签订合同

25.1　中标人、采购人应当自中标通知书发出之日起 30 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。

25.2　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，也可以重新开展政府采购活动。

25.3　联合体中标的，联合体各方应当共同与采购人签订合同，就采购合同约定的事项向采购人承担连带责任。

25.4　政府采购合同不能转包。

25.5　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》。政府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，分包供应商就分包项目承担责任。

25.6　“政采贷”融资指引：详见《投标人须知资料表》。

26 询问与质疑

26.1　询问

26.1.1　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》。

26.1.2　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。

26.2　质疑

26.2.1　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，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。

26.2.2　供应商对招标文件中涉及的项目属性、采购预算、最高限价、划分的

采购包与合同分包、供应商资格条件、采购需求、评审标准、政府采购政策功能落实要求及采购合同等由采购人提出的内容及采购活动结束后对采购结果提出质疑的，由采购人依法作出答复；供应商对政府采购法律法规中规定的政府采购组织程序提出质疑的，由采购代理机构依法作出答复。

26.2.3 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。

26.2.4 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。

26.2.5 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。

26.3 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》。

27 代理费

27.1 收费对象、收费标准及缴纳时间见《投标人须知资料表》。由中标人支付的，中标人须一次性向采购代理机构缴纳代理费，投标报价应包含代理费用。

第三章　资格审查

一、资格审查程序

1　开标结束后，采购人将根据《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《资格证明文件》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《中华人民共和国政府采购法》第二十二条规定	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。	提供证明文件的电子件或电子证照
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》

序号	审查因素	审查内容	格式要求
1-3	投标人信用记录	查询渠道：信用中国网站和中国政府采购网（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、政府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	落实政府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	中小企业政策证明文件	具体要求见第一章《投标邀请》	
2-1-1	中小企业证明文件	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》

序号	审查因素	审查内容	格式要求
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
3	本项目的特定资格要求	如有，见第一章《投标邀请》	
3-1	本项目对于联合体的要求	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 项规定。 3、本表序号 3-3 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供应商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供应商确定资质等级。 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。 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、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”

序号	审查因素	审查内容	格式要求
3-3	其他特定资格要求	如有，见第一章《投标邀请》 注：如联合体中有同类资质的供应商按照联合体分工承担相同工作的，均应当提供资质证书电子件或电子证照。	提供证明文件的电子件或电子证照
4	投标保证金（本项目不涉及）	按照招标文件的规定提交投标保证金。	
5	获取招标文件	在规定期限内通过北京市政府采购电子交易平台获取所参与包的招标文件。 注：如本项目接受联合体，且供应商为联合体时，联合体中任一成员获取文件即视为满足要求。	

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

1.1　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。

1.2　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《商务技术文件》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分投标；
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。 4）采购的产品若属于《强制性产品认证目录》的产品，则投标人所报产品必须获得经国家市场监督管理总局指定的认证机构出具的、处于有效期之内的强制性产品认证证书。
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《政府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。

2 投标文件有关事项的澄清或者说明

2.1 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（若投标人为事业单位或其他组织或分支机构，可为单位负责人）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。

2.2 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**。

2.3 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分投标，其**投标无效**。

2.4 投标文件报价出现前后不一致的，按照下列规定修正：

2.4.1 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 2.4.2-2.4.7 项规定修正。

2.4.2 开标时，在北京市政府采购电子交易平台上显示的投标报价内容与投标文件中相应内容不一致的,以开标时显示的投标报价内容为准；

2.4.3 大写金额和小写金额不一致的，以大写金额为准；

2.4.4 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；

2.4.5 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。

2.4.6 同时出现两种以上不一致的，按照前款规定的顺序修正。

2.4.7 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**。

2.5 落实政府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。

2.5.1 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。

2.5.2 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_4__%的扣除，用扣除后的价格参加评审。

2.5.3 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。

2.5.4 价格扣除比例对小型企业和微型企业同等对待，不作区分。

2.5.5 中小企业参加政府采购活动，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。

2.5.6 监狱企业提供了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的，视同小微企业。

2.5.7 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》的，视同小微企业。

2.5.8 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。

3 投标文件的比较和评价

3.1 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。

3.2 评标方法和评标标准

3.2.1 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。

3.2.2 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：_____

3.2.3 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）__详见第四章评标程序、评标方法和评标标准___。

4 确定中标候选人名单

4.1 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：投标人评审得分相同的，按投标报价由低向高顺序排列。得分且投标报价相同的，以技术部分得分顺序排列。

4.2 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。

4.3 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。

4.4 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。

4.5 □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___名中标候选人。

☑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）评标委员会推荐所有进入评标排序且符合核心产品（如有）要求的投标人为中标候选人。

5 报告违法行为

5.1 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。

二、评标标准

评分部分	评分因素	评分标准	分值	分值属性
价格部分（10分）	价格	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。 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。	10	客观
商务部分（22分）	证书	1、投标人具有有效的质量管理体系认证书、有效的信息安全管理体系认证证书，每提供1个证书得2分，最高得4分（提供以上两个证书复印件）。 2、投标人所投的政务云平台通过网络安全等级保护三级测评，提供测评报告复印件得3分，否则不得分。 3、投标人所提供的云平台通过商用密码应用安全性评估，提供评估报告复印件得2分，否则不得分。 4、投标人所提供云平台通过中央网信办云计算服务安全评估，提供截图证明得3分，否则不得分。	12	客观
	类似业绩	提供2022年1月1日至递交投标文件截止时间具有与本项目类似的案例（以合同签订日期为准），每个得2分，该项最多10分。 注：须提供合同复印件，合同至少包含首页、内容页、金额页、盖章页等关键内容页，不满足以上条件不得分。	10	客观
技术部分（68分）	服务团队	1、投标人提供1名项目负责人（项目经理）、1名技术负责人及不少于9名项目团队人员，提供加盖投标人公章的人员清单得1分。 2、项目组人员（除项目经理和技术负责人之外）拥有中级及以上工程师职称、注册信息安全专业人员证书（CISP）、网络工程师证书、信息安全工程师证书者，每提供一个得0.5分，最多得2分（同一人员不重复得分）。 3、项目经理具有信息系统项目管理师（高级）证书，得2分。	6	客观

		4、技术负责人具备注册信息安全专业人员证书或网络工程师证书得 1 分，未提供证书不得分。 注：提供证书复印件。		
	总体服务方案	总体服务方案 ①需求分析和整体入云方案②基础服务方案③扩展服务方案④VPN 区硬件租用建设服务方案 方案内容详细，专门针对本项目，符合采购需求和实际情况视为完全符合；方案内容属于通用类，非专门针对本项目，部分符合实际情况视为部分符合；方案内容复制粘贴采购需求，非专门针对本项目，不符合实际情况或未提供视为不符合。（每符合 1 点得 1.5 分，部分符合得 0.5 分，不符合不得分；此项最高 6 分）	6	主观
	技术要求	满足技术要求中全部技术指标得 25 分。 ▲代表重要指标 30 项：正偏离或全部无偏离得 15 分；每有 1 项负偏离减 0.5 分，减完为止； #代表比较重要指标 40 项，正偏离或全部无偏离得 10 分；每有 1 项负偏离减 0.25 分，减完为止。 租用防火墙产品（VPN 防火墙、业务域防火墙、数据库域防火墙、管理域防火墙）符合公安部第二代防火墙（GA / T 1177-2014）标准，提供检测报告复印件，每有一项产品符合得 1 分，最高得 4 分。	29	客观
	业务系统及数据迁移承诺函	投标人提供加盖公章的迁移时限承诺，承诺至少应包括满足需求的迁移时间、承诺完成系统迁移部署、承诺满足业务连续性要求。 承诺 1 天内（包含 1 天）完成系统迁移，迁移过程中保证应用系统业务延续不中断，得 4 分； 承诺超过 1 天，但在 3 天内（包含 3 天）完成系统迁移，迁移过程中保证应用系统业务延续不中断，得 3 分； 承诺超过 3 天，但在 5 天内（包含 5 天）完成系统迁移，迁移过程中保证应用系统业务延续不中断，得 2 分； 承诺超过 5 天，但在 7 天内（包含 7 天）完成系统迁移，迁移过程中保证应用系统业务延续不中断，得 1 分； 超过 7 天或未提供完成系统迁移不得分。	4	客观
	业务系	迁移方案	6	主观

	统及数据迁移方案	①系统迁移方案②风险评估方案③应急预案。 方案内容详细，专门针对本项目，符合采购需求和实际情况视为完全符合；方案内容属于通用类，非专门针对本项目，部分符合实际情况视为部分符合；方案内容复制粘贴采购需求，非专门针对本项目，不符合实际情况或未提供视为不符合。（每符合 1 点得 2 分，部分符合得 1 分，不符合不得分；此项最高 6 分）		
	安全服务方案	安全服务方案 ①安全保障措施②安全管理方案。 方案内容详细，专门针对本项目，符合采购需求和实际情况视为完全符合；方案内容属于通用类，非专门针对本项目，部分符合实际情况视为部分符合；方案内容复制粘贴采购需求，非专门针对本项目，不符合实际情况或未提供视为不符合。（每符合 1 点得 3 分，部分符合得 1.5 分，不符合不得分；此项最高 6 分）	6	主观
	运维服务方案	运维服务方案 ①项目团队②应急处置与故障恢复方案③运维保障方案④项目管理方案⑤风险控制方案⑥技术支持方案。 方案内容详细，专门针对本项目，符合采购需求和实际情况视为完全符合；方案内容属于通用类，非专门针对本项目，部分符合实际情况视为部分符合；方案内容复制粘贴采购需求，非专门针对本项目，不符合实际情况或未提供视为不符合。（每符合 1 点得 1 分，部分符合得 0.5 分，不符合不得分；此项最高 6 分）	6	主观
	培训方案	培训方案 ①培训计划②培训方案。 方案内容详细，专门针对本项目，符合采购需求和实际情况视为完全符合；方案内容属于通用类，非专门针对本项目，部分符合实际情况视为部分符合；方案内容复制粘贴采购需求，非专门针对本项目，不符合实际情况或未提供视为不符合。（每符合 1 点得 2 分，部分符合得 1 分，不符合不得分；此项最高 4 分）	4	主观
	本项目中落实 ESG 理念的工作措施	供应商根据项目特点提供本项目落实 ESG 理念工作措施。 措施完整合理、内容详细，专门针对本项目，符合采购需求和实际情况视为符合；方案内容属于通用类，非专门针对本项目，部分符合采购需求和实际情况视为部分符合；方案内容对采购需求进行简单复制、非专门针对本项目，不符合实际情况或未提供视为不符合。 （符合得 1 分，部分符合得 0.5 分，不符合不得分。此	1	主观

		项最高 1 分。）		

第五章　采购需求

一、采购标的

1. 采购标的

序号	租用服务类别	服务项	计价单位	数量
1.	定制化物理服务器	配置 1：2 路 10 核 2.0GHz，192G 内存，2 块 600G SAS 硬盘，2 个 HBA 卡，4 个万兆端口	台	64
2.		配置 2：4 路 10 核 2.0GHz，288G 内存，2 块 600G SAS 硬盘，2 个 HBA 卡，4 个万兆端口	台	23
3.		刀片服务器：4 颗 CPU，8*16GB DDR4，2*600GB 12G SSD 2.5 寸硬盘， 2*10GE 接口卡，2*10Gb FCoE 接口卡，1*RAID 卡，刀片服务器	台	32
4.		（刀片服务器机框）：10*FAN，6*POWER，2*OA 管理模块，单相电源输入，统一基础架构系统，含网卡：4 个 10GB 光模块、4 个 8GB FC 模块、4 个 GE 电口模块。	台	4
5.	小型机物理服务器	配置核心数*处理器主频≥40GHz,256GB 内存,2 块 600G 以上 SSD 硬盘（含操作系统）	台	8
6.	集中式存储 1	SAN 架构存储系统，标配双控制器;配置 48Gb 缓存；配置虚拟资源调配软件、数据迁移软件、数据镜像功能、支持存储虚拟化及存储网关复制功能、块级压缩软件；12 个 16Gb FC 端口，控制器数量*2；企业级 SSD；支持 FC 、ISCSI 、NFS、CIFS、FCOE；支持 FCoE 主机接口；管理方式 GUI/CLI；10000 转速 SAS 盘，做完 raid 1+0 后容量为 50TB；10000 转速 SAS 盘做完 raid5 后容量为 50TB，支持存储扩容。多路径负载均衡软件。	台	3
		SAN 架构存储硬盘框(2U,交流\240V 高压直流,2.5″,级联模块,25 盘位，1.8TB 10K RPM SAS 硬盘单元(2.5″)25 个。	台	2

7.	集中式存储2	SAN 架构存储系统，标配双控制器;配置 48Gb 缓存；配置虚拟资源调配软件、数据迁移软件、数据镜像功能、支持存储虚拟化及存储网关复制功能、块级压缩软件；12 个 16Gb FC 端口，控制器数量*2；企业级 SSD；支持 FC 、ISCSI 、NFS、CIFS、FCOE；支持 FCoE 主机接口；管理方式 GUI/CLI；10000 转速 SAS 盘，做完 raid 1+0 后容量为 30TB；10000 转速 SAS 盘做完 raid5 后容量为 70TB，支持存储扩容。多路径负载均衡软件。	台	3
8.	集中式存储3	SAN 架构存储系统，标配双控制器;配置 48Gb 缓存；配置虚拟资源调配软件、数据迁移软件、数据镜像功能、支持存储虚拟化及存储网关复制功能、块级压缩软件；12 个 16Gb FC 端口，控制器数量*2；企业级 SSD；支持 FC 、ISCSI 、NFS、CIFS、FCOE；支持 FCoE 主机接口；管理方式 GUI/CLI；10000 转速 SAS 盘，做完 raid 1+0 后容量为 50TB；10000 转速 SAS 盘做完 raid5 后容量为 50TB，支持存储扩容。多路径负载均衡软件。	台	1
		2 套 SAN 架构存储盘柜：硬盘框(2U,交流\240V 高压直流,2.5″,级联模块,25 盘位，1.8TB 10K RPM SAS 硬盘单元(2.5″)25 个。	台	2
9.	对象存储	2 颗 12 核 2.4GHz 处理器，256GB 内存，2 块 480GB RI SSD，空余硬盘插槽 14 个，2 块 2 端口万兆光接口网卡（包含多模光模块），空余 PCIE 插槽 1 个，4 端口千兆电接口 MLOM 网卡，三副本，实际可用 200TB	台	1
10.	光纤交换机1	万兆 48 个 10000BASE-T 电口以太网交换机，(全部端口激活，含 48*10Gb 多模 SFP)-单电源(交流)	台	2
11.	光纤交换机2	光纤交换机-48 端口(全部端口激活，含 48*16Gb 多模 SFP)-单电源(交流)	台	14
12.	路由器	主机*1，双主控，双电源，满配交换网板，万兆光≥2；千兆电≥8；千兆光≥8；千兆 WAN≥2，2 个万兆多模光模块；2 个千兆多模光模块	台	2
13.	核心交换机	以太网交换机主机，支持 48 个 100/1000/10000BASE-T 电口，支持 4 个 10G BASE-X SFP+端口，支持 2 个插槽，无电源需风扇	台	6

14.	接入交换机	以太网交换机主机，支持 48 个 100/1000/100000BASE-T 电口，支持 4 个 10G BASE-X SFP+端口，支持 2 个插槽，无电源需风扇	台	14
15.	抗拒绝服务系统	2U，交流冗余电源，2*USB 接口，1*RJ45 串口，2*GE 管理口，2 个万兆 SFPP 插槽（不含光纤接口模块），支持万兆多模光纤接口模块、万兆单模光纤接口模块，3 个链路扩展卡插槽。含 64 字节 2G 容量许可。最大 4G 清洗容量。	台	2
16.	VPN 防火墙	标准 2U 机架式设备，冗余电源，吞吐量 18G，并发连接数 450 万。6 个千兆电口，4 个千兆光口，4 个万兆光口(含光模块),国密算法	台	6
17.	防病毒网关	标准 2U 机架式设备，冗余电源，吞吐量 12G，防毒墙吞吐量 2.5G，并发连接数 220 万。6 个千兆电口，4 个千兆光口，1 个 RJ45 串口，2 个 USB 接口。	台	4
18.	流量控制	2U 设备，单电源，千兆电口 6 个，千兆光口 2 个，万兆光口 2 个（支持接口扩展），吞吐量 2.5Gbps，并发会话数 150 万，可实现用户的上网行为管理，流量控制，身份认证，应用识别，规则库可升级	台	4
19.	业务域防火墙	标准 2U 机架式设备，冗余电源，吞吐量 16G，并发连接数 300 万。6 个千兆电口，4 个千兆光口，2 个万兆光口。	台	4
20.	数据库域防火墙	标准 2U 机架式设备，冗余电源，吞吐量 16G，并发连接数 300 万。6 个千兆电口，4 个千兆光口，2 个万兆光口。	台	4
21.	管理域防火墙	标准 2U 机架式设备，冗余电源，吞吐量 16G，并发连接数 300 万。6 个千兆电口，4 个千兆光口，2 个万兆光口。	台	2
22.	应用负载均衡	2U 设备,6 千兆电口,8 个千兆光口,L4 层吞吐量 11Gbps、L4 并发连接数 940 万、L4 新建连接数 30 万，L7 新建连接数 15 万，冗余电源。设备支持串接、旁路部署、支持三角传输，设备支持虚拟化负载功能	台	4
23.	数据库审计	2U，含交流冗余电源模块，2*USB 接口，1*RJ45 串口，千兆电口≥4 个，千兆光口≥4 个，万兆光口≥2 个，4T SATA 硬盘。含数据库入侵检测模块，包含 SQL 注入、提	台	4

		权、缓冲区溢出检测等功能。 SQL 处理性能 40000 条/秒，存储天数≥180 天，日志检索≥60000 条/秒		
24.	堡垒机	标准 2U 机架式设备，硬盘≥2TB，企业级，千兆电口≥6 个，提供≥600 个资源授权，提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护三级建设要求	台	3
25.	NTP 时间服务器	授时精度 1-10ms；	台	1
26.	应用流量分析	双电源，磁盘存储空间 16TB， 4 个千兆电口/光口数据口或者 1 个万兆光口，2 个千兆管理口，处理能力≤2Gbps 或 每秒 10K 以内 TCP 会话。	台	1
27.	网络审计系统	标准机架式设备，硬盘≥1TB，冗余电源，千兆电口≥4 个，千兆光口≥4 个，具备 RJ45 串口和 USB 接口。默认接口均可作为监听口。	台	2
28.	TAP 分路器	流量复制/汇聚一体化	台	1
29.	安全态势感知系统	标准机架式设备，CPU≥4 核，物理内存≥32G，SSD ≥128G，SATA≥4T*4，支持 RAID50，单电源，≥6 个千兆电口，1 个 DB9 串口，6 个 USB 接口。	台	1
30.	安全态势感知系统探针	标准机架式设备，千兆电口≥4 个，千兆光口≥4 个，1 个 RJ45 串口，2 个 USB 接口。支持流量性能≥1.5Gbps，包转发率≥2.232Mbps，每秒新建连接数≥10 万，最大并发连接数≥200 万，CPU≥2 核，物理内存≥4G，硬盘≥SATA 1T。功能：1、IDS 漏洞利用检测；2、异常会话检测；3、Web 攻击检测；4、僵尸网络检测；5、违规访问检测，包含升级服务	台	2
31.	日志审计系统	标准机架式设备，支持≥400 个主机审计许可，系统盘≥64G，硬盘≥8TB，千兆电口≥6 个；支持获取各种主流网络及数据库访问行为，支持 Syslog、WMI、OPSEC Lea、SNMP trap 专用协议等协议事件日志，支持通过 Http、Https、FTP、SFTP、SMB 等协议获取各类文件型	台	2

		日志，支持基于 SQL/XML 标准内容获取； 2 套审计节点许可-100 ：每许可证包含 100 个节点审计许可。		
32.	网络流量回溯分析	网络接口，2 个千兆采电口采集口，2 个千兆采光口采集口，2 个电口管理口；流量处理能力：800Mbps，数据包处理能力：200，000pps，TCP/UDP 会话处理能力：每秒 50，000，存储空间 8TB	台	1
33.	容灾备份一体机	机架式，800W（1+1）冗余电源，2 颗 64 位八核处理器，128GB 高速缓存；16 个热插拔位，配备 480TB 以上硬盘,2 个千兆以太网接口，2 个万兆口。	台	3

服务子类	服务项	单位	数量
平台云主机服务（包含 X86、ARM、C86）	vCPU（vCPU ARM 架构主频不低于 2.4GHz，C86 和 x86 主频不低于 2.2GHz，平均虚拟化率，即物理 CPU/虚拟 CPU≥1/4,虚拟 CPU 利用率不低于物理 CPU 的 25% ）	1CPU	2367
	内存	1GB	6040
GPU 卡算力服务（适配 X86、ARM、C86）	GPU 显存（需同时租用算力资源、云主机或物理服务器资源，联合使用）	1 GB	368
	半精度浮点运算能力（需同时租用 GPU 显存、云主机或物理服务器资源，联合使用）	1 TFLOPS	1160
普通性能存储	普通存储（单盘技术指标:单盘 IOPS2000-5000）	100GB	1411
高性能存储	高性能存储（单盘技术指标：单盘 IOPS10000-25000）	100GB	2820
静态存储	提供大容量、高可靠的数据存储服务，具备 PB 级线性扩展能力	1TB	246
本地备份服务	本地备份服务	100GB	1411
异地备份服务	异地备份服务	100GB	120
互联网链路服务	互联网链路带宽	1Mb	455
	互联网 IP 地址租用服务、并提供备案服务	1IP	44
主机负载均衡服务	主机负载均衡服务	1IP（内网）	24
远程接入服务	远程接入服务	1 账号	96

SSL 证书服务	提供 SSL 证书服务	1 域名	1
Web 应用防火墙（WAF）	针对网站及 Web 应用系统提供应用层安全防护，支持各类 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护（200Mbps）	1 套	17
商用操作系统套餐	Windows Server 套餐：Windows Server 租用、安装及维护。	1 套	350
	国产 Linux 套餐：国产 Linux 操作系统服务租用、安装及维护。	1 套	48
开源操作系统套餐	提供开源操作系统安装和维护服务。	1 套	245
商用数据库套餐	国产商用数据库租用、安装及维护（至少支持 3 种国产数据库）	1 套	2
主机杀毒服务	主机杀毒服务	台	734
主机漏洞扫描加固	主机漏洞扫描加固	台	734
网页防篡改服务	网页防篡改服务	1 站点	10
VPN 专线接入服务	提供 VPN 接入政务云环境服务	1 套	1
数据库审计服务	数据库审计服务	1 套	13

2. 项目背景

随着北京城市副中心行政办公区一期工程逐步完成，北京市规划和自然资源委员会的信息化系统逐步完成了整体迁移入云工作。北京市规划和自然资源委员会对上云系统资源进行整合优化后，目前共有 11 个重要信息系统，包括：

- 规划编制与实施监督平台
- 批后监管与全过程监督平台
- 自然资源监测管理平台
- 不动产登记信息管理基础平台
- 综合执法与专项治理平台

- 多规合一协同信息平台
- 国土空间基础信息平台
- 项目审批办事服务平台
- 领导决策指挥平台
- 行政办公平台
- 北京市规划和自然资源委员会门户

为落实北京市信息化搬迁信息系统迁移进度要求，北京市规划和自然资源委员会目前已完成政务云互联网区、政务外网区和政务外网 VPN 区所有业务系统的迁移上云。

二、商务要求

1. 交付（实施）的时间（期限）和地点（范围）

项目交付地点：采购人指定地点。

服务期限：投标人提供 12 个月的政务云资源租用服务，自 2026 年 1 月 1 日起，至 2026 年 12 月 31 日止。

2. 付款条件（进度和方式）

本项目分三笔支付：

合同生效后【15】个工作日内，中标人向采购人提供合同价款的 10%作为履约保函，用以保证中标人全面地履行本合同项下的各种义务。

1. 在收到中标人提供的履约保函后 15 个工作日内，采购人向中标人支付合同总金额的 60%；

2. 中标人按照合同约定完成 6 个月的政务云租用服务，提交中期运维服务报告及相关材料，并通过中期验收后，采购人向中标人支付服务费的 30%。

3. 中标人按照合同要求完成全部 12 个月租期服务工作，提交政务云服务工作总结报告及相关材料，并通过终期验收后，采购人向中标人支付服务费的 10%。

三、技术要求

1. 基本要求

1.1 采购标的需实现的功能或者目标

1.1.1 总体目标

本项目的总体目标是通过租用市级政务云服务，搭建满足北京市规划和自然资源委员会业务系统安全稳定的基础平台运行环境，并对运行环境进行持续优化与改造，充分优化系统整体兼容性，提高系统可靠性。同时，须满足北京市规划和自然资源委员会现有本地及异地备份工作要求，确保业务数据的安全。

1.1.2 技术目标

投标人需完成北京市规划和自然资源委员会非密信息系统迁移上云工作，并将已完成上云的业务系统（政务云互联网区、政务外网区和政务外网 VPN 区的全部业务系统）无缝迁移至中标云服务商政务云平台，并根据本招标的项目服务内容及技术要求提供相关设备，根据服务内容提供相关的集成、运维等服务。

1.2 需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

1.2.1 国家及北京市有关政策

《关键信息基础设施安全保护条例》（中华人民共和国国务院令第 745 号）

《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）

《政府采购需求管理办法》(财库〔2021〕22 号)

《关于促进政府采购公平竞争优化营商环境的通知》（财库〔2019〕38 号）

《关于进一步提高政府采购透明度和采购效率相关事项的通知》（财办库〔2023〕243 号）

《工业和信息化部信息通信管理局关于督促互联网网络接入服务企业依法持证经营的通知》（工信管函〔2018〕84 号）

《云计算服务安全评估办法》（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部公告 2019 年 2 号）

《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文〔2014〕14 号）

《基于云计算的电子政务公共平台顶层设计指南》

《北京市财政局关于印发<北京市政府采购负面清单>的通知》（京财采购〔2020〕1345 号）

《北京市财政局关于落实好政府采购支持中小企业发展的通知（京财采购〔2022〕1143 号）

《关于印发<关于推进我市政务信息系统整合共享的实施方案>的通知》（京经信委发〔2017〕89 号）

《北京市人民政府关于印发<北京市政务信息资源管理办法（试行）>的通知》（京政发〔2017〕37号）

《关于印发<北京市市级政务云管理办法>的通知》（京经信函〔2019〕150号）

《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）

《北京市“十四五”时期智慧城市建设控制性规划要求（试行）》（京大数据发〔2021〕2号）

1.2.2 国家相关标准

《国家电子政务外网安全接入平台技术规范》

《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）

《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）

《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）

《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）

《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）

《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）

《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）

《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）

《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）

《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）

《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）

《信息安全技术 云计算服务安全能力评估方法》GB/T 34942—2017

《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）

《信息技术 云资源监控指标体系》（GB/T 37938-2019）

《电子信息系统机房设计规范》（GB50174-2017）

《数据中心电信基础设施标准》（ANSI/TIA-942）

《综合布线系统工程设计规范》（GB 50311—2016）

《云计算关键领域安全指南 V4.0》

1.2.3 北京市相关标准

《政务云平台建设技术要求》（DB11/T 2169-2023）

《北京市政务云安全技术规范 IaaS 云计算平台分册》

《北京市政务云安全技术规范 IaaS 云计算平台安全监管接口分册》

《北京市政务云安全技术规范 信息安全服务接口分册》

注：服务标准涉及的国家标准及北京市标准有更新的，执行最新标准。

2. 服务内容及要求/货物技术要求

2.1 基础及扩展服务要求

（1）计算服务

按照采购人的有关管理规定及具体需求提供计算服务，包括：云主机租用服务，云主机租用服务可弹性提供扩展 CPU、内存及数据盘磁盘，实例可用性达 99.99%，用户对云主机有完全的控制权，支持主流操作系统，如 windows server 系列、Linux 发行版、国产 Linux 等。

① 支持存储裸设备映射（RDM），可以将存储设备上的LUN直接映射给虚拟机使用，并且支持SCSI指令使用透传模式或者非透传模式；

② 应满足云主机之间、CPU之间隔离保护要求；

③ 支持资源的动态调整，根据业务的负载情况实现业务系统虚拟机的动态扩展和回收；

④ 支持异构虚拟化能力，如KVM多种虚拟化技术；

⑤ 云主机出现故障时，支持自动重启或者迁移，保障业务连续性；

⑥ 支持虚拟机热迁移，可在不同代CPU资源池中进行虚拟机热迁移；

⑦ 云计算资源性能要求包括但不限于如下：

✧物理服务器 CPU 主频应不低于 2.40GHz；

✧ 主机内存硬件配置不低于DDR4-2400MHz；

✧可用性不低于 99.99%。

（2）存储服务

按照采购人的有关管理规定及具体需求提供存储服务，包括：普通存储服务、高性能

存储服务、静态存储服务、本地备份服务和异地备份服务，要求稳定可靠，不会因单一部件故障、单一路径故障等原因导致业务停用、数据丢失，可靠性 99.9999%。

① 支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储；

② 支持块存储、对象存储、文件存储等多种存储方法，满足数据备份、视频存储等不同应用场景使用要求；

③ 支持存储资源扩展能力，例如：PB级扩展；

④ 支持磁盘容错技术，如磁盘故障后节点的自动平衡和重构、硬盘故障检测和处理、集群节点出现单盘故障时不影响业务运行等；

⑤ 存储资源性能要求包括但不限于如下：

✧吞吐量：高性能存储系统的读写带宽应不低于 1000MB/s,IOPS 不低于 20000;普通性能存储系统的读写带宽应不低于 200MB/s，IOPS 不低于 1000。

✧支持高可靠性，可靠性不低于 99.9999%；

（3）网络服务

按照采购人的有关管理规定及具体需求提供网络服务，包括：互联网链路带宽服务、互联网 IP 地址租用服务、主机负载均衡服务、远程接入服务和 WAF 防护服务。

网络系统提供稳定的数据传输能力，一般要求如下：

① 具备多运营商网络接入服务的能力；

② 数据中心组网架构设计可采用大二层网络架构，支持云主机无障碍动态迁移；

③ 应采用集群部署网络控制，以保障升级时业务不中断；

④ 应实现自动化动态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；

⑤ 具备边界防火墙和VPC防火墙隔离能力，分别针对不同的流量进行安全策略防护与配置；

⑥ 具备高可用虚拟IP能力，在集群或主备场景下，云主机可绑定高可用虚拟IP，达到高可用访问效果；

⑦ 采用双活网络架构，降低单点故障带来的稳定风险；为入云系统划分安全区域，合理制定访问规则。

⑧ 网络系统性能要求包括但不限于如下：

✧云内骨干线路带宽不低于 10Gb/s；

✧服务器业务带宽不低于 1Gb/s；

✧平均可用性不低于 99.9%。

（4）商用操作系统套餐

按照采购人的有关管理规定及应用系统需求，提供云主机的 Windows 操作系统租用、安装及维护服务和国产 Linux 操作系统服务租用、安装及维护。

（5）商用数据库套餐

按照采购人的有关管理规定及应用系统需求，提供人大金仓企业版租用、安装服务。

（6）主机杀毒服务

按照采购人的有关管理规定及应用系统需求，对云主机提供防病毒软件，实现与云服务商使用的云平台对接，在不消耗虚拟机资源的情况下，对虚拟化环境进行有效的病毒防护和查杀。

（7）主机漏洞扫描加固服务

按照采购人的有关管理规定及应用系统需求，提供每月对全部在用云主机漏洞扫描服务，以发现操作系统、数据库、中间件等层面存在的安全漏洞，并配合系统主责部门进行安全加固。

（8）安全服务

按照采购人的有关管理规定及应用系统安全防护需求，提供网页防篡改服务和数据库审计服务。

（9）VPN 专线接入服务

按照应用系统需求，提供 VPN 接入政务云环境服务（1GB 以上）。

2.2 物理租用设备要求

2.2.1 x86 物理服务器 1

技术指标	指标要求
兼容性	为了简便运维和保障设备兼容性，要求 4 路服务器、2 路服务器与本项目存储设备兼容
外观要求	标准 2U 机架式服务器
▲基本配置：	处理器配置数量：2 个

CPU/内存/硬盘/接口	主频:≥2.0GHz，≥10 核，L3 缓存≥13.75MB
	配置内存槽位≥24 个
	内存类型：ECC DDR4 RDIMM /LRDIMM 内存插槽
	内存配置容量：≥128GB
	要求支持 SDDC、双设备数据更正 DDDC、内存镜像、内存冗余位校验 ECC 校验，内存 Rank 热备技术
	内置硬盘类型：热插拔 SAS/SATA/SSD 硬盘；
	硬盘配置数目：≥2 块，600GB 10K rpm SAS 硬盘，
	硬盘扩展能力： 服务器支持多种机框类型，且服务器最大可扩展≥31 个热插拔 2.5 寸硬盘或≥20 个热插拔 3.5 寸硬盘槽位+4 个 2.5 寸盘，或≥28*NVMe PCIE SSD 盘；配置≥8 个 2.5 寸硬盘槽位。
	Raid 卡支持 RAID 0，1，10
	支持 2*M.2 SATA SSD，支持硬 RAID1，支持免开箱热插拔
	配置 2*GE 电口+4*10GE 光口（含光模块）； 配置 2*双口 16GB FC HBA 卡
I/O 扩展	支持 PCI-E I/O 插槽扩展总数：≥10 个；
	支持双宽 GPU 槽位≥2 个
节能	提供铂金超高效率电源，效率≥94%
#电源风扇	满配冗余电源和风扇
可管理性	可管理和维护性: 1. 集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示； 2.具有图形管理界面及其他高级管理功能； 3.配置独立的远程管理控制端口，支持远程监控图形界面，可实现与操

	作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作
	支持中文 BIOS 界面
	租用产品具备带外硬件故障错误数据收集，由带外管理模块进行故障分析，告警，日志导出；故障数据库支持自动定位故障源。

2.2.2 x86 物理服务器 2

技术指标	指标要求
兼容性	为了简便运维和保障设备兼容性，要求 4 路服务器、2 路服务器与本项目存储设备兼容
外观	4U 机架式，可放入 42U 标准机柜。
▲基本配置：CPU/内存/硬盘/接口	主频≥2.0GHz，核数≥10 核，L3 缓存≥13.75MB
	CPU 数量：≥4 颗
	内存扩展能力：最大支持≥48 个内存插槽
	内存配置容量：≥256 GB DDR4 内存
	内置硬盘类型：支持热插拔 SAS/SATA/SSD 硬盘
	最大硬盘数≥8，配置≥2 块 2.5 寸 600G 10K SAS 盘。
	Raid 卡支持 RAID0/1/10/5/50/6，带 1G cache 和掉电保护功能；
	配置 2*GE 电口+4*10GE 光口（含光模块）； 配置 2*双口 16GB FC HBA 卡
I/O 扩展	最大支持≥15 个 PCI-E I/O 插槽；
#电源	配置≥2 个热插拔白金交流电源，单个电源≥1200W；
风扇	满配冗余对旋风扇，支持单风扇失效
环境温度	长期工作环境温度支持 5-40 度
可管理性	可管理和维护性: 1. 集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示； 2.具有图形管理界面及其他高级管理功能；3.配置独立的远程管理控制端口，支持远程监控图形界面，可实现与操作系统无关的远程对服务器

	的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作
	提供黑匣子 Black Box 功能；

2.2.3 刀片服务器

技术指标	指标要求
▲基本配置：CPU/内存/硬盘/接口	**CPU 数量：≥4 颗**
	主频≥2.1GHz，核数≥10 核，缓存≥25MB
	配置≥128GB DDR4 2133MHz RDIMM 内存
	配置 48 个内存插槽
	支持 SAS/SATA 硬盘配置
	最大硬盘数≥4；配置≥2 块 600GB SAS 10K 转 2.5 寸热插拔硬盘
	配置独立的 RAID 卡，支持 RAID0，1，10.
	配置 2*10GE 接口卡，2*10Gb FCoE 接口卡。
兼容性	支持主流操作系统
#可管理性	可管理和维护性:1. 集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示；2.具有图形管理界面及其他高级管理功能；3.配置独立的远程管理控制端口，支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作
	刀片上管理软件自主研发

2.2.4 刀片服务器机箱

技术指标	指标要求
设备类型高度	一体化刀片服务器，高度≥12U
刀片容量能力	**单框可支持≥16 刀片**
	同一机框可同时支持多代 CPU 刀片混插能力

▲网络互联模块	支持≥4 个交换插槽
	支持 GE 交换、10GE 交换、25GE、40GE、IB FDR/EDR 交换、8G/16G FC 交换、FCoE 交换；
	配置冗余交换模块
管理能力	支持内置触摸液晶屏，可以进行基本参数的配置和维护操作
	支持本地 KVM 功能，通过一个物理接口可以集中呈现管理框内所有刀片，不支持该功能的配置和刀箱数量相等的外置 KVM 交换机
	机箱内管理模块上实现无状态计算，无需外置管理节点既可实现 MAC 地址和 WWN 号的池化分配和 BIOS，网卡，HBA 卡的配置管理，基于硬件刀片的迁移。
工作温度	支持 5-40℃，节能环保；
#电源	配置≥6 个冗余热插拔交流电源，电源模块额定功率≤3000W。
#网卡配置	4 个 10GB 光模块、4 个 8GB FC 模块、4 个 GE 电口模块。

2.2.5 小型机物理服务器（含操作系统）租用服务

技术指标	指标要求
基本要求	标准机架式，UNIX 服务器，非刀片式架构
▲基本配置：CPU/内存/硬盘/接口	64 位的 RISC 处理器 处理器插槽≥2 实配≥2 颗 CPU；CPU 主频≥3.89GHz 单颗 CPU 核数≥6 核 每核心支持线程数≥8 处理器每核心三级缓存≥8MB 支持四级缓存，最大缓存支持≥128G
	实配≥512GB 内存
	实配≥2 块 600G SSD 硬盘
	实配≥12 个万兆以太网电口；实配≥8 个万兆以太网光口
操作系统	支持 AIX UNIX，Red Hat Linux， SUSE Linux 操作系统； 支持 UNIX 操作系统的系统加固；支持对可执行程序的主动防御保护；支持对要保护的资源进行授权访问控制。

	配置持 AIX UNIX 操作系统
#光纤通道卡	实配≥4 个 16Gb 光纤接口光纤通道卡，
电源风扇	冗余电源，冗余风扇
I/O 插槽	支持 11 个 PCIe 插槽
光盘驱动器	DVD-ROM 1 个
分区支持	支持硬件分区或逻辑分区，CPU、内存、IO 等资源可以在各个分区之间在线调配，分区之间系统资源能在不需要停机的情形下，动态调整包括处理器能力、内存容量、I/O 插槽等系统资源。
可用性	系统有硬件部件自动纠错及损坏隔离功能的装置，支持双机或多机集群
其他要求	提供本部分系统集成安装所需导轨、线缆等设备（原厂配套）

2.2.6 集中式存储 1

技术指标	指标要求
兼容性	**与服务器兼容；**
#架构	实配 SAN 和 NAS 统一存储，配置 NAS 协议（包括 NFS 和 CIFS）、IP SAN 和 FC SAN 协议
	支持 SAN 和 NAS 一体化，不需额外配置 NAS 网关
▲关键硬件指标	**配置统一存储，双控制器缓存容量≥48GB（统一存储缓存，不含任何性能加速模块或 NAS 网关缓存、FlashCache、PAM 卡，SSD Cache 等）；**
	支持 8Gbps FC、1Gbps iSCSI、10Gbps iSCSI、10Gbps FCoE，16Gbps FC，56(IB；
	双控制器最大支持≥40 个主机接口，配置配置≥12*16G FC 主机接口（配置满足使用的光跳线）
	最大支持≥12*4*12Gbps SAS3.0 磁盘通道，配置 4*4*12Gbps SAS3.0 磁盘通道；
	支持 SSD，SAS，NL-SAS 中的 3 种类型以上硬盘；
	配置 10000 转速 SAS 盘，做完 raid1+0 后容量≥50TB；10000 转速 SAS 盘做完 raid5 后容量≥50TB

	双控制器下，最大支持磁盘插槽个数≥730；
	支持 RAID 0、RAID 1、RAID3、RAID 10、RAID 5 等；
	冗余电源、风扇、控制器、缓存断电保护功能；
	磁盘、电源、IO 模块需要能实现不停机热插拔；
虚拟化功能	具备数据均衡分布技术
	支持异构虚拟化功能；
软件配置	配置自动精简配置，结合业务应用，进行空间的预分配，增加业务空间分配的灵活性，保证后续业务平滑扩展；
	配置多租户功能，实现隔离租户间的资源，分权分域
	支持 Cache 缓存分区功能，保障关键业务资源使用；支持智能缓存加速功能；
	支持服务质量控制功能，保证关键业务；
	配置卷镜像使用许可；
	配置数据迁移许可
	支持本地高可靠双活，可提供双活架构，实现两套核心存储数据双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。
兼容性	获得 Vmware VAAI、SRM、VASA 兼容性认证；
管理维护	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储服务器的图形化管理配置和监控软件。

2.2.7 集中式存储 2

技术指标	指标要求
兼容性	**与服务器兼容；**
＃架构	**实配 SAN 和 NAS 统一存储，配置 NAS 协议（包括 NFS 和 CIFS）、IP SAN 和 FC SAN 协议**
	支持 SAN 和 NAS 一体化，不需额外配置 NAS 网关
▲关键硬件指标	**配置统一存储，双控制器缓存容量≥48GB（统一存储缓存，不含任何性能加速模块或 NAS 网关缓存、FlashCache、PAM 卡，SSD Cache 等）；**
	支持 8Gbps FC、1Gbps iSCSI、10Gbps iSCSI、10Gbps FCoE，16Gbps FC，56(IB；

	双控制器最大支持≥40 个主机接口，配置配置≥12*16G FC 主机接口（配置满足使用的光跳线）
	最大支持≥12*4*12Gbps SAS3.0 磁盘通道，配置 4*4*12Gbps SAS3.0 磁盘通道；
	支持 SSD，SAS，NL-SAS 中的 3 种类型以上硬盘；
	配置 10000 转速 SAS 盘，做完 raid1+0 后容量≥30TB；10000 转速 SAS 盘做完 raid5 后容量≥70TB
	双控制器下，最大支持磁盘插槽个数≥730；
	支持 RAID 0、RAID 1、RAID3、RAID 10、RAID 5 等；
	冗余电源、风扇、控制器、缓存断电保护功能；
	磁盘、电源、IO 模块需要能实现不停机热插拔；
虚拟化功能	具备数据均衡分布技术
	支持异构虚拟化功能；
软件配置	配置自动精简配置，结合业务应用，进行空间的预分配，增加业务空间分配的灵活性，保证后续业务平滑扩展；
	配置多租户功能，实现隔离租户间的资源，分权分域
	支持 Cache 缓存分区功能，保障关键业务资源使用; 支持智能缓存加速功能;
	支持服务质量控制功能，保证关键业务；
	配置卷镜像使用许可；
	配置数据迁移许可
	支持本地高可靠双活，可提供双活架构，实现两套核心存储数据双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。
兼容性	获得 Vmware VAAI、SRM、VASA 兼容性认证；
管理维护	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储服务器的图形化管理配置和监控软件。

2.2.8 集中式存储 3

技术指标	指标要求
兼容性	**与服务器兼容；**

#架构	实配 SAN 和 NAS 统一存储，配置 NAS 协议（包括 NFS 和 CIFS）、IP SAN 和 FC SAN 协议
	支持 SAN 和 NAS 一体化，不需额外配置 NAS 网关
▲关键硬件指标	**配置统一存储，双控制器缓存容量≥48GB（统一存储缓存，不含任何性能加速模块或 NAS 网关缓存、FlashCache、PAM 卡，SSD Cache 等）；**
	支持 8Gbps FC、1Gbps iSCSI、10Gbps iSCSI、10Gbps FCoE，16Gbps FC，56G IB；
	双控制器最大支持≥40 个主机接口，配置配置≥12*16G FC 主机接口（配置满足使用的光跳线）
	最大支持≥12*4*12Gbps SAS3.0 磁盘通道，配置 4*4*12Gbps SAS3.0 磁盘通道；
	支持 SSD，SAS，NL-SAS 中的 3 种类型以上硬盘；
	配置 10000 转速 SAS 盘，做完 raid1+0 后容量≥50TB；10000 转速 SAS 盘做完 raid5 后容量≥50TB
	2 套 SAN 架构存储盘柜：硬盘框(2U,交流\240V 高压直流,2.5″,级联模块,25 盘位，1.8TB 10K RPM SAS 硬盘单元(2.5″)25 个。
	双控制器下，最大支持磁盘插槽个数≥730；
	支持 RAID 0、RAID 1、RAID3、RAID 10、RAID 5 等；
	冗余电源、风扇、控制器、缓存断电保护功能；
	磁盘、电源、IO 模块需要能实现不停机热插拔；
虚拟化功能	具备数据均衡分布技术
	支持异构虚拟化功能；
软件配置	配置自动精简配置，结合业务应用，进行空间的预分配，增加业务空间分配的灵活性，保证后续业务平滑扩展；
	配置多租户功能，实现隔离租户间的资源，分权分域
	支持 Cache 缓存分区功能，保障关键业务资源使用；支持智能缓存加速功能；
	支持服务质量控制功能，保证关键业务；
	配置卷镜像使用许可；
	配置数据迁移许可

	支持本地高可靠双活，可提供双活架构，实现两套核心存储数据双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。
兼容性	获得 Vmware VAAI、SRM、VASA 兼容性认证；
管理维护	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储服务器的图形化管理配置和监控软件。

2.2.9 对象存储

技术指标	指标要求
自主可控	拥有自主知识产权，非 OEM 产品，非联合产品。
软硬解耦	支持工业标准的 x86 或 ARM 通用硬件，硬件不限定品牌，不限定硬件部件的型号及技术参数。升级、扩容的过程中用户可以选择自行增加硬件部件。
▲硬件要求	**服务器节点数量≥3；** 每节点配置要求如下： **CPU：≥2 颗 X86 12 核 2.4GHz 处理器** **内存：≥96G 内存** **系统盘：≥2 块 480GB SSD** **缓存盘：≥2 块 3.2TB MU SSD** **数据盘：≥12 块 18TB SATA HDD** **网卡：≥2 块 2 端口万兆光接口网卡（包含多模光模块），≥1 端口千兆电接口 MLOM 网卡**
数据可靠	支持 1~6 副本。 支持在线修改副本数，在线修改精简 EC 到 EC（比如 4+2:1 改为 4+2）。 支持根据拓扑节点设置权重。 采用优选的 EC 算法，以少量的冗余信息保证数据可靠性，以 CPU 计算时间换取空间，比多副本机制获得更多的有效存储容量。支持 2+1,4+2,4+2:1,8+2，8+2:1 等多种纠删保护机制。块和文件支持全场景 EC；对象支持 EC
	针对在线实时读写数据时做 CRC（Cyclic Redundancy Check）校验，防止静默数据错误。
	支持基于 Layer2 协议头，Layer3 协议，Layer4 协议优先级等的组合流分

	类、ACL，CAR，Remark，Schedule 等动作、PQ，DWRR，PQ+DWRR 等队列调度方式、WRED，尾丢弃等拥塞避免机制、流量整形
数据空间利用率	支持存储池数据压缩，界面可显示压缩比，开启压缩，性能下降不超过 5%
性能优化	支持 SSD 构成高速缓存，采用创新性的 IO 聚合技术，将小块随机 IO 聚合成大块顺序 IO，可支持高并发和高负载下的持续稳定的性能，EC 可以获得跟副本相当的性能
	支持存储池 bypass，可智能 I/O 过滤大块数据

2.2.10 光纤交换机 1

技术指标	指标要求
光纤通道端口	**交换机模式：48 个 10GESFP+端口**
可扩展性	可堆叠。
背板带宽	4Tbps/64Tbps。
▲端口配置	**配置≥48 个光模块-SFP+-10G-多模模块(850nm,0.3km,LC)。**
Vlan	支持 Access，Trunk，Hybrid 方式、default VLAN、QinQ、MUX VLAN、GVRP
QOS	支持基于 Layer2 协议头，Layer3 协议，Layer4 协议优先级等的组合流分类、ACL，CAR，Remark，Schedule 等动作、PQ，DWRR，PQ+DWRR 等队列调度方式、WRED，尾丢弃等拥塞避免机制、流量整形
组播管理	支持 IGMP Snooping、IGMP Proxy、IGMP，PIM-SM，MBGP 等组播路由协议、支持组播流量抑制、组播 VLAN、组播 VxLAN
#电源	**双电源，交流**

2.2.11 光纤交换机 2

技术指标	指标要求
光纤通道端口	**交换机模式：48 个端口**
可扩展性	完全 fabric 架构，最多可有 239 台交换机。
端口交换速度	支持 2、4、8 和 16 Gbps 端口速率自动感应。

▲端口配置	**配置≥48 个 16Gb/s 端口（全激活），并可以向下兼容 8Gbps、4Gbps、2Gbps 等端口。配置≥48 个 16Gbps SFP。**
ISL 链路聚合	基于帧的链路聚合，每条 ISL 链路最多 8 个 16 Gbit/sec 端口；每条 ISL 链路速率最高 128 Gbit/sec；
集合带宽 1	768 Gbit/sec：48 端口× 16 Gbit/sec (线速)
最大帧	2112 字节净负荷
帧缓冲	可动态分配 8192 帧
#电源	**双电源，交流**

2.2.12 路由器

技术指标	指标要求
▲性能/架构	**支持交换容量≥71Tbps 支持包转发率≥11000Mpps**
	整机业务载板插槽≥8 个（不包含主控和交换网板槽位）
	主控板和交换网板物理隔离，带独立交换网板并满配，独立交换网板数量≥2，交换板和业务板不允许共享槽位
	设备支持双主控、双电源 M+N 冗余，支持机箱内双主控热备，要求所有业务板卡及电源、风扇均可热插拔
	整机高度≤6U
	投标设备和接入设备共机柜，因此要求深度≤300mm
	运行温度：-40~65℃
#协议与功能	支持 IPv4、Ipv6：
	1、支持 IPv4 路由表容量≥12M，IPv6 路由表容量≥10M
	2、支持 IPv4 转发表容量≥4M，IPv6 转发表容量≥2M
	支持 RIP、OSPF、IS-IS、BGP 等路由协议
	支持并实配 MPLS，MPLS VPN
	支持 PIM-SM、IGMP、MBGP、MSDP、MPLS VPN、NG-MVPN 组播协议
	支持按需灵活配置的低时延、以太场景类 SDH 的 IP 硬管道业务保障能力技术，保障业务带宽
	支持 FRR 功能：IP/LDP/TE/VPN FRR

增值业务	随板支持 NAT 功能，不需要配置业务卡
	随板支持 IPsec 功能，不需要配置业务卡
	随板支持 Netstream 功能，不需要配置业务卡
	随板支持 GRE 功能，不需要配置业务卡
SDN	支持广域网智能调优
	支持 VXLAN、EVPN、Segment Routing 等技术
	支持智能隧道 CBTS 功能
	支持 IP+光的 SDN 方案，充分利用数通和传输资源对用户网络进行智能化应用
BRAS 用户性能	**整机上线速度可达：** **整机 PPPOE 用户接入速率≥370 个/秒** **整机 IPOE 用户接入速率≥495 个/秒**
	整机用户数≥32K
接口类型	**设备支持 100GE，40GE，10GE，GE/FE，155M POS，622M POS，155M CPOS，E1/CE1，GE 彩光口和 CSFP 口，支持 622M/155M POS 自适应**
高可靠性	支持硬件 BFD，5ms 发包频率
配置维护	支持配置回滚功能，提供智能化维护管理体验
#配置	主机*1，双主控，双电源，满配交换网板，万兆光≥2；千兆电≥8；千兆光≥8；千兆 WAN≥2，2 个万兆多模光模块；2 个千兆多模光模块。

2.2.13 核心交换机

技术指标	指标要求
▲性能端口	**交换容量≥6.4Tbps，包转发率≥2800Mbps**
	为了提高设备可靠性，支持电源 1+1 备份，风扇框 1+1 备份
	支持 100G/40G/25G QSFP28 接口、万兆以太光口、万兆以太电口
	支持业务扩展插卡数≥4
二层	支持 M-LAG 或 vPC 等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现）

三层	支持静态路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP 等路由协议
	支持 BFD for OSPF、BGP、IS-IS 和 Static Route
	支持 IPv6 VXLAN over IPv4
可靠性	支持 IPv6 VXLAN over IPv4
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备
#配置	主机*1 配置千兆电≥48，万兆光≥4 个；40G 接口≥2 个；双电源；40G 堆叠线缆 1 条；3 个万兆多模光模块

2.2.14 接入交换机

技术指标	指标要求
▲性能端口	**交换容量≥650Gbps，包转发率≥400Mpps**
	为了提高设备可靠性，支持模块化可插拔双电源
	支持 48 个万兆电口，4 个万兆光口
	支持业务扩展插卡数≥1，可扩展支持 4 个 40GE QSFP+端口
三层	支持静态路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP 等路由协议
	支持 Ipv4 路由表≥8K
	支持 IPv4/IPv6 双协议栈，支持 IPv6 Ping、IPv6 Tracert、IPv6 Telnet，支持 6to4、ISATAP、手动配置 tunnel
	支持 DHCPv4/v6 client/relay/server，支持对 ND、DHCPv6、MLD 等 IPv6 协议报文进行攻击溯源和惩罚
可靠性	支持 G.8032 标准以太环网协议
虚拟化	支持堆叠，主机堆叠数不小于 9 台
	支持纵向虚拟化，作为纵向子节点零配置即插即用
	支持 CPU 防攻击功能
	支持 DHCP Snooping，IP Source Guard，SAVI 等安全特性
#配置	主机*1，配置千兆电≥48，万兆光≥4 个；40G 接口≥2 个；双电源；40G 堆叠线缆 1 条；3 个万兆多模光模块

2.2.15 抗拒绝服务系统

技术指标	指标要求
▲性能参数	双电源，配置 1*RJ45 串口，2*GE 管理口，2 个万兆 SFPP 插槽（不含光纤接口模块），3 个链路扩展卡插槽；
部署方式	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；
网络特性	支持链路聚合功能；支持端口联动功能，支持 IPv4 / v6 NAT 地址转换；支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口；
路由支持	支持静态路由，ECMP 等价路由；支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持多播路由协议；支持路由异常告警功能； 支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能；
#基础功能	访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式； 访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况； 访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制； 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；
DDoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 支持内网访问控制，配置内网区域只允许指定的 IP 地址或 IP 范围对外进行访问，防止内部伪造源 IP 对外 DoS 攻击的情况 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；支持对信任区域主机外发的异常流量进

技术指标	指标要求
	行检测，如 ICMP，UPD，SYN，DNS Flood 等 DDoS 攻击行为； 支持 CC 攻击防护； 支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；
僵尸主机检测	支持通过静态特征识别定位僵尸恶意软件，恶意软件识别特征总数在 40 万条以上；
威胁地理位置感知	支持将检测到的应用层攻击行为按照 IP 地址的地理位置信息进行动态展示，实时监测和展示最新的攻击威胁信息；
安全可视化	支持在首页多维度的展示发现的安全威胁，如攻击风险，漏洞风险，终端安全威胁和数据风险等，并支持将所有发现的安全问题进行归类汇总，并针对给出相应的解决方法指引； 支持报表以 HTML、Excel、PDF 等格式导出；

2.2.16 VPN 防火墙

技术指标	指标要求
▲性能参数	2U 机架设备，双电源，存储≥1T SATA；；含千兆电口≥6 个，千兆光口≥4 个，万兆光口≥4 个，串口（RJ45）≥1 个，USB 口≥2 个； 吞吐量≥18Gbps，SSL 最大加密流量≥400Mbps；IPSecVPN 推荐接入隧道数≥1000，IPSecVPN 加密速度≥800Mbps；密码算法和技术符合国家法律法规和相关标准，密码产品和服务通过国家密码管理部门的核准或许可。
部署方式	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；
网络特性	支持链路聚合功能；支持端口联动功能，支持 IPv4 / v6 NAT 地址转换； 支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口；
#路由支持	支持静态路由，ECMP 等价路由；支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持多播路由协议；支持路由异常告警功能； 支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能；
#基础功能	访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户

	（组），应用/服务类型，时间组的细化控制方式； 访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况； 访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制； 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；
DDoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；
入侵防护功能	设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能； 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
僵尸主机检测	设备具备独立的僵尸网络识别库，特征总数在 40 万条以上； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告； 支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，

	定位僵尸网络控制服务器的地址；
安全可视化	支持对经过设备的流量进行分析，发现被保护对象存在的漏洞（非主动扫描），并根据被保护对象发现漏洞数量进行 TOP 10 排名，列出每个服务器发现的漏洞类型以及数量，支持生成和导出威胁报告，报告内容包含对整体发现的漏洞情况进行分析；（提供威胁报告） 支持在首页多维度的展示发现的安全威胁，如攻击风险，漏洞风险，终端安全威胁和数据风险等，并支持将所有发现的安全问题进行归类汇总，并针对给出相应的解决方法指引； 支持报表以 HTML、Excel、PDF 等格式导出；
标准	符合公安部第二代防火墙（GA / T 1177-2014）标准。

2.2.17 防病毒网关

技术指标	指标要求
▲性能接口	2U 机架设备，双电源，存储≥1T SATA；；含千兆电口≥6 个，千兆光口≥4 个，串口（RJ45）≥1 个，USB 口≥2 个，吞吐量≥12Gbps;
部署方式	支持网关模式，支持 NAT、路由转发、DHCP 等功能；支持网桥模式，以透明方式串接在网络中；支持同时开启网关和网桥模式。
实时监控	提供设备实时 CPU、内存、磁盘占用率、会话数、在线用户数、网络接口等信息 实时提供 IP 流量、应用流量排名、流量管理状态、DHCP 状态、在线用户管理
#病毒防御	支持对 HTTP，FTP，SMTP，POP3 协议进行病毒文件检测
	内置病毒特征数量超过 1000 万。
	支持对常见压缩文件格式的检测，如 zip，rar，7z 等。
	支持杀毒文件类型自定义
	支持杀毒白名单功能，可以根据 URL 或者 IP 进行排除不检测病毒
	支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤；

		检测到病毒后的操作支持阻断，记录杀毒日志。
流量管理	多线路技术	网关必须能同时连接多条外网线路，且支持多线路复用和智能选路技术
	虚拟多线路	必须支持将多条外网线路虚拟映射到设备上，实现对多线路的分别流控；
	应用流控	支持基于应用类型划分与带宽分配
	网站流控	支持基于网站类型的划分与带宽分配
	文件流控	支持基于文件类型划分与分配带宽
	时间控制	支持基于时间段的带宽划分与分配策略
	目标 IP 流控	支持基于访问行为的目标 IP 实现带宽划分与分配
用户认证	认证方式	支持基于用户名/密码、单点登陆以及基于 IP 地址、MAC 地址、计算机名的识别等多种认证方式
	单点登陆	支持 AD 域结合、Proxy、POP3、web 表单等多种单点登陆方式，简化用户操作；可强制指定用户、指定 IP 段的用户必须使用单点登录
	新用户认证	支持添加到指定本地组、临时账号和不允许新用户认证等新用户认证策略
	强制 AD 认证	必须由指定用户使用 AD 域账户登录操作系统，否则禁止上网
	页面跳转	认证成功的用户支持页面跳转，包括最近请求页面、管理员制定 URL、注销页面等
	帐户导入	支持 CSV 格式文件导入、扫描导入和从外部 LDAP 服务器上导入
	组织结构	支持从 LDAP 服务器导入账户及分组信息
应用智能识别		支持应用更新版本后的主动识别和控制。 支持对 1000 种以上应用 2500 种以上的应用动作、用户名进行识别，可以识别 P2P、IM、OA 办公应用、数据库应用、ERP 应用、软件升级应用、木马外联、炒股软件、视频应用、代理软件、网银等协议；
僵尸病毒防御		支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制

	服务器的交互行为和其他可疑行为；
设备管理	支持 SSL 加密 WEB 方式管理设备 支持邮件、短信（可扩展）等告警方式，可提供管理员登陆、日志存储空间不足等告警设置 提供图形化排障工具，便于管理员排查策略错误等故障 提供路由、网桥、旁路等部署模式的配置引导，提供保护服务器、保护内网用户上网安全、保证内网用户上网带宽、配置引导，简化管理员配置
数据中心	设备必须支持内置数据中心。
日志报表系统	支持自定义统计指定 IP/用户组/用户/应用在指定时间段内的服务器安全风险、终端安全风险等内容，并形成报表
	支持将统计/趋势等报表自动发送到指定邮箱
	支持导出安全统计/趋势等报表，包括网页、PDF 等格式

2.2.18 流量控制

技术指标	指标要求
▲性能参数	标准 2U 机架式尺寸，单电源，含千兆电口≥6 个，千兆光口≥2 个，万兆光口≥2 个，硬盘≥1TB SATA；承载带宽性能≥500Mb，支持用户数≥5000；
部署方式	支持网关（路由），网桥模式部署，支持两台及两台以上设备同时做主机的部署模式，支持基于虚拟化平台的软件版本，支持 NAT、路由转发、DHCP、多路桥接功能等功能；
IPV6	所有功能都支持部署在 IPv6 环境中
#设备管理	支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web 关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等；
	具有 IPSecVPN 远程加密访问和连接的模块，并能提供 IPSecVPN 客户端授权远程接入访问；
实时监控	提供设备实时 CPU、内存、磁盘占有率、会话数、在线用户数、系统

	时间、网络接口、当天网络质量、最近发现移动终端等信息；
	针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向 web 访问质量检测
用户管理	支持触发式 WEB 认证，静态用户名密码认证；支持 LDAP、Radius、POP3、Proxy 等第三方认证；支持数据库认证；支持以 USB-Key 方式实现双因素身份认证，支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等；支持短信认证方式，支持微信认证
	同一个账号，支持与指定数量的多个终端进行自动绑定；
	支持二维码认证，管理员扫描访客的二维码后对其网络访问授权
	支持认证页面分权分域管理。启用后，普通管理员只能看到自己有权限的页面，其他管理员页面不可见。系统管理员可以将某个页面授权给指定的普通管理员管理。
	可设置用户密码不能等于用户名；新密码不能与旧密码相同；可设置密码最小长度；可设置密码必须包括数字或字母或特殊字符；
终端管理	支持识别终端操作系统版本、系统补丁安装情况，指定目录下的文件情况；支持识别终端系统后台运行的进程信息，防止间谍软件的运行；支持终端调用管理员指定脚本/程序以满足个性化检查要求；
应用控制	设备内置应用识别规则库，支持超过 4700 条应用规则数，支持超过 2100 种以上的应用，660 种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率；
	支持对加密 HTTPS、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电邮客户端的邮件进行关键字过滤；
	支持对加密 HTTPS、POP3-SSL、POP3、IMAP、IMAP-TLS、IMAP-SSL、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电邮客户端邮件内容的审计。
	用户指定应用上网流速超过预设阈值后，网关自动提醒该用户；
	支持上网策略对象的自动过期功能；
	设备内置业界知名杀毒引擎；必须支持 HTTP 下载、FTP 下载、POP3、

	SMTP 杀毒；支持对 HTTP、FTP 等下载中启用文件类型杀毒；病毒库支持通过服务器或本地加载病毒库方式定期升级；
流量控制	能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等。
	支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；
上网日志管理	设备必须支持内置数据中心和独立数据中心，支持日志高性能模式处理，精简冗余日志；
	提供服务器虚拟化产品与外置 DC 联动，服务器虚拟化能够根据实际用户和流量规模合理分配硬件资源，保障最优资源分配。同时，外置 DC 能够与服务器虚拟化底层联动，优化磁盘读写，提高查询速度
	管理员登录数据中心只能审计指定用户组的上网行为日志；
	支持基于时间段/用户/用户组/终端类型/位置等维度的应用流速趋势、网站分类流速趋势报表
	支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱
	内置多套日志模板与日志平台对接，至少支持以下平台：派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。

2.2.19 业务域防火墙

技术指标	指标要求
▲性能参数	2U 机架设备，双电源，存储≥1T SATA；；含千兆电口≥6 个，千兆光口≥4 个，万兆光口≥2 个，串口（RJ45）≥1 个，USB 口≥2 个； 吞吐量≥16Gbps，SSL 最大加密流量≥400Mbps；IPSec VPN 推荐接入隧道数≥1000，IPSec VPN 加密速度≥600Mbps；
部署方式	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；
网络特性	支持链路聚合功能；支持端口联动功能，支持 IPv4 / v6 NAT 地址转换；支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口；

#路由支持	支持静态路由，ECMP 等价路由；支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持多播路由协议；支持路由异常告警功能； 支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能；
#基础功能	访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式； 访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况； 访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制； 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；
DDoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；
入侵防护功能	设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能； 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
僵尸主机检测	设备具备独立的僵尸网络识别库，特征总数在 40 万条以上； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够

	对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；（需提供具备相关云端查杀能力的证明） 支持通过云端的大数据分析平台,发现和展示整个僵尸网络的构成和分布,定位僵尸网络控制服务器的地址；
安全可视化	支持对经过设备的流量进行分析，发现被保护对象存在的漏洞（非主动扫描），并根据被保护对象发现漏洞数量进行 TOP 10 排名，列出每个服务器发现的漏洞类型以及数量，支持生成和导出威胁报告，报告内容包含对整体发现的漏洞情况进行分析；（提供威胁报告） 支持在首页多维度的展示发现的安全威胁，如攻击风险，漏洞风险，终端安全威胁和数据风险等，并支持将所有发现的安全问题进行归类汇总，并针对给出相应的解决方法指引； 支持报表以 HTML、Excel、PDF 等格式导出；
标准	符合公安部第二代防火墙（GA / T 1177-2014）标准。

2.2.20 数据库域防火墙

技术指标	指标要求
▲性能参数	2U 机架设备，双电源，存储≥1T SATA；；含千兆电口≥6 个，千兆光口≥4 个，万兆光口≥2 个，串口（RJ45）≥1 个，USB 口≥2 个； 吞吐量≥16Gbps，SSL 最大加密流量≥400Mbps；IPSecVPN 推荐接入隧道数≥1000，IPSec VPN 加密速度≥600Mbps；
部署方式	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；
网络特性	支持链路聚合功能；支持端口联动功能，支持 IPv4 / v6 NAT 地址转换； 支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口；
#路由支持	支持静态路由，ECMP 等价路由；支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持多播路由协议；支持路由异常告警功能； 支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、应用

	类型以及国家地域来进行选路的策略路由选路功能；
#基础功能	访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式； 访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况； 访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制； 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；
DDoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；
入侵防护功能	设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能； 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
僵尸主机检测	设备具备独立的僵尸网络识别库，特征总数在 40 万条以上； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并

	在云端进行沙盒检测，并下发威胁行为分析报告； 支持通过云端的大数据分析平台,发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；
安全可视化	支持对经过设备的流量进行分析，发现被保护对象存在的漏洞（非主动扫描），并根据被保护对象发现漏洞数量进行 TOP 10 排名，列出每个服务器发现的漏洞类型以及数量，支持生成和导出威胁报告，报告内容包含对整体发现的漏洞情况进行分析；（提供威胁报告） 支持在首页多维度的展示发现的安全威胁，如攻击风险，漏洞风险，终端安全威胁和数据风险等，并支持将所有发现的安全问题进行归类汇总，并针对给出相应的解决方法指引； 支持报表以 HTML、Excel、PDF 等格式导出；
标准	符合公安部第二代防火墙（GA / T 1177-2014）标准。

2.2.21 管理域防火墙

技术指标	指标要求
▲性能参数	2U 机架设备，双电源，存储≥1T SATA；；含千兆电口≥6 个，千兆光口≥4 个，万兆光口≥2 个，串口（RJ45）≥1 个，USB 口≥2 个； 吞吐量≥16Gbps，SSL 最大加密流量≥400Mbps；IPSec VPN 推荐接入隧道数≥1000，IPSec VPN 加密速度≥600Mbps；
部署方式	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；
网络特性	支持链路聚合功能；支持端口联动功能，支持 IPv4 / v6 NAT 地址转换； 支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口；
#路由支持	支持静态路由，ECMP 等价路由；支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持多播路由协议；支持路由异常告警功能； 支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能；
#基础功能	访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式； 访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过

	期、规则超长时间未有匹配等情况； 访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 支持根据国家/地区来进行地域访问控制； 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；
DDoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；
入侵防护功能	设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能； 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
僵尸主机检测	设备具备独立的僵尸网络识别库，特征总数在 40 万条以上； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告； 支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；
安全可视化	支持对经过设备的流量进行分析，发现被保护对象存在的漏洞（非主动扫

	描），并根据被保护对象发现漏洞数量进行 TOP 10 排名，列出每个服务器发现的漏洞类型以及数量，支持生成和导出威胁报告，报告内容包含对整体发现的漏洞情况进行分析；（提供威胁报告） 支持在首页多维度的展示发现的安全威胁，如攻击风险，漏洞风险，终端安全威胁和数据风险等，并支持将所有发现的安全问题进行归类汇总，并针对给出相应的解决方法指引； 支持报表以 HTML、Excel、PDF 等格式导出；
标准	符合公安部第二代防火墙（GA / T 1177-2014）标准。

2.2.22 应用负载均衡

技术指标	指标要求
▲性能参数	标准 2U 机架设备，冗余电源，内存≥8GB，SSD 硬盘≥240GB，含千兆电口≥6 个，千兆光口≥8 个，吞吐量≥11Gbps，并发连接数≥940W；
部署	支持串接部署方式和旁路部署方式，支持三角传输模式。 支持对不少于 20 条的线路进行流量负载均衡，最多可扩展支持到 64 条线路 对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得 Active-Active 运行的能力。
多合一功能	单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。开通 HTTP 压缩、HTTP 缓存、TCP 连接复用、SSL 卸载等功能，无需额外购买相应授权。
编程控制	通过某种编程语言（如 lua）实现自定义的流量编排，对 TCP、SSL、HTTP 和 HTTPS 等类型的流量进行分发、修改和统计等操作。
#链路负载均衡	支持静态 IP 和 PPPOE 两种线路接入方式。 支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。 内置完备的 IP 地址库，无需手动导入并支持自动更新，可查看并编辑各国家、国内各省份的 IP 地址段和国内各大运营商 IP 地址段，并可灵活匹配 IP 地址库进行流量调度分发，实现链路负载功能。

	支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。 支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。
#服务器负载	支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规 HTTP 应用可配置基于反映 URL 失效的 HTTP 响应状态码的观测判断机制，对于复杂应用可配置基于 RST 关闭连接和零窗口等异常 TCP 传输行为的观测判断机制。 支持面向服务器健康度的弹性调控机制，可通过监控业务流中的 TCP 传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。 支持图片优化技术，通过对图片格式的转换，减少传输流量，提升 web 页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的 WebP 或 JPEG 格式，优化加速效果。
浪涌保护	对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包
会话保持机制	支持源 IP、Cookie（插入/被动/改写）、HTTP-Header、Radius、SSL Session ID 等多种会话保持机制。
链路健康检查	支持多种链路检测方法，能够通过 PING、TCP、HTTP 等方式监控链路的连通性。 支持链路冗余机制，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅。

2.2.23 数据库审计

技术指标	指标要求
▲性能要求	标准 2U 机架式设备，千兆电口≥4 个，千兆光口≥4 个，万兆光口≥2 个，冗余电源，SQL 吞吐（峰值）≥40000 条/s，存储天数≥180 天，日志检索≥60000 条/秒
部署方式	审计方式：旁路交换机镜像、 Agent 抓包、单机（采集器）、多机（管

	理器）、支持虚拟化平台部署 数据库审计旁路镜像模式部署不影响数据库性能和网络架构； 数据库审计 Agent 抓包方式支持业务系统和数据库一体化部署的审计
	多机部署支持集中管理，可集中管理多台采集器审计的事件、分析，实现统一配置、统一报表、统一查询；
	支持导入到主流虚拟化平台以模板的方式部署 支持 Sangfor-HCI（vma 格式）、Kvm（qcow2 格式）、Vmware（ova 格式）
#审计能力	支持多种数据库类型的审计 支持 Oracle 数据库审计、SQL-Server 数据库审计、DB2 数据库审计、MySQL 数据库审计、Informix 数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql 数据库审计、sysbase 数据库审计。 支持同时审计多种数据库及跨多种数据库平台操作 支持在 windows 平台上安装插件的方式审计，插件方式更快捷更稳定，无需改变系统内核和驱动的原有工作方式来支撑审计，有效防止修改内核或驱动带来的系统崩溃隐患。
	超长 SQL 语句解析、记录、账号、关联 SQL 操作语句绑定变量参数。
	支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌。
	支持客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数、影响行数、响应内容等实现对敏感数据库操作的精细监控;
	支持 HTTP 请求审计，可指定 GET、POST、URL、响应码进行精细审计。
	支持时间段、源 IP、业务系统、搜索关键字等对 WEB 审计日志进行精细检索。管理员操作日志检索。
	深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库类型、操作类型、SQL 语句、SQL 模版、客户端程序名、响应码、影响行数、返回行数、SQL 预计响应时间。

	支持三层架构下 web 要素审计。 提供 web 审计日志的查询页面，支持通过日期、源 IP、业务系统、以及指定 url 地址作为搜索关键字进行过滤查询，查询结果包括源区域、目的区域、操作对象、影响结果及其 web 三层关联信息。
	允许查看 SQL 语句会话日志、柱状图、会话视图等。
数据库安全	内置大量 SQL 安全规则包括如下： 内置大量的 SQL 安全规则可以针对导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等。
	SQL 语句安全检测：暴库、撞库：识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。
	支持基于 SQL 命令的 webshell 检测：提供 webshell 日志查询功能，可查看 webshell 攻击的时间、源 IP、业务系统、webshell 名称、webshell 所在目录
统计分析	支持以源 IP、业务主机、操作类型、SQL 模版、数据库用户为维度的数据库行为排行。
	支持吞吐量分析，包括 SQL 语句吞吐量排行、SQL 语句吞吐量趋势、SQL 操作类型吞吐量排行、SQL 操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势。
	精细化日志秒级查询：通过 SQL 串模式抽取保障磁盘 IO 的读写性能；分离式存储 SQL 语句保障数据审计速度快，TB 级日志秒级查询、支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多 SQL 语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询。

	支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询。
	支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。
风险分析	旁路主动发 rest 包阻断技术 Netfilter 框架技术可针对 IP、端口、业务系统做精准阻断。
响应方式	提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 管理员支持下面几种角色
	支持系统异常、磁盘空间占用过高、采集器离线等告警。
系统管理	支持日志备份和日志恢复。支持 Syslog 方式向外发送审计日志；支持 SNMP 方式，提供系统运行状态给第三方网管系统；

2.2.24 堡垒机

技术指标	指标要求
▲规格性能	标准 2U 机架式设备，硬盘≥2TB，企业级，冗余电源，千兆电口≥6 个
	提供≥600 个资源授权，提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护三级建设要求
支持类型	支持 windows 系统、linux/unix 系统、网络设备
	支持 KVM、Vmware、数据库、http/https 等
#用户与资产管理	支持批量导入、导出用户信息及设备信息
	支持从 windows AD 域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式
	支持 Windows AD 域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号
	支持资源发现功能，可自动发现目标网段内的设备
	支持 windows 系统、网络设备、linux/unix 系统、数据库等设备账号的收集功能
运维授权	支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个

	用户授予多个资产，用户组向资产组授权
	支持跨部门的交叉授权操作
认证管理	同时支持本地口令认证、LDAP 认证、AD 认证、短信认证、Radius、usbkey、动态口令认证
改密计划	支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式
	支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容
	支持口令有效期设置，用户账号口令到期强制用户修改自身口令
	支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存
访问审批	支持自定义多级审批流程，可设置一级或多级审批人，每级审批流程可以指定通过投票数，用户访问关键设备需相关审批人逐级审批通过才允许访问
紧急运维	支持紧急运维流程，当运维人员需对目标设备进行紧急运维时，可通过紧急运维流程直接访问目标设备，同时记录为紧急运维工单，便于相关审批人事后对该流程进行确认以及审计员事后查看
双人复核	支持双人复核登陆，登录时必须经过第二人授权后才能登录，第二人可通过远程授权或同终端授权两种方式实现授权
访问控制	支持用户访问时间策略、资源访问时间策略、用户 IP 地址策略
命令过滤	支持基于单条操作命令或命令组设置行为规则，当运维人员输入违规命令时（包括通过 table 键、上下键、复制等方式）自动进行告警或阻断
命令审批	支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行
	命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人；
行为审计	支持对常见设备运维操作进行记录（至少包括 windows 主机、linux/unix 主机、网络设备等），审计信息至少包括以下内容：用户账户、起止时间、登陆 IP、设备 IP、设备名称、设备类型、访问账号、访问协议等信息
配置审计	支持对堡垒主机的配置行为进行审计记录
运维自查	支持运维审计自查询功能，用户可查看自身的运维审计历史
审计报表	支持自定义报表，可记录审计报表模板，可生成图形报表，并提供 EXCAL、CSV、WORD、PDF、HTML 等格式导出

备份与维护	支持手动和自动定期备份配置信息，支持配置信息本地备份及异地 FTP 备份
	支持系统配置还原，可以还原至任一备份点
	具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚
管理能力	支持 NTP 系统时间同步配置，保证审计日志拥有可靠的时间戳
	支持告警对外转发，转发方式支持 syslog、SNMP 等方式
动作流	支持通过动作流配置完美支持所有 C/S 系统的单点登录功能
虚拟化部署	支持云端快速部署，实现远程运维管理的规范化；可按照运维人员数量，调整云端服务器配置，即可实现性能优化。
客户端兼容	全面支持 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端。
HA 功能	需支持 HA，配置信息实时同步，配置过程在 web 界面完成

2.2.25 NTP 时间服务器

技术指标	指标要求
物理类型	机架式
CPU	32 位 CPU 双核处理器
授时精度	≤10ms
支持协议	NTP/SNTP V10，V20，V30，V40，SNMP，UDP，Telnet，IP，TCP
网口数量	**≥2 个 10/100M 自适应以太网**
吞吐量	**可满足每秒每口不少于 2000 次时间请求**
授时记录	**至少保存最新 50 条**
卫星接收机	**至少应支持或兼容北斗**
输出接口	**支持 RS232/485，IRIG-B，10M，1PPS**

2.2.26 应用流量分析

技术指标	指标要求
规格	1U 机箱，双电源
#存储空间	≥16TB
#流量接入	4 个千兆电口/光口数据口或者 1 个万兆光口，2 个千兆管理口
实时分析流量	≥ 2Gbps
#模块配置	1 个 Ni-Network 模块，采集器 1 个，分析 L2-L4 层协议；

	Ni-Application 模块 1 个，持 Web 用户体验，性能分析以及 Oracle， SQL Server， MySQL， PostgreSQL 的 SQL 语句，用户，并发连接数监控

2.2.27 网络审计系统

技术指标	指标要求
▲性能参数	标准 2U 机架式设备，硬盘≥1TB，冗余电源，千兆电口≥4 个，千兆光口≥4 个，具备 RJ45 串口和 USB 接口。默认接口均可作为监听口。
#部署方式	支持网关（路由），网桥，旁路模式，两台及两台以上设备同时做主机的部署模式，支持基于虚拟化平台的软件版本，支持 NAT、路由转发、DHCP、多路桥接功能等功能；
#IPV6	所有功能（认证、应用控制、内容审计、报表等）都支持部署在 IPv6 环境中
#设备管理	支持攻击、双机切换告警、移动管理告警、web 关键字过滤告警、磁盘/CPU/内存异常告警等；
	具有 IPSec VPN 远程加密访问和连接的模块，并能提供 IPSec VPN 客户端授权远程接入访问；
实时监控	提供设备实时 CPU、内存、磁盘、会话数、用户数、网络接口、网络质量、移动终端等信息；
	针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向 web 访问质量检测
用户管理	支持触发式 WEB 认证，静态用户名密码认证；支持 LDAP、Radius、POP3、Proxy 等第三方认证；支持数据库认证；支持以 USB-Key 方式实现双因素身份认证，支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等；支持短信认证方式，支持微信认证
	同一个账号，支持与指定数量的多个终端进行自动绑定；
	支持二维码认证，管理员扫描访客的二维码后对其网络访问授权
	可设置用户密码不能等于用户名；新密码不能与旧密码相同；可设置密

	码最小长度；可设置密码必须包括数字或字母或特殊字符；
应用控制	设备内置应用识别规则库，支持超过 4700 条应用规则数，支持超过 2100 种以上的应用，660 种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率；
	支持对加密 HTTPS、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电邮客户端的邮件进行关键字过滤；（提供实际测试效果图）
	支持对加密 HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-TLS 、IMAP-SSL、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电邮客户端邮件内容的审计。（提供实际测试效果图）
	用户指定应用上网流速超过预设阈值后，网关自动提醒该用户；
	支持上网策略对象的自动过期功能；
	设备内置业界知名杀毒引擎; 必须支持 HTTP 下载、FTP 下载、POP3、SMTP 杀毒；支持对 HTTP、FTP 等下载中启用文件类型杀毒；病毒库支持通过服务器或本地加载病毒库方式定期升级；
#上网行为审计	支持记录全部或者指定类别 URL、网页标题、网页正文内容、关键字网页正文内容、SSL 加密网页的内容; 审计 SSL 网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成，解决管理员给每台 PC 单独安装证书的问题； 支持对网页过滤和网页审计分开控制，支持审计指定类型的 URL，其他 URL 类型不予审计，以提高审计效率; 支持在审计时，将行为与内容分离，即可分别设置只审计用户行为还是审计内容； 支持审计用户的明文发帖内容； 支持网页内容审计后的网页快照功能； 支持审计用户的 Webmail 邮件外发行为，支持 webmail 形式发送的附件审计，并能精准到原始邮件；能审计用户通过 SSL 加密 Webmail 网站外发邮件的内容、邮件的正文及附件、使用邮件客户端外发 SSL 加密邮件的邮件内容； 必须能审计记录无后缀名的文件外发行为，篡改后缀名的文件外发行为; 必须能将压缩包解压后识别文件类型并记录；

	必须能对加密文件外发行为识别并记录； 记录 Web qq、mini qq、Web msn、qq mail 等 Web IM 的聊天内容、登陆和注销行为，且不需要安装插件； 审计用户通过 iphone/ipad 登陆 web IM 聊天行为和内容；支持记录 QQ、MSN、skype、飞信、雅虎通等 IM 聊天行为和内容；支持用户离线情况下审计 IM 聊天行为和内容；支持根据 QQ、MSN 账号查询 IM 聊天行为和内容；记录 QQ、MSN 传文件动作和所传文件内容，并可指定记录传文件类型和文件长度；支持同时审计 QQ 聊天内容和 QQ 传文件内容。 支持对阿里旺旺、路透等应用的聊天，群聊天等内容的审计 支持审计通过 FTP 上传的文件名和内容、通过 FTP 下载的文件名、支持审计 TELNET 执行的命令； 审计用户使用 P2P、流媒体、炒股、网络游戏、FTP、Telnet 等应用行为； 记录用户在指定时间段内使用指定应用的总时长、网络应用流量、产生的总流量、应用的总流量； 必须能审计来自外网访问内网站的行为、外网在内网服务器下载上传文件的行为、外网在内网服务器发帖的行为、外网从内网服务器上收发邮件的行为； 支持审计管理员的操作日志、系统日志等；
上网日志管理	设备必须支持内置数据中心和独立数据中心，支持日志高性能模式处理，精简冗余日志；
	提供服务器虚拟化产品与外置 DC 联动，服务器虚拟化能够根据实际用户和流量规模合理分配硬件资源，保障最优资源分配。同时，外置 DC 能够与服务器虚拟化底层联动，优化磁盘读写，提高查询速度
	管理员登录数据中心只能审计指定用户组的上网行为日志；
	支持基于时间段/用户/用户组/终端类型/位置等维度的应用流速趋势、网站分类流速趋势报表
	支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱
	内置多套日志模板与日志平台对接，至少支持以下平台：派博、任子行、

	网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。

2.2.28 TAP 分路器

技术指标	**指标要求**
基本配置	流量复制/汇聚一体化： 流量复制引擎复制能力不小于 6Gb： 支持 6 个千兆电口输入/输出模式灵活切换： 支持以太网封装无关性支持： 支持输出端口开启流量回送功能： 支持 console、IP/WEB、SNMP 等管理：
全双工线速流量复制	支持 1->N、M->N、M->N 路流量复制汇聚 支持所有端口线速工作不丢包

2.2.29 安全态势感知系统

技术指标	指标要求
▲性能参数	标准 1U 机架式设备，CPU≥4 核，物理内存≥32G，SSD ≥128G，SATA ≥4T*4，支持 RAID50，单电源，≥6 个千兆电口，1 个 DB9 串口，6 个 USB 接口。
资产自动识别	支持自动识别网络内部主机网段和外网网段； 支持通过流量中的应用内容自动区分网络内部网段 IP 是属于 PC 还是服务器；
自动识别服务器信息	支持自动识别资产，在不影响内部网络的前提下，通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息，如：操作系统、开放的端口号等；
	支持自动识别已知服务器，通过被动检测机制，对经过探针的流量进行分析，识别已知服务器对外提供的所有服务、已开放端口及端口传输的协议/应用等；
弱密码扫描	支持通过镜像流量检测数据包中存在的用户名和密码信息，通过分析密码的强度检测网络中存在的弱密码风险；

Web 明文检测	支持通过镜像流量检测 web 流量中是否存在可截获的口令信息，分析 web 业务系统是否存在明文传输情况，避免因明文传输导致信息泄露的风险。；
漏洞报告	支持流量分析实时发现操作系统、数据库、web 应用等存在的漏洞风险，看清网络脆弱性，并支持生成漏洞检测报告。
僵尸网络检测	具备僵尸网络识别能力，行为规则近 40 万条，并能够与 CNCERT、VIRUSTOTAL 等国内外权威机构共享威胁情报； 支持通过云端沙盒对全球威胁情报源进行验证，提取有效信息形成规则定期更新到僵尸网络识别库，增量提升检测能力；
恶意 DNS 协议检测	支持 DNSFlow 分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意 DNS 协议；
SMB 检测	支持 SMBFlow 分析引擎，利用机器学习技术，发现主机传输可疑文件、恶意软件行为、文件或关键目录的可疑操作行为以及 SMB 暴力破解等；
邮件检测	支持 SMTPFlow 分析引擎，利用机器学习技术技术，发现主机发送可疑附件的邮件行为、伪造发件人发送邮件、发送钓鱼网站邮件和垃圾邮件等行为；
Webshell 攻击检测	支持 HttpFlow 分析引擎，利用机器学习技术，发现绕过防御的 webshell 攻击，并能够大幅度降低传统检测技术带来的误判；
失陷业务检测	支持检测业务的异常行为，从而识别业务是否已失陷被控制，并设立失陷等级和威胁等级展示当前业务的状态和产生的威胁程度；
风险用户检测	支持检测网络内部用户的异常行为，要求能够基于僵尸网络识别库，检测用户是否存在风险，并通过可视化方式展示：风险用户对业务产生的影响、内部的横向攻击、风险/违规行为等；
异常行为检测	支持 NetFlow 分析引擎，利用 UEBA 方式来检测服务器外发异常，包括是否正在进行 DoS 攻击、网络内部的横向探测：如 IP 扫描、端口扫描、数据收集（如到其他服务器下载）或数据传输（将数据传给其他服务器或外网）。
APT C&C 通信	支持检测主机与 C&C 服务器通信行为，支持区分国内外区域；
可疑行为	支持检测从未知站点下载可执行文件、访问恶意链接、使用 IRC 协议进行通信、浏览最近 30 天注册域名、下载文件格式与实际文件不符、基于行为检测的木马远控、比特币挖矿等可疑访问行为，支持区分国内外区域和显示可疑行为访问趋势；；

隐蔽通信	支持检测隧道、Tor 暗网通信、端口反弹等对外通信方式，支持区分国内外区域；
违规访问	支持检测违规访问策略黑名单或违反了白名单，或者违反了下一代防火墙中的应用控制策略的行为
风险访问	支持检测服务器对外发起的远程登录、远程桌面、数据库等风险应用访问
外连攻击	支持检测主机对外发起的攻击行为
数据索引	支持记录用户网络当中南北向和东西向的访问信息，包括时间、五元组、具体应用、归属地、访问次数、流量大小等各类实时信息；
	依托于大数据检索能力，提供详细的日志查询功能，便于事后取证；
漏洞利用攻击检测	支持对服务器、客户端的各种应用发起的漏洞攻击进行检测，包括 20 种攻击类型共 9000+以上规则；
WEB 应用攻击检测	支持检测针对 WEB 应用的攻击，如 SQL 注入、XSS、系统命令等注入型攻击； 支持跨站请求伪造 CSRF 攻击检测； 支持对 ASP，PHP，JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测； 支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；
	要求具备独立的 Web 应用检测规则库，Web 应用检测规则总数在 3000 条以上；
宏观监控	支持图形化大屏的横向威胁大屏展示，包括但不限于横向威胁趋势，威胁类型分布、被访问业务 TOP5、攻击源 TOP5、违规访问源 TOP5、可疑访问源 TOP5、风险访问源 TOP5；
微观监控	支持展示外网对网络内部尝试（或已成功）进行的远程登陆、数据库访问等行为，可查看明细列表，内容包括但不限于外网 IP、受影响网络内部主机 IP、外部风险访问者数等；
	支持对业务的外连行为进行监测，以可视化的方式展示业务外连的地域分布、是否存在风险、外连趋势等，并提供详细的外连日志查询；
	支持基于用户/业务维度的访问关系梳理，可呈现该用户/业务已经通过哪些应用、协议和端口访问了哪些业务，这些访问是否是攻击、违规、远程

	登陆等行为，IT 人员可清晰的看出已对哪些业务存在影响，也能推导当前用户是否已失陷（或可疑）。
综合安全风险报告	支持提供 Word 格式报表形式的综合风险报告，包含安全风险概况、业务与终端安全详情分析、安全规划建议等，综合分析业务系统和终端的安全风险详情；
摘要报告	支持提供 PDF 格式报表形式的摘要报告，包含总体摘要、安全感知详情、UEBA 行为画像、安全规划建设建议等，从整体展示安全状况，快速了解业务和网络的安全风险
联动响应	支持与防火墙设备进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击 IP；
安全告警	支持以邮件的形式及时将发现的失陷业务、失陷用户、攻击成功事件等安全事件进行告警，支持根据安全事件类型配置发送间隔和触发条件；

2.2.30 安全态势感知系统探针

技术指标	指标要求
▲性能参数	标准 2U 机架式设备，千兆电口≥4 个，千兆光口≥4 个，1 个 RJ45 接口，2 个 USB 接口，支持流量性能≥1.5Gbps，包转发率≥2.232Mbps，每秒新建连接数≥10 万，最大并发连接数≥200 万，CPU≥2 核，物理内存≥4G，硬盘≥SATA 1T。
部署模式	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响
资产发现	具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等
#基础检测功能	具备报文检测引擎，可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等，具备多种的入侵攻击模式或恶意 URL 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录，在特征事件触发时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，

	影响系统，对应 CVE 编号
异常会话检测	可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内的多场景网络异常通信行为分析能力。
深度监测能力	可提供网络流量的会话级视图，根据网络流量的正常行为轮廓特征建立正常流量模型，判别流量是否出现异常，对原始流记录进行异常检测，可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗，IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型; 支持对节点检测节点内部主机外发的异常流量进行检测支持对信任区域主机外发的异常流量进行检测，如 ICMP，UPD，SYN，DNS Flood 等 DDoS 攻击行为; 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解检测功能; 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测
高级检测	支持 5 种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求
	支持 DNS 审计日志，主要用于平台 dns flow 分析引擎进行安全分析;HTTP 审计日志，主要用于平台 http flow 分析引擎进行安全分析；SMB 审计日志，主要用于平台 SMB flow 分析引擎进行安全分析；同步 SMTP、POP3、IMAP 审计日志，主要用于平台 Mail flow 分析引擎进行安全分析，同步 AD 域协议审计日志，主要用于平台 AD 域分析引擎进行安全分析
Web 应用安全检测能力	支持 HTTP 1.0/1.1，HTTPS 协议的安全威胁检测; 支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；支持跨站请求伪造 CSRF 攻击检测；支持对 ASP，PHP，JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测; 产品应具备独立的 Web 应用检测规则库，Web 应用检测规则总数在 3000 条以上;

	支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； 支持对被 Web 网站是否被挂黑链进行检测
僵尸网络检测	支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 具备独立的僵尸主机识别特征库，恶意软件识别特征总数在 35 万条以上； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁特征；
违规访问检测	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式
流量记录	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式
管理功能	能够支持时间同步 支持设备内置简单命令行管理窗口，便于基础运维调试 能够提供网络管理功能，可进行静态路由配置 多次登录失败将锁定账号 5 分钟内不得登录 可支持在线升级和离线升级，并依托安全感知平台进行统一管控 可支持用户初次登陆强制修改密码功能。 可实时监控设备的 CPU、内存、存储空间使用情况。 能够监控监听接口的实时流量情况
集中管控	支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；

2.2.31 日志审计系统

技术指标	具体功能要求
产品结构	要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁；
▲产品架构	标准2U机架式设备，支持≥400个主机审计许可证书，系统盘≥64G，硬盘≥8TB，千兆电口≥6个；支持获取各种主流网络及数据库访问行为，支持Syslog、WMI、OPSEC Lea、SNMP trap专用协议等协议事件日志，支持通过Http、Https、FTP、SFTP、SMB等协议获取各类文件型日志，支持基于SQL/XML标准内容获取；
操作系统	深度定制优化的Linux系统；
管理方式	B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端；
设备部署	提供旁路接入模式，设备部署不影响原有网络结构；
数据存储	所供系统设备必须自带本地存储功能； 可用物理磁盘空间>=1TB；日志存储量至少十亿条；（指标以原厂公开资料为准）； RAID架构以保证数据可靠性，（指标以原厂公开资料为准）； 支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)；
网络接口	审计主机至少提供千兆RJ45*6（一路数据传输口；一路系统管理口）； 网络接口支持电口，可升级为光口；
处理性能	日志采集能力：3000条/秒以上
数据采集	支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]； 支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、

	Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神] 支持Opsec Lea日志采集； 支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控； 支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储； 支持文本型日志原始文件管理，可将系统作为日志服务器使用；
监控功能	支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况； 支持自定义配置实时监控的日志类型； 支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警； 支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况； 支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作；
报表分析功能	系统内置多种类报表模板； 支持动态\静态（日报、周报、月报）两种系统生成方式； 支持报告的邮件转发、生成提醒功能；支持多人邮件接收； 支持自定义审计报告； 支持导出html、Excel、PDF； 支持管理员自定义审计报表模板；
查询分析功能	支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索； 支持以日志类型、时间范围及条件字段快速检索过滤； 支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询；

	支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件； 支持查询模版创建、修改、删除功能； 支持查询结果导出；
策略管理功能	支持内置归并策略，对HTTP数据进行自动归并处理； 支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件； 支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问； 支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略； 规则条件设定支持逻辑运算符与支持正则表达式； 支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息； 支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息；
数据管理功能	支持按日志属性、日志类型、时间范围进行数据备份； 支持WEB界面备份及日志恢复导入工作； 支持自动与手动两种备份归档方式； 系统支持以FTP上传方式将归档文件存储到第三方存储系统中；
系统配置功能	支持审计系统用户（组）管理（添加、修改、删除、停用、启用）； 支持资产管理，即所有采集日志源管理维护； 支持密码长度、复杂度，密码猜测自动锁定账号以及系统超时设置安全策略； 支持证书页面生成下载； 支持系统配置备份恢复； 支持时间同步页面配置； 支持页面方式系统升级以及设备关闭、重启； 支持从WEB界面查看网卡IP设置，修改静态路由设置等内容； 支持安全页面（SSL）证书下载；
系统自身安全	系统内置安全防火墙；支持控制访问审计主机范围； 必需提供内部通讯检查机制，传输 128 加密；

	管理接口支持串口或电口的方式管理； 管理界面与其他功能模块分离；
日志数据安全	审计日志文件方式存储； 审计日志加密导出审计系统； 支持对所有审计管理员操作审计系统的动作进行审计；
日志权限	审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明； 支持日志类型、IP 地址权限设置； 支持页面功能模块权限设置；
系统升级二次开发	在设备维保期内，厂家提供对系统软件的升级服务，保证系统软件为最新版本； 根据用户需求定制开发相关内容，包括关联报表和特定业务日志审计等功能；
系统许可	内置不低于 50 个主机审计许可证书；

2.2.32 网络流量回溯分析

技术指标	指标要求
系统架构	标准机架式硬件设备。
#硬件接口	千兆电口采集口≥2 个，千兆光口采集口≥2 个，千兆管理端口≥2 个。
▲处理性能	数据包实时线速处理能力≥800Mbps，，数据包处理能力≥200,000pps，TCP/UDP 会话处理能力≥ 每秒 50，000 系统存储容量≥8TB
界面要求	支持全中文界面和资料文档。
	支持中英文双语协议解码功能，须在一个图形界面中同时显示中文、英文解码。
数据采集	能够实现链路聚合功能，能将多网卡的流量聚合捕获分析。
	支持数据包回放功能，能够将已捕获的数据包文件在系统上进行回放分析，实现与实时采集链路相同的分析功能。
	支持 VxLAN 虚链路分析，能够根据 VxLAN ID 设置虚链路，实现对 SDN 网络特定 VxLAN 流量的分析。
数据分析	数据包以专用格式存储，采用 C/S 架构控制台软件读取和导出，不能

	用其他工具读取并导出。
	支持按秒级精度进行流量趋势展现，刷新频率为 1 秒。
	能够对 TCP 会话中的详细应用数据传输过程进行深入分析，能够区分每一个应用交易处理请求和响应，对传输过程中的重传、重复的确认进行统计，对应用交易处理间隔响应进行分析。
	专用控制台可以按任意时间、IP 等方式过滤下载原始数据包，并支持 cap、pcap、cscpkt、rapkt 等格式数据包的即时解码、导出，而不需要借助第三方协议分析工具。
#流量回溯	可对历史数据统计分析结果进行下载并进行二次分析，二次分析结果包括数据包解码和数据流分析视图，可以查看数据包的详细信息，分析结果可导出。
	能在流量趋势视图中选择任意历史时间段的数据进行诊断分析，可以查看选定时间段的统计分析结果，统计分析结果包括概要统计、网络应用、IP 地址、物理地址、IP 会话、物理会话、TCP 会话、UDP 会话、警报日志等。
监测分析	能够根据端口、端口组、IP 地址、IP 地址组、IP 地址+端口、HTTP 应用请求中的 URL 值等自定义应用，针对自定义的应用进行流量监测分析。
交易分析	可以通过配置文件的方式对 XML 交易的识别方式、XML 交易的匹配方式、交易输出内容、交易的响应时间等级进行设置和统计。
产品和技术培训	提供专业的网络分析技术培训，培训课程包括：网络分析技术基础、常见网络异常行为、TCP 协议介绍、TCP 传输分析、应用交易处理分析、DOS 攻击原理及分析、端口扫描原理及分析、网络分析方法总结等。

2.2.33 容灾备份一体机

技术指标	指标要求
▲配置	机架式，标配原厂导轨，支持标准机柜。 配置 2 颗 64 位八核处理器。 配置≥128GB 内存。 可支持 16 个热插拔位，配备≥480TB 硬盘。

	网口：≥2 个千兆以太网接口，≥2 个万兆口 两个冗余热插拔 800W 交流电源
#功能项	设备基于存储系统专用的嵌入式系统，设备底层为存储架构，存储系统及软件预装在独立的存储介质中，不占用 RAID 硬盘组的存储空间。
	支持 RAID 0、RAID 1、RAID 5、RAID6、RAID 50、RAID 60、RAID TP（三重奇偶校验）等多种 Raid 方式。其中 Raid TP 应能够在不配置热备磁盘的前提下，可实现任意三块磁盘损坏数据不丢失。
	支持 Windows、Linux、UNIX、AIX、Solaris、 HP-UX 等主流操作系统，以及龙芯、飞腾、鲲鹏、海光、兆芯架构下中标麒麟、银河麒麟等操作系统
	提供 Oracle 、SQLServer 等数据库的一致性代理功能，保证任意快照时刻的数据库均可挂载启动。

2.3 安全及扩展服务

（1）安全要求

投标人应保证业务应用系统的支撑环境，包括但不限于服务器、网络、存储等相关物理环境能满足安全等保三级要求，并积极配合采购人根据业务系统具体等保需求，开展相应等保评估、检查、整改等工作。投标人管辖范围内的硬件、软件及支撑环境资源，至少达到业务系统的最高安全等级要求。

（2）扩展要求

投标人应按照各系统的特点灵活调整计算、存储等各类资源供给，并能够根据业务数据的变化及时扩容或缩减存储空间，确保系统高峰时段或特殊时期的访问需求。

2.4 应用系统迁移及业务连续性要求

（1）迁移经验要求

投标人必须具备系统迁移能力，可根据业务特点制定应用系统迁移部署方案，配合用户完成系统迁移部署、运行和安全保障，迁移过程中保证应用系统业务延续不中断。

（2）迁移进度要求

本项目需要在 7 天内（包含 7 天）完成系统迁移，在合同签订后，中标人根据承诺迁移周期及采购人需求完成政务云测试、试运行、系统迁移上线工作，并且不能改变和影响

采购人原有系统的功能、技术状态、数据完整性。

（3）迁移费用要求

针对已经在政务云平台上的试运行应用系统的迁移需求，为确保迁移过程中数据不丢失、系统业务不中断，本次中标人负责与原政务云平台的服务商进行主动对接，系统迁移所需各项费用（包括但不限于中标人迁移测试阶段的云资源费用、业务系统部署费用、调试费等），由本次中标人负责解决并包含在本次投标报价中。

3. 验收标准

中标人确定后，按照合同要求开始服务工作。

验收标准按照合同中约定的服务内容、服务方案、服务质量等要求执行。

项目验收分为项目中期检查和项目终验：

1．项目中期检查验收：中标人向采购人提交工作阶段总结和相关材料，得到采购人认可后，由采购人组织开展项目中期检查验收。检查标准以本合同附件以及相关说明文档为标准，具体时间和地点由双方商议安排，检查结果出具书面意见。

2．项目终验：中标人向采购人提交工作整体总结和相关材料，得到采购人认可后，由采购人组织开展项目终验。终验标准以本合同附件以及相关说明文档为标准，具体时间和地点由双方商议安排，终验结果出具书面意见。

4.其他要求

4.1.服务要求

（1）服务方式

投标人需利用监控系统或人工对硬件设备及应用系统的运行情况进行 7*24 小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。

投标人负责设立技术支持热线，并安排专人值守，为北京市规划和自然资源委员会提供 7*24 小时热线支持服务。投标人针对采购人要求的云平台运维服务相关内容，需指定专业技术能力较强的工程师，根据采购人要求配合开展相关维护服务。

（2）安全及保密要求

投标人须严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏给第三方。

（3）响应的及时性

投标人应当提供高效的系统维护服务，有效防范系统风险，系统对应负责人 7*24 小时电话畅通，在系统发生除宕机外的其他故障问题时，投标人应在 10 分钟内响应，在 1 个小时之内使系统恢复正常，故障处理完毕后提供相关系统宕机报告。

（4）重点保障要求

为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求投标人根据业务周期性特点，加大运维保障力度，保证在业务高峰期内系统平稳运行。

4.2 考核要求

根据北京市级政务云考核要求，按照制定的绩效考核指标体系及服务承诺要求，对服务质量的考核。

政务云服务实行季度考核制。考核工作主要分为两部分：基本指标和综合指标，具体内容如下：

（1）考核标准

类别	序号	服务指标项	考核标准	单项指标
基本指标	1	服务团队稳定性	考核周期（季度）内，团队稳定，人员配备充实，工作规范有序，得 5 分，反之得 0 分；	10
			考核周期（季度）内，服务团队与其他单位有效协作得 5 分，发现一次不合作扣 1 分，扣完为止。	
	2	系统安全稳定	考核周期（季度）内，无因政务云引起的安全事故发生，得 20 分；	20
			考核周期（季度）内，因政务云引起的安全事故发生次数不高于 1 次，得 10 分；	
			考核周期（季度）内，因政务云环境引起的安全事故发生次数≥2 次，得 0 分；	
			考核周期（季度）内，发生一次因政务云引起的市级安全事故通报，本项直接得 0 分。	
	3	保密管理	考核周期（季度）内，无因政务云引起的敏感信息的事件泄露等情况发生，得 10 分；	10

			考核周期（季度）内，因政务云引起的敏感信息的事件泄露出现≥1 次，得 0 分。	
	4	系统故障合计	考核周期（季度）内，发生因政务云引起的重大安全事故（详见合同范本中附件 2 的《重大违约行为表》），本项得 0 分；	10
			考核周期（季度）内，发生因政务云引起的严重安全事故（详见合同范本中附件 3 的《严重违约行为表》），本项得 3 分；	
			考核周期（季度）内，发生因政务云引起的一般安全事故（详见合同范本中附件 4 的《一般违约行为表》），本项得 5 分；	
			考核周期（季度）内，未发生因政务云引起任何安全事件，本项得 10 分。	
	5	系统故障恢复时间	考核周期（季度）内，因政务云引起的系统故障或丢失数据等情况平均恢复时间≤30 分钟，得 10 分；	10
			考核周期（季度）内，因政务云引起的系统故障或丢失数据等情况平均恢复时间＞30 分钟且≤60 分钟，得 5 分；	
			考核周期（季度）内，因政务云引起的系统故障或丢失数据等情况平均恢复时间＞60 分钟，得 0 分。	
	6	未及时发现系统故障或发现故障未及时报告	考核周期（季度）内，出现故障及时发现、发现故障及时报告，得 10 分；	10
			考核周期（季度）内，出现故障未及时发现或发现故障未及时报告，发现 1 次扣 2 分，扣完为止。	
综合指标	7	服务态度、客户满意度	服考核周期（季度）内，务态度、客户满意度综合评价为优，得 10 分；	10
			考核周期（季度）内，服务态度、客户满意度综合评价为良，得 5 分；	

			考核周期（季度）内，服务态度、客户满意度综合评价为不佳，得 0 分。	
	8	运维工作完成及时性	考核周期（季度）内，服务工作完成及时性评价为优，得 10 分；	10
			考核周期（季度）内，服务工作完成及时性评价为良，得 5 分；	
			考核周期（季度）内，服务工作完成及时性评价为不佳，得 0 分。	
	9	文档完整性和质量	考核周期（季度）内，项目文档齐全、规范、完整、准确，得 10 分；	10
			考核周期（季度）内，文档完整性、规范性和质量较好，得 5 分；	
			考核周期（季度）内，文档完整性、规范性和质量不佳，得 0 分。	

（2）支付依据

在一个考核周期内，通过对各项考核指标进行打分和计算，汇总出在考核周期内的服务指标考核值：

如果服务指标考核值低于 60 分，则由采购人考核小组研究决定是否支付本周期服务费，但最多支付该支付周期内服务费的 50%；

如果服务指标考核值大于等于 60 分，并且低于 70 分，则支付该周期内服务费的 80%；

如果服务指标考核值大于等于 70 分，并且低于 80 分，则支付该周期内服务费的 90%；

如果服务指标考核值大于等于 80 分，则支付该周期内服务费的 100%。

若出现服务指标考核值低于 80 分的情况，则在第二笔款和第三笔款的支付时扣除相应服务费。

（3）考核方式为采购人组织成立考核小组，基于服务考核指标，对服务工作进行评估。

4.3 售后服务及培训要求

（1）投标人提供 1 名项目负责人（项目经理）、1 名技术负责人及不少于 9 名项目团队人员，为本项目提供运维和技术支持服务工作，其中项目经理与技术负责人不可兼任。项目团队人员在项目实施过程中未经采购人同意不得随意更换。

其中：项目经理应具有信息系统项目管理师（高级）证书，技术负责人应具备注册信息安全专业人员证书或网络工程师证书。项目组人员（除项目经理和技术负责人之外）应具有中级及以上工程师职称、注册信息安全专业人员证书（CISP）、网络工程师证书、信息安全工程师证书。

（2）投标人提供 7×24 小时技术支持，为采购人提供良好的咨询服务。保证系统 7×24 小时不间断稳定运行，系统故障时间不能超过 1 小时（经北京市规划和自然资源委员会或主管部门批准的系统停机维护时间除外）。

（3）提供 7×24 小时的网络安全事件应急响应服务，协助分析安全故障和事件原因，提供相应咨询，协助处理安全故障、消除入侵路径并协助采购人恢复系统正常工作，对故障 10 分钟内响应。

（4）对采购人进行培训，中标人负责按采购人要求布置培训环境，提供培训教师和培训教材。

4.4 政策性采购需求：

为在项目中充分落实《政府采购法》规定的“政府采购应当有助于实现国家的经济和社会发展政策目标”等相关要求，以项目为载体推动北京市环境社会治理(ESG)体系高质量发展，请供应商提供在本项目中落实 ESG 理念的工作措施。

第六章　拟签订的合同文本

北京市市级政务云服务协议

项目名称：　政务云租用

甲　　方：　北京市规划和自然资源委员会

乙　　方：

合同签订时间：　　年　　月　　日

甲乙双方根据《中华人民共和国民法典》及相关法律法规的规定，在《北京市市级政务云管理办法》的基础上，经过友好协商，就乙方为甲方提供北京市政务云服务(下称“服务”)事宜订立以下协议，以资共同遵守。

第一条 项目角色定义

1、云服务商：协议乙方，_____。

2、使用单位：协议甲方，北京市规划和自然资源委员会。

3、政务云管理单位：北京市政务服务和数据管理局。

4、云综合监管服务商：经政务云管理单位授权，开展政务云安全、技术监督管理和服务评价的单位。

5、信息系统服务商：为甲方提供信息系统等建设或维护服务的服务商。

第二条 服务内容

1、 甲方应按照《北京市市级政务云管理办法》的有关规定，将如下信息系统部署或迁移至乙方云平台，同时对信息系统开展运维工作。

1	北京市规划和自然资源委员会规划编制与实施监督平台
2	北京市规划和自然资源委员会批后监管与全过程监督平台
3	北京市规划和自然资源委员会自然资源监测管理平台
4	北京市不动产登记信息管理基础平台
5	北京市规划和自然资源委员会综合执法与专项治理平台
6	北京市规划和自然资源委员会多规合一协同信息平台
7	北京市规划和自然资源委员会国土空间基础信息平台
8	北京市规划和自然资源委员会项目审批办事服务平台
9	北京市规划和自然资源委员会领导决策指挥平台
10	北京市规划和自然资源委员会行政办公平台
11	北京市规划和自然资源委员会门户

2、本协议期限内，乙方向甲方上面 11 个平台系统，提供如下扩展云服务或云资源租用服务。甲方根据业务需要，与乙方协商选择云服务项目，如下：

（1）政务云租用服务（详见附件 1 分项明细及报价表）

（2）基础安全保障服务

基础安全保障服务是云服务商应具备的云平台层安全保障能力，使用单位无需购买即可

享受服务，具体服务内容如下表：

服务类别	服务目录	项目
安全管理服务	运维人员管理	7x24 小时运维人员管理、安全登记
	机房运维管理	机房设备管理、安全控制
	应急演练	协助云使用单位进行安全应急演练
安全技术服务	物理访问控制	机房进出控制、监控等
	机房三防服务	机房防火、防盗、防雷电
	设备访问审计	设备访问记录、日志统计、安全事件
	出口流量监测	出口流量控制、检测，并且可观测数据，互联网网络行为审计
	本地抗 DDoS 防护	云平台整体提供总带宽为 10Gb 的抗 DDoS 防护
	防火墙安全防护	出口安全
	防入侵监测 IPS	防入侵监测
	远程接入服务	提供 1 个远程登录堡垒机的运维账号
	租户隔离	租户虚拟化层隔离
	租户内部访问控制	租户内部访问权限控制，用户可以自由分配
	云主机监控	提供云上资源的基本监控，CPU、内存使用率等
	角色权限管理	提供通过代入角色实现获取操作权限

第三条 服务水平

1、乙方应为甲方提供本协议约定的全部服务，协助甲方开展信息系统部署迁移工作，做好云主机等云资源或云服务的运维工作。

2、乙方应配合甲方搭建信息系统上云的测试环境，测试期由甲乙双方协商确定。

3、乙方为甲方提供的服务质量应符合国家有关质量法规、质量标准的规定及相关行业的标准。

4、乙方提供的云平台整体可用性应不低于 99.99%，数据可靠性应不低于 99.9999%，云平台应按照等保三级标准建设并通过测评，云平台可按需 7 个自然日快速扩容。

5、乙方提供的云平台应具备资源动态调整机制，根据甲方信息系统运行情况进行资源的动态调整，如遇信息系统使用高峰期，经双方协商可短期内提供的云资源扩容服务，如需要长期使用扩容服务，以北京市级政务云基础服务目录价格为准双方协商费用，并签订补充协议。

6、乙方应提供技术服务热线(7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法，方式应包括邮件、电话、即时通讯工具等。邮件：_____，电话：_____。

7、在服务期内，提供 7*24 小时的现场和技术支持服务，对故障 10 分钟内响应。

8、乙方须具备故障快速定位和恢复能力，故障定位排除时限不超过 60 分钟。

第四条 项目小组及人员要求

甲乙双方应各指派一名代表作为本项目负责人，项目负责人职责范围包括：

1、制定项目计划：牵头制定项目计划。

2、跟踪项目执行：迁移方案设计，云服务使用培训，云服务各阶段验收，服务成果确认等管理工作。

3、项目检查和控制：检查云服务使用过程中各阶段工作质量和进度。协调各种资源，确保项目按计划进度实施。

4、项目沟通协调：负责协调解决组织接口及技术接口问题，沟通项目售前、售后情况，解决云服务使用过程中出现的相关问题。

5、甲方项目负责人及联系方式：_____。

6、乙方项目负责人及联系方式：_____。

第五条 服务期限

1、乙方应自协议签署之日起，在甲方提交《北京市市级政务云服务统一工单》后10个工作日内，完成云资源分配、新用户创建，并交付使用。

2、乙方为甲方提供为期 12 个月的政务云资源租用服务，自 2026 年 1 月 1 日起，至 2026 年 12 月 31 日止。

3、合同履行期限：2026 年 1 月 1 日起至 2027 年 3 月 31 日止。

4、本协议期满，乙方应协助甲方完成系统及数据的迁移，以免丢失重要信息。

第六条 服务验收

1、项目验收分为项目中期检查和项目终验：

（1）项目中期检查验收：乙方应于 2026 年 7 月 15 日前，向甲方提交运维工作阶段总结和相关材料，得到甲方认可后，由甲方组织开展项目中期检查。检查标准以本合同附件以及相关说明文档为标准，具体时间和地点由甲乙双方商议安排，检查结果出具书面意见。

（2）项目终验：乙方应于 2027 年 1 月 15 日前向甲方提交运维工作整体总结和相关材料，得到甲方认可后，由甲乙双方组织对项目进行验收，验收标准以本合同附件以及相关说明文档为标准，具体时间和地点由甲乙双方商议安排，验收结果出具书面意见。

（3）验收结果分为通过与不通过。对于未通过的情况，由乙方按照甲方的意见采取补救措施后再次进行项目验收。如两次验收不通过，甲方有权单方解除本合同，并有权要求乙方退还甲方已支付的全部费用（含利息，按全国银行间同业拆借中心公布的贷款市场报价利率计算），并按照总费用的 10%向甲方支付违约金，赔偿给甲方造成的全部损失。

2、验收材料清单如下：

阶段	**输出成果**	**成果形式**
云服务商选择阶段	《服务协议》	纸质/电子
系统入云阶段	政务云服务需求调研表，附：系统现状拓扑图、信息系统资产清单	纸质/电子
系统运行阶段	政务云运维服务方案	纸质/电子
	日常运维、巡检工作记录、事件处理报告	纸质/电子
	服务维护操作流程、工作手册	纸质/电子
	服务周报、月报（含云资源清单、云效率、云主机备份、数据库运行、数据备份、安全设备监控分析及安全防护情况，重要核心系统运行情况等）	纸质/电子
	漏洞扫描报告/月	纸质/电子
	应急预案，应急演练方案、报告	纸质/电子

	政务云服务总结报告（年报）	纸质/电子
	其他（云平台重大事件通知、重保期间值守记录、服务满意度调查表等）	纸质/电子

第七条 服务费用及支付方式

本协议总金额共计人民币小写：_____元，大写：人民币_____整。上述合同价款已包含乙方为完成合同约定全部工作和义务所需的一切费用，包括增值税在内的全部税金；除此之外，甲方无需再向乙方支付任何费用。

1、合同生效后【15】个工作日内，乙方向甲方提供合同价款的10%作为履约保函，即人民币小写：_____元，大写：_____元整，用以保证乙方全面地履行本合同项下的各种义务。

2、第一笔款：在甲方收到乙方提供的履约保函后15个工作日内，甲方向乙方支付合同款的60%，即人民币小写：_____元，大写：_____元整；

3、第二笔款：乙方完成6个月的租期服务工作，提交中期运维服务报告及相关材料，并经甲方检查验收后，甲方向乙方支付合同款的30%，即人民币小写：_____元，大写：元整；

4、第三笔款：乙方按照合同要求完成12个月租期服务工作，提交政务云服务工作总结报告及相关材料，并通过终期验收后，甲方向乙方支付合同款的10%，即人民币小写：元，大写：_____元整。

5、乙方收取相应款项前，应向甲方提供正式等额发票，因乙方未提供发票造成付款延迟，甲方不承担违约责任。

6、以上具体支付进度和比例以财政拨款到位情况为准。乙方不得因此向甲方提出索赔或主张权利。

第八条 甲方权利义务

1、甲方有权对乙方提供的各项服务进行监督、检查和评价。

2、甲方应提出有关管理、技术需求和要求，协调乙方与信息系统服务商的关系，协调信息系统服务商配合调研、迁移、运维、安全和应急演练等过程的工作。

3、甲方需按照《北京市市级政务云管理办法》的要求申请、变更、退出云服务；在系统入云、上线、服务变更、退出等关键节点，甲方应提前提交《北京市市级政务云服务统一工单》相应部分内容至政务云管理单位进行备案作为工作依据。甲方应按本协议约定使用乙

方提供的云资源，做到资源专用，协议未约定或未提交《北京市市级政务云服务统一工单》至政务云管理单位备案的信息系统不得部署入云。

4、甲方的信息系统在迁移、部署到乙方云平台之前，应开展必要的系统入云安全测试。

5、甲方负责本单位信息系统和相关基础软件的日常维护、管理、安全和应急保障。

6、甲方应确保部署在政务云平台的软件具有合法授权，不得擅自安装、使用非法软件。

7、甲方如需对已上线信息系统进行维护升级、渗透测试、安全加固等操作， 应提前告知乙方。

8、甲方有权要求乙方现场技术指导、处理故障及其他服务。

9 、甲方其他的权利义务：无。

第九条 乙方权利义务

1、乙方须按照协议所约定的服务内容标准向甲方提供相关资源和服务。

2、乙方应针对甲方建立健全信息系统管理配套制度，包括：运维制度、应急预案、安全保障制度、运行监管办法等。

3、乙方负责云平台基础安全保障和运维工作。

4、乙方应负责本单位人员的安全培训、技术培训，确保工作人员符合岗位要求。

5、乙方需按照有关规定进行操作，确保各系统不被人为损坏。

6、乙方负责提供资源调度管理和维护，提供云主机状态监控，对甲方所购买使用的资源提供运维服务，未经授权不得擅自修改信息系统数据或发布信息等。

7、乙方负责管理甲方申请的 IP 地址，为甲方提供 IP 地址分配和管理服务 。

8、信息系统正式上线后，乙方需定期向甲方提供政务云服务报告，以便甲方及时获取政务云资源或服务的使用情况。

9、甲方如需乙方提供重启服务器操作时，乙方有权要求甲方提供书面申请。除本款约定外，乙方原则上不接受甲方提出的其他可能对甲方服务器造成损坏的任何操作要求。

10、乙方应提供技术支持服务，以维护甲方系统的正常运行。

11、重大活动期间，乙方应配合甲方制定重保方案并提供云平台的现场值守等服务。

12、乙方应配合甲方制定信息系统应急预案，并配合开展信息系统应急演练工作，做好日常应急响应工作。

13、乙方接到甲方故障报告后，应及时做好相关信息的登记工作，并进行故障排查。乙方应定时向甲方反馈检查进度及结果，故障排除后，乙方应将结果及时反馈甲方并做好书面报告和故障记录。

14、由于甲方指定的其他技术服务提供商提供的软件或产品的缺陷，造成的信息系统运行故障、安全漏洞、信息泄露等事故，乙方不承担相应责任，但需要配合甲方进行整改。

15、当甲方入云信息系统出现严重影响政务云平台安全稳定运行的事件时，乙方有权暂时中断甲方的云服务并通知甲方，事件处理完毕后恢复服务。

16、乙方其他的权利义务：服务期间乙方应就作业安全制定完整可行的方案，作业人员应严格遵守各项规章制度，乙方工作人员在履行本合同期间自身遭受人身损害、财产损失，或致甲方、任何第三方人身损害、财产损失，其后果均由乙方承担，甲方概不负责。

第十条 安全责任边界

1、甲方安全责任

（1）甲方承担本单位入云信息系统的基础软件、信息系统、数据等方面的安全责任。

（2）甲方负责组织信息系统的应急演练，如有需要，甲方有权要求乙方配合应急演练。

2、乙方安全责任

（1）乙方承担云平台层面（主要包括物理资源、计算资源、存储资源、网络资源）的安全责任。

（2）乙方在取得甲方许可后，开展云平台应急演练；乙方有义务配合甲方完成信息系统的应急演练。

（3）乙方须按照《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14 号）的要求和有关网络安全标准，落实并通过所建设的云平台的第三方网络安全审查。

第十一条 知识产权归属

1、乙方保证向甲方提供的服务成果是其独立实施完成或取得相应授权，不存在任何侵犯第三方专利权、商标权、著作权等合法权益的情形。如因乙方提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究甲方责任的，乙方应负责解决并赔偿因此给甲方造成的全部损失。

2、双方在对外宣传（如在各自官网、市场营销活动）时，如有涉及对方的内容，应提前通知对方，在取得对方同意后方可发布信息 。

3、在本协议签订前已经存在的或履行过程中产生的其他与本协议无关的成果，包括但不限于设计方案、各种说明书、测试数据资料、计算机软件以及其他技术文档，知识产权归属原权利人所有。

4、本协议执行期间产生的相关电子文档（技术文档等）的知识产权归甲方所有，未经

甲方书面许可，乙方不得对本次项目所形成的资料及文件擅自复制，或向第三方透露、转让、扩散，或用于本合同外的项目。否则，乙方应承担由此引起的法律后果及赔偿甲方的所有损失。

第十二条 违约责任及协议解除

1.乙方违反本合同任意一条均视为违约，乙方须向甲方支付违约金为合同总价款的3‰，计人民币_____元整（¥_____元）。

2、在运营期间，如发生附件 2 中所列 A 级事件 1 次，甲方有权解除本协议，乙方除应向甲方返还已付款项，还应支付合同金额20%的违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

3、在运营期间，如发生附件 2 所列 B 级事件 3 次，甲方有权解除本协议，乙方除应向甲方返还已付款项，还应支付合同金额20%的违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

4、乙方提供服务过程中可能发生的违约行为及相应应承担的违约金详见附件 3、4 规定，违约金优先从尾款中抵扣，超过尾款部分由乙方支付。系同一事件或原因导致的事故，甲方不可就同一事件重复要求乙方承担违约责任，经甲乙双方协商，择其重者确定乙方支付违约金的办法。

5、在运营期间出现下列情况，甲方向乙方提出整改要求和期限，且乙方在规定期限内未能履行甲方正当要求的，甲方有权与乙方解除本合同，已完成成果归甲方所有，乙方除应返还甲方已付款项外，还应支付合同金额的20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任：

（1）多次在云综合监管服务商已发出整改通知后未正确处置，出现问题并造成 B 级及以上事故；

（2）重大活动期间所承诺的骨干人员和管理人员未到场；

（3）连续 2 个月所承诺的运维服务人员人数未达到协议要求。

6、乙方擅自将工程转包、分包给第三方实施的，甲方有权解除合同，已经完成的项目成果归甲方所有，乙方除应向甲方返还已收取的合同款项外，还应向甲方支付本合同金额的20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

7、乙方违反保密义务的，应当赔偿甲方因此遭受的全部损失，并按合同金额的20%向甲方支付违约金。情节严重的，应依法追究相关责任人的法律责任。

8、合同生效后，甲方应按照合同约定支付费用，因甲方原因未能按时支付，甲方需以

欠付金额为基数，按照银行同期贷款利率标准支付相应违约金。任何一方的违约行为给他方造成其他损失的，均应承担相应的赔偿责任，具体事宜以双方友好协商为准。

第十三条 退出

1、服务期内，如乙方提出退出要求，需在服务期截止前至少 6 个月向甲方提出退出申请，并获得甲方的书面许可后方可退出，对于由此给甲方带来的经济损失，由甲乙双方协商解决。

2、服务期内，如出现政务云管理单位责令乙方退出，相关补偿费用甲乙双方另行协商;在信息系统迁移和交接工作中，乙方应在甲方提出系统迁出需求后 15 天内配合甲方完成信息系统迁移的相关工作，包含梳理迁出系统的云资源、安全策略配置等。确保系统在新环境运行稳定后，关停原服务，并对原有系统数据进行安全擦除。否则乙方除应返还甲方已付款项外，还应支付合同金额的 20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。

第十四条 免责条款

1、本协议中不可抗力指地震、台风、火灾、水灾、战争、罢工以及其他双方共同认同的不能预见、不能避免并不能克服的客观情况。

2、由于网络运营商的核心设备故障造成的网络中断、阻塞，从而影响到系统的正常访问或响应速率降低，属于不可控事件和不可抗力，甲方应对此表示认同。

3、由于不可抗力致使协议无法履行的，受不可抗力影响一方应立即将不能履行本协议的事实书面通知对方，并在不可抗力发生之日起 15 天内提供相关政府部门或公证机关出具的证明文件。

4、由于不可抗力致使协议无法履行的，本协议在不可抗力影响范围及其持续期间内将中止履行，本协议执行时间可根据中止的时间相应顺延，双方无须承担违约责任。不可抗力事件消除后，双方应就协议的履行及后续问题进行协商，按照该事件对协议履行的影响程度，决定继续履行协议或终止协议。

第十五条 保密条款

1、乙方因承接本协议约定项目所知悉的该项目信息或甲方信息，以及在项目实施过程中所产生的与该项目有关的全部信息均为甲方的保密信息，乙方应按照甲方关于保密工作的相关要求，对上述保密信息承担保密义务。未经甲方书面同意，乙方不得将甲方保密信息透露给任何第三方。

2、乙方应对上述保密信息予以妥善保存，并保证仅将其用于与完成本协议项下约定项

目实施有关的用途或目的。在缺少相关保密条款约定时，对上述保密信息，乙方应至少采取适用于对自己核心机密进行保护的同等保护措施和审慎程度进行保密。

3、乙方保证将保密信息的披露范围严格控制在直接从事该项目工作且因工作需要有必要知悉保密信息的工作人员范围内，对乙方非从事该项目的人员一律严格保密。

4、乙方应保证在向其工作人员披露甲方的保密信息前，认真做好员工的保密教育工作，明确告知其将知悉的为甲方的保密信息，并明确告知其需承担的保密义务及泄密所应承担的法律责任，并要求全体参与该项目的人员签署书面《保密协议》。

5、任何时间内，一经甲方提出要求，乙方应按照甲方指示在收到甲方书面通知后 5 日内将含有保密信息的所有文件或其他资料归还甲方，且不得保留任何复印件及数据备份。

6、非经甲方特别授权，甲方向乙方提供的任何保密信息并不包括授予乙方该保密信息包含的任何专利权、商标权、著作权、商业秘密或其它类型的知识产权。

7、乙方需要定期向政务云管理单位和云综合监管服务商提交云平台及入云系统相关信息，内容包括但不限于：云资源租用情况、系统迁移进展、已租用资源的使用绩效情况、安全监控分析、IP 管理、重大活动值守、工作建议等，此时如涉及甲方信息，不属于保密违约。

8、乙方承担上述保密义务的期限为协议有效期间及协议终止后 1 年。

9、承担上述保密义务的责任主体为乙方（含乙方工作人员）。如乙方或乙方工作人员违反了上述保密义务，乙方均应向甲方承担全部责任，乙方应支付合同金额的 20%作为违约金，违约金未能弥补甲方全部损失的，乙方应继续承担赔偿责任。情节严重的，甲方将追求乙方的相关工作人员的法律责任。

10、乙方发现涉密的信息及载体可能被泄露或已经被泄露时，应及时穷尽手段采取有效措施防止知悉范围及损失的进一步扩大，并及时向甲方通报相关情况。

第十六条 争议的解决

1、本协议按中华人民共和国相关法律、法规进行解释。

2、因履行合同所发生的一切争议，双方应友好协商解决，协商不成的，按下列第（2）种方式解决：

（1）提交北京仲裁委员会仲裁，仲裁裁决为终局裁决；

（2）依法向甲方住所地有管辖权的人民法院起诉。

第十七条 协议内容变更

在本协议履行过程中，甲方提出服务需求变更，应与乙方协商一致并签署补充协议；在

变更达成一致前，双方应继续履行其原约定义务。

第十八条 廉政承诺

1、合同双方承诺共同加强廉洁自律、反对商业贿赂。

2、甲方及其工作人员不得索要礼金、有价证券和贵重物品；不得在乙方报销应由本单位或个人支付的费用；不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬；不得参加乙方安排的超标准宴请和娱乐活动。

3、乙方不得向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品； 不得为其报销应由甲方单位或个人支付的费用；不得向甲方工作人员支付劳务报酬；不得安排甲方工作人员参加超标准宴请及娱乐活动。

第十九条 其他

1、本协议自双方法定代表人或其委托代理人签名并加盖本单位合同专用章或单位公章后生效，至双方履行完毕本协议约定的全部义务时终止。

2、未尽事宜，经双方协商一致，签订书面补充协议，补充协议与本协议不一致的，以补充协议为准。

3、本协议一式 陆份，甲、乙双方各执 叁 份，每份具有同等法律效力。

附件：

（一）本合同的组成文件如下：

1.在合同实施过程中双方共同签署的补充与修正文件；

2.本合同正文；

3.本合同附件：

（1）《分项明细及报价表》

（2）《重大违约行为表》

（3）《严重违约行为表》

（4）《一般违约行为表》

4.项目实施方案。

（二）上述文件均为本合同的组成部分，并互为补充和解释，与主合同具有同等法律效力。甲、乙双方同意在出现合同理解上的不明确或不一致时，以所列顺序在前的为准执行，如果同一顺序的文件中的约定之间产生歧义或不一致，则以签署时间在后的为准。

（以下无正文）

委托人（甲方）	名称（或姓名）	**北京市规划和自然资源委员会**			合同专用章 或 单位公章 年　月　日
	联系人（承办人）	（签章）			
	住所（通讯地址）	北京市通州区承安路 1 号	邮　政编码	101160	
	电话		传真		
	开户银行	北京银行燕京支行			
	账号	20000036505700020494413			
受托人（乙方）	名称（或姓名）				合同专用章 或 单位公章 年　月　日
	联系人（经办人）	（签章）			
	住所（通讯地址）		邮政编码		
	电话		传真		
	开户银行				

	账号		

附件 1：《分项明细及报价表》

附件 2：《重大违约行为表》

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（云服务商主责）	服务中断	云平台整体	因非不可抗力造成超过 30%以上信息系统中断、影响人数 50 万以上、导致 500 万元以上经济损失。	2小时以上	A级	1次
	重大篡改事件	信息系统	在重大或特别重大保障期间，因云服务商的安全隐患原因造成的系统被恶意篡改事件。事件发生后云服务商未按照应急预案进行处置，造成信息安全事件处置延误。且该事件被国家级机构或媒体通报、市级领导批示或关注的。	30分钟以上		
	数据丢失	等保三级或重要信息系统的核心业务数据	因非不可抗力造成的云平台超过 3个信息系统丢失超过1个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	等保三级或重要信息系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在24小时内做有效处置或应急防护措施，造成信息系统在重大或特别重大保障期间被恶意篡改或敏感信息泄露事件。	——		
	服务中断	云平台整体	因非不可抗力造成超过 10%至 30%信息系统中断、影响人数10万以上、导致100万元以上经济损失。	2小时以上	B级	一年内3次以上
	重大篡改事件	信息系统	因云服务商的安全隐患原因造成的系统被恶意篡改事件，事件发生后云服务商未按照应急预案进行处 置，造成信息安全事件处置延误， 且该事件被市级机构或媒体通报、市级领导批示或关注的。	30 分钟以上		
	数据丢失	信息系统核心业务数据	因非不可抗力造成 1 个信息系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	信息系统	被第三方安全机构通报云平台存在安全隐患，云服务商未在 24 小时内做有效处置或应急防护措施，造成信息系统被恶意篡改或敏感信息泄露事件。	——		

附件 3：《严重违约行为表》

罚款金额=信息系统云服务费/服务月数*惩罚系数（惩罚系数参见《严重违约行为表》）

序号	问题描述	惩罚系数
1	所提供的云服务可用性低于99.99%，或数据可用性低于99.9999%，出现问题并造成重大损失的	200%
2	因未做好系统和数据互备，由于另一家云服务商服务中断，而导致系统和数据无法正常应用的，但影响未达到 B 级及以上事故影响的	200%
3	因所提供的安全服务出现故障，导致某系统网页被篡改，造成重大影响	600%
4	因所提供的安全服务出现故障，导致某系统数据丢失，造成重大影响	600%
5	因所提供的安全服务出现故障，导致某系统被入侵，造成重大影响	600%
6	在云安全监管服务商已发出整改通知后未正确处置，出现问题并造成重大事故	200%
7	平均响应时间大于 10 分钟且小于 30 分钟，造成重大事故	200%
8	运维需求平均响应时间大于 30 分钟且小于 60 分钟，造成重大事故	200%
9	运维需求平均故障恢复时间大于60 分钟且小于 90 分钟，造成重大影响	100%
10	运维需求平均故障恢复时间大于90 分钟且小于 120 分钟，造成重大影响	200%
11	现场无人值守超过大于 1 小时且小于 2 小时，造成重大事故	100%
12	现场无人值守超过大于 2 小时且小于 4 小时，造成重大事故	200%

附件 4：《一般违约行为表》

罚款金额=信息系统云服务费/服务月数*惩罚系数（惩罚系数参见《一般违约行为表》）

序号	问题描述	惩罚系数
1	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，出现问题但未造成重大损失的	50%
2	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，且在服务期内接到用户投诉此类情况 3 次以上的	20%
3	在运营期间，甲方对乙方实施月度考核，如乙方连续3次未能通过考核，经限期整改后仍不能达到甲方要求的	20%
4	在运营期内，如乙方未能按照用户方的扩容需求，在7个自然日内完成云平台的资源扩容，且经管理单位书面通知仍未能限期满足用户需求的	20%
5	因所提供的云服务或安全服务出现故障，造成某系统宕机2小时以上	30%
6	因所提供的云服务或安全服务出现故障，造成某系统连续宕机3次以上或累计8小时以上	60%
7	在云安全监管服务商已发出整改通知后未正确处置，出现问题的，未造成重大影响	50%
8	运维需求平均响应时间大于 10 分钟且小于 30 分钟，出现问题但未造成重大影响	30%
9	运维需求平均响应时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	50%
10	运维需求平均故障恢复时间大于 60 分钟且小于 90 分钟，出现问题但未造成重大影响	30%
11	运维需求平均故障恢复时间大于90 分钟且小于 120 分钟，出现问题但未造成重大影响	50%
12	现场无人值守超过大于 1 小时且小于 2 小时，出现问题但未造成重大影响	30%
13	现场无人值守超过大于 2 小时且小于 4 小时，出现问题但未造成重大影响	50%

第七章　投标文件格式

投标人编制文件须知

1、投标人按照本部分的顺序编制投标文件（资格证明文件）、投标文件（商务技术文件），编制中涉及格式资料的，应按照本部分提供的内容和格式（所有表格的格式可扩展）填写提交。

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、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（非实质性格式）

投 标 文 件

（资格证明文件）

项目名称：

采购编号/包号：

投标人名称：

1　满足《中华人民共和国政府采购法》第二十二条规定

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：_____（**请投标人填写“采购人名称”**）

在参与本次项目投标中，我单位承诺：

（一）具有良好的商业信誉和健全的财务会计制度；

（二）具有履行合同所必需的设备和专业技术能力；

（三）有依法缴纳税收和社会保障资金的良好记录；

（四）参加政府采购活动前三年内，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政府采购活动，但期限已经届满的情形）；

（五）我单位不属于政府采购法律、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）；

（六）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）；

（七）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政府采购活动均须填写）：

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：供应商承诺不实的，依据《政府采购法》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　落实政府采购政策需满足的资格要求（如有）

2-1 中小企业政策证明文件

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 中小企业证明文件

中小企业声明函（货物）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，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：_____

日 期：_____

[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。

中小企业声明函（工程、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格式

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定，本单位**（请进行选择）**：

□**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：_____**（请投标人填写“采购人名称”）**

我单位参加贵单位组织采购的采购编号为_____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）	占该采购包**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）（采购编号/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 其它落实政府采购政策的资格要求（如有）

3　本项目的特定资格要求（如有）

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：

一、 由_____牵头，_____、_____参加，组成联合体共同进行招标项目的投标工作。

二、 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。

三、 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》。

四、 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。

五、 _____负责_____，具体工作范围、内容以投标文件及合同为准。

六、 _____负责_____，具体工作范围、内容以投标文件及合同为准。

七、 _____负责_____（如有），具体工作范围、内容以投标文件及合同为准。

八、 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。

九、 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。

十、 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. 联合体各方成员须在本协议上共同盖章。

3-2 其他特定资格要求

二、商务技术文件格式

投标文件（商务技术文件）封面（非实质性格式）

投 标 文 件

（商务技术文件）

项目名称：

采购编号/包号：

投标人名称：

1　投标书（实质性格式）

投标书

致：_____**（请投标人填写“采购人名称”）**

我方参加你方就_____（项目名称，采购编号/包号）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 180 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（实质性格式）

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、提交、撤回、修改_____（项目名称）投标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投标有效期届满之日止。

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）：_____

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）及委托代理人的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。

法定代表人（单位负责人）身份证明

致：_____**（请投标人填写“采购人名称”）**

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）身份证或护照等身份证明文件电子件：

投标人名称（加盖公章）：_____

法定代表人（单位负责人）（签字或签章）：_____

日期：_____年_____月_____日

3　投标分项报价表（实质性格式）

投标分项报价表

（格式示例一，适用于设备采购）

采购编号/包号：_____ 项目名称：_____报价单位：人民币元

序号	分项名称	制造商	产地/国别	制造商统一社会信用代码	制造商规模	制造商绝对所有权拥有者所属性别	外商投资类型	品牌	规格、型号	单价（元）	数量	合价（元）
1												
2												
3												
4												
…												
											总价（元）	

说明：制造商规模请填写“大型”、“中型”、“小型”、“微型”或“其他”，中小企业的定义见第二章《投标人须知》。

制造商绝对所有权拥有者所属性别请填写“男”或“女”， 指拥有制造商 51%以上绝对所有权的性别；绝对所有权拥有者可以是一个人，也可以是多人合计计算。

外商投资类型请填写“外商单独投资”、“外商部分投资”或“内资”。

（格式示例二，适用于服务类项目）

采购编号/包号：_____ 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。

4.制造商规模列应填写“大型”、“中型”、“小型”、“微型”或“其他”，且不应与《中小企业声明函》或《拟分包情况说明》中内容矛盾。制造商绝对所有权拥有者所属性别请填写“男”或“女”， 指拥有制造商 51%以上绝对所有权的性别；绝对所有权拥有者可以是一个人，也可以是多人合计计算。外商投资类型请填写“外商单独投资”、“外商部分投资”或“内资”。

投标人名称（加盖公章）：_____

日期：_____年_____月_____日

4　合同条款偏离表（实质性格式）

合同条款偏离表

采购编号/包号：_____　　项目名称：_____

序号	招标文件条目号（页码）	招标文件要求	投标文件内容	偏离情况	说明
对本项目合同条款的偏离情况（应进行选择，未选择**投标无效**）： □**无偏离**（如无偏离，仅选择无偏离即可；无偏离即为对合同条款中的所有要求，均视作供应商已对之理解和响应。） □**有偏离**（如有偏离，则应在本表中对负偏离项逐一列明，否则**投标无效**；对合同条款中的所有要求，除本表列明的偏离外，均视作供应商已对之理解和响应。）					

注：“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

5　采购需求偏离表（实质性格式）

采购需求偏离表

采购编号/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。此表中若无任何文字说明，内容为空白的，**投标无效。**
2.“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

6　中小企业证明文件

说明：

1）中小企业参加政府采购活动，应当出具《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，以证明中小企业身份。《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。

4）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）》及本项目文件规定的中小企业划分标准所属行业执行。

中小企业声明函（货物）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，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：_____

日 期：_____

[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。

中小企业声明函（工程、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）*；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）*；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格式

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位**（请进行选择）**：

□**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：

7　拟分包情况说明

拟分包情况说明

致：_____**（请投标人填写“采购人名称”）**

我单位参加贵单位组织采购的采购编号为_____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：		

注：

1. 如本项目（包）允许分包，且投标人拟进行分包时，必须提供；如未提供，或提供了但未填写分包承担主体名称、拟分包合同内容、拟分包合同金额，**投标无效**。

2.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**。

3. 投标人“为落实政府采购政策”而向中小企业分包时请仔细阅读资格证明文件格式 2-1 中说明，并建议按要求在资格证明文件中提供相关全部文件；投标人非“为落实政府采购政策”而向中小企业分包时，建议在本册提供。

投标人名称（盖章）：_____

日期：_____年_____月_____日

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）（采购编号/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：

1. 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**；且建议按照采购文件要求在资格证明文件部分提供；

2. 投标人满足《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）第九条有关规定，拟享受中小企业政策优惠措施的，仍需提供本协议，否则不予认可；

3. 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，否则不予认可。

8　招标文件要求提供或投标人认为应附的其他材料

8-1 投标人信息采集表

投标人信息	
投标人名称	
投标人统一社会信用代码	
投标人地址	
投标人性质	
投标人规模	
投标人绝对所有权拥有者所属性别	
外商投资类型	
外商投资国别	
委托代理人信息	
委托代理人姓名	
委托代理人手机号	
委托代理人邮箱	

注：1.投标人如为联合体，则应填写联合体各成员信息。

2.投标人性质请填写：“企业”、“社会组织”、 “公益二类事业单位”、“从事生产经营活动事业单位”、“农村集体经济组织”、“基层群众性自治组织”或“个人”。

3.投标人规模请填写：“大型”、“中型”、“小型”、“微型”或 “其他”，且不应与《中小企业声明函》或《拟分包情况说明》中内容矛盾。

4.投标人绝对所有权拥有者所属性别请填写：“男”或“女”，指拥有投标人 51%以上绝对所有权的性别；绝对所有权拥有者可以是一个人，也可以是多人合计计算。

5.外商投资类型请填写：“外商单独投资”、“外商部分投资”或“内资”。

6.属于“内资”的，无需填写“外商投资国别”。属于“外商单独投资”、“外商部分投资”的，外商投资国别请填写：“欧资企业”、“美资企业”、“日资企业”、“其他”。

7.请投标人按要求填写，该信息采集表不作为实质性格式和内容进行评审使用。

8-2 制造商信息采集表（货物类采购项目需填写）

序号	分项名称	制造商	外商投资类型	外商投资国别
1				
2				
3				
4				
…				

注：1.外商投资类型请填写：“外商单独投资”、“外商部分投资”或“内资”。

2.属于“内资”的，无需填写“外商投资国别”。属于“外商单独投资”、“外商部分投资”的，外商投资国别请填写：“欧资企业”、“美资企业”、“日资企业”、“其他”。

3.请申请人按要求填写，该信息采集表不作为实质性格式和内容进行评审使用。

8-3 操作系统、CPU 信息采集表（计算机、服务器采购项目需填写）

计算机信息				
商品名称	**商品品牌**	**商品型号**	**计算机操作系统**	**计算机 CPU 型号**
服务器信息				
商品名称	**商品品牌**	**商品型号**	**服务器操作系统**	**服务器 CPU 型号**

注：请投标人按要求填写，该信息采集表不作为实质性格式和内容进行评审使用。