

# 黑龙江省政府采购中心

## 竞争性磋商文件

项目名称：政务云服务商采购项目

项目编号：**SC[2021]0170**

## 第一章磋商邀请

黑龙江省政府采购中心受黑龙江省公安厅的委托，采用竞争性磋商方式组织采购政务云服务商采购项目。欢迎符合资格条件的国内供应商参加投标。

### 一.项目概述

#### 1.名称与编号

项目名称：政务云服务商采购项目

批准文件编号：黑财购备字[2021]02951号

采购文件编号：SC[2021]0170

#### 2.内容及分包情况（技术规格、参数及要求）

包号	货物、服务和工程名称	数量	采购需求	预算金额（元）
1	政务云服务商采购	1	详见采购文件	0.10

### 二.供应商的资格要求

1.供应商应符合《中华人民共和国政府采购法》第二十二条规定的条件。

2.到提交响应文件的截止时间，供应商未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。（以通过查询“信用中国”网站和“中国政府采购网”网站的信用记录内容为准。）

3.其他资质要求：

合同包1（政务云服务商采购）：无

### 三.获取磋商文件的时间、地点、方式

获取磋商文件的期限：详见竞争性磋商公告；

获取磋商文件的地点：详见竞争性磋商公告；

获取磋商文件的方式：供应商须在公告期内凭用户名和密码，登录黑龙江省政府采购网，选择“交易执行-应标-项目投标”，在“未参与项目”列表中选择需要参与的项目，确认参与后即可获取磋商文件。

### 其他要求

1.本项目采用“现场在线开标”模式进行开标，投标人需到达开标现场。

2.本项目采用“不见面开标”模式进行开标投标人无需到达开标现场，开标当日在投标截止时间前30分钟登录黑龙江省政府采购网进行签到，选择“交易执行-开标-供应商开标大厅”参加远程开标。请投标人使用投标客户端严格按照招标文件的相关要求制作和上传电子投标文件，并按照相关要求参加开标。

3.本项目将采用电子评标的方式，为避免意外情况的发生处理不及时导致投标失败，建议投标人需在开标时间前1小时完成投标文件上传，否则产生的一系列问题将由投标人自行承担。

### 四.磋商文件售价

本次磋商文件的售价为 无 元人民币。

### 五.询问提起与受理：

项目经办人：王似玉 联系方式：0451-87220729

### 六.质疑提起与受理：

1.对采购文件的质疑：

项目经办人：王似玉 联系方式：0451-87220729

2.对评审过程和结果的质疑：

质疑经办人：业务监督处毛绪斌电话：0451-87220739 黄鑫华电话：0451-87220771

#### 七.递交投标（响应）文件截止时间、开标时间及地点：

递交投标（响应）文件截止时间：详见竞争性磋商公告

投标地点：详见竞争性磋商公告

开标时间：详见竞争性磋商公告

开标地点：详见竞争性磋商公告

#### 八.联系方式：

##### 1. 采购代理机构

采购代理机构名称：黑龙江省政府采购中心

地址：黑龙江省哈尔滨市南岗区汉水路379号

联系人：王似玉

联系电话：0451-87220729

账户名称：系统自动生成的缴交账户名称

开户行：详见供应商须知

账号：详见供应商须知

##### 2. 采购人信息

采购单位名称：黑龙江省公安厅

地址：南岗区中山路145号

联系人：徐昊

联系电话：82696068

黑龙江省政府采购中心

## 第二章 供应商须知

### 一、前附表：

序号	条款名称	内容及要求
1	分包情况	共1包
2	采购方式	竞争性磋商
3	开标方式	现场网上开标
4	评标方式	现场网上评标
5	是否专门面向中小企业采购	{ {面向中小企业预留情况} }
6	评标办法	合同包1（政务云服务商采购）：综合评分法
7	获取磋商文件时间（同磋商文件提供期限）	详见磋商公告
8	保证金缴纳截止时间（同递交响应文件截止时间）	详见磋商公告
9	电子响应文件递交	电子响应文件在投标截止时间前递交至黑龙江省政府采购网--政府采购云平台
10	投标文件数量	<p>（1）加密的电子投标文件 1 份（需在投标截止时间前上传至“黑龙江省政府采购网--黑龙江省政府采购管理平台”）；</p> <p>（2）为避免上传的电子投标文件出现无法使用的情况，若项目采用现场开标方式时，投标人需自行携带投标客户端生成的备用电子标投标文件（.备用文件）U盘（或光盘）份；若项目采用远程开标方式时，在代理机构开启备用文件上传功能后，投标人需自行上传备用电子标投标文件（.备用文件）。</p> <p>（3）纸质投标文件（正本）份；纸质投标文件（副本）份。1份。</p>
11	中标人确定	采购人授权磋商小组按照评审原则直接确定中标（成交）人。
12	备选方案	不允许
13	联合体投标	包1： 不接受
14	采购机构代理费用	无
15	代理费用收取方式	不收取

16	投标保证金	<p>本招标项目采用“虚拟子账户”方式收退投标保证金，请供应商按照本磋商文件的相关要求进行缴纳。</p> <p>同时，本项目允许供应商按照相关法律法规自主选择以支票、汇票、本票、保函等非现金形式缴纳保证金。选择非“虚拟子账户”进行保证金缴纳的，供应商应当在响应文件中附相关证明材料，同时在开标现场提供证明材料原件。</p> <p>备注：若本项目采用远程不见面开标，请将相关证明材料原件扫描添加至响应文件中。</p> <p>政务云服务商采购：保证金人民币：0.00元整。</p> <p>开户单位：系统自动生成的缴交账户名称。</p> <p>开户银行：供应商在黑龙江省政府采购网--政府采购云平台获取磋商文件后，根据其提示自行选择要缴纳的投标保证金银行。</p> <p>银行账号：黑龙江省政府采购网根据供应商选择的投标保证金银行，以合同包为单位，自动生成供应商所投合同包的缴纳银行账号（即多个合同包将对应生成多个缴纳账号）。供应商应按照所投合同包的投标保证金要求，缴纳相应的投标保证金。</p> <p>特别提示：</p> <ol style="list-style-type: none"> <li>1、供应商应认真核对账户信息，将投标保证金足额汇入以上账户，并自行承担因汇错投标保证金而产生的一切后果。</li> <li>2、供应商在转账或电汇的凭证上应按照以下格式注明，以便核对：“（招标编号：***、合同包：***）的投标保证金”。</li> <li>3、投标保证金缴纳、退还联系人：王似玉</li> <li>4、咨询电话：0451-87220729</li> </ol>
----	-------	---

17	电子招投标	<p>各投标人应当在投标截止时间前上传加密的电子投标文件至“黑龙江省政府采购网”未在投标截止时间前上传电子投标文件的，视为自动放弃投标。投标人因系统或网络问题无法上传电子投标文件时，请在工作时间及时拨打联系电话4009985566按5转1号键。</p> <p><b>网上开标（投标人需到开标现场）：</b></p> <ol style="list-style-type: none"> <li>1. 项目采用电子开标（网上开标），如在开标过程中出现意外情况导致无法继续进行电子开标时，改为非加密电子投标文件开标。本项目采用电子评标（网上评标），只对加密电子投标文件进行评审，如在评标过程中出现意外情况导致无法继续进行电子评标时，改为非加密电子投标文件评标。</li> <li>2. 电子投标文件是指通过投标客户端编制，在电子投标文件中，涉及“加盖公章”的内容应使用单位电子公章完成。加密后，成功上传至黑龙江省政府采购网的最终版指定格式电子投标文件。</li> <li>3. 使用投标客户端，经过编制、签章，在生成加密投标文件时，会同时生成非加密投标文件，供投标人刻录使用。U盘（或光盘）由投标人自行刻录、存储，投标人必须保证电子存储设备能够正常读取。U盘（或光盘）表面、外包装上应简要载明项目编号、项目名称、投标单位名称等信息。</li> <li>4. 投标人的法定代表人或其授权代表应当按照本招标公告载明的时间和地点参加开标。开标时，投标人应当使用 CA 锁在招标文件规定的时间内完成投标文件在线解密。</li> <li>5. 开标时出现下列情况的，将视为逾期送达或者未按照招标文件要求密封的投标文件，采购人、采购代理机构应当拒收。 <ul style="list-style-type: none"> <li>（1） 投标人代表未按招标文件要求参加开标会的或开标现场未携带CA锁的；</li> <li>（2） 投标人未在规定时间内完成电子投标文件在线解密；</li> <li>（3） 经检查数字证书无效的投标文件；</li> <li>（4） 投标人自身原因造成电子投标文件未能解密的；</li> <li>（5） 开标现场无法使用系统进行电子开评标时，投标人未按招标文件要求提供非加密电子版投标文件的。</li> </ul> </li> </ol> <p>本招标项目的投标人必须在开标时间开始后完成所投全部标段的电子投标文件在线解密。投标人必须保证在规定时间内完成全部标段的电子投标文件解密。</p>
18	电子响应文件 签字、盖章要求	<p>应按照第七章“响应文件格式”要求，使用单位电子签章（CA）进行签字、加盖公章。</p> <p>说明：若涉及到授权代表签字的可将文件签字页先进行签字、扫描后导入加密电子响应文件。</p>
19	投标客户端	<p>投标客户端需要自行登录“黑龙江省政府采购网--政府采购云平台”下载。</p>
20	有效供应商家数	<p>包1：3</p> <p>此数约定了开标与评标过程中的最低有效供应商家数，当家数不足时项目将不得开标、评标或直接废标；文件中其他描述若与此规定矛盾以此为准。</p>
21	报价形式	<p>合同包1（政务云服务商采购）：总价</p>
22	其他	
23	项目兼头兼中规则	<p>无</p>

### 三、投标须知

#### 1.投标方式

1.1投标方式采用网上投标，流程如下：

供应商应在黑龙江省政府采购网（<http://hljcg.hlj.gov.cn>）提前注册并办理电子签章CA，CA用于制作投标时盖章、加密和开标时解密（CA办理流程及驱动下载参考黑龙江省政府采购网（<http://hljcg.hlj.gov.cn>）办事指南-CA办理流程）具体操作步骤，在黑龙江省政府采购网（<http://hljcg.hlj.gov.cn/>）下载政府采购供应商操作手册。

**1.2 缴纳投标保证金（如有）。**本采购项目采用“虚拟子账号”形式收退投标保证金，每一个供应商在所投的每一项目下合同包会对应每一家银行自动生成一个账号，称为“虚拟子账号”。在进行投标信息确认后，应通过应标管理-已投标的项目，选择缴纳银行并获取对应不同包的缴纳金额以及虚拟子账号信息，并在开标时间前，通过转账至上述账号中，付款人名称必须为投标单位全称且与投标信息一致。

若出现账号缴纳不一致、缴纳金额与供应商须知前附表规定的金额不一致或缴纳时间超过开标时间，将导致保证金缴纳失败。

**1.3 查看投标状况。**通过应标管理-已投标的项目可查看已投标项目信息。

## **2. 特别提示**

**2.1 缴纳保证金时间以保证金到账时间为准，**由于投标保证金到账需要一定时间，请供应商在投标截止前及早缴纳。

### 三、说明

#### 1.总则

本磋商文件依据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》和《政府采购竞争性磋商采购方式管理暂行办法》（财库〔2014〕214号）及国家和自治区有关法律、法规、规章制度编制。

供应商应仔细阅读本项目信息公告及磋商文件的所有内容（包括变更、补充、澄清以及修改等，且均为磋商文件的组成部分），按照磋商文件要求以及格式编制响应文件，并保证其真实性，否则一切后果自负。

本次竞争性磋商项目，是以磋商公告的方式邀请非特定的供应商参加投标。

#### 2.适用范围

本磋商文件仅适用于本次采购公告中所涉及的项目和内容。

#### 3.投标费用

供应商应承担所有与准备和参加投标有关的费用。不论投标结果如何，采购代理机构和采购人均无义务和责任承担相关费用。

#### 4.当事人：

4.1“采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。本磋商文件的采购人特指本项目采购单位。

4.2“采购代理机构”是指本次招标采购项目活动组织方。本磋商文件的采购代理机构特指黑龙江省政府采购中心。

4.3“供应商”是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。

4.4“磋商小组”是指根据《中华人民共和国政府采购法》等法律法规规定，由采购人代表和有关专家组成以确定成交供应商或者推荐成交候选人的临时组织。

4.5“供应商”是指经磋商小组评审确定的对磋商文件做出实质性响应，取得与采购人签订合同资格的供应商。

#### 5.合格的供应商

5.1符合本磋商文件规定的资格要求，并按照要求提供相关证明材料。

5.2单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

5.3为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

#### 6.以联合体形式投标的，应符合以下规定：

6.1联合体各方应签订联合体协议书，明确联合体牵头人和各方权利义务，并作为响应文件组成部分。

6.2联合体各方均应当具备政府采购法第二十二条规定的条件，并在响应文件中提供联合体各方的相关证明材料。

6.3联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

6.4联合体各方中至少应当有一方符合采购人规定的资格要求。由同一资质条件的供应商组成的联合体，应当按照资质等级较低的供应商确定联合体资质等级。

6.5联合体各方不得再以自己名义单独在同一项目中投标，也不得组成新的联合体参加同一项目投标。

6.6联合体各方应当共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任。

6.7投标时，应以联合体协议中确定的主体方名义投标，以主体方名义缴纳投标保证金，对联合体各方均具有约束力。

#### 7.语言文字以及度量衡单位

7.1所有文件使用的语言文字为简体中文。专用术语使用外文的，应附有简体中文注释，否则视为无效。

7.2所有计量均采用中国法定的计量单位。

7.3所有报价一律使用人民币，货币单位：元。（项目存在特殊要求时，以实际要求为准）

#### 8.现场踏勘

- 8.1磋商文件规定组织踏勘现场的，采购人按磋商文件规定的时间、地点组织供应商踏勘项目现场。
- 8.2供应商自行承担踏勘现场发生的责任、风险和自身费用。
- 8.3采购人在踏勘现场中介绍的资料和数据等，不构成对磋商文件的修改或不作为供应商编制响应文件的依据。

## 9.其他条款

无论中标与否供应商递交的响应文件均不予退还。

## 四、磋商文件的澄清和修改

1.提交首次响应文件截止之日前，采购人、采购代理机构或者磋商小组可以对已发出的磋商文件进行必要的澄清或者修改，澄清或者修改的内容作为磋商文件的组成部分。澄清或者修改的内容可能影响响应文件编制的，采购人、采购代理机构应当在提交首次响应文件截止时间至少5日前；不足5日的，采购人、采购代理机构应当顺延提交首次响应文件截止时间。同时在“黑龙江省政府采购网”上发布澄清或者变更公告进行通知。澄清或者变更公告的内容为磋商文件的组成部分，供应商应自行上网查询，采购人或采购代理机构不承担供应商未及时关注相关信息的责任。

## 五、响应文件

### 1.响应文件的构成

响应文件应按照磋商文件第七章“响应文件格式”进行编写（可以增加附页），作为响应文件的组成部分。

### 2.响应报价

2.1供应商应按照“第四章采购内容与要求”的需求内容、责任范围以及合同条款进行报价。并按“开标一览表”和“分项报价明细表”规定的格式报出总价和分项价格。投标总价中不得包含磋商文件要求以外的内容，否则，在评审时不予核减。

2.2报价包括本项目采购需求和投入使用的所有费用，如主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

2.3报价不得有选择性报价和附有条件的报价。

2.4对报价的计算错误按以下原则修正：

- (1) 响应文件中开标一览表（报价表）内容与响应文件中相应内容不一致的，以开标一览表（报价表）为准；
- (2) 大写金额和小写金额不一致的，以大写金额为准；
- (3) 单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价。

注：修正后的报价供应商应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，但不得超出响应文件的范围或者改变响应文件的实质性内容，供应商不确认的，其投标无效。

### 3.投标有效期

3.1投标有效期从提交响应文件的截止之日起算。响应文件中承诺的投标有效期应当不少于磋商文件中载明的投标有效期。投标有效期内供应商撤销响应文件的，采购人或者采购代理机构可以不退还投标保证金。

3.2出现特殊情况需要延长投标有效期的，采购人以书面形式通知所有供应商延长投标有效期。供应商同意延长的，应相应延长其投标保证金的有效期，但不得要求或被允许修改或撤销其响应文件；供应商拒绝延长的，其投标失效，但供应商有权收回其投标保证金。

### 4.保证金

#### 4.1保证金的缴纳：

供应商在提交响应文件的同时，应按供应商须知前附表规定的金额、开户银行、行号、开户单位、账号和磋商文件本章“投标须知”规定的投标保证金缴纳要求递交投标保证金，并作为其响应文件的组成部分。

#### 4.2保证金的退还：

(1) 供应商在投标截止时间前放弃投标的，自所投合同包结果公告发出后5个工作日内退还，但因供应商自身原因导致无法及时退还的除外；

(2) 未成交供应商投标保证金，自成交通知书发出之日起5个工作日内退还；

(3) 成交供应商投标保证金，自政府采购合同签订之日起5个工作日内退还。

**4.3**有下列情形之一的，投标保证金将不予退还：

- (1) 成交后，无正当理由放弃中标资格；
- (2) 成交后，无正当理由不与采购人签订合同；
- (3) 在签订合同时，向采购人提出附加条件；
- (4) 不按照磋商文件要求提交履约保证金；
- (5) 要求修改、补充和撤销响应文件的实质性内容；
- (6) 要求更改磋商文件和中标结果公告的实质性内容；
- (7) 法律法规和磋商文件规定的其他情形。

## **5.响应文件的修改和撤回**

**5.1**供应商在提交响应截止时间前，可以对所递交的响应文件进行补充、修改或者撤回。补充、修改的内容旁签署（法人或授权委托人签署）、盖章、密封和上传至系统后生效，并作为响应文件的组成部分。

**5.2**在提交响应文件截止时间后到磋商文件规定的投标有效期终止之前，供应商不得补充、修改、替代或者撤回其响应文件。

## **6.响应文件的递交**

**6.1**在磋商文件要求提交响应文件的截止时间之后送达或上传的响应文件，为无效响应文件，采购单位或采购代理机构拒收。采购人、采购代理机构对误投或未按规定时间、地点进行投标的概不负责。

## **7.样品（演示）**

**7.1**磋商文件规定供应商提交样品的，样品属于响应文件的组成部分。样品的生产、运输、安装、保全等一切费用由供应商自理。

**7.2**开标前，供应商应将样品送达至指定地点，并按要求摆放并做好展示。若需要现场演示的，供应商应提前做好演示准备（包括演示设备）。

**7.3**评审结束后，供应商与采购人共同清点、检查和密封样品，由供应商送至采购人指定地点封存。未成交供应商将样品自行带回。

# **六、开标、评审、结果公告、中标通知书发放**

## **1.开标程序**

**1.1**主持人按下列程序进行开标：

- (1) 宣布开标纪律；
- (2) 宣布开标会议相关人员姓名；
- (3) 供应商对已提交的加密文件进行解密，由采购人或者采购代理机构工作人员当众宣布供应商名称和磋商文件规定的需要宣布的其他内容（以开标一览表要求为准）
- (4) 参加开标会议人员对开标情况确认；
- (5) 开标结束，响应文件移交磋商小组。

### **1.2**开标异议

供应商代表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，应当当场提出询问或者回避申请，开标会议结束后不再接受相关询问、质疑或者回避申请。

**1.3**供应商不足三家的，不得开标。

**1.4**备注说明：

(1) 若本项目采用不见面开标，开标时供应商使用 CA证书参与远程响应文件解密。供应商用于解密的CA证书应为该响应文件生成加密、上传的同一把 CA证书。

(2) 若本项目采用不见面开标，供应商在开标时间前30分钟，应当提前登录开标系统进行签到，填写联系人姓名与联系号码；在系统约定时间内使用CA证书签到以及解密，未成功签到或未成功解密的视为其无效投标。

(3) 供应商对不见面开标过程和开标记录有疑义，应在开标系统规定时间内在不见面开标室提出异议，采购代理机构在网上开标系统中进行查看及回复。开标会议结束后不再接受相关询问、质疑或者回避申请。

## 2.评审（详见第六章）

## 3.结果公告

3.1成交供应商确定后，采购代理机构将在黑龙江省政府采购网发布中标结果公告，中标结果公告期为 1 个工作日。

3.2项目废标后，采购代理机构将在黑龙江省政府采购网上发布废标公告，废标结果公告期为 1 个工作日。

## 4.中标通知书发放

发布中标结果的同时，成交供应商可自行登录“黑龙江省政府采购网--政府采购云平台”打印中标通知书，中标通知书是合同的组成部分，中标通知书对采购人和成交供应商具有同等法律效力。

成交通知书发出后，采购人不得违法改变中标结果，成交供应商无正当理由不得放弃中标。

## 七、询问、质疑与投诉

### 1.询问

1.1供应商对政府采购活动事项有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构应当在3个工作日内做出答复，但答复的内容不得涉及商业秘密。供应商提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知其向采购人提出。

1.2为了使提出的询问事项在规定时间内得到有效回复，询问采用实名制，询问内容以书面材料的形式亲自递交到采购代理机构，正式受理后方可生效，否则，为无效询问。

### 2.质疑

2.1潜在供应商已依法获取招标文件，且满足参加采购项目基本条件的潜在供应商，可以对招标文件提出质疑；递交响应文件的供应商，可以对该项目采购过程和中标结果提出质疑。采购中心应当在正式受理供应商的书面质疑后七个工作日内作出答复，但答复的内容不得涉及商业秘密。

2.2对招标文件提出质疑的，应当在首次获取招标文件之日起七个工作日内提出；对采购过程提出质疑的，为各采购程序环节结束之日起七个工作日内提出；对中标结果提出质疑的，为中标结果公告期届满之日起七个工作日内提出。

2.3质疑供应商应当在规定的时限内，以书面形式一次性地向采购中心递交《质疑函》和必要的证明材料，不得重复提交质疑材料，《质疑函》应按标准格式规范填写。

2.4供应商可以委托代理人进行质疑。代理人提出质疑，应当递交供应商法定代表人签署的授权委托书，其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。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

2.5供应商提出质疑应当递交《质疑函》和必要的证明材料。《质疑函》应当包括下列内容：

- (1) 供应商的姓名或者名称、地址、联系人及联系电话；
- (2) 质疑项目的名称、编号；
- (3) 具体、明确的质疑事项和与质疑事项相关的请求；
- (4) 事实依据；
- (5) 必要的法律依据；
- (6) 提出质疑的日期；

(7) 供应商首次下载招标文件的时间截图。

2.6有下列情形之一的，采购中心不予受理：

- (1) 按照“谁主张、谁举证”的原则，应由质疑供应商提供质疑事项的相关证据、依据和其他有关材料，未能提供的；
- (2) 未按照补正期限进行补正或者补正后仍不符合规定的；
- (3) 未在质疑有效期限内提出的；
- (4) 超范围提出质疑的；
- (5) 同一质疑供应商一次性提出质疑后又提出新质疑的。

2.7有下列情形之一的，质疑不成立：

- (1) 质疑事项缺乏事实依据的；
- (2) 质疑供应商捏造事实或者提供虚假材料的；
- (3) 质疑供应商以非法手段取得证明材料的。

2.8质疑的撤销。质疑正式受理后，质疑供应商申请撤销质疑的，采购中心应当终止质疑受理程序并告知相关当事人。

2.9对虚假和恶意质疑的处理。对虚假和恶意质疑的供应商，报省级财政部门依法处理，记入政府采购不良记录，推送省级信用平台，限制参与政府采购活动。有下列情形之一的，属于虚假和恶意质疑：

- (1) 主观臆造、无事实依据进行质疑的；
- (2) 捏造事实或提供虚假材料进行质疑的；
- (3) 恶意攻击、歪曲事实进行质疑的；
- (4) 以非法手段取得证明材料的。

### 3.投诉

3.1质疑人对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内做出书面答复的，可以在答复期满后十五个工作日内向监督部门进行投诉。投诉程序按《政府采购法》及相关规定执行。

3.2供应商投诉的事项不得超出已质疑事项的范围。

## 第三章 合同与验收

### 一、合同要求

#### 1.一般要求

1.1采购人应当自中标通知书发出之日起30日内，按照磋商文件和成交供应商响应文件的规定，与成交供应商签订书面合同。所签订的合同不得对磋商文件确定的事项和成交供应商响应文件作实质性修改。

1.2合同签订双方不得提出任何不合理的要求作为签订合同的条件。

1.3政府采购合同应当包括采购人与成交供应商的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

1.4采购人与成交供应商应当根据合同的约定依法履行合同义务。

1.5政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。

1.6政府采购合同的双方当事人不得擅自变更、中止或者终止合同。

1.7拒绝签订采购合同的按照相关规定处理，并承担相应法律责任。

1.9采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在省级以上人民政府财政部门指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

#### 2.合同格式及内容

2.1具体格式见本磋商文件后附拟签订的《合同文本》（部分合同条款），响应文件中可以不提供《合同文本》。

2.2《合同文本》的内容可以根据《民法典》和合同签订双方的实际要求进行修改，但不得改变范本中的实质性内容。

## 二、验收

成交供应商在供货、工程竣工或服务结束后，采购人应及时组织验收，并按照磋商文件、响应文件及合同约定填写验收单。

### 政府采购合同（合同文本）

甲方：\*\*\*（填写采购单位）

地址（详细地址）：

乙方：\*\*\*（填写中标供应商）

地址（详细地址）：

合同号：

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法律法规，甲、乙双方就（填写项目名称）（政府采购项目编号、备案编号：），经平等自愿协商一致达成合同如下：

#### 1.合同文件

本合同所附下列文件是构成本合同不可分割的部分：

- (1)合同格式以及合同条款
- (2)中标结果公告及中标通知书
- (3)磋商文件
- (4)响应文件
- (5)变更合同

2.本合同所提供的标的物、数量及规格等详见中标结果公告及后附清单。

#### 3.合同金额

合同金额为人民币 万元，大写：

#### 4.付款方式及时间

\*\*\*（见磋商文件第四章）

#### 5.交货安装

交货时间：

交货地点：

#### 6.质量

乙方提供的标的物应符合国家相关质量验收标准，且能够提供相关权威部门出具的产品质量检测报告；提供的相关服务符合国家（或行业）规定标准。

#### 7.包装

标的物的包装应按照国家或者行业主管部门的技术规定执行，国家或业务主管部门无技术规定的，应当按双方约定采取足以保护标的物安全、完好的包装方式。

#### 8.运输要求

- (1)运输方式及线路：
- (2)运输及相关费用由乙方承担。

#### 9.知识产权

乙方应保证甲方在中国境内使用标的物或标的物的任何一部分时，免受第三方提出的侵犯其知识产权的诉讼。

#### 10.验收

(1)乙方将标的物送达至甲方指定的地点后，由甲乙双方及第三方（如有）一同验收并签字确认。

(2)对标的物的质量问题，甲方应在发现后向乙方提出书面异议，乙方在接到书面异议后，应当在 日内负责处理。甲方逾期提出的，对所交标的物视为符合合同的规定。如果乙方在响应文件及磋商过程中做出的书面说明及承诺中，有

明确质量保证期的，适用质量保证期。

(3) 经双方共同验收，标的物达不到质量或规格要求的，甲方可以拒收，并可解除合同且不承担任何法律责任，

### 11.售后服务

(1) 乙方应按磋商文件、响应文件及乙方在磋商过程中做出的书面说明或承诺提供及时、快速、优质的售后服务。

(2) 其他售后服务内容： (响应文件售后承诺等)

### 12.违约条款

(1) 乙方逾期交付标的物、甲方逾期付款，按日承担违约部分合同金额的违约金。

(2) 其他违约责任以相关法律法规规定为准，无相关规定的，双方协商解决。

### 13.不可抗力条款

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在 天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，双方协商解决。

### 14.争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成可以采用下列方式解决：

(1) 提交 仲裁委员会仲裁。

(2) 向 人民法院起诉。

### 15.合同保存

合同文本一式五份，采购单位、供应商、政府采购监管部门、采购代理机构、国库支付执行机构各一份，自双方签订之日起生效。

16.合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

甲方： (章)

乙方： (章)

采购方法人代表： (签字)

供应商法人代表： (签字)

开户银行：

开户银行：

帐号：

帐号：

联系电话：

联系电话：

签订时间 年 月 日

附表：标的物清单（主要技术指标需与响应文件相一致）（工程类的附工程量清单等）

名称	品牌、规格、标准/主要服务内容	产地	数量	单位	单价（元）	金额（元）
**	**	**	**	**	**	**
合计：人民币大写：**元整						¥：**

## 第四章 采购内容与技术要求

### 一、项目概况：

坚持将黑龙江省公安大数据智能化建设融入大数据国家战略和“数字龙江”建设大局，把总体建设构架全量融入政务云建设，形成安全合规的龙江警务云，为大数据智能化建设项目(一期)、视频图像共享平台项目部署上云提供计算、存储、网络、安全、运维等云资源与云服务保障支撑。

合同包1（政务云服务商采购）

### 1.主要商务要求

标的提供的时间	合同签订后15个日历日内向用户交付用户所需的相关云资源与云服务
标的提供的地点	黑龙江省公安厅
投标有效期	从提交投标（响应）文件的截止之日起90日历天
付款方式	1期：支付比例100%，按照《黑龙江省省级政务云管理暂行办法》规定，省政务云服务费用按服务目录计算并按“先用后付、先审再付”原则进行结算。省营商环境建设监督局根据实际产生的服务类别、内容和实际采购价格核算服务费用，在每年9月底前审核汇总后提交省财政厅，下一年度由使用单位支付
验收要求	1期： 1、本次项目交付内容需符合省营商局政务云相关标准，纳入省政务云管理。 2、提供的IaaS服务、PaaS服务、运维运营服务、安全访问服务、网络服务等需达到项目功能、性能需求，并按公安云计算平台、公安大数据安全标准及规范，通过公安部或委托第三方机构进行的符合性测试和检测及安全等级保三级评测。 3、提供的各类服务需与公安网用户域、数据域，视频专网、公安业务网、各类公安专网按照公安部安全访问标准联通，提供相应安全访问和数据通道能力。 4、可交付的计算、存储、网络、安全资源不低于项目需求，并能够根据业务发展及时扩容。 5、项目提供的云管平台具备项目中的多云管理能力需求，能够纳管多地数据中心不同形态云资源。
履约保证金	
其他	续约条款，本项目采用1+1+1合同方式，采购单位（甲方）追加采购的项目预算变动幅度不超过本项目预算金额的10%的前提下，采购人（甲方）可以根据成交单位（乙方）在服务期的各项考核结果、岗位培训、服务质量等情况综合考量是否继续和成交单位续签合同。

### 2.技术标准与要求

序号	核心产品要求 （“△”）	品目名称	标的名称	单位	数量	分项预算单价 （元）	分项预算总价 （元）	招标技术要求
1		计算机设备和软件 租赁服务	计算机设备和软件 租赁服务	项	1. 00	0.10	0.10	详见附表一

附表一：计算机设备和软件租赁服务

参数性质	序号	具体技术(参数)要求

★	1	项目的计算、存储、网络、安全、运维等云服务与云资源需全量融入省政务云整体建设，是省政务云中满足公安业务应用与网络需求的公安业务专属云。
★	2	符合公安部大数据建设指导内容，充分遵循公安部公安大数据建设各类标准规范、指导建议、测试验证、评价标准等要求。满足公安部大数据智能化建设要求，提供云支撑构架和组件开发，提供涵盖IaaS和PaaS层的云计算服务，提供按需、弹性的计算、存储、网络资源池，同时通过资源服务能力构建负载均衡、弹性主机、资源编排等各种自动化云服务，提供标准服务接口支撑上层平台服务层、数据服务层、业务应用层的稳定运行。建设内容结构框图参考详见图附件1。（附件在公告中下载）
★	3	满足公安部下发的《公安云计算框架指南》与《公安大数据规范性文件汇编第一部分：公安云计算平台》分层解耦、异构兼容的技术要求。为保证云计算平台在和公安部对接更加平滑、稳定，云服务商所提供云平台在IaaS、PaaS等功能和接口方面应符合公安部部标要求，并通过公安部基准环境、异构兼容环境相关测试。
★	4	提供的计算、存储、网络、安全、运维等云服务与云资源的支撑软硬件除用户特别需求外，应满足国家安可标准，需随政务云整体建设或用户需求进行软硬件安可替代迭代演进，提供满足用户业务需求的安可软硬件环境。演进迭代过程中，不能降低资源与服务能力，能够平滑过度，不对用户业务造成稳定性、可靠性及业务中断等问题影响，在安可替代升级过程中，完成用户相关业务系统及功能的适配开发改造及迁移等工作。
★	5	提供的计算、存储、网络、安全、运维等云服务与云资源网络需满足公安部新一代公安信息网建设要求，需按新一代公安信息网标准接入相应汇聚节点及视频网，各业务运行于相应业务域网络。业务网络、管理网络、运维网络需符合新一代公安信息网建设标准及公安视频网标准。与公安业务网络、新一代公安信息网用户域、公安虚拟专网、公安视频专网、移动警务网、公安卫星通信网、政务网及互联网等网络对接，提供满足公安部标准要求的，与公安业务网络及其他接入网络的安全访问与数据交换通道能力，进行相应安全访问与数据交互。按公安部标准根据公安业务区域分别提供独立的云服务及资源，包括但不限于公安数据域、视频云区域，要求采用完全物理隔离方式建设，公安数据域、公安视频云域均需提供完整的IaaS、PaaS层运行、运营、维护、网络、安全及管理环境。
★	6	根据《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)标准的第三级安全保护能力要求，以及《GADS J 300-2019公安大数据安全总体技术框架》相关标准规范的要求提供整体云平台安全能力，保证云平台内的计算、存储、网络资源可以稳定、安全、可靠的对外提供服务，满足“安全、可信、合规”的要求，依据公安大数据安全标准规范要求，实现立体化纵深防御安全体系，通过云安全的开放架构，与云、网络协同联动，形成云网安一体化安全体系，保护云计算平台的安全。

★	7	<p>提供为公安业务定制的云管门户，开放云平台运维、运营、安全等各管理、监控层面及功能与公安“云检”“云哨”“云制”平台对接支撑。提供但不限于按公安部要求的相关功能、接口规范（详见各章节中的各类接口标准）和标准提供IaaS服务、PaaS服务、运维运营服务、安全访问服务、新一代公安信息网划域隔离服务、二次开发服务等；环境建设后及时启动测试，须通过公安部或委托第三方机构进行的符合性测试和检测及安全等保三级测评，后期使用须与公安部大数据平台对接，能够实现数据、运维、管理等相关方面对接，能够纳管地市大数据中心云平台、大数据平台，实现数据、运维、管理等相关方面对接。实现省、市两级云平台统一纳管、统一运维、统一运营、资源协同的全省“一片云”的整体规划需求。</p>
★	8	<p>本项目依据公安大数据规范性技术文件中的各层建设标准包括但不限于如下：1）、《GA/DSJ 111-2019 公安云计算平台 IaaS层 计算资源技术要求》2）、《GA/DSJ 112-2019 公安云计算平台 IaaS层 存储资源技术要求》3）、《GA/DSJ 113-2019 公安云计算平台 IaaS层 网络资源技术要求》4）、《GA/DSJ 121-2019 公安云计算平台 PaaS层 计算服务技术要求》5）、《GA/DSJ 122-2019 公安云计算平台 PaaS层 存储服务技术要求》6）、《GA/DSJ 123-2019 公安云计算平台 PaaS层 服务实例技术要求》7）、《GA/DSJ 124-2019 公安云计算平台 PaaS层 服务资源技术要求》8）、《GA/DSJ 300-2019公安大数据安全总体技术框架》9）、《GA/DSJ 350-2020公安大数据安全 安全访问与数据交换技术设计要求》10）、《GA/DSJ 351-2020公安大数据安全 零信任体系技术设计要求》</p>
★	9	<p>提供的云服务与云资源网络需满足公安部新一代公安信息网建设及公安视频网标准要求，提供的云计算平台需按新一代公安信息网标准接入相应汇聚节点及视频网，各业务区域运行于相应业务域网络。业务网络、管理网络、运维网络需符合新一代公安信息网及视频网建设标准。计算网络、存储网络、业务网络带宽不低于万兆，形成一个高性能、高可靠、可扩展的网络平台，满足公安业务对网络的大带宽、低延时、高可靠要求，支持并满足与其他网络的高效数据交换和联通共享，接入链路的带宽、冗余性需满足用户业务承载需求，实现网络统一运维。按照新一代公安信息网与公安视频专网标准进行网络拓扑规划、网络配置、网络VPC、VPN、路由表、ACL及其他网络参数调整与实施，实现与公安业务网络、新一代公安信息网用户域、公安虚拟专网、公安视频专网、移动警务网、公安卫星通信网、政务网及互联网等网络的对接。云服务商应完成云计算平台公安数据域、公安视频网域网络建设和隔离，并且符合公安部要求，能够做到与其他网络安全隔离和互通。网络拓扑参考详见图附件2。（附件在公告中下载）</p>
★	10	<p>提供的云资源、云服务需要与用户其他网络进行安全访问与数据交互，云服务商需按公安部标准为本次项目上云系统提供安全访问与数据交换通道服务，具备冗余性设计，并能够根据用户业务需求发展，提供服务能力扩展，满足《GA/DSJ 300-2019 公安大数据安全 总体技术框架》、《GA/DSJ 350-2020公安大数据安全 安全访问与数据交换技术设计要求》、《GA/DSJ 351-2020公安大数据安全 零信任体系技术设计要求》。安全访问与数据交换能力框架图参考详见图附件3。（附件在公告中下载）</p>

★	11	<p>数据资源的访问服务分为安全访问、数据交换两大类：安全访问模式要求基于零信任体系和安全防护体系提供的安全能力对访问主体、全省7万民警及其终端、原公安网业务系统及其他接入网业务、终端发起的访问请求，进行细粒度的管理和控制，防止违规行为发生，进行数据泄露检测和应用保护，并阻止网络威胁。访问敏感数据时提供虚拟桌面服务，防止敏感数据流出。数据交换模式要求基于零信任体系和安全防护体系提供的安全能力实现数据接入区与用户接入区、社会企事业单位网络、党/政/军机关网络、电子政务外网、互联网等其它网络之间的数据安全交换。</p>
★	12	<p>用户接入能力要求：用户包括用户接入区用户、公安机关驻地外用户以及其它网络用户。用户访问应用前应首先通过零信任体系中的认证服务进行身份认证，访问过程中应对用户身份合法性进行持续校验，确保用户身份可信。用户接入区用户接入，应通过零信任体系的环境感知服务感知接入终端的安全状态，确保终端安全可信，实现安全接入。公安机关驻地外用户接入，应采用虚拟专网（VPN）技术接入新一代公安信息网，再通过零信任体系的环境感知服务感知接入终端的安全状态，确保终端安全可信，实现安全接入。其它网络用户接入，应先采用虚拟专网（VPN）技术，并通过虚拟桌面接入新一代公安信息网，再通过零信任体系的环境感知服务感知接入终端的安全状态，确保终端安全可信，实现安全接入。</p>
★	13	<p>用户接入能力要求： 传输流量加解密：利用安全防护体系中网络传输加密服务进行链路通信加密，支持国密算法加密，确保数据传输过程中的机密性、完整性。在对网络流量进行检测时应对加密流量进行解密，确保安全检测效果。 虚拟桌面：用户访问时，可利用虚拟桌面技术，提升敏感数据防护能力，应通过虚拟桌面技术，实现敏感数据不出数据接入区，支持零信任体系对虚拟桌面身份进行统一验证，确保虚拟桌面接入的安全可信。 网络访问控制：在用户访问应用和数据的过程中，应利用安全防护体系中网络访问控制服务，实现安全访问相关的网络访问控制，使各组件只能访问授权的网络资源。 应用访问控制：在用户访问应用的过程中，应通过零信任体系对用户身份、应用身份进行统一验证，并进行应用级的权限控制。 功能访问控制：在用户访问应用功能的过程中，应通过零信任体系对用户身份、应用身份进行统一验证，并进行功能级的权限控制。 服务访问控制：在应用访问服务的过程中，应通过零信任体系对用户身份、应用身份进行统一验证，并进行服务级的权限控制。 数据访问控制：在应用访问数据的过程中，应通过零信任体系对用户身份、应用身份进行统一验证，并进行数据级权限控制。 网络威胁防护：利用安全防护体系中的相关安全服务，实现网络入侵防御、应用攻击防护等安全能力：<b>a)</b>网络入侵防御：利用网络入侵防御服务，阻止或限制对数据中心的网络攻击和异常行为；<b>b)</b>应用攻击防护：利用应用安全防护服务，检测并阻止攻击应用的行为。 网络安全检测：利用安全防护体系中的相关安全服务，检测网络流量，实现网络威胁检测、数据泄露检测、攻击诱捕等安全能力：<b>a)</b>网络威胁检测：利用网络威胁检测服务，采集、分析网络流量，发现网络攻击行为；<b>b)</b>数据泄露检测：利用数据泄露检测服务，获取、还原、解析网络流量，检测数据传输过程中的敏感信息，发现数据泄露行为；<b>c)</b>攻击诱捕：利用攻击诱捕服务，模拟网络/应用环境，引诱并发现攻击行为，分析攻击特征及攻击手法。</p>

★	14	<p>数据交换能力要求：设备准入控制：数据交换过程中，应对公共网络、专用网络接入数据交换的设备利用安全防护体系的网络访问控制服务，进行准入控制及身份验证。</p> <p>网络访问控制：数据交换过程中，应利用安全防护体系的网络访问控制服务，实现其它网络应用和服务仅可访问已授权的网络资源。服务访问控制：应用与数据服务数据交换过程中，应通过零信任体系对用户身份、应用身份进行统一验证，并进行服务级权限控制。数据访问控制：数据服务存取数据过程中，应通过零信任体系对用户身份、应用身份进行统一验证，并进行数据级权限控制。网络威胁防护：利用安全防护体系中的相关安全服务，实现网络入侵防御、网络恶意代码防护等安全能力：a)网络入侵防御：利用网络入侵防御服务，阻止或限制针对数据中心的网络攻击和异常行为；b)网络恶意代码防护：利用恶意代码防护服务，对网络流量中的恶意代码进行检测和清除。安全隔离与交换：在其它网络或用户接入区的系统、应用、服务与数据接入区的应用、服务进行数据交换的过程中，利用安全防护体系的网络隔离交换服务，实现数据传输协议剥离、传输模式控制，保证不同网络间的数据安全交换。网络安全检测：利用安全防护体系中的相关安全服务，检测网络流量，实现网络威胁检测、数据泄露检测、攻击诱捕等安全能力：a)网络威胁检测：利用网络威胁检测服务，采集、分析网络流量，发现网络攻击行为；b)数据泄露检测：利用数据泄露检测服务，获取、还原、解析网络流量，检测数据传输过程中的敏感信息，发现数据泄露行为；c)攻击诱捕：利用攻击诱捕服务，模拟网络/应用环境，引诱并发现攻击行为，分析攻击特征及攻击手法。日志采集：数据交换过程中，应采集设备、应用、服务等相关安全日志、告警等数据，并统一发送至用户建设的“三云”系统。</p>
---	----	---

★	15	<p>安全访问区服务要求，提供但不限于以下服务能力： 1、前/后端网关防护服务：提供对接入安全防护，包括支持网络访问控制、包过滤、状态检测；支持地址、转换映射，包括静态、动态转换等，提供吞吐量不少于200Gbps；最大支持并发连接数不少于1亿；每秒新建连接数不少于100万。 2、核心交换服务：提供交换容量不低于2Tbps，包转发率不低于700 Mpps处理能力；支持Guest VLAN、Voice VLAN，支持基于MAC/协议/IP子网/策略/端口的VLAN；三层支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议，支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议；支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGP EVPN，实现自动建立隧道；支持Telemetry、SNMP V1/V2/V3、Telnet、RMON、SSH。 3、接入交换服务：提供交换容量不低于700Gbps，包转发率不低于450Mpps处理能力；支持静态路由、RIP、RIPng、OSPF、OSPFv3、ISIS、BGP等路由协议；支持VXLAN二层网关、三层网关；支持BGP-EVPN协议；支持G.8032以太环保护协议。 4、可信接入检控服务提供零信任的用户可信检控能力，包括但不限于： a) 利用安全防护体系中网络传输加密服务进行链路通信加密，支持国密算法加密，确保数据传输过程中的机密性、完整性。在对网络流量进行检测时应对加密流量进行解密，确保安全检测效果。 b)检查与控制： 1)协议格式检查与控制：提供请求和响应报文头、报文格式检查能力，支持HTTP、WebSocket及虚拟桌面等的通信协议，根据检查结果阻断或放行； 2)令牌检查与控制：提供用户令牌、应用令牌检查能力，支持令牌格式、签名、内容、有效期的安全检查，根据检查结果阻断或放行； 3)终端身份检查与控制：提供接入终端的身份核验能力，支持终端身份签名、格式、时间戳、唯一性的安全检查，根据检查结果阻断或放行； 4)用户访问权限检查与控制：提供用户对应用访问检查能力，根据检查结果阻断或放行； c)日志记录与报送：提供用户访问日志、检控告警记录及上报能力。 d)网络吞吐量不低于10Gbps，HTTPS吞吐量不低于2Gbps，并发连接数不低于10万；</p>
---	----	---

★	16	<p>5、可信应用/数据检控提供零信任的业务应用与数据交互的检控能力，需依据用户访问、数据交换模式提供对应的支撑能力，能力要求包括但不限于：<b>a)加密流量解密</b>：在安全访问模式，应提供SSL/TLS加密流量解密能力，实现安全检测；<b>b)检查与控制</b>：<b>1)令牌检查与控制</b>：提供用户令牌、应用令牌检查能力，支持令牌格式、签名、内容、有效期的安全检查，根据检查结果阻断或放行；<b>2)协议格式检查与控制</b>：在安全访问模式，提供请求和响应报文头、报文体的格式检查能力，支持HTTP、WebSocket等应用层协议检测能力；在数据交换模式，提供数据库协议、文件传输协议等协议等能力，根据检查结果阻断或放行；<b>3)业务应用访问权限检查与控制</b>：在安全访问模式，提供业务应用对应用服务/数据服务访问检查能力，提供应用API访问敏感信息的监控，根据检查结果阻断或放行；<b>4)数据交换内容检查与控制</b>：在数据交换模式，提供文件、数据等内容检控能力，支持对结构化数据、非结构化数据进行内容检查，依据检查结果进行阻断或放行；<b>c)验证签名</b>：数据交换模式支持数据验证签名能力，对数据标签、事件标签中签名的有效值进行检查，依据检查结果进行阻断或放行；<b>d)日志记录和报送</b>：提供业务应用访问/数据交换的日志、检控告警记录及上报能力。<b>e)可信应用/数据检控提供网络吞吐量不低于10Gbps，HTTPS吞吐量不低于2Gbps，并发连接数不低于10万</b>；<b>6、虚拟云桌面服务</b>：用户访问时，可利用虚拟桌面技术，提升敏感数据防护能力：通过虚拟桌面技术，实现敏感数据不出数据接入区，数据不落地要求；支持零信任体系对虚拟桌面身份进行统一验证，确保虚拟桌面接入的安全可信；支持云桌面资源规格（CPU、内存等）桌面模板（操作系统、应用软件）自定义，提供虚拟桌面申请、启动、关闭、重启、删除、配置管理等生命周期操作；可提供不少于500个云桌面节点（含计算、存储等资源）；每个云桌面配置最少4核心CPU，8G内存，300G硬盘。</p>
---	----	--

★	17	<p>数据交换区服务要求提供但不限于以下服务能力： 1、抗DDOS防护网关服务：流量监测能力不小于35G。 2、前/后端网关防护服务：提供对接入安全防护，包括支持网络访问控制、包过滤、状态检测；支持地址、转换映射，包括静态、动态转换等，提供吞吐量服务能力不少于240Gbps；最大支持并发连接数不少于1亿；每秒新建连接数不少于100万。 3、核心交换服务：提供交换容量不低于2Tbps，包转发率不低于700 Mpps处理能力；支持Guest VLAN、Voice VLAN，支持基于MAC/协议/IP子网/策略/端口的VLAN；三层支持RIP、 OSPF、 ISIS、 BGP等IPv4动态路由协议，支持RI Png、 OSPFv3、 ISISv6、 BGP4+等IPv6动态路由协议；支持VxLAN功能，支持Vx LAN二层网关、三层网关，支持BGP EVPN，实现自动建立隧道；支持Telemetry、 SNMP V1/V2/V3、 Telnet、 RMON、 SSH。 4、接入交换服务：提供交换容量不低于700Gbps，包转发率不低于450Mpps处理能力；支持静态路由、RIP、RIPng、 O SPF、 OSPFv3、 ISIS、 BGP等路由协议；支持VXLAN二层网关、三层网关；支持BG P-EVPN协议；支持G.8032以太环保护协议。 5、设备准入控制服务：网络吞吐量不低于8Gbps；最大并发认证数不低于1000次/秒；加密吞吐量不低于2Gbps；支持设备认证客户端数量不少于1000个；提供设备注册、设备身份证书管理、多因子等功能。支持认证客户端与网关采用数字证书+设备指纹认证，提供服务器认证客户端，认证客户端支持采集服务器CPU序列号、MAC、硬盘序列号、操作系统、安装列表、进程等信息，形成设备唯一指纹；支持与数据交换服务、隔离交换系统等第三方系统对接，支持通过API传递认证结果。 6、安全数据交换系统服务：具有分布式集群管里能力、集群负载均衡和高可用能力，支持任意多套数据交换系统组建集群，可实现统一集中化配置。支持各类主流各版本数据库同步、消息总线同步、文件交换同步（含GB级别大文件）、API服务交换等功能，数据库同步速率不低于10000条/秒；消息同步速率速率不低于7000条/秒；API注册数量不少于200，并发不少于1000，按秒实现调度任务 7、安全视频交换系统服务：可提供基于视频流的安全交换服务，支持海康、大华、宇视、科达、华三、华为、普天、海能达、天地伟业等主流视频厂商协议识别和适配；支持信令消息解析、识别，并可设定安全策略进行控制。支持并符合公安部视频标准规范，支持标清、高清万路以上视频流接入。</p>
---	----	---

★	18	<p>数据交换区服务要求提供但不限于以下服务能力：<b>8、安全隔离与单向传输服务</b>：可通过多机集群部署，根据配置参数进行任务分担，满足用户单向传输性能需求，通过单向隔离控制保障数据传输安全，符合公安部标准要求。<b>9、可信数据检控</b>提供零信任的业务应用与数据交互的检控能力，需依据用户访问、数据交换模式提供对应的支撑能力，能力要求包括但不限于：<b>a)加密流量解密</b>：在安全访问模式，应提供SSL/TLS加密流量解密能力，实现安全检测；<b>b)检查与控制</b>：<b>1)令牌检查与控制</b>：提供用户令牌、应用令牌检查能力，支持令牌格式、签名、内容、有效期的安全检查，根据检查结果阻断或放行；<b>2)协议格式检查与控制</b>：在安全访问模式，提供请求和响应报文头、报文体的格式检查能力，支持HTTP、WebSocket等应用层协议检测能力；在数据交换模式，提供数据库协议、文件传输协议等协议等能力，根据检查结果阻断或放行；<b>3)业务应用访问权限检查与控制</b>：在安全访问模式，提供业务应用对应用服务/数据服务访问检查能力，提供应用API访问敏感信息的监控，根据检查结果阻断或放行；<b>4)数据交换内容检查与控制</b>：在数据交换模式，提供文件、数据等内容检控能力，支持对结构化数据、非结构化数据进行内容检查，依据检查结果进行阻断或放行；<b>c)验证签名</b>：数据交换模式支持数据验证签名能力，对数据标签、事件标签中签名的有效值进行检查，依据检查结果进行阻断或放行；<b>d)日志记录和报送</b>：提供业务应用访问/数据交换的日志、检控告警记录及上报能力。<b>e)可信数据检控</b>提供网络吞吐量不低于10Gbps，HTTPS吞吐量不低于2Gbps，并发连接数不低于10万；</p>
★	19	<p>安全检测区服务要求提供但不限于以下服务能力：<b>1、流量采集复制分流服务</b>：支持基于端口的M:N流量复制分发；支持基于流的M: N流量复制分发；支持基于HASH的报文负载分担；支持基于轮询的报文负载分担；支持10GE端口聚合；支持40GE端口聚合；支持静态聚合、动态聚合。<b>2、集中采集服务</b>：支持SYSLOG协议、SNMP v2 /SNMP v3协议、FTP方式采集或接收安全访问和数据交换通道中各设备数据信息；支持数据范式化处理，包括嵌套拆分、字段检查、合并等处理。采集速率不低于2000E PS;吞吐量不低于4000Mbps；<b>3、网络流量采集服务</b>：支持L2~L7层进行流量解析；支持边界接入平台业务和应用识别，网络流量处理速率、流量格式化数据入库性能满足用户需求。<b>4、网络威胁检测服务</b>：支持 HTTP Get、Head、Put、Post 等多种协议方法检查；支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20余种协议和应用的攻击检测和防御；支持自定义入侵防御特征，包括 IP、TCP、UDP、IGMP、ICMP等网络层的各项参数设置特征；支持对数据包进行协议异常检测，支持 IP 地址、通信端口扫描异常检测；支持对未知攻击探测行为的检测，与用户建设的安全应用对接，提供数据及接口支持。<b>5、数据防泄漏检测服务</b>：支持HTTP、FTP、SQL等常规应用协议解析；支持对文本数据进行模式匹配，包括精确匹配、模糊匹配、正则匹配，识别敏感内容，与用户建设的安全应用对接，提供数据及接口支持。<b>6、攻击诱捕服务</b>：支持多种蜜罐类型，包括：高交互、内网漫游、内网渗透、外网渗透、工控、认证攻击、高级认证攻击、ARP欺骗；高低交互蜜罐搭配，拟态诱导攻击者深入攻击，获取更多黑客信息；实时监测，采用主动响应措施，及时切断风险源，保证系统自身安全；回溯攻击行为，有针对性主动防御。攻击记录留存时间不低于12个月；与用户建设的安全应用对接，提供数据及接口支持。</p>

★	20	带外管理区服务要求提供但不限于以下服务能力： <b>1、管理网络网关防护服务</b> ：提供对带外管理区的接入安全防护 <b>2、管理网络核心交换服务、管理网络带外交换服务 3、可信运维服务</b> ：支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理；支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令；支持域认证与双因子认证结合使用；
★	21	数据域服务要求提供数据域边界网关防护服务，支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MS等；能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、内容安全统一界面进行安全策略配置；支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议；基于特征的攻击检测和防御；

★	22	<p>互联网+政务服务区的边界接入提供但不限于以下安全服务： 1、前端/后端网关防护服务：提供接入安全防护，包括支持网络访问控制、包过滤、状态检测；支持地址、转换映射，包括静态、动态转换等，提供吞吐量服务能力不少于10Gbps。 2、抗DDOS防护网关服务：能够抵抗DDOS攻击，清洗能力不低于8G。 3、设备准入控制服务：网络吞吐量不低于8Gbps；最大并发认证数不低于1000次/秒；加密吞吐量不低于2Gbps；支持设备认证客户端数量不少于1000个；提供设备注册、设备身份证书管理、多因子等功能。支持认证客户端与网关采用数字证书+设备指纹认证，提供服务器认证客户端，认证客户端支持采集服务器CPU序列号、MAC、硬盘序列号、操作系统、进程等信息，形成设备唯一指纹；支持与数据交换服务、隔离交换系统等第三方系统对接，支持通过API传递认证结果 4、安全数据交换系统服务：具有分布式集群管理里能力、集群负载均衡和高可用能力。支持各类主流各版本数据库同步、消息总线同步、文件交换同步（含GB级别大文件）、API服务交换等功能，数据库同步速率不低于10000条/秒；消息同步速率速率不低于7000条/秒；API注册数量不少于200，并发不少于1000，按秒实现调度任务 5、安全隔离与单向传输服务：支持数据库同步、文件交换等功能；支持TCP流转UDP数据包。支持根据配置参数进行任务分担。 6、集中采集服务：支持SYSLOG协议、SNMP v2/v3协议、FTP方式采集或接收各设备数据信息；支持数据范式化处理，包括嵌套拆分、字段检查、合并等处理。 7、集中监控与级联管理服务：提供对边界平台、链路、业务的统一管理与管理；支持对平台和接入业务提供信息注册和管理功能；提供对接入设备的安全、网络、系统和业务应用的运行情况实时监测；提供对平台自身的运行状况实时监测，对监测、报警、安全事件等数据的查询和统计，提供实时动态监测平台当前运行总体情况；按时间段、应用系统、单位分析统计业务、流量、异常信息；对平台各组件操作配置、平台承载的业务应用、平台内设备的网络行为等内容进行安全审计和异常事件的追踪。支持将本地平台、接入业务、运行状态、安全审计等信息，上报给上级单位平台，为上级接入平台对本地接入平台的注册管理、运行状态、安全审计等方面信息的浏览、综合查询及统计分析提供所必须的数据 8、数据库防火墙服务：支持多种主流类型数据库，包括：ORACLE、MYSQL、SQLSERVER、POSTGRESQL、DB2、KINGBASE、Hadoop,Spark(SQL),Presto,ES等；支持环境感知、资源访问控制、行列控制、脱敏、数据库审计等功能。数据库连接数10000以上。</p>
★	23	<p>安全访问过程中，应采集设备、应用、服务等相关安全日志、告警等数据，并统一发送至用户建设的“三云”系统。相关安全策略、安全设置等安全控制与用户建设的“三云”系统联动对接。</p>
★	24	<p>云服务商应按需提供的IaaS层计算资源服务包括但不限于：弹性云主机服务、裸金属服务、镜像服务、容器服务等，服务须严格参照公安部功能及接口规范要求，符合《GA/DSJ 111-2019 公安云计算平台 IaaS层 计算资源技术要求》。</p>

★	25	<p>弹性云主机服务：提供按硬件配置、操作系统和网络需求交付的弹性的、动态的计算能力，资源动态分配，动态共享。提供上电即用的虚拟机业务，基于虚拟化技术，满足按需快速发放。按用户需求提供不同规格的CPU、内存、磁盘空间，提供优先级、权重、网络带宽等不同的Qos服务质量；提供不同的操作系统类型（包括但不限于Windows、Suse、Redhat等）的虚拟机，用户可进行自助管理和控制的功能。可以根据需求进行扩展和收缩。不同类型的弹性云主机匹配不同的应用场景，可以根据用户的业务诉求选择相应的云服务器。弹性云主机服务需通过统一服务门户或者web管理控制台，让用户自主的完成服务实例的申请、释放、变更等操作，从而灵活使用弹性云主机服务，提供包括但不限于以下能力。</p> <ul style="list-style-type: none"> <li>• 支持多类型，多规格CPU、内存、硬盘、网络的云服务器的选择和变更。</li> <li>• 支持多种类型云硬盘供选择，例如分布式存储、SAN存储，支持云硬盘的扩容，当磁盘空间不足时，可以通过扩容原有磁盘空间满足需求。</li> <li>• 网络自定义，自由划分子网、设置网络访问策略，通过VPC（虚拟私有云服务）实现虚拟私有云网络管理，用户可自助规划VPC内网络的IP地址范围。</li> <li>• 提供公共镜像能力和私有镜像服务，免安装快速部署操作系统与软件。</li> <li>• 提供VNC控制台、远程终端和API等多种管理方式，解决系统问题，进行各项操作；包括但不限于对服务器进行启动、重启、关机等操作。</li> <li>• 实例反亲和性：支持在控制台上创建一个或多个反亲和性组；在一个反亲和性组中的实例将分配到不同的物理主机上来保证高可用。</li> <li>• 支持不停机增加网卡、存储盘，不停机修改虚拟机名称。</li> <li>• 支持在删除虚拟机时清空所挂载的磁盘数据，确保磁盘数据不可被恢复。</li> <li>• 支持启动、重启、正常关闭、强制关闭虚拟机。</li> <li>• 支持查询指定虚拟机当前状态、虚拟机所属的用户、虚拟机创建的时间、虚拟机磁盘等信息。</li> <li>• 支持挂起运行的虚拟机，将虚拟机的状态信息保存到磁盘，虚拟机处于挂起状态，同时会释放掉占用的CPU、内存等资源。</li> <li>• 支持恢复挂起的虚拟机，将虚拟机的信息从磁盘取出，并重新分配相关的资源，使虚拟机处于运行状态。</li> <li>• 在同一应用需要多台相同的虚拟机时，将多台虚拟机均衡分布在不同的物理机上，实现应用的可靠性提升。</li> <li>• 支持对启动中的虚拟机系统磁盘和所有数据盘创建即时快照，包括但不限于能够指定快照名称、提供描述信息。</li> </ul>
---	----	---

★	26	<p>裸金属服务：提供专属的物理服务器，裸金属服务器上不运行虚拟化层，直接安装用户OS，提供卓越的计算性能，满足核心应用场景对高性能、稳定性、高安全性的需求。发放后的裸金属服务器可以与虚拟机网络互通，同时可以和其他云产品灵活结合使用。对于不适合虚拟机部署的应用可以使用裸金属服务，例如：数据库集群、OLAP(联机分析处理)型应用（大数据、重载应用）等。裸金属服务须具有但不限于以下功能：</p> <ul style="list-style-type: none"> <li>• 裸金属资源池可根据需要规划多种物理服务器规格（CPU、内存、硬盘），可以根据不同场景的业务需求进行选择不同类型的物理服务器。</li> <li>• 裸金属服务实例相对于裸金属服务器没有性能损失，专属于单个用户，可以提供显著的计算性能和I/O吞吐量。</li> <li>• 快速部署，裸金属实例需30分钟完成开通，满足用户的紧急需求。</li> <li>• 支持高性能、高可靠的超大型关键业务、核心数据库的裸金属服务器需求。</li> <li>• 支持自助申请和挂载云硬盘，支持多规格多类型云硬盘挂载。</li> <li>• 支持网络自定义，自由规划裸金属IP地址。</li> <li>• 裸金属实例可以与弹性云实例规划到同一个VPC(虚拟私有云)，用户可以方便的管理、配置内部网络；为每个裸金属实例可以提供公网IP和私网IP，用于不同的连接场景。公网IP可以对外连接互联网；私网IP可以内部连接使用。</li> <li>• 可配置丰富的镜像，免安装快速部署操作系统与软件。</li> <li>• 提供多样化的管理方式：管理方便，用户可以通过Web页面或者开放API，同时管理一个、数百个、甚至数千个裸金属实例。支持裸金属服务器实例关键性能监控，以便快速发现定位主机故障。</li> <li>• 提供完整控制能力：完全控制，用户可以完全控制自己创建的裸金属实例，拥有每个实例的管理员访问权。</li> <li>• 提供裸金属服务器生命周期管理，包括启动、关机、重启、删除等。</li> <li>• 提供多种操作系统版本的安装，支持主流（包括但不限于）CentOS、SUSE Linux、Red Hat Linux等Linux操作系统。</li> <li>• 裸金属实例支持多种登录方式（密码、密钥），密码防暴力破解，满足用户的登录安全需求。对于Windows的裸金属实例，用户只能使用密码登录。</li> </ul>
★	27	<p>镜像服务：镜像是弹性云主机实例可选择的运行环境模板，包括操作系统和预装的软件(可包括公共应用软件以及用户私有应用软件)。向用户提供某种应用的一组服务器及软件的集合，如数据基础环境、中间件基础环境等应用，是一种应用模板自动化服务。服务由虚拟机，及虚拟机使用的网络信息、安装的软件包、脚本组成，管理员可自定义创建、修改、删除、复制、共享应用模板，将模板发布为可供申请的应用服务，实现进行业务发放。镜像应用模板：是将虚拟机模板、软件包、弹性伸缩组、脚本资源，按照特定的关系有机结合，使用应用模板能够快速部署应用实例。可以快速高效地为云主机租户在云平台中提供便捷的应用服务，实现云主机应用部署环境的快速发放。镜像服务须具有但不限于以下功能：</p> <ul style="list-style-type: none"> <li>• 系统管理员可通过制作/注册镜像创建公共镜像 — 系统管理员可以通过ISO原始镜像来制作公共镜像； — 系统管理员可以通过已有本地镜像文件上传镜像，然后注册为公共镜像； — 系统管理员可对公共镜像进行管理，修改镜像属性、更新镜像、删除镜像。</li> <li>• 系统管理员可以将公共镜像导出到本地</li> <li>• 用户可通过云服务器创建私有镜像 — 用户可以指定云主机制作整机镜像，整机镜像同时包含系统盘镜像和所有的数据盘镜像。</li> <li>• 用户可以通过本地镜像文件上传私有镜像，用户可以对私有镜像管理，导出私有镜像</li> <li>• 提供win、linux等主流操作系统授权，含租用、安装等技术支持服务</li> </ul>

★	28	<p>容器服务：一种内核虚拟化技术，可以提供轻量级的虚拟化，以便隔离进程和资源，而且不需要提供指令解释机制以及全虚拟化的其他复杂性。容器可以避免传统虚拟化技术带来的过高的性能损耗，同时基于容器部署应用可以更快速部署和调整业务。集群管理：支持在虚拟机和物理机上创建容器的集群，修改、删除查询集群，同时支持基于用户的集群权限管理，包括但不限于读写权限。容器镜像和软件包管理：容器技术突出的优点就是开发运维一体化。通过把应用及其所依赖的软件包、操作系统文件等封装在容器镜像中，使得应用在开发、测试和发布过程中都具有相同的运行环境，带来极大的便利。容器管理平台具有提供上传，下载，查找容器镜像和软件包的功能。租户可以创建自己的镜像和软件仓库，创建时可指定镜像仓库属性为私有或公有。可以创建、删除、修改、查询、共享、列举镜像。容器应用管理：可以快速创建、运行、停止容器，用户可以在平台上编排和部署容器应用，并提供模板编排或图形化编排这两种应用编排方式。应用组件管理：支持创建应用组件，修改、列举、查询和删除应用组件。容器应用调度：云容器应用调度能力基于容器调度引擎（如Kubernetes）实现，为容器化的应用提供资源调度、部署运行、服务发现、扩容缩容等整套容器生命周期管理功能。在部署新容器实例时，Kubernetes可以根据预先设定的亲和性/反亲和性策略选择一个恰当的宿主机来部署新实例。一类容器的多实例之间的负载均衡既可以采用Kubernetes带有的NodePort方式，也可以采用平台提供的软负载均衡器。主要功能包括但不限于：</p> <ol style="list-style-type: none"> <li>1. 提供支持动态横向扩展的宿主机管理能力，支持集群负载线性扩容，支持不停机状态下主机在线添加，横向扩充集群节点。</li> <li>2. 支持控制组件自动分发，实现新节点快速初始化及统一纳管。</li> <li>3. 具备完善的宿主机监控能力，能够对机器运行状态、存储情况、CPU和内存使用情况、磁盘I/O、网路负载等关键指标进行实时采集与展示。</li> <li>4. 支持容器生命周期管理，包括创建、删除、启动、停止、重启等。</li> <li>5. 支持多种网络组建模式，可满足扁平网络、vlan、vxlan等组网技术接入，并提供完善的网络管理功能。</li> <li>6. 具备接入本地存储、分布式存储的能力，支持基于LVM容器卷管理功能。</li> <li>7. 提供基于分布式存储技术的容器镜像仓库，用于统一存储容器镜像，同时提供容器镜像在线管理功能，支持镜像上传、删除等基本操作，支持镜像版本管理。</li> </ol>
★	29	<p>云服务商需提供但不限于如下IaaS层存储资源服务，包括分布式块存储服务、对象存储服务、文件存储服务等，服务须严格参照公安部功能及接口规范要求，符合《GA/DSJ 112-2019 公安云计算平台 IaaS层 存储资源技术要求》。</p>

★	30	<p>分布式块存储服务：采用分布式存储架构，通过软件层面的去中心化架构和数据冗余技术，将多个独立服务器自带的存储组成的一个存储资源池，对外提供统一的、持久性存储服务的存储系统。大容量、高性能、强扩展、高可用是分布式块存储的关键能力。利用分布式存储设备为虚拟主机和裸金属服务器提供的额外的存储卷(虚拟硬盘)，具有更高的数据可靠性，更高的I/O吞吐能力和更加简单易用等特点，适用于文件系统、数据库或者其他需要块存储设备的系统软件或应用。分布式块存储提供云硬盘服务，是一种可弹性扩展的虚拟块存储设备，可以在线进行操作，使用方式与传统服务器硬盘完全一致，可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据持久化存储。提供但不限于以下功能： 1. 支持弹性挂载/卸载。支持按需创建指定配置的云硬盘，挂载到单个实例。磁盘不受实例运行时间的影响。将磁盘挂载到实例后，可以像使用其他物理硬盘一样使用它，支持将磁盘从实例中卸载，并将其挂载到另一个实例。 2. 能够根据业务对存储读写性能需求，通过变更业务存储磁盘类型功能调整，来改变读写性能，以应对实例存储业务性能调整的诉求。 3. 支持弹性可扩展。可以自由配置存储容量，按需扩容，以满足业务数据扩容需求。 4. 支持快照功能。可以通过拍摄磁盘的时间点快照来备份数据，防止因篡改和误删导致的数据丢失，保证在业务故障时能够快速回退。同时可以从快照创建新的磁盘，并将其挂载到其他实例，以便为多种业务提供数据资源。 5. 支持共享盘。支持多个实例并发读写访问同一个共享盘，以满足集群、高可用能力的关键业务需要多个实例同时访问一个磁盘的应用场景。</p>
★	31	<p>对象存储服务：基于对象的海量存储服务，为提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删除、上传、下载、删除对象等。对象存储适合存放任意类型的文件。可存储文档、图片、音视频等非结构化数据的云存储服务，提供海量、安全、高可靠、低成本的数据存储能力。对象存储服务提供服务使用、管理、容灾的全套解决方案，降低采购、部署、优化、维护专用存储设备的成本。提供但不限于以下功能： 1. 支持多种类型存储对象的上传下载，例如图片、音频、视频、文本、日志等 2. 提供定制化对象存储中间件及监控检查的内核组件。 3. 支持对存储对象的分组管理，并实现基于分组的权限控制，支持设置访问策略，如公开、私密。 4. 支持断点下载和大文件的分片上传。 5. 支持多种异构存储环境的对接。 6. 支持存储规格定义，如定义存储容量、类型、带宽等指标，支持基于存储规格的分配。 7. 支持多副本及纠删存储冗余机制，保证数据高可靠性。支持数据检查：存储前一致性检查，确保存入数据是上传数据。 8. 支持线性扩展能力，支持海量数据存储能力。 9. 提供在线全生命周期管理，包括服务申请、审核、自动部署，实例的启停、升级、销毁及监控等。 10. 提供日志记录功能，方便追查访问来源以及进行多维度的统计分析。 11. 具备完善的多用户隔离机制，保障用户数据的私密性。 12. 同时提供给内部服务，如镜像(公有镜像和私有镜像保存在对象存储)，大数据，备份等服务作为存储空间。</p>

★	32	<p>文件存储服务：文件存储系统通过标准的文件访问协议，提供多共享、高可靠和高可用等特性的文件访问。应用可以挂载并使用平台预先分配的文件系统。文件系统具有文件与目录操作、文件访问以及文件访问控制功能。提供但不限于以下功能：1. 协议支持。提供NFS、CIFS、FTP等标准接口，提供百PB容量、千亿文件的超大规模横向扩展能力和单一文件系统，应用于海量非结构化数据的存储。2. 并行访问。支持以一种协议创建的文件能够通过其它协议以相同的权限访问。支持文件的并行访问，多个计算节点可以同时访问同一个文件系统实例。3. 数据安全。支持用户数据与用户指令的信息传输安全，避免用户数据和用户指令在传输过程中被非法授权访问。支持用户隔离、文件系统标准权限控制等多种安全机制。支持文件的只读保护，在文件保护期间不能进行修改和删除。4. 数据冗余。支持多种数据冗余机制，确保数据在硬盘或单节点发生故障时不丢失。5. 数据备份/恢复。支持数据远程备份/恢复。6. 精简配置。支持精简配置，对分配的文件存储容量根据实际用量进行动态分配。7. 配额管理。支持配额管理功能，实现在同一个共享文件系统中，为不同用户/部门或者不同目录分配不同的使用空间，并对其空间大小进行管理。8. 文件系统查询。支持查询有访问权限的文件系统列表及相关信息。9. 文件系统挂载点查询。支持查询有访问权限的文件系统挂载点及相关信息。</p>
★	33	<p>云服务商应提供但不限于如下IaaS层网络资源服务，除公安部要求提供的包括虚拟私有云服务、VPN服务、虚拟负载均衡服务、弹性IP服务，还应考虑业务实际需求和实用性需求，提供其他包括虚拟防火墙服务、安全组服务，其中公安部要求提供的服务部分须严格参照公安部功能及接口规范要求，符合《GA/DSJ 113-2019 公安云计算平台 IaaS层 网络资源技术要求》。</p>
★	34	<p>虚拟私有云服务：VPC即虚拟私有云服务，通过逻辑方式进行网络隔离，提供安全、隔离的网络环境，提供与传统网络无差别的虚拟网络，提升用户中资源的安全性，简化用户的网络部署。在VPC中可以定义安全组、VPN、IP地址段、带宽等网络特性。用户可以自定义安全组内与组间弹性云主机服务器的访问规则，加强弹性云主机服务器的安全保护。虚拟私有云服务须具有但不限于以下功能：</p> <ul style="list-style-type: none"> <li>• 支持子网管理 – 可以创建多个子网，指定子网申请虚拟IP，以及修改私有IP地址。</li> <li>– 支持IPv4，IPv6双栈场景。</li> <li>• 路由管理 – 配置VPC的默认路由，把指定目的网段的报文发给指定下一跳。</li> <li>– 支持IPv4，IPv6双栈场景。</li> <li>• VPC间三层互通 – 支持租户使用私有业务IP地址在安全隔离的VPC之间实现三层路由互通。</li> <li>– 支持IPv4，IPv6双栈场景。</li> </ul>
★	35	<p>VPN服务：虚拟专用网络（VPN），用于分支机构和VPC之间建立一条安全加密的通信隧道，把已有数据中心和云上的网络打通。虚拟专用网络服务须具有但不限于以下功能：</p> <ul style="list-style-type: none"> <li>• 支持IKE加密算法 AES-128，AES-192，AES-256，3DES；</li> <li>• 支持IKE完全正向保密 GROUP2，GROUP5，GROUP14；</li> <li>• 支持IKE版本 V1，V2；</li> <li>• 支持IPSEC认证算法 sha-256，sha-384，sha-512，sha1，md5；</li> <li>• 支持IPSEC加密算法 AES-128，AES-192，AES-256，3DES；</li> <li>• 支持IPSEC传输协议 ESP，AH，AH-ESP。</li> </ul>

★	36	<p>虚拟负载均衡服务通过将访问流量自动分发到多台弹性云主机，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。提供但不限于以下功能： 1. 支持四层和七层的负载均衡服务，可以根据业务的种类采用不同的协议进行负载。 2. 支持在线监听器设置。每个负载均衡实例，可以创建多个不同端口的负载，满足不同业务的负载均衡功能。监听器可以选择多种负载均衡的策略，提供轮询、最小连接数、源地址等多种转发规则，满足不同业务场景的要求。 3. 支持会话保持。会话保持可以将来自同一个客户端的请求始终发给同一个后端服务器，通过 <b>cookie</b> 的方式来实现。 4. 提供可视化监控及报警功能。可以通过可视化界面查看资源使用情况，包括存储使用率、内存使用率、CPU使用率、网络流入速率、网络流出速率、网络流入包数、网络流出包数、网络连接数等。</p>
★	37	<p>弹性IP服务：提供云计算平台内合法的静态IP地址的服务。可以通过申请弹性IP达到连通弹性云主机与公安网的目的。将弹性IP地址和路由网络中关联的虚拟机绑定，可以实现业务资源与公安网互通。通过弹性IP，可从公安网访问云主机。当所关联云主机故障或需要升级时，可以迅速将弹性IP 地址重新映射到另一个正常工作的备用云主机，无需变更云主机客户端的配置继续从备用云主机获得服务，从而降低业务影响。提供但不限于以下功能： 1. 用户自主的完成服务的开通与关闭，让用户灵活使用弹性IP 服务，达到即开即用，用完归还的目标。 2. 支持从公安网访问云主机的目的IP地址转换。 3. 支持从云主机访问公安网的源IP 地址转换。 4. 支持从公安网访问负载均衡服务的虚拟IP。</p>
★	38	<p>虚拟防火墙服务，用于子网级别的安全防护，虚拟防火墙服务提供防火墙安全服务，保护了云上业务的安全。通过vFW的创建和ACL规格的设置，实现云主机之间、云主机和外部网络的安全访问和隔离。虚拟防火墙服务具有但不限于以下功能： • 规则匹配域支持：源端口，源IP地址，目的端口，目的IP地址，协议； • 可以调整规则的顺序； • 协议支持：TCP, UDP, ICMP, ANY； • 支持IPv4, IPv6双栈场景。 • 管理用户可以在云管界面进行虚拟防火墙以及虚拟防火墙规则的禁用与启用； • 支持虚拟防火墙单条防火墙规则聚合。</p>
★	39	<p>安全组服务：一组对实例的访问规则的集合，为同一个VPC内具有相同安全保护需求并相互信任的实例提供访问策略。安全组服务通过web管理控制台，让用户自主的完成服务的开通与关闭，让用户灵活使用安全组服务，达到即开即用，用完归还的目标。安全组服务具有但不限于以下功能： • 默认出方向放行。 • 同一个安全组的云主机默认可相互访问。 • 可以灵活配置出方向和入方向规格。 • 管理方便，用户可以通过web页面或者开放API，同时管理一个、数十个、甚至上百个安全组实例。 • 完全控制，用户可以完全控制自己创建的安全组实例。 • 支持IPv4, IPv6双栈场景。</p>
★	40	<p>授时服务对下可为每台云主机及设备提供高精度的标准时间作为基准时钟，对上自动与公安部NTP服务器保持一致，同时为云平台分布式系统提供基本保证，服务于分布式应用、计算机网络运行、监控等。</p>

★	41	<p>云服务商需提供但不限于如下PaaS层计算服务，须严格参照公安部功能及接口规范要求，符合《GA/DSJ 121-2019 公安云计算平台 PaaS层 计算服务技术要求》。各类组件要求符合《公安云计算平台框架指南》和公安云计算异构兼容接口标准。需要充分考虑各类应用对组件的需求，要求基于开放社区Apache Hadoop，不使用任何私有架构和组件。包括但不限于以下服务：流式计算、离线计算、实时计算、内存计算、图计算等。</p>
★	42	<p>流式计算服务提供满足低时延的数据处理场景，高并发处理数据，时延在毫秒级，且兼具可靠性流式计算方案。同时，需提供数据分发以及并行化计算的流数据处理引擎，用于实时布控、实时监控预警、实时统计等实时性要求非常高的场景，具备分布式、可靠、容错特性。通过流式计算，可从各种数据来源中连续捕获和存储TB级以上数据，支持进行实时分析、在线机器学习、信息流处理、连续性的计算、分布式RPC（通过网络调用远程计算任务）等各种操作，实现流数据的秒级计算。提供但不限于以下功能：1. 支持次秒级计算不断流入的数据；2. 支持分布式弹性计算，计算能够在多个线程、进程和服务器节点之间并行进行，支持横向扩展节点增加计算能力；3. 支持多种数据源的流数据输入，包括分布式消息队列kafka、mqtt、web socket、http、flume等；4. 在某个计算节点宕机时，能够自动检测，并将该任务自动分发至其它存活节点，同时管理节点通过也需具备容错；5. 可靠的消息处理：保证每个消息至少能得到一次完整处理。任务失败时，能够从消息源重试消息；6. 支持Java、Python等多种编程语言，提升易用性；7. 自动化云中交付资源隔离的流计算服务实例。每个服务实例具有独立的流式计算集群，每个服务实例独占CPU、内存和磁盘IO；8. 提供可视化界面对作业任务进行管理，包括任务的创建、启动、停止以及任务状态和各项指标监控等；9. 支持以数据表格和图表方式展示物理资源的使用情况，如存储使用率、内存使用率、CPU使用率等；以及组件节点的运行状态、连接数等。并支持针对相关指标的阈值告警功能。</p>
★	43	<p>提供实时计算能力，主要满足公安对于自助分析、交互式查询场景的需求，主要用于数据实时读写和数据实时分析两个场景。数据实时读取主要满足对海量数据（TB级以上）写入及查询的需求，如卡口车辆数据实时写入及车辆轨迹查询；数据实时分析主要满足公安对于交互式场景的数据处理需求，主要提供实时关联、比对、碰撞功能，可自助根据数据筛选条件，即时分析和查询海量的数据。实时计算服务采用分布式交换查询分析数据仓库技术，支持标准SQL对数据的并行插入、删除、改、查询等功能。提供但不限于以下功能：1. 采用高速分布式并行计算引擎；提供高性能的结构化数据的即时及复杂查询功能；2. 支持数据实时采集，保证可以完整的收集到所有数据，为实时应用提供实时数据；支持对实时数据进行数据检索查询和其它处理；支持通过横向扩展增加实时计算能力；3. 支持百亿级数据OLAP多维分析实时计算，满足百亿级以上数据的实时查询、比对、关联碰撞需求；4. 支持SQL标准语法；支持多种计算方式和性能优化策略，支持通过SQL进行交互式数据处理，兼容SQL-92, SQL-99, SQL-2003, OLAP扩展，支持SQL并行优化器；5. 支持多用户模式，用户间资源隔离，为每个用户分配申请的计算资源和存储资源。</p>

★	44	<p>提供离线计算能力，主要用于公安海量数据的批量计算、指标汇总计算、数据挖掘等场景提供基础计算服务，如人员轨迹分析、串并案分析等，保障TB/PB级的海量数据处理能够稳定、高可靠的运行。离线计算框架服务设计：分布式计算框架采用类似MapReduce框架，将大事务分散到不同设备处理。分布式数据库设计：建立在离线计算服务上的数据仓库框架，提供大数据平台批处理计算能力，能够对结构化/半结构化数据进行批量分析汇总完成数据计算。提供类似SQL的Hive Query Language语言操作结构化数据。提供但不限于以下功能： 1. 自动化云中交付兼容主流Hadoop MapReduce/Spark框架的分布式离线计算组件。支持分布式横向扩展和弹性计算：能够支持数据存储的分布式扩展及计算任务的分布式运行。支持根据需求弹性增加和移除工作节点，应对业务高峰。 2. 支持自动将一个作业待处理的大数据划分为多个数据块，每个数据块由一个计算任务执行，并自动调度计算节点来处理相应的数据块。 3. 支持可视化集群配置和多类型作业管理。支持分布式横向扩展和弹性计算：能够支持数据存储的分布式扩展及计算任务的分布式运行。支持根据需求弹性增加和移除工作节点，以从容应对业务高峰。支持多种资源调度策略：对服务实例中各个作业任务，根据其优先级、资源使用限制自动进行调度，设置多种资源调度算法，满足不同场景的多任务资源调度。兼容多种数据接口，方便数据间的相互交换与访问。支持通过编写SQL或者类SQL处理数据，降低数据开发的复杂性。 4. 支持任务编排，提供工作流程管理功能，用户可以对计算任务进行编排，安排任务执行计划、执行顺序等，从整体上提升数据自动化计算处理能力。 5. 提供包括用户认证、用户权限（数据访问权限、服务组件使用权限）和数据加密等在内的一系列安全机制。集群在响应用户请求时，对用户身份进行认证；同时校验用户是否有权限访问数据以及是否有权限使用该服务组件。可以对服务中的数据进行加密，确保数据安全。 6. 支持以数据表格和图表方式展示物理资源的使用情况，如存储使用率、内存使用率、CPU使用率等，以及组件节点的运行状态、连接数等。并支持针对相关指标的阈值告警功能。</p>
★	45	<p>提供图计算能力，图数据库也叫图形数据库，是NoSQL数据库的一种类型，它应用图形理论存储实体之间的关系信息，基于HBase的分布式存储机制，能够支持百亿节点，千亿关系的海量数据，提供基于Spark的数据导入和基于Elasticsearch的索引机制，应用在关系分析和反电诈等领域。 1. 图引擎：包括图存储引擎和图处理引擎，其中图存储支持按节点、边表达关系数据；图处理引擎负责将数据并行转换为图结构数据及并行执行图运算； 2. 图操作支持：支持对图结构进行查询、增、删、改等操作，并支持事务； 3. API 支持：支持通过CLI、JAVA、REST API 等多种方式操作图数据库，方便对接各应用。提供但不限于以下功能： (1)全分布式，Hadoop生态无缝集成，百亿点千亿边，秒级查询。 (2)提供易用的Rest接口，方便数据的查询分析。提供对图计算和图挖掘简洁易用的而丰富的接口。 (3)提供图数据接入、属性转换、子图构造等图基础操作。 (4)提供以顶点为中心的图计算编程框架。 (5)支持最短路径、网页排名、三角计数、K-核中心性算法等多种图算法。 (6)支持离线批量导入和实时流导入，对导入性能进行深度优化。</p>

★	46	<p>提供内存计算能力。内存计算在计算过程中数据无需落地存储，能够极大降低计算过程的IO开销，提升计算效率。内存计算服务需提供快速的计算、写入、交互式查询的框架，避免一个离线计算工作流中的多个任务对同一个数据集进行计算时的IO瓶颈。同时，内存计算服务还需支持交互式的数据挖掘，由于基于内存的计算架构，可以很方便处理迭代计算。另外，内存计算服务可以与离线计算服务、流式计算服务等共用基础的资源调度框架以实现计算资源复用。提供但不限于以下功能：1. 支持并行/分布式计算，具备网络拓扑、RPC通信、系统同步、持久化、日志等功能特性，加速数据访问，将数据读取速度从毫秒级提升到纳秒级。2. 支持内存数据管理，包括字典编码、数据压缩、内存中数据格式、数据操作、内存索引、内存中并发控制和事务。3. 支持对实时数据流进行高通量、容错处理，可以对多种数据源（如Kdfka、Flume、Twitter、Zero和TCP 套接字）进行类似Map、Reduce和Join等复杂操作，并将结果保存到外部文件系统、数据库或应用到实时仪表盘。4. 提供多种语言开发接口（Java/Scala/Pyhton），简单快速的编写并行的应用处理大数据量。5. 支持内存本地化，能把大数据量和计算量分散到不同的处理器中，不同的服务器之间可以共享一组数据，单一服务器的宕机不影响任何计算。</p>
★	47	<p>云服务商需提供但不限于如下PaaS层存储服务，须严格参照公安部功能及接口规范要求，符合《GA/DSJ 122-2019 公安云计算平台 PaaS层 存储服务技术要求》。需要充分考虑各类应用对组件的需求，要求基于开放社区Apache Hadoop，不使用任何私有架构和组件，各类组件要求符合《公安云计算平台框架指南》和公安云计算异构兼容接口标准。包括但不限于以下服务：分布式文件系统、分布式列数据库、分布式关系型数据库、关系数据库、图数据库、内存数据库、全文检索数据库等。</p>
★	48	<p>提供分布式文件系统。文件系统管理的物理存储资源不一定直接连接在本地节点上，而是通过计算机网络与节点相连。客户端并非直接访问底层的数据存储区块，而是通过网络，以特定的通信协议和服务器沟通，并借由通信协议的设计，在客户端或服务端根据访问控制授权访问文件系统。提供但不限于以下功能：1.全分布式架构：客户端访问时，控制节点只负责元数据查询，数据节点负责具体数据存取。无单点瓶颈，性能线性扩展。2.高可靠性：数据采用多副本或者纠删码存储，保证数据可靠性控制节点无单点故障，控制节点采用异地多活技术，保证控制节点的可靠性和访问性能。3.支持异地容灾：支持数据异地同步复制和异步复制。4.支持分布式高可用横向扩展：可在不同数据节点设置多副本策略，实现数据的高可靠性存储；对管理节点进行HA设置，实现分布式文件系统管理节的高可用性5.支持快照，支持在一个特定时间存储一个数据拷贝，可以将失效的集群回滚到之前一个正常的时间点上。同时支持元数据快照。6.支持存储管理百MB、数百TB、甚至PB级大小的文件数据。7.提供数据权限管理，对不同应用的用户可限制其只能访问自身的文件。支持用户的配额限制。8.提供文件操作审计日志功能，记录文件操作的时间、客户端的IP、应用名称等相关内容，供后期审计使用。9.提供 RestfulAPI 服务，实现文件上传、下载、删除、目录创建、列出文件列表等服务，满足应用开发对文件系统的服务需求。10.可视化的集群监控、管理、配置维护功能。11.支持分级存储：分布式存储支持数据分级存储，根据数据的不同访问热度的数据存储于不同性能的存储介质（如：SSD/SAS/SATA），以达到最高性价比。</p>

★	49	<p>提供分布式列式数据库，用于存储结构化数据与半结构化数据，提供海量的存储能力和实时的查询、分析能力，并具有高并发、低延迟和灵活的水平拓展的特性，能提供高吞吐量的数据访问，适合大规模数据集方面的应用。提供但不限于以下功能：1.支持基于键值方式数据访问，提供通过 RESTful API形式的访问。2.提供定制化开发分布式文件、列族数据库、文档数据库、健康检查的内核组件。3.支持以数据表的形式组织数据，提供处理结构化、半结构化数据的存储和访问服务。4.提供对大规模数据和高并发访问要求的服务，读写并发随节点数量水平扩展。5.采用分布式文件数据存储，支持分布式冗余存储保证数据可靠性。6.支持资源使用情况的可视化展示，如存储使用率、内存使用率、CPU使用率，组件节点的运行状态等，支持针对相关指标的阈值告警功能。7.提供服务的自动化创建功能，并可对服务实例进行启停、配置修改、规格调整和删除等管理操作。8.提供数据的多副本机制，保证数据安全性和可靠性</p>
★	50	<p>提供分布式关系型数据库。支持单机关系型数据库的传统关系模型存储模型，SQL查询语言接口，提供完备的分布式事务保障机制。分布式关系数据库支持多节点和高可用的部署架构，适用于关系型事务处理和分析结果的汇总展示等场景中使用。提供但不限于以下功能：1.支持将数据库实例绑定到应用程序，并创建唯一的访问凭证。2.提供无单点故障的高可用集群模式，支持统一的数据库访问层，应用通过访问层访问数据库集群，访问层能够实现故障迁移；如果某个集群节点宕机，访问层能够自动连接到新的节点。3.支持数据库集群的负载均衡、读写分离和分库分表的功能。4.提供关系数据库服务的自动化创建功能，并可对每个服务实例进行启停、可视化配置修改、规格调整和删除等管理操作。5.支持数据库服务规格的定义，创建不同规格的数据库集群。6.提供在线数据库服务的账号、权限管理功能。7.提供多种备份策略，如自动备份、手动备份、逻辑备份和物理备份等。8.提供可视化的数据恢复功能。9.提供对数据库服务节点的内存、CPU、网络和数据引擎的性能指标监控。</p>

★	51	<p>提供关系型数据库。支持强事务处理能力，可提供低时延、高可用和高可靠性的结构化数据存取服务，适用于单表记录在十亿条以内或者数据量小于<b>1TB</b>，有频繁的数据插入和修改操作，以及对一致性和原子性要求较高的应用场景。提供但不限于以下功能：</p> <ol style="list-style-type: none"> <li>1. 提供资源隔离的服务实例管理，每个实例独占CPU、内存和磁盘I/O。</li> <li>2. 支持数据库集群的负载均衡、读写分离和分库分表的功能。</li> <li>3. 提供关系型数据库服务的自动化创建功能，并可对每个服务实例进行启停、可视化配置修改、规格调整和删除等管理操作。</li> <li>4. 支持数据库服务规格的定义，创建不同规格的数据库集群。</li> <li>5. 提供多种备份策略，如自动备份、手动备份、逻辑备份和物理备份等。</li> <li>6. 提供可视化的数据恢复功能。</li> <li>7. 支持按照不同规格申请数据库服务，规格属性包括节点数、CPU、内存、存储空间。</li> <li>8. 提供在线全生命周期管理，包括服务申请、审核、自动部署、实例的启停、升级、销毁及监控等。</li> <li>9. 提供在线的对数据库服务节点的监控及告警功能，监控项包括：存储使用率、内存使用率、CPU使用率、数据库实例平均每秒钟的输入流量、数据库实例平均每秒钟的输出流量、平均每秒SQL语句的执行次数、平均每秒事务数、当前活跃连接数、当前总连接数、数据库实例每秒IO请求次数等。</li> <li>10. 提供数据库实例的性能优化功能，包括慢SQL统计、大表检查、空表检查等。</li> <li>11. 提供SQL执行终端界面，支持SQL脚本的在线执行。</li> <li>12. 提供数据库实例配置参数的在线维护，包括最大连接数、读入缓冲区大小、查询缓冲区大小、慢查询时间大小等。</li> </ol>
★	52	<p>提供多维分析数据库。分布式并行数据库服务用来处理PB级海量结构化数据存储和分析，主要用于OLAP（联机分析处理）等数据仓库分析场景。由众多拥有独立且互不共享CPU、内存、存储等系统资源的逻辑节点组成，将业务数据分散存储在多个物理节点上，数据分析任务被推送到数据所在位置就近执行，并行完成大规模数据的快速分析。提供开放标准SQL接口供业务使用，数据查询分析时集群节点并发执行；提供查询优化能力，结合数据分布情况选择最优的查询和处理方案。支持集群水平线性扩展，确保数据在节点间均匀分布。支持redhat和SUSE等主流linux平台，具备share d-nothing/MPP架构，具备高性能，高扩展性，高可用等特性，支持PB级的数据存储和分析能力。并行数据库数据跨所有节点均匀分布，所有节点以并行方式工作，提供标准SQL接口，支持SQL92,99,2003标准，支持JDBC/ODBC标准接口。须具备但不限于如下功能：</p> <ol style="list-style-type: none"> <li>1、支持分布式存储：将数据可均分分布在各物理节点，能够实现I/O并行和CPU并行。</li> <li>2、支持分布式计算：采用流水线方式，实现了高度并行的计算能力。在集群范围内，可生成分布式执行计划，合理利用集群资源，将计算下发到各个数据节点执行，并行利用节点的计算能力。支持行列混存。</li> <li>3、具备高可用能力：从硬件到软件，设计无单点故障，高可用，双副本，HA，自动故障检测技术，实现双层保护。</li> <li>4、支持数据分区管理：在一个节点内部对数据按照用户指定的策略对数据做进一步的水平分表，将表按照指定范围划分为多个数据互不重叠的部分。</li> <li>5、支持全文检索：提供了全文检索能力，全文检索提供了查询可读性文档的能力，并且通过查询相关度将结果进行排序。</li> </ol>

★	53	<p>提供分布式内存数据库。提供数据的快速读写能力，用于缓解对后端关系型数据库的访问压力，增强业务的并发处理性能，同时，也可以利用其数据持久化的功能，在保障高性能的同时进行数据存储，保证用户的数据安全。常见应用场景如：后端热点数据缓存、Session共享等。在业务中可用来保存黑名单库，利用内容数据库快速读写的特性与其他工具配合用于实时布控、实时比对、数据快速查询等业务场景以提升作战响应能力。提供但不限于以下功能：1. 高速：提供毫秒级的数据访问速率。2. 可操作性:提供API、web命令行控制台、配置可视化界面等方便上层数据应用操作内存和内存管理。3. 分布式支持:除单机内存数据库外，能够支持分布式部署。4. 持久化：支持定期异步数据持久化策略，提供操作日志及 Replication功能。</p>
★	54	<p>提供图数据库。主要用于支撑分析挖掘、展示处理要素之间的多重关系，如人与人的关系、人与车关系、人与组织关系、人与物品的关系，车与车关系等。关系类数据的价值挖掘对于提升情报探索、线索追查、研判分析等业务场景的分析效率具有重要的意义。提供但不限于以下功能：1. 图引擎：包括图存储引擎和图处理引擎，其中图存储支持按节点、边来表示关系数据；图处理引擎负责将数据并行转换为图结构数据及并行执行图运算。2. 图操作支持：支持对图结构进行增、删、改等操作，并支持事务；支持对大图中的点、边、属性的精确检索、模糊检索、范围检索等各种查询。3. API支持：支持通过JAVA、C++、REST API等多种方式操作图数据库，方便对接各应用。4. 可视化配置、部署、运维、监控支持。</p>
★	55	<p>提供全文数据库服务，主要应用于人员、车辆、企事业单位等电子档案的全文检索以及结构化数据的关联查询分析等场景，面向一线民警的高并发结构化数据关联检索类场景。全文数据库是指从海量非结构化数据提取出可以识别、处理的索引信息，再对索引信息进行检索，从而达到对海量非结构化数据进行快速检索的目的。全文索引服务实现可弹性扩展的自动化部署，通过API来进行数据索引管理，配合其他关系或非关系数据库，起到高效的索引和全文索引功能支撑。提供但不限于以下功能：1. 支持服务实例中创建多个搜索应用，支持定义应用的配置参数、数据模型、索引结构、搜索特性等。2. 引分片策略，保障集群高可用。3. 提供对搜索特性的可视化配置。4. 提供内置分词算法。5. 提供搜索服务的用户管理和数据权限控制。6. 提供服务的自动化创建功能，并可对每个服务实例进行启停、配置修改、规格调整和删除等管理操作。7. 提供对自定义分词包的上传、删除等功能。8. 提供日志记录功能，方便追查访问来源以及进行多维度的统计分析。9. 提供数据的多副本机制，保证数据安全性和可靠性。10. 实时、高效：能够实时更新索引数据，并且能够实现PB级数据的快速检索。</p>

★	56	<p>按需提供如下PaaS层服务实例相关服务，包括但不限于创建服务实例、删除服务实例、修改服务实例、获取服务实例列表、查询服务实例详情，服务须严格参照公安部功能及接口规范要求，符合《GA/DSJ 123-2019 公安云计算平台 PaaS层 服务实例技术要求》。服务实例是公安云计算平台各服务进行实例化后对外提供服务的统称，例如分布式文件系统、分布式列式存储、离线计算、流式计算等多种不同类型的服务。</p> <p>需满足但不限于如下功能：</p> <ul style="list-style-type: none"> <li>• 支持创建服务实例，支持公安云计算平台各组件实例的部署。</li> <li>• 支持服务实例的删除，删除服务实例时，自动回收服务实例占用的各项资源。</li> <li>• 支持服务实例的修改功能，包括集群规模的增加、缩减。其中，缩减可由手动支持。</li> <li>• 支持获取所有已部署的服务实例列表。</li> <li>• 支持获取已部署服务实例的详细信息，包括服务实例的资源配额、健康状态、告警信息等信息。</li> </ul>
★	57	<p>按需提供如下PaaS层服务资源相关服务，包括但不限于提供服务资源的注册、发布、撤销、查询、修改、注销等功能，服务须严格参照公安部功能及接口规范要求，符合《GA/DSJ 124-2019 公安云计算平台 PaaS层 服务资源技术要求》。需提供但不限于如下功能：</p> <ul style="list-style-type: none"> <li>• 支持三种服务资源状态：已注册、已发布、已注销。云计算平台服务资源提交注册申请，将其服务资源进行注册，以方便进行资源统一管理。服务发布时，通过控制指令通知对应服务资源启用该资源服务；服务撤销时，通过控制指令通知对应服务资源停用该资源服务；发布和撤销可以反复操作；当服务资源不再对外提供服务时，可以通过注销操作关闭该服务。</li> <li>• 支持服务资源注册。</li> <li>• 支持服务资源发布。</li> <li>• 支持服务资源撤销。</li> <li>• 支持服务资源查询。</li> <li>• 支持服务资源修改。</li> <li>• 支持服务资源注销。</li> </ul>
★	58	<p>提供完整的安全服务能力，服务功能需满足《GA/DSJ 300-2019 公安大数据安全 总体技术框架》，同时满足资源租户构建等保三级要求，结合云计算的安全需求，提供的安全能力包括但不限于：安全态势感知服务，安全指数服务，主机安全服务，边界防火墙服务，数据库审计服务，Web应用防火墙服务，网页防篡改服务，云堡垒机服务，漏洞扫描服务，密钥管理服务，数据加密服务，云防火墙，综合日志审计服务，漏洞及补丁修复服务等，按公安部要求，可以将安全管理服务与监控数据上传，具备相应接口，对接省厅大数据智能化建设中的“云检”、“云制”、“云哨”平台，满足所需数据对接、管理、安全能力对接等要求，按用户需求提供二次开发服务，配合进行相应的开发对接。按用户需求提供安全响应及安全问题处理服务，包括但不限于以下：</p>
★	59	<p>云主机加固服务：云主机（虚拟机）防暴力破解、webshell检测、安全基线、虚拟化加固等功能；提供强制访问控制、完整性检测、防格式化、双因子认证和组合式密码认证、自我保护、统一管理、灵活多样的策略模板，支持windows/Linux/Unix系统，负责主机加固与安全处理。</p>
★	60	<p>云堡垒机服务：统一账户管理、角色授权、实时监控、运维安全管理。提供身份认证和权限管理功能，可以管理用户（比如警种、系统或应用程序）账号，并且可以控制这些用户对其名下资源的操作权限。</p>
★	61	<p>病毒查杀服务：对主机操作系统、文件提供病毒防护与查杀服务，实现对网络病毒、文件病毒、操作系统病毒的统一防护。</p>

★	62	漏洞扫描服务：集Web漏洞扫描、操作系统漏洞扫描、数据库漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测五大核心功能，自动发现网站或服务器在网络中的安全风险，为云上业务提供多维度的安全检测服务，形成最终扫描结果清单，负责相关漏洞修复，补丁安装等。
★	63	安全问题响应服务：根据漏洞扫描结果及用户需求，进行相关漏洞修复、补丁修复等漏洞修复工作。针对出现的安全问题提供应急处理服务，对发现的安全问题进行定位，对造成问题的漏洞给出解决建议及进行处理。
★	64	态势感知服务：基于环境，动态洞悉安全风险，以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置，并提出相应报告，支持决策与行动。
★	65	专业渗透测试服务：由专业渗透工程师对系统进行应用和主机两个层面安全渗透测试，发现系统中存在的各类安全问题，完成测评之后，出具安全渗透报告，负责完成安全问题修复。
★	66	数据库审计、防火墙、入侵检测、入侵防御等满足用于用户安全防护需求的部署与服务。
★	67	云服务商应具备实现省市两级大数据中心的备份容灾的解决方案和实施能力，按需求完成省市两级中心对接，满足公安厅大数据中心容灾备份需求，能够将数据完整同步或异步给地市大数据中心，形成省、市多中心体系，地市大数据中心能够通过一份完整数据实现大数据应用创新服务本地域同时可服务全省。在省厅服务不可用时，地市大数据中心能够替代省厅核心应用对外支撑服务。云服务商需至少具备如下容灾服务能力，包括云硬盘高可用服务、云服务器高可用服务、云服务器容灾服务、云服务器高可用服务+云服务器容灾服务等。
★	68	云硬盘高可用服务，为虚拟机和裸金属中的云硬盘提供本地存储双活保护。当单套存储设备发生故障时，数据零丢失，业务不中断，通过云数据中心结合存储双活实现单可用区内的云硬盘容灾。
★	69	云服务器高可用服务为虚拟机提供同城数据中心间的高可用保护。当生产中心发生灾难时，被保护的云服务器能够自动或手动切换到灾备中心。服务可应对的场景包括： <ul style="list-style-type: none"> <li>• 适用于在距离&lt;100公里，网络时延&lt;2ms的两个数据中心，构建云主机高可用容灾的场景，用于整站点故障时虚拟机的故障切换。</li> <li>• 适用于应用和数据库等无法拆分的老旧应用，全部用云服务器部署，业务系统自身无容灾能力，需要云平台提供云服务器的容灾保护。</li> <li>• 可应对大规模设备故障和数据中心故障、计划内停机，例如：计划性停电、日常运维等。</li> </ul>
★	70	云服务器容灾服务，为云服务器提供跨区域异地容灾保护，当生产中心故障，可在异地容灾中心快速恢复云服务器。生产中心的云服务器还可叠加配置本地存储双活保护，形成本地存储双活+异地远程复制存储环形容灾，当生产中心单套存储设备发生故障时，数据零丢失，业务不中断。仅在生产中心发生整站点灾难时，才需要切换到异地容灾中心。

★	71	云服务器容灾服务，支持两地三中心容灾，为云服务器提供同城两个数据中心间的高可用保护及和异地容灾保护，并形成同城存储双活+异地远程复制的存储环形容灾。当生产中心发生灾难时，可自动或手动切换到同城容灾中心，恢复被保护的云服务器（数据零丢失）；在同城两个数据中心都发生灾难时，可在异地容灾中心手动恢复受保护的虚拟机。
★	72	云服务器备份服务可为虚拟机和裸金属服务器创建备份，利用备份数据恢复虚拟机和裸金属服务器业务数据，最大限度保障用户数据的安全性和正确性，确保业务安全。云硬盘备份服务可为云硬盘创建备份，利用备份数据恢复云硬盘，最大限度保障用户数据的安全性和正确性，确保业务安全。应急处理服务，对发现的安全问题进行定位，对造成问题的漏洞给出解决建议及处理。
★	73	按公安部要求，可以将云平台运维管理数据上传，具备相应接口，对接省厅大数据智能化建设中的“云检”、“云制”、“云哨”平台，满足所需数据对接、管理、安全能力对接等要求，负责进行二次开发，配合进行相应的开发对接工作。为用户提供的运营、运维功能及云管门户要求根据用户实际业务进行功能、流程和界面的个性化定制开发，例如各部门、地市租户申请、审核、分配、回收等相应云资源需要根据需求进行流程定制；具备云资源计费功能，计费规则可定制；各类统计需求可定制。
★	74	多样化运维服务接口：提供满足用户要求的多样化运维服务接口，包括但不限于：计算服务接口、存储服务接口、网络服务接口、灾备服务接口、安全服务接口、异构资源池对接服务接口、公共组件接口等。
★	75	云资源运维管理需提供包含资源管理、集中监控、可视化、运维分析、安装部署等功能模块在内的功能，以支撑日常运维、系统变更、运营分析等运维业务场景，实现多个数据中心与混合云的集中运维管理。
★	76	自动化运维：云服务商需为管理员提供作业管理，自定义配置操作参数和执行脚本、管理执行目标以及存储参数文件的平台。构建丰富的运维操作库，如内置批量修改操作系统缺省用户密码、批量为操作系统打补丁的日常操作，标准化各种运维场景。并通过编排管理向管理员提供将运维操作库的单个操作，通过图形化的方式编排组合的能力，更大程度上满足各业务场景的自动化运维操作。自动化运维需为用户管理员提供但不限于如下功能： <ul style="list-style-type: none"> <li>• 作业：支持作业管理：支持定义作业，可选择多个设备对象和需要执行的操作名称；支持定义立即、定时单次和周期执行计划。支持作业历史，提供作业执行历史详情查询，可查看作业执行情况。</li> <li>• 操作库：支持脚本管理：支持编辑操作集，用户可以定义执行脚本，支持python、Shell、VBS、Bat、PowerShell等多种格式。支持编排管理：当需要执行一套流程化的操作时，编排管理支持将操作库的单个操作或编排，通过图形化的方式继续编排组合，形成满足各种业务场景的运维流程。支持的预置场景：内置批量修改linux操作系统密码（python/shell）和批量打linux操作系统补丁(shell)原子操作。</li> <li>• 配置：支持文件管理：当需要配置操作及编排的文件参数或调取软件包时，文件管理可作为上传及存储参数、补丁包等文件的管理平台，以便在配置执行操作或编排时选择文件类型的参数。支持资源管理：支持EC S、BMS、物理主机、管理虚拟机远程安装Agent。支持安全策略：可以通过控制策略设定控制时间，暂时禁止执行所有操作和编排，也支持控制时间段内的例外添加。</li> </ul>

★	77	<p>提供多种设备和资源的统一监控能力，包括监控概览，云服务监控，物理设备和云资源监控。服务监控对云管理平台系统服务以及云服务系统运行时的节点性能指标和进程性能指标进行实时监控，记录服务运行时节点和进程关键性能指标的变化趋势，提示服务运行时的告警信息，通过对服务，节点，实例等不同维度的监控呈现所监控服务节点和进程的详细监控数据，帮助用户管理员及时预防潜在的服务运行风险。</p>
★	78	<p>物理设备和资源池监控：用户管理员可以查看所有录入的物理资源的分类及数量，且为进入计算资源、网络资源、存储资源和机房提供一个方便的入口。用户管理员可以通过物理资源列表，查看资源的数据来源，运行状态等；也可单击资源列表中的名称链接，查看资源的概率、资源详情、拓扑视图，当前告警和性能指标。资源池管理及监控可实时监控计算、存储、网络资源池，支持查看IaaS资源池、异构虚拟化资源池等的资源、容量、负载信息，方便运维人员及时全面的了解资源池的运行情况。同时，提供容量预测和资源分析能力。可提前预测资源容量趋势，发现闲置资源，识别瓶颈资源，以指导运维人员进行容量规划、资源回收、扩容等，最终达到提供资源利用率的目的。</p>
★	79	<p>云资源和业务系统监控：云资源和业务系统信息来自云平台运营管理系统。用户管理员可对云资源和业务系统进行监控。云资源管理通过计算、存储、网络、数据库、安全方面，实时查看数据中心云资源使用情况，提供资源详情、告警、拓扑等信息，帮助运维人员快速、全面了解云上资源的当前情况，进而分析出业务的运行状况和健康度，并及时响应异常报警，保证应用程序顺畅运行。基于业务系统统一监控，用户管理员一方面可以监控和统计各级业务系统下的资源、资源配额和使用情况，帮助运维人员及时发现异常、评估风险。另一方面，提供基于业务系统的资源闲置分析和资源瓶颈分析能力，支撑运维人员查看各级业务系统的资源使用率，及时识别瓶颈风险，提升资源使用率。容量分析：用户管理员可以直接选择当前位置，查询客户关注的基础资源容量，包括当前和历史资源数据。另一方面，可以直接通过云服务容量界面查询弹性云服务器的已发放个数。</p>
★	80	<p>应用分析：在云上统一部署IT支撑系统和业务系统之后，需要运维管理系统能够从业务的视角来监控相关资源的健康情况，并能够支持量化评估、辅助定界定位，缩短平均修复时间（MTTR），提高业务连续性。云管理平台提供以应用为中心的应用分析能力，通过健康度、繁忙度得分评估应用资源的运行情况；通过资源闲置分析，提升资源使用率；通过资源瓶颈分析，识别资源瓶颈风险。同时，支持对应用的总览、拓扑视图、性能分析、告警统计和负载分析等全方位查看和展示。用户管理员可查看应用数量统计、应用健康度/繁忙度状态统计和应用列表。用户配置的应用部署云主机实例，系统将自动关联出服务器，交换机，路由器等设备，构建出完整的应用拓扑。拓扑视图分虚拟化层、服务器层、网络层清晰的展示应用及其相关资源的健康度、繁忙度、告警和性能数据，方便故障定界。</p>

★	81	<p>运维可视化：运维管理系统通过集中监控的实时大屏，可直观展现云数据中心的整体概况、业务数据等信息，可以全方位地了解云数据中心的运行状况。运维管理系统在实时大屏中预置“数据中心总览”、“资源池概览”、“多级云资源总览”、“业务系统资源详情”、“云驾驶舱”等多个业务视角大屏，用于展示数据中心信息，并投射到大屏上进行显示，以获得最佳的监控效果，可视化运维内容可按用户需求定制。当数据中心评估默认提供的可视化部件无法直观清晰地展示用户管理员需要的数据信息时，用户管理员可以创建可视化部件，分析数据特征，选择合适的图表并配置数据及样式信息。用户管理员可以创建Dashboard，分析监控数据的特征，将可视化部件进行全新组合，满足监控和演示的需求。</p>
★	82	<p>报表数据分析：运维管理系统支持对告警、性能、资源以及租户的报表数据进行业务分析。用户管理员可以执行自定义报表、查看报表、管理周期报表任务、设置报表或任务访问权限等任务。当用户管理员需要单次或周期性查看某张报表数据时，可以创建报表周期任务，关联需要的报表。当任务执行成功后，用户管理员可定时查看生成的报表或定时接收邮件。</p>

★	83	<p>配置管理主要提供但不限于以下主要功能：<b>资源仓库</b>：对物理设备、虚拟资源、云服务资源和自定义资源进行统一管理，支持资源合并、资源打标签和建立资源间关系。<b>物理设备资源管理</b>实现对物理设备资源的统一管理，通过自动同步和手动录入物理设备，添加物理位置，实现资源的增加、删除、修改、查看、合并和关联标签。物理设备资源包括机柜、X86服务器、服务器机柜、路由器、防火墙、交换机、负载均衡、存储设备、存储节点和FC交换机。<b>虚拟资源管理</b>实现对虚拟化资源的统一管理，用户管理员可查看虚拟资源的资源信息、资源关系和变更记录。虚拟资源包含区域、资源池、可用分区、主机组、虚拟机、宿主机、磁盘、规格和镜像。<b>云服务资源管理</b>实现对云服务资源的统一管理，用户管理员可实现对云服务资源的增加、删除、修改、查看和关联标签。云服务资源包括云服务、服务、部署组件、部署实例、部署节点、云服务软件包、服务软件包和组件软件包。如果预置的资源类型不能满足用户需要，可自定义资源类型，自定义资源支持自定义资源关联标签，以及资源实例的增加、删除、修改和查看。<b>资源变更</b>：提供资源变更查询功能，帮助用户查看资源的历史变化记录。当资源发生了新增、删除、更新等变更时，可在变更记录中查看资源变更的详情，及时了解资源发生变更的时间、操作人等。<b>模型管理</b>：提供数据中心资源模型管理，提供常用资源模型，并支持模型自定义。<b>资源类型分组管理</b>。<b>CMDB</b>对资源类型进行分组，按照分组层次展示资源类型，可方便查看和管理资源类型。<b>资源类型管理</b>。支持资源类型的增加、删除、修改、查看操作，帮助用户管理员管理资源类型。对资源类型可以进行属性和资源关系管理，支持对资源属性的增加、修改、删除、查看操作，通过拖拽、可视化编辑等方式提供快捷的属性扩展功能，帮助用户管理员管理资源属性；<b>支持对资源位置管理</b>：提供数据中心物理位置信息管理，物理位置模型最多可规划<b>6级</b>，包括国家-&gt;地区-&gt;省份-&gt;城市-&gt;数据中心-&gt;机房。<b>标签管理</b>：给资源按数据中心、部门、项目和业务系统打标签，支持自定义标签。查看预置标签类型下已创建的标签，可以根据需要增加、删除或修改标签，也可以查看当前标签已关联的资源；当预置标签类型无法满足用户管理员的需求时，用户管理员可以根据需要自定义所需的标签类型，并在自定义标签类型下增加、删除或修改标签。同时支持同步运营面标签数据，查看运营面各标签与资源的关联关系。</p>
★	84	<p><b>云用户管理</b>：组织机构管理。用户中心建立统一的组织机构，定期下发或者机构发生变化下发到各个子系统；<b>用户管理</b>。创建用户基本信息（用户名、密码、真实姓名、手机号码、人员类型、组织机构），人员类型包括政府人员、运维人员、上云软件提供商。</p>

★	85	<p>支持多云云管理能力：云服务商所提供云管平台需支持多资源池统一管理，能够同时对OpenStack、华为HCS、华三cloudos、阿里飞天云、腾讯tstack等云平台构建的资源池进行统一资源调配、统一监控、统一运维。云管理平台可以同时接入多个地市数据中心的多个不同网络形态的资源池，功能包括：</p> <ul style="list-style-type: none"> <li>• 多资源池统一管理：云管理平台可以同时接入多个分布在不同区域的资源池；一个业务系统可以使用多个资源池下资源。</li> <li>• 资源分区管理：每个资源池下包括一个或多个可用分区，可用分区与可用分区之间在设计上是相互独立的，也就是说它们会有独立的供电、独立的物理网络设备等，这样假如一个可用分区出现问题时也不会影响另外的可用分区。</li> <li>• 基于SLA的资源调度：一个可用分区可以包含多种SLA等级的集群、存储池，租户申请云主机、云磁盘时可以选择SLA等级，例如可用分区下可以包含不同存储介质（SATA、SAS、SSD）的存储池，租户可以申请指定存储介质级别的磁盘。</li> </ul>
★	86	<p>统一运营服务能力：提供方便快捷的可定制运营平台，以供用户使用。云服务的运营需考虑以下几个方面的要求：用户角色体系建设完善、组织结构规划设计合理、云服务上线管理、能够快速接入云服务和集成云服务控制台、提供统一的运营Portal、预置的丰富业务。考虑运营安全和数据安全，避免数据丢失或泄露风险，云服务商具有计算机信息系统安全专用产品销售许可证（增强级）GA部销售许可证，信息安全技术云操作系统安全检验要求（增强级），信息安全技术通用渗透测试检测条件，通过可信云开源解决方案评估。云服务提供商需提供基于云服务的运营管理能力供用户使用，主要功能包括：租户管理、多级业务系统、服务目录管理、订单管理、计量计价、多云管理、操作日志等。管理类云服务需提供专用云服务，包括：自定义线下服务、应用管理等。运营系统管理需提供对运营系统本身的管理，包括：云服务人员门户、云服务上线管理、云管理人员管理、系统日志等。</p>
★	87	<p>角色和权限划分要求 系统中按照专有云业务特点，将用户划分为云管理人员、云使用人员、云服务人员等不同角色，根据角色分工来定义权限和分配流程。各角色的权限定义如下：云用户管理员具有如下权限：云资源申请、变更、释放的审批；云资源以及资源池使用以及运行情况监控。云服务人员具有如下权限：业务系统、组织机构、云网络基本信息配置。云使用人员具有如下权限：申请、变更、释放云资源；自助服务的申请；本业务员申请的资源使用、维护。还可按用户需求定制其他角色和权限 □</p>
★	88	<p>提供单点登录：用户只需要在云运营管理平台上登录一次，就可以访问中所有的应用系统以及VPN、堡垒机等设备：1）统一身份认证。当用户登录运营平台时，会被引导到认证系统中进行登录；根据用户提供的用户名和口令，认证系统进行身份校验；用户再访问平台下的应用的时候，就会将该用户对应的此应用的token带上，作为自己认证的凭据，用户访问门户下的任意应用，都不用再次进行登录。2）登录状态检查。因系统安全需要，允许服务端在需要时对当前登录用户的登录状态进行检查。3）和云上网络安全设备进行用户统一认证。 □</p>

★	89	<p>云运营管理：云管理平台服务中心需提供云服务接入和上线管理，用户可以从服务目录上跳转到云服务控制台申请相应的云资源或直接在云服务控制台申请相应的云资源。对于已经申请到的云资源，用户可以使用、维护、变更、释放。云平台可以同时接入多个Region和云服务接入。Region指提供云服务的地理区域，可以分布在不同地域，不同Region提供的云服务能力可以不同，运营用户管理员可以随时查看所有的Region列表和Region内云服务列表。</p> <p>1、服务申请：用户可在自助服务门户的服务目录中查看到管理员预定义的各类服务，并根据自己的业务需要选择相应的服务跳转到对应的云服务控制台申请云资源。详细的云服务产品参数参见相关云服务的产品手册。</p> <p>2、服务审批：云管理人员可以审批来自云使用人员提交的服务申请。</p> <p>3、服务维护：用户可以通过云服务控制台对已申请到的云资源进行维护操作，例如VNC登录虚拟机、虚拟机上/下电、虚拟机绑定弹性IP、磁盘绑定虚拟机。详细的操作请参见相应的云服务文档。</p> <p>4、服务变更：对于已发放的云资源，用户可以通过云服务控制台对服务参数进行变更。如，用户可以申请将一台已发放的4G内存的虚拟机变更为8G内存，每个服务允许变更的能力参见各云服务的产品手册。</p> <p>5、标签管理：对于已发放的云资源，用户可以通过标签对云资源进行标识，方便后续按不同维度统计。</p> <p>6、服务删除：对于不再使用的资源，用户可以在各个云服务console上释放资源，系统会自动释放用户的资源。</p> <p>7、用户可以自助门户对虚拟机进行日常维护工作，包括并不仅限于密码修改、windows自助挂盘等，并可以根据用户需求进行功能定制开发。</p>
★	90	<p>□ 省市两级云平台协同 地市级大数据中心云平台，作为本次建设的省级云平台的子中心，省级云平台和子中心通过协同机制能够实现管理协同、资源协同、数据协同、统一运维统一管理，云服务商须作出三个方面的明确规划，且应具备可落地性，能够提供相应的服务。</p> <p>管理协同 充分发挥省厅“枢纽”和地市“重心”的两级云平台价值，统筹省市两级架构、统一标准，实现两级云协同。省厅云平台按统一的标准，提供两级云的管理接口、资源调度接口、计算协同接口，地市云节点对接省厅统一管理接口、资源调度接口和计算协同接口，实现省厅云平台对全省资源的统一管理。</p> <p>资源协同 省市通过将省、市云计算平台的权限打通，实现省级云计算平台可以调用地市空闲云计算资源的能力，充分发挥云计算的弹性能力，在重大安保活动、重大案件侦办中的作用。两级云的资源协同功能应该包括省厅云平台与地市云节点可实现跨云的服务申请和发放，跨云业务部署能力等调度能力；省市两级可相互借调申请弹性云主机服务、镜像服务、云硬盘服务和快照等服务。</p> <p>数据协同 为满足省级云平台与地市云平台之间的计算互通需求，避免多中心数据同步和复制工作，实现分布在不同云平台的数据即时访问和交互分析，全面提高远程数据访问的效率，降低数据复制成本和工作量。为了更好的支撑省市两级数据联动和跨域研判分析，在两级云的建设上下一步引入计算协同服务，实现了大数据时代的数据中心计算互通，支撑了智能化的省市协同创新应用。省级云平台和地市云平台的大数据组件采用统一架构和标准，省厅与地市分别建设协同计算服务引擎，通过协同计算引擎实现分布在省市两级不同大数据组件上的数据资源统一视图，实现全省数据和计算资源的统一服务。云运营商需提出相应的解决方案，并负责实现省、市两级云平台对接，提供的云平台具备管理协同、资源协同、数据协同能力。</p>

★	91	根据《公安机关云计算平台框架指南》平台总体框架图的定义，云计算平台各类服务在满足指南功能要求的前提下，应提供相关标准接口，实现云服务的标准调用及异构融合。
★	92	本次提供的所有云服务应按照分层解耦原则来设计和实现，统一的接口标准，实现公安大数据智能化建设由数据驱动资源的基础，应完全遵循公安的云计算平台标准，公安大数据平台在遵循IaaS、PaaS、DaaS和SaaS四层解耦的总体设计的同时，每一层提供的各种服务也需要解耦，各自通过标准接口对外提供服务。满足接口标准：计算平台应满足公安云计算平台相关接口标准要求，要求每一层中各个对外提供的服务接口实现标准化，每一层服务符合统一的接口标准定义，从而实现云平台中不同层次、不同服务的解耦。以实现黑龙江公安对全省云计算的统一管理、资源共享协同，并满足公安大数据平台对于云计算平台资源的标准化调用使用。
★	93	异构兼容接口标准：在遵循IaaS、PaaS、DaaS和SaaS四层解耦的总体设计的同时，每一层提供的各种服务也需要解耦，各自通过标准接口对外提供服务。IaaS、PaaS、DaaS和SaaS层间解耦是通过本层的服务解耦并向其它层提供服务来完成。具体要求包括： • 不同层次解耦，提供上下层的服务支撑和服务调用； • 同层不同服务解耦，实现多服务供应商之间的云服务兼容，灵活移植现有资源实现微服务化改造扩展。平台的IaaS、PaaS、DaaS和SaaS层间解耦是通过本层的服务解耦并向其它层提供服务完成。
★	94	不同层次解耦：I层弹性主机服务以标准服务接口向P层全文数据库提供服务，全文数据库服务以标准接口向D层索引服务提供服务，索引服务以标准接口向S层各应用提供服务，各层服务模块又各自遵循运维管理标准、运营管理标准由统一云管平台进行运维运营管理。参照上述逻辑，要求每一层中各个对外提供的服务接口实现标准化，从而实现云平台中不同层次、不同服务的解耦。
★	95	同层不同服务解耦：根据业务规划，从IaaS、PaaS、DaaS等各层服务内容，同一层服务分别由不同服务组成，对外提供标准服务接口。面向不同的应用服务，分别由不同的IaaS、PaaS或者是DaaS服务支撑。
★	96	云服务商需针对本项目制定运维服务方案，在运维期内提供包括但不限于以下技术支持和服务，有专业化云运营团队，提供在用户方的驻场服务，在运维期内负责平台优化、云主机资源调整、存储资源调整、网络安全策略调整、系统安全加固、漏洞补丁修复、安全应急响应处理、数据备份等运维工作，负责按用户需求进行二次开发服务，负责进行应用上云适配等对接工作，为用户提供业务系统部署上云、迁移上云等服务。
★	97	需提供用户驻场本地服务，现场驻场团队中至少1人负责云平台的日常运维，1人负责平台网络的日常运维，1人负责平台网络安全的日常运维，2人负责应用上云及相关开发服务的日常运维，驻场人员技术实力需满足工作要求，并获得用户认可，如果不能满足工作要求，应调换满足需求的技术人员提供驻场服务。

★	98	除现场驻场运维团队外，还需组建项目技术支持团队，保障云平台稳定运行、云服务及资源可靠，负责配合DaaS、SaaS应用上云、按用户需求进行云平台对外服务接口开发，配合进行第三方软件、平台调用对接云平台各项功能的适配与技术支持，降低交付周期和风险。
★	99	云平台资源交付要求：云服务商应具备足够云资源服务能力满足本次项目，能够在项目中标合同签订后15日内向用户交付用户申请的相关云资源与云服务，配合用户业务及应用部署，网络接入等。云服务商为公安用户提供的云平台资源应预留足够的扩容申请量，满足用户新的资源申请，保证可在资源申请后3日内及时交付；云服务商应根据用户申请量的增长趋势，提前进行专有云平台相关资源扩容，保障能够及时交付公安用户申请资源。
★	100	版本迭代升级要求：提供云计算平台、安全访问等硬件的在线升级维护服务，提供本地及实时远程运维中心技术、故障恢复等支持服务，保证平台架构版本的先进性和持续可演进性，并在版本升级时，配合DaaS、SaaS厂商进行相应的升级版本适配及二次开发对接服务。
★	101	云服务商需按项目需求提供各类云资源与云服务，并纳入省政务云资源目录，用户可在省政务云资源目录中选择申请相应云资源与服务，可供用户选择的云资源、云服务功能、性能及规格需不低于本项目需求。
★	102	云服务、云资源性能及动态灵活调整要求：云服务商提供的计算、存储、网络、安全、运维等云服务、云资源性能，需满足用户业务需求，应及时优化调整提供的服务与资源性能，保障用户业务的性能需求，不能因提供的资源与服务性能问题影响用户业务；云服务商可按照用户业务需求，进行灵活动态的计算、存储、网络、安全、运维等云服务、云资源需求调整。可根据用户业务预估及突发性峰值，快速进行资源调整，保障用户业务高可用性能、高稳定性。在用户业务调整或需求调整时，能够保证快速按需提供相应的云资源与云服务，包括新增云服务等内容，并纳入政务云服务目录补充。
★	103	云服务商除提供云平台运维监测、运维管理、安全监测、安全管理接口外，还提供包括但不限于机房环境动力监控接口、消防监控接口等。能够提供SYSLOG、RestAPI、JDBC、SNMP、Socket、MQ、HTTP等各类通用协议接口，具备向第三方系统发送的配置、告警及性能数据的能力，支持基于最常用的HTTP协议或者基于消息中间件，支持post模式进行对接，配合用户在第三方平台进行相关应用开发建设。
★	104	项目提供的所有设备需要独立的机房运营区域，物理隔离封闭式管理，达到公安部标准要求，具备完备的机房消防、环境动力监控、UPS电源、空调、门禁等达到电信等级IDC机房的环境与安全保障。
说明		对于不允许偏离的实质性要求和条件，在上表中以“★”的方式标明。

## 第五章 供应商资格证明及相关文件要求

供应商应提交证明其有资格参加投标和中标后有能力履行合同的相关文件，并作为其响应文件的一部分，所有文件必须真实可靠、不得伪造，否则将按相关规定予以处罚。

### 1.法人或者其他组织的营业执照等证明文件，自然人的身份证明：

(1) 法人包括企业法人、机关法人、事业单位法人和社会团体法人；其他组织主要包括合伙企业、非企业专业服务机构、个体工商户、农村承包经营户；自然人是指《中华人民共和国民法通则》（以下简称《民法通则》）规定的具有完全民事行为能力、能够承担民事责任和义务的公民。如供应商是企业（包括合伙企业），要提供在工商部门注册的有效“企业法人营业执照”或“营业执照”；如供应商是事业单位，要提供有效的“事业单位法人证书”；供应商是非企业专业服务机构的，如律师事务所，会计师事务所要提供执业许可证等证明文件；如供应商是个体工商户，要提供有效的“个体工商户营业执照”；如供应商是自然人，要提供有效的自然人身份证明。

(2) 这里所指“其他组织”不包括法人的分支机构，由于法人分支机构不能独立承担民事责任，不能以分支机构的身份参加政府采购，只能以法人身份参加。“但由于银行、保险、石油石化、电力、电信等行业具有其特殊性，如果能够提供其法人给予的相应授权证明材料，可以参加政府采购活动”。

### 2.供应商应符合《中华人民共和国政府采购法》第二十二条规定的条件，提供标准格式的《资格承诺函》。

### 3.财务状况报告，依法缴纳税收和社会保障资金的相关材料（详见资格性审查表要求）

### 4.具有履行合同所必须的设备和专业技术能力的声明。

### 5.供应商加政府采购前三年内在经营活动中没有重大违法记录书面声明函。

### 6.信用记录查询

(1) 查询渠道：通过“信用中国”网站([www.creditchina.gov.cn](http://www.creditchina.gov.cn))和“中国政府采购网”([www.ccgp.gov.cn](http://www.ccgp.gov.cn))进行查询；

(2) 查询截止时点：本项目资格审查时查询；

(3) 查询记录：对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单、信用报告进行查询；

7.采购人或采购代理机构应当按照查询渠道、查询时间节点、查询记录内容进行查询，并存档。对信用记录查询结果中显示供应商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供应商作无效投标处理。

### 8.按照磋商文件要求，供应商应当提交的资格、资信证明文件。

## 第六章 评审

### 一、评审要求

#### 1. 评标方法

综合评分法：是指响应文件满足磋商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。（最低报价不是中标的唯一依据。）

#### 2. 评标原则

2.1 评审活动遵循公平、公正、科学和择优的原则，以磋商文件和响应文件为评审的基本依据，并按照磋商文件规定的评审方法和评审标准进行评审。

2.2 具体评审事项由磋商小组负责，并按磋商文件的规定办法进行评审。

#### 3. 磋商小组

3.1 磋商小组由采购人代表和评审专家共3人以上单数组成，其中评审专家人数不得少于磋商小组成员总数的2/3。

3.2 磋商小组成员有下列情形之一的，应当回避：

(1) 参加采购活动前三年内，与供应商存在劳动关系，或者担任过供应商的董事、监事，或者是供应商的控股股东或实际控制人；

(2) 与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

(3) 与供应商有其他可能影响政府采购活动公平、公正进行的关系；

3.3 磋商小组负责具体评标事务，并独立履行下列职责：

(1) 审查、评价响应文件是否符合磋商文件的商务、技术等实质性要求；

(2) 要求供应商对响应文件有关事项作出澄清或者说明，与供应商进行分别磋商；

(3) 对响应文件进行比较和评价；

(4) 确定成交候选人名单，以及根据采购人委托直接确定供应商；

(5) 向采购人、采购代理机构或者有关部门报告评审中发现的违法行为；

(6) 法律法规规定的其他职责。

#### 4. 澄清

磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。供应商的澄清、说明或者更正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。

4.1 磋商小组不接受供应商主动提出的澄清、说明或更正。

4.2 磋商小组对供应商提交的澄清、说明或更正有疑问的，可以要求供应商进一步澄

#### 5. 有下列情形之一的，视为供应商串通投标

5.1 不同供应商的响应文件由同一单位或者个人编制；（不同供应商响应文件上传的项目内部识别码一致）；

5.2 不同供应商委托同一单位或者个人办理投标事宜；

5.3 不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；

5.4 不同供应商的响应文件异常一致或者投标报价呈规律性差异；

5.5 不同供应商的响应文件相互混装；

5.6 不同供应商的投标保证金为从同一单位或个人的账户转出；

说明：在项目评审时被认定为串通投标的供应商不得参加该合同项下的采购活动

## 6.有下列情形之一的，属于恶意串通投标

- 6.1 供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关情况并修改其响应文件或者响应文件；
- 6.2 供应商按照采购人或者采购代理机构的授意撤换、修改响应文件或者响应文件；
- 6.3 供应商之间协商报价、技术方案等响应文件或者响应文件的实质性内容；
- 6.4 属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；
- 6.5 供应商之间事先约定由某一特定供应商成交、成交；
- 6.6 供应商之间商定部分供应商放弃参加政府采购活动或者放弃成交、成交；
- 6.7 供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商成交、成交或者排斥其他供应商的其他串通行为。

## 7.投标无效的情形

- 7.1 详见资格性审查、符合性审查和磋商文件其他投标无效条款。

## 8.废标（终止）的情形

8.1 出现下列情形之一的，采购人或者采购代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

- (1) 因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；
- (2) 出现影响采购公正的违法、违规行为的；
- (3) 在采购过程中符合磋商要求的供应商或者报价未超过采购预算的供应商不足3家的，但经财政部门批准的情形除外；
- (4) 法律、法规以及磋商文件规定其他情形。

## 9.定标

9.1 磋商小组按照磋商文件确定的评审方法、步骤、标准，对响应文件进行评审。评审结束后，对供应商的评审名次进行排序，确定供应商或者推荐成交候选人。

## 10.其他说明事项

若出现供应商因在投标客户端中对应答点标记错误，导致评审专家无法进行正常查阅而否决供应商投标的情况发生时，由投标人自行承担责任。

## 二、政府采购政策落实

### 1.节能、环保要求

采购的产品属于品目清单范围的，将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，具体按照本磋商文件相关要求执行

### 2.对小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除

依照《政府采购促进中小企业发展管理办法》、《关于政府采购支持监狱企业发展有关问题的通知》和《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》的规定，凡符合要求的小型、微型企业、监狱企业或残疾人福利性单位，按照以下比例给予相应的价格扣除：（监狱企业、残疾人福利性单位视同为小、微企业）

合同包1（政务云服务商采购）

序号	情形	适用对象	价格扣除比例	计算公式
----	----	------	--------	------

序号	情形	适用对象	价格扣除比例	计算公式
1	小型、微型企业，监狱企业，残疾人福利性单位	非联合体	10%	本项目对属于小型和微型企业的投标人的投标报价给予相应百分比的扣除，用扣除后的价格参与评审。残疾人福利性单位视同小型、微型企业，享受同等价格扣除，但同时属于残疾人福利性单位和小微企业的，不重复价格扣除。
2	小型、微型企业，监狱企业，残疾人福利性单位	联合体	2%	本项目对属于小型和微型企业的投标人的投标报价给予相应百分比的扣除，用扣除后的价格参与评审。残疾人福利性单位视同小型、微型企业，享受同等价格扣除，但同时属于残疾人福利性单位和小微企业的，不重复价格扣除。
注：（1）上述评标价仅用于计算价格评分，成交金额以实际投标价为准。（2）组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。				

### 3.价格扣除相关要求

3.1所称小型和微型企业应当同时符合以下条件：

- （1）符合中小企业划分标准；
- （2）提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物。本项所称货物不包括使用大型企业注册商标的货物。
- （3）中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准。
- （4）小型、微型企业提供中型企业制造的货物的，视同为中型企业。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。

3.2在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策：

- （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民法典》订立劳动合同的从业人员。

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《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策。

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。

3.3供应商属于小微企业的应填写《中小企业声明函》；监狱企业须供应商提供由监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件；残疾人福利性单位应填写《残疾人福利性单位声明函》，否则不认定价格扣除。

说明：供应商应当认真填写声明函，若有虚假将追究其责任。供应商可通过“国家企业信用信息公示系统”（<http://www.gsxt.gov.cn/index.html>），点击“小微企业名录”（<http://xwqy.gsxt.gov.cn/>）对供应商和核心设备制

造商进行搜索、查询，自行核实是否属于小微企业。

3.4提供供应商的《中小企业声明函》、《残疾人福利性单位声明函》（格式后附，不可修改），未提供、未盖章或填写内容与相关材料不符的不予价格扣除。

### 三、评审程序

#### 1.资格性审查和符合性审查

1.1资格性审查。依据法律法规和磋商文件的规定，对响应文件中的资格证明文件等进行审查，以确定投标供应商是否具备投标资格。（详见后附表一资格性审查表）

1.2符合性审查。依据磋商文件的规定，从响应文件的有效性、完整性和对磋商文件的响应程度进行审查，以确定是否对磋商文件的实质性要求作出响应。（详见后附表二符合性审查表）

1.3资格性审查和符合性审查中凡有其中任意一项未通过的，评审结果为未通过，未通过资格性审查、符合性审查的投标单位按无效投标处理。

#### 2.磋商

（1）磋商小组所有成员应当集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

（2）在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时、同时通知所有参加磋商的供应商。

供应商应当按照磋商文件的变动情况和磋商小组的要求进行最终报价或重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

#### 3.最后报价

3.1磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价。最后报价是供应商响应文件的有效组成部分。

3.2已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。

#### 4.政府采购政策功能落实

对于小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除。

#### 5.综合评分（详见后附表三详细表）

由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分（得分四舍五入保留两位小数）。

#### 6.汇总、排序

6.1评审结果按评审后总得分由高到低顺序排列。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。上述相同的，按照提供优先采购产品证明材料的数量进行排序；以上均相同的属于保护环境、不发达地区和少数民族地区企业的优先。

#### 表一资格性审查表

合同包1（政务云服务商采购）

具有独立承担民事责任的能力	在中华人民共和国境内注册的法人或其他组织或自然人，投标时提交有效的营业执照（或事业法人登记证或身份证等相关证明）副本复印件。
有依法缴纳税收和社会保障资金的良好记录	提供投标截止日前6个月内任意1个月依法缴纳税收和社会保障资金的相关材料。如依法免税或不需要缴纳社会保障资金的，提供相应证明材料。

具有良好的商业信誉和健全的财务会计制度	供应商必须具有良好的商业信誉和健全的财务会计制度（提供2020年度财务状况报告或基本开户行出具的资信证明）。
履行合同所必须的设备和专业技术能力	按投标（响应）文件格式填报设备及专业技术能力情况。
参加采购活动前3年内，在经营活动中没有重大违法记录	参照投标（报价）函相关承诺格式内容。重大违法记录，是指供应商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。（较大数额罚款按照发出行政处罚决定书部门所在省级政府，或实行垂直领导的国务院有关行政主管部门制定的较大数额罚款标准，或罚款决定之前需要举行听证会的金额标准来认定）
信用记录	供应商未被列入“信用中国”网站(www.creditchina.gov.cn)“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以采购代理机构于投标（响应）截止时间当天在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网（http://www.ccgp.gov.cn/）查询结果为准，如相关失信记录已失效，供应商需提供相关证明资料）。
供应商必须符合法律、行政法规规定的其他条件	单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加本采购项目（包组）投标。为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参与本项目投标。投标（报价）函相关承诺要求内容。

表二符合性审查表：

合同包1（政务云服务商采购）

投标报价	投标报价（包括分项报价，投标总报价）只能有一个有效报价且不超过采购预算或最高限价，投标报价不得缺项、漏项。
投标文件规范性、符合性	投标文件的签署、盖章、涂改、删除、插字、公章使用等符合招标文件要求；投标文件文件的格式、文字、目录等符合招标文件要求或对投标无实质性影响。
主要商务条款	审查投标人出具的“满足主要商务条款的承诺书”，且进行签署、盖章。
联合体投标	符合关于联合体投标的相关规定。
技术部分实质性内容	1.明确所投标的的产品品牌、规格型号或服务内容或工程量； 2.投标文件应当对招标文件提出的要求和条件作出明确响应并满足招标文件全部实质性要求。
其他要求	招标文件要求的其他无效投标情形；围标、串标和法律法规规定的其它无效投标条款。

表三详细评审表：

政务云服务商采购

评审因素	评审标准
分值构成	满足招标文件要求通过初步评审的且投标报价最低的为评标基准价。符合小型、微型企业等规定进行价格调整的，以调整后的价格计算评标基准价和投标报价。
	1、技术部分85.0分 2、商务部分15.0分

<p>设计方案 (15.0分)</p>	<p>1、投标人方对项目理解透彻，整体项目设计思路清晰，设计具有扩展性、先进性、合理性。能提供结构完整且合理的项目总体设计，各子系统设计合理、完备，技术架构层次清晰、各项功能描述清楚合理，针对项目中未明确要求部分提出合理化建议与设计，设计方案应包括总体设计、平台架构图、网络拓扑图、功能描述、组织架构、实施计划、质量管理体系及人员、云平台资源与云服务提供保障措施、培训方案、售后服务方案；满分10分，缺少一项扣1分，分数扣完为止。 2、安全访问与数据交换服务要求参考网络服务技术要求内容，云服务商可以根据黑龙江省公安厅的业务现状进行设计及适当优化调整，但不得实质性低于所列需求。提供总体设计、具体服务能力说明、服务功能性描述、架构图、数据流向图。满分5分，缺一项扣1分，分数扣完为止。每项服务方案内容中每有一处不合理、或与本项目实际情况不相符的扣1分。</p>
<p>技术要求 (10.0分)</p>	<p>平台供应商应提供，由公安部计算机信息系统安全产品质量监督检验中心针对《GA/DSJ 公安云计算平台技术要求》相关7个标准（标准编号包括111、112、113、121、122、123、124）的检测报告中，基于部级标准配置模型的基准环境下，公安云计算平台符合性测试结果，并加盖平台供应商原厂公章。根据测试通过率评分，不提供报告不得分。测试报告获取日期不得晚于本项目开标日期 IaaS层技术要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； IaaS层接口要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； PaaS层技术要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； PaaS层接口要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； 平台供应商应提供，由公安部计算机信息系统安全产品质量监督检验中心针对《GA/DSJ 公安云计算平台技术要求》相关7个标准（标准编号包括111、112、113、121、122、123、124）的检测报告中，基于异构环境下，公安云计算平台符合性测试结果，并加盖平台供应商原厂公章。根据测试通过率评分，不提供报告不得分。测试报告获取日期不得晚于本项目开标日期 IaaS层技术要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； IaaS层接口要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； PaaS层技术要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； PaaS层接口要求检测通过率，95%以上得1分，85%以上得0.5分，其余不得分； 平台供应商应提供，由公安部计算机信息系统安全产品质量监督检验中心针对《GA/DSJ 公安云计算平台技术要求》相关7个标准（标准编号包括111、112、113、121、122、123、124）的检测报告中，异构兼容环境下对接测试报告，并加盖平台供应商原厂公章。根据测试对接平台数量评分，不提供报告不得分。测试报告获取日期不得晚于本项目开标日期 测试对接异构兼容平台数量，1个及以上得2分，不提供不得分</p>

技术部分	混合云管理 (6.0分)	支持多云服务，同时对OpenStack、华为HCS、华三cloudos、阿里飞天云、腾讯tstack等云平台混合云管理，用户可以通过混合云统一Portal申请全栈云服务，提供产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中一项或多项的证明材料并加盖云服务提供商及证明材料中产品厂商公章。满分6分，未提供证明材料和不符合要求的不得分。
	云运营管理 (5.0分)	支持用户资源申请、变更、删除服务的申请、流程审批；提供自助服务功能；用户可以自助门户对虚拟机进行日常维护工作，包括并不仅限于密码修改、windows自助挂盘等，并可以根据用户需求进行功能定制开发，提供产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中一项或多项的证明材料并加盖云服务提供商及证明材料中产品厂商公章。满分5分，未提供证明材料和不符合要求的不得分。
	云安全服务 (10.0分)	1、为保障公安业务数据安全性，要求云平台产品PaaS层支持构建加密服务，密钥资源可统一管理，对文件系统加密，提供产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中一项或多项的证明材料并加盖云服务提供商及证明材料中产品厂商公章。满分5分，未提供证明材料和不符合要求的不得分。2、支持虚拟防火墙单条防火墙规则聚合，一条安全规则中支持多个网段/多个端口，聚合为一条规则，减少规则数量，提高运维效率。提供产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中一项或多项的证明材料并加盖云服务提供商及证明材料中产品厂商公章。满分5分，未提供证明材料和不符合要求的不得分。
	云硬盘 (5.0分)	支持云硬盘服务。用户可以通过管理平台为虚拟机或者物理机申请磁盘，用户可以将申请到的磁盘空间分配给一台或者多台虚拟机/物理机使用。提供产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中一项或一项以上的证明材料并加盖云服务提供商及证明材料中产品厂商公章。满分5分，未提供证明材料和不符合要求的不得分。
	云用户管理 (5.0分)	对上云的组织机构、用户、人员、业务系统进行维护和管理；创建用户基本信息（用户名、密码、真实姓名、手机号码、人员类型、组织机构等），人员类型包括政府人员、运维人员、上云软件提供商等。维护业务系统的干系人。提供产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中一项或一项以上的证明材料并加盖云服务提供商及证明材料中产品厂商公章。满分5分，未提供证明材料和不符合要求的不得分。
	安全访问区服务 (6.0分)	供应商需提供可信接入检控服务、可信应用检控服务和可信数据检控服务，3项服务，每项服务可提供证明材料对招标要求的功能、性能予以佐证，（提供材料应包含产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中的一项或一项以上的证明材料并加盖云服务提供商及证明材料中产品厂商公章）。每项服务得2分，满分6分，未提供证明材料和不符合要求的不得分。

数据交换区服务 (6.0分)	<p>供应商需提供安全数据交换系统服务、安全视频交换系统服务和可信数据检控服务，3项服务，每项服务可提供证明材料对招标要求的功能、性能予以佐证，（提供材料应包含产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中的一项或一项以上的证明材料并加盖云服务提供商及证明材料中产品厂商公章）。每项服务得2分，满分6分，未提供证明材料和不符合要求的不得分。</p>
安全检测区服务 (4.0分)	<p>供应商需提供流量采集复制分流服务、网络流量采集服务，2项服务，每项服务可提供证明材料对招标要求的功能、性能予以佐证，（提供材料应包含产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中的一项或一项以上的证明材料并加盖云服务提供商及证明材料中产品厂商公章）。每项服务得2分，满分4分，未提供证明材料和不符合要求的不得分。</p>
互联网+政务服务区的边界接入 (4.0分)	<p>供应商需提供安全数据交换系统服务、数据库防火墙服务，2项服务，每项服务可提供证明材料对招标要求的功能、性能予以佐证，（提供材料应包含产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中的一项或一项以上的证明材料并加盖云服务提供商及证明材料中产品厂商公章）。每项服务得2分，满分4分，未提供证明材料和不符合要求的不得分。</p>
登录管理 (4.0分)	<p>用户只需要在公安云运营管理平台上登录一次，就可以按权限访问应用系统以及VPN、堡垒机等设备。提供产品厂商证明文件、产品技术白皮书、官网证明截图、第三方检测报告中一项或一项以上的证明材料并加盖云服务提供商及证明材料中产品厂商公章。满分4分，未提供证明材料和不符合要求的不得分。</p>
能力服务要求 (5.0分)	<p>为保证云服务商能够顺利协助租户完成应用部署上云及业务迁移、运维等工作，云服务商应在用户方配备常驻服务团队，团队成员不少于5人，且应具备所使用云平台厂商提供的中级及或中级以上认证资质。满分5分，每一人不满足条件扣1分，扣完为止，未提供资质证明和不符合要求的不得分。</p>
<p>商务部分</p> <p>资质证明 (15.0分)</p>	<p>1、云服务商采用的云平台产品厂商获得ITSS（中国电子工业标准化技术协会）云计算服务能力一级证书得5分，其余等级云计算服务能力证书或未提供不得分，提供证书复印件并加盖云服务提供商及云平台制造商公章。</p> <p>2、云服务商采用的云平台应为云平台制造商自主研发、成熟稳定、安全可靠的云计算平台产品。提供相关证明材料（包含但不限于软件著作权等）并加盖云服务提供商及云平台产品制造商公章。满分5分，未提供证明材料和不符合要求的不得分。</p> <p>3、云服务商提供的云平台产品制造商具有计算机信息系统安全专用产品销售许可证（增强级）GA部销售许可证，信息安全技术云操作系统安全检验要求（增强级），信息安全技术通用渗透测试检测条件，提供相关证明材料并加盖云平台产品制造商公章。满分5分，未提供证明材料和不符合要求的不得分。</p>

## 第七章 响应文件格式与要求

供应商提供响应文件应按照以下格式及要求进行编制，且不少于以下内容。

### 响应文件封面

(项目名称)

### 响应文件封面

(正本/副本)

项目编号：**SC[2021]0170**

所投采购包：第 包

(供应商名称)

年 月 日

## 响应文件目录

- 一、投标承诺书
- 二、开标一览表
- 三、授权委托书
- 四、投标保证金
- 五、供应商基本情况表
- 六、供应商应符合《中华人民共和国政府采购法》第二十二条规定的条件，提供标准格式的承诺函。
- 七、联合体协议书
- 八、中小企业声明函
- 九、监狱企业
- 十、残疾人福利性单位声明函
- 十一、分项报价明细表分项报价明细表
- 十二、项目组成人员一览表
- 十三、技术偏离表
- 十四、项目实施方案、质量保证及售后服务承诺等
- 十五、主要商务要求承诺书
- 十六、供应商业绩情况表
- 十七、各类证明材料

格式一：

投标承诺书

采购单位、黑龙江省政府采购中心：

1.按照已收到的 项目（项目编号： ）磋商文件要求，经我方 （供应商名称） 认真研究投标须知、合同条款、技术规范、资质要求和其它有关要求后，我方愿按上述合同条款、技术规范、资质要求进行投标。我方完全接受本次磋商文件规定的所有要求，并承诺在中标后执行磋商文件、响应文件和合同的全部要求，并履行我方的全部义务。我方的最终报价为总承包价，保证不以任何理由增加报价。

2.我方同意磋商文件关于投标有效期的所有规定。

3.我方郑重声明：所提供的响应文件内容全部真实有效。如经查实提供的内容、进行承诺的事项存在虚假，我方自愿接受有关处罚，及由此带来的法律后果。

4.我方将严格遵守《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关法律、法规规定，如有违反，无条件接受相关部门的处罚。

5.我方同意提供贵方另外要求的与其投标有关的任何数据或资料。

6.我方将按照磋商文件、响应文件及相关要求、规定进行合同签订，并严格执行和承担协议和合同规定的责任和义务。

7.我单位如果存在下列情形的，愿意承担取消中标资格、接受有关监督部门处罚等后果：

- (1) 中标后，无正当理由放弃中标资格；
- (2) 中标后，无正当理由不与招标人签订合同；
- (3) 在签订合同时，向招标人提出附加条件或不按照相关要求签订合同；
- (4) 不按照磋商文件要求提交履约保证金；
- (5) 要求修改、补充和撤销响应文件的实质性内容；
- (6) 要求更改磋商文件和中标结果公告的实质性内容；
- (7) 法律法规和磋商文件规定的其他情形。

详细地址：

邮政编码：

电话：

电子函件：

供应商开户银行：

账号/行号：

供应商法人签字： （加盖公章）

年 月 日

格式二：

开标一览表

说明：

- 1.所有价格均系用人民币表示，单位为元。
- 2.价格应按照“供应商须知”的要求报价。
- 3.格式、内容和签署、盖章必须完整。
- 4.《开标一览表》中所填写内容与响应文件中内容不一致的，以开标一览表为准。

注：采用电子招投标的项目无需编制该表格，投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成开标一览表（首轮报价表、报价一览表）或分项报价表，若在响应文件中出现非系统生成的开标一览表（首轮报价表、报价一览表）或分项报价表，且与投标客户端生成的开标一览表（首轮报价表、报价一览表）或分项报价表信息内容不一致，以投标客户端生成的内容为准。

法定代表人或授权委托人（签字）：

加盖公章：

年 月 日

格式三：

授权委托书

本人\_\_\_\_\_（姓名）系\_\_\_\_\_（供应商名称）的法定代表人，现委托\_\_\_\_\_（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改招标项目响应文件、签订合同和处理有关事宜，其法律后果由我方承担。委托期限：\_\_\_\_\_。

代理人无转委托权。

投标人：\_\_\_\_\_（加盖公章）  
 法定代表人：\_\_\_\_\_（签字）  
 授权委托人：\_\_\_\_\_（签字）

法定代表人身份证扫描件  国徽面	法定代表人身份证扫描件  人像面
授权委托人身份证扫描件  国徽面	授权委托人身份证扫描件  人像面

\_\_\_\_年\_\_\_\_月\_\_\_\_日

**格式四：**

投标人基本情况表

投标人名称		注册资金	
注册地		注册时间	
法定代表人		联系电话	
技术负责人		联系电话	
开户银行			
开户银行账号			
主营范围：			
企业资质：			

**格式五：**

投标保证金

供应商应在此提供保证金的凭证的复印件。

**格式六：**

供应商应符合《中华人民共和国政府采购法》第二十二条规定的条件，标准格式的承诺函。

**资格承诺函**

黑龙江省政府采购中心：

- 1.符合《中华人民共和国政府采购法》第二十二条规定的条件；
  - (1)具有独立承担民事责任的能力；
  - (2)具有良好的商业信誉和健全的财务会计制度；
  - (3)具有履行合同所必需的设备和专业技术能力；
  - (4)有依法缴纳税收和社会保障资金的良好记录；
  - (5)参加本次政府采购活动前三年内，在经营活动中没有重大违法记录；
  - (6)符合国家法律、行政法规规定的其他条件。
- 2.我公司作为本项目参加政府采购活动的供应商、法定代表人/单位负责人近3年内不具有行贿犯罪记录。

3. 我公司在截至投标截止日未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

本公司对上述承诺的内容事项真实性负责。如经查实上述承诺的内容事项存在虚假，我公司愿意接受以提供虚假材料谋取中标追究法律责任。

供应商（单位盖章）：

日期：

格式七：（不属于可不填写内容或不提供）

#### 联合体协议书

\_\_\_\_\_（所有成员单位名称）自愿组成\_\_\_\_\_（联合体名称）联合体，共同参加\_\_\_\_\_（项目名称）招标项目投标。现就联合体投标事宜订立如下协议。

- 1.（某成员单位名称）为（联合体名称）牵头人。
2. 联合体各成员授权牵头人代表联合体参加投标活动，签署文件，提交和接收相关的资料、信息及指示，进行合同磋商活动，负责合同实施阶段的组织和协调工作，以及处理与本招标项目有关的一切事宜。
3. 联合体牵头人在本项目中签署的一切文件和处理的一切事宜，联合体各成员均予以承认。联合体各成员将严格按照磋商文件、响应文件和合同的要求全面履行义务，并向招标人承担连带责任。
4. 联合体各成员单位内部的职责分工如下：\_\_\_\_\_。
5. 本协议书自所有成员单位法定代表人或其授权代表签字或盖单位章之日起生效，合同履行完毕后自动失效。
6. 本协议书一式\_\_\_\_\_份，联合体成员和招标人各执一份。

协议书由法定代表人签字的，应附法定代表人身份证明；由授权代表签字的，应附授权委托书。

联合体牵头人名称：\_\_\_\_\_（加盖公章）  
法定代表人或其授权代表：\_\_\_\_\_（签字）  
联合体成员名称：\_\_\_\_\_（加盖公章）  
法定代表人或其授权代表：\_\_\_\_\_（签字）

\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日

格式八：（不属于可不填写内容或不提供）

#### 中小企业声明函（工程、服务）

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

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

……  
以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：  
日期：

#### 中小企业声明函（货物）

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

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

.....  
以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。  
本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：  
日期：

格式九：（不属于可不填写内容或不提供）

#### 监狱企业

提供由监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

格式十：（不属于可不填写内容或不提供）

#### 残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_单位的\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（加盖公章）：  
日期：

格式十一：

#### 分项报价明细表

序号	标的名称	品牌、规格型号/主要服务内容	制造商名称	产地	数量	单位	单价 (元)	总价 (元)
1								
2								
3								
...								

注：采用电子招投标的项目无需编制该表格，投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成开标一览表（首轮报价表、报价一览表）或分项报价表，若在响应文件中出现非系统生成的开标一览表（首轮报价表、报价一览表）或分项报价表，且与投标客户端生成的开标一览表（首轮报价表、报价一览表）或分项报价表信息内容不一致，以投标客户端生成的内容为准。

格式十二：

#### 主要商务要求承诺书

我公司承诺可以完全满足本次采购项目的**所有主要商务条款要求**（如标的提供的时间、标的提供的地点、投标有效期、采购资金支付、验收要求、履约保证金等）。若有不符合或未按承诺履行的，后果和责任自负。

如有优于磋商文件主要商务要求的请在此承诺书中说明。

具体优于内容（如标的提供的时间、地点，质保期等）。

特此承诺。

供应商名称：（加盖公章）

年月日

格式十三：

技术偏离表

序号	标的名称	招标技术要求		投标人提供响应内容	偏离程度	备注
1		★	1.1			
			1.2			
			.....			
2		★	2.1			
			2.2			
			.....			
.....						

说明：

1. 供应商应当如实填写上表“供应商提供响应内容”处内容，对磋商文件提出的要求和条件作出明确响应，并列明具体响应数值或内容，只注明符合、满足等无具体内容表述的，将视为未实质性满足磋商文件要求。
2. “偏离程度”处可填写满足、响应或正偏离、负偏离。
3. 佐证文件名称及所在页码：系指能为投标产品提供技术参数佐证或进一步提供证据的文件、资料名称及相关佐证参数所在页码。如直接复制采购文件要求的参数但与佐证材料不符的，为无效投标。
4. 上表中“招标技术要求”应详细填写招标要求。

格式十四：

项目组成人员一览表

序号	姓名	本项目拟任职务	学历	职称或执业资格	身份证号	联系电话
1						
2						
3						
.....						

按磋商文件要求在本表后附相关人员证书。

注：

1. 本项目拟任职务处应包括：项目负责人、项目联系人、项目服务人员或技术人员等。
2. 如供应商中标，须按本表承诺人员操作，不得随意更换。

格式十五：

项目实施方案、质量保证及售后服务承诺等内容和格式自拟。

格式十六：

供应商业绩情况表

序号	使用单位	业绩名称	合同总价	签订时间
1				
2				
3				
4				
...				

供应商根据上述业绩情况后附销售或服务合同复印件。

格式十七：

各类证明材料

- 1.磋商文件要求提供的其他资料。
- 2.供应商认为需提供其他资料。