

双鸭山市政府采购中心

公开招标文件

项目名称：双鸭山市政府网站集约化平台和机房等保加固(二次)

项目编号：**[230501]SZCG[GK]20220012-1**

第一章 投标邀请

双鸭山市政府采购中心受双鸭山市人民政府办公室的委托，采用公开招标方式组织采购双鸭山市政府网站集约化平台和机房等保加固(二次)。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：双鸭山市政府网站集约化平台和机房等保加固(二次)

批准文件编号：双财购核字[2022]00948号

采购项目编号：[230501]SZCG[GK]20220012-1

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	双鸭山市政府网站集约化平台和机房等保加固	1	详见采购文件	4,548,340.00

二.投标人的资格要求

1.投标人应符合《中华人民共和国政府采购法》第二十二条规定的条件。

2.到提交投标文件的截止时间，投标人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（双鸭山市政府网站集约化平台和机房等保加固）：无

三.获取招标文件的时间、地点、方式

获取招标文件的地点：详见招标公告；

获取招标文件的方式：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招标文件。

其他要求

1.采用“现场网上开标”模式进行开标，投标人需到达开标现场。

2.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。“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。”

3.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。

注：开标模式详见供应商须知-开标方式

四.招标文件售价

本次招标文件的售价为 无 元人民币。

五.递交投标文件截止时间、开标时间及地点：

递交投标文件截止时间：详见招标公告

投标地点：详见招标公告

开标时间：详见招标公告

开标地点：详见招标公告

备注：所有电子投标文件应在投标截止时间前递交至黑龙江省政府采购管理平台，逾期递交的投标文件，为无效投标文件。

六.询问提起与受理：

项目经办人： 巩瀚极 联系方式： 0469-4252104

七.质疑提起与受理：

1.对采购文件的质疑按要求以书面形式提供纸质材料：

项目经办人： 巩瀚极 联系方式： 0469-4252104

2.对评审过程和结果的质疑按要求以书面形式提供纸质材料：

采购中心质疑受理人：周崇 电话： 0469-4252107

八.公告发布媒介：

中国政府采购网 黑龙江省政府采购网

联系信息

1. 采购代理机构

采购代理机构名称：双鸭山市政府采购中心

地址：黑龙江省双鸭山市尖山区站前路行政审批大厅5楼

联系人： 巩瀚极

联系电话： 0469-4252104

账户名称：系统自动生成的缴交账户名称

开户行：详见投标人须知

账号：详见投标人须知

2. 采购人信息

采购单位名称：双鸭山市人民政府办公室

地址：双鸭山市尖山区城投大厦70号

联系人： 邹宏伟

联系电话： 18944691717

双鸭山市政府采购中心

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	公开招标
3	开标方式	不见面开标
4	评标方式	现场网上评标
5	是否专门面向中小企业采购	合同包1（双鸭山市政府网站集约化平台和机房等保加固）：否
6	评标办法	合同包1（双鸭山市政府网站集约化平台和机房等保加固）：综合评分法
7	获取招标文件时间（同招标文件提供期限）	详见招标公告
8	保证金缴纳截止时间（同递交投标文件截止时间）	详见招标公告
9	电子投标文件递交	电子投标文件在投标截止时间前递交至黑龙江省政府采购网--政府采购管理平台
10	投标文件数量	（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”）
11	中标人确定	采购人授权评标委员会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	代理服务收费方式	不收取。

1 6	履约保证金	<p>履约保证金： 中标方向双鸭山市政府采购中心提交合同总价5%的履约保证金，履约保证金提交后合同生效，履约验收合格后5个工作日内无息返还。</p> <p>缴纳履约保证金开户行、账号、户名</p> <p>开户行：中国建设银行股份有限公司双鸭山东华支行</p> <p>帐号：23050165370009999999</p> <p>户名：双鸭山市公共资源交易中心</p> <p>备注：项目编号</p> <p>如有疑问请与我中心财务部工作人员联系。</p> <p>查询电话：0469-4252105</p> <p>特别提示：</p> <p>1、供应商应认真核对账户信息，将履约保证金足额汇入以上账户，并自行承担因汇错履约保证金而产生的一切后果。</p> <p>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：“（电汇时，须注明项目编号以SZCG***号为准，无需填写文字内容）的履约保证金”。</p>
--------	-------	---

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>不见面开标（远程开标）：</p> <p>1. 项目采用不见面开标（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，将会由开标负责人视情况来决定是否允许投标人导入非加密电子投标文件继续开标。本项目采用电子评标（网上评标），只对通过开标环节验证的电子投标文件进行评审。</p> <p>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。</p> <p>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，投标人请自行留存。</p> <p>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模式等要求参加开标，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。</p> <p>5. 开标时，投标人应当使用 CA 证书在开始解密后30分钟内完成投标文件在线解密，若出现系统异常情况，工作人员可适当延长解密时长。（请各投标人在参加开标以前自行对使用电脑的网络环境、驱动安装、客户端安装以及CA证书的有效性等进行检测，保证可以正常使用。具体环境要求详见操作手册）</p> <p>6. 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、采购代理机构应当视为投标无效处理。</p> <p>（1） 投标人未按招标文件要求参加远程开标会的；</p> <p>（2） 投标人未在规定时间内完成电子投标文件在线解密；</p> <p>（3） 经检查数字证书无效的投标文件；</p> <p>（4） 投标人自身原因造成电子投标文件未能解密的。</p> <p>7. 供应商必须保证在规定时间内完成已投项目的电子响应文件解密，并在规定时间内进行签章确认，未在规定时间内签章的，视同接受开标结果。</p>
18	电子投标文件 签字、盖章要求	<p>应按照第七章“投标文件格式”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投标文件。</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--政府采购管理平台”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；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（双鸭山市政府网站集约化平台和机房等保加固）：总价</p>
22	投标有效期	<p>从提交投标（响应）文件的截止之日起90日历天</p>
23	其他	

2	项目兼投兼中	兼投兼中： -
4	规则	

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：

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用于制作投标文件时盖章、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>）CA在线办理）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本采购项目不缴纳投标保证金。

若出现账号缴纳不一致、缴纳金额与投标人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，请投标人在投标截止前及早缴纳。

三、说明

1.总则

本招标文件依据《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《政府采购货物和服务招标投标管理办法》（财政部令第87号）及国家和自治区有关法律、法规、规章制度编制。

投标人应仔细阅读本项目信息公告及招标文件的所有内容（包括变更、补充、澄清以及修改等，且均为招标文件的组成部分），按照招标文件要求以及格式编制投标文件，并保证其真实性，否则一切后果自负。

本次公开招标项目，是以招标公告的方式邀请非特定的投标人参加投标。

2.适用范围

本招标文件仅适用于本次招标公告中所涉及的项目和内容。

3.投标费用

投标人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。本招标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。本招标文件的采购代理机构特指双鸭山市政府采购中心。

4.3“投标人”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“评标委员会”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中标人或者推荐中标候选人的临时组织。

4.5“中标人”是指经评标委员会评审确定的对招标文件做出实质性响应，取得与采购人签订合同资格的投标人。

5.合格的投标人

5.1符合本招标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、管理关系的不同投标人，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、检测等服务的投标人，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，并作为投标文件组成部分。

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，并在投标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。由同一资质条件的投标人组成的联合体，应当按照资质等级较低的投标人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。

8.现场踏勘

- 8.1招标文件规定组织踏勘现场的，采购人按招标文件规定的时间、地点组织投标人踏勘项目现场。
- 8.2投标人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，不构成对招标文件的修改或不作为投标人编制投标文件的依据。

9.其他条款

- 9.1无论中标与否投标人递交的投标文件均不予退还。

四、招标文件的澄清和修改

1.采购人或采购代理机构对已发出的招标文件进行必要的澄清或修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构应当在投标截止时间15日前，不足15日的，顺延投标截止之日，同时在“黑龙江省政府采购网”、“黑龙江省公共资源交易网”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招标文件的组成部分，投标人应自行上网查询，采购人或采购代理机构不承担投标人未及时关注相关信息的责任。

五、投标文件

1.投标文件的构成

投标文件应按照招标文件第七章“投标文件格式”进行编写（可以增加附页），作为投标文件的组成部分。

2.投标报价

2.1投标人应按照“第四章招标内容与要求”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招标文件要求以外的内容，否则，在评审时不予核减。

2.2投标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投标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）开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
- （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：修正后的报价投标人应当采用书面形式，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，但不得超出投标文件的范围或者改变投标文件的实质性内容，投标人不确认的，其投标无效。

3.投标有效期

3.1投标有效期从提交投标文件的截止之日起算。投标文件中承诺的投标有效期应当不少于招标文件中载明的投标有效期。投标有效期内投标人撤销投标文件的，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投标人延长投标有效期。投标人同意延长的，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投标文件；投标人拒绝延长的，其投标失效，但投标人有权收回其投标保证金。

4.投标保证金

4.1投标保证金的缴纳：

投标人在提交投标文件的同时，应按投标人须知前附表规定的金额、开户银行、行号、开户单位、账号和招标文件本章“投标须知”规定的投标保证金缴纳要求递交投标保证金，并作为其投标文件的组成部分。

4.2投标保证金的退还：

- （1）投标人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，但因投标人自身原因导致无法及时退还的除外；
- （2）未中标供应商投标保证金，自中标通知书发出之日起5个工作日内退还；

(3) 中标供应商投标保证金，投标保证金转为履约保证金。

4.3有下列情形之一的，投标保证金将不予退还：

- (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) 不按照招标文件要求提交履约保证金；
- (5) 要求修改、补充和撤销投标文件的实质性内容；
- (6) 要求更改招标文件和中标结果公告的实质性内容；
- (7) 法律法规和招标文件规定的其他情形。

5.投标文件的修改和撤回

5.1投标人在提交投标截止时间前，可以对所递交的投标文件进行补充、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，并作为投标文件的组成部分。

5.2在提交投标文件截止时间后到招标文件规定的投标有效期终止之前，投标人不得补充、修改、替代或者撤回其投标文件。

6.投标文件的递交

6.1在招标文件要求提交投标文件的截止时间之后送达或上传的投标文件，为无效投标文件，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招标文件规定投标人提交样品的，样品属于投标文件的组成部分。样品的生产、运输、安装、保全等一切费用由投标人自理。

7.2开标前，投标人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，投标人应提前做好演示准备（包括演示设备）。

7.3评标结束后，中标供应商与采购人共同清点、检查和密封样品，由中标供应商送至采购人指定地点封存。未中标投标人将样品自行带回。

六、开标、评审、结果公告、中标通知书发放

1.网上开标程序

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) 投标人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（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，投标文件移交评标委员会。

1.2开标异议

投标人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投标人不足三家的，不得开标。

1.4备注说明：

- (1) 若本项目采用不见面开标，开标时投标人使用 CA证书参与远程投标文件解密。投标人用于解密的CA证书应为该投

标文件生成加密、上传的同一把 CA证书。

(2) 若本项目采用不见面开标, 投标人在开标时间前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) 投标人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 中标供应商确定后, 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, 中标供应商可自行登录“黑龙江省政府采购网--政府采购管理平台”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中标供应商具有同等法律效力。

中标通知书发出后, 采购人不得违法改变中标结果, 中标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 潜在投标人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; 递交投标文件的供应商, 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投标人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。

3.0接收质疑函的方式：为了使提出的质疑事项在规定时间内得到有效答复、处理，质疑采用实名制，且由法定代表人或授权代表亲自递交至采购代理机构，正式受理后方可生效。

联系部门：采购人、采购代理机构（详见第一章 投标邀请）。

联系电话：采购人、采购代理机构（详见第一章 投标邀请）。

通讯地址：采购人、采购代理机构（详见第一章 投标邀请）。

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，按照招标文件和中标供应商投标文件的规定，与中标供应商签订书面合同。所签订的合同不得对招标文件确定的事项和中标供应商投标文件作实质性修改。

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中标人的名称和住所、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采购人与中标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。

1.8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具体格式见本招标文件后附拟签订的《合同文本》（部分合同条款），投标文件中可以不提供《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

中标供应商在供货、工程竣工或服务结束后，采购人应及时组织验收，并按照招标文件、投标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：***（填写中标投标人）

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)招标文件
- (4)投标文件
- (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

***（见招标文件第四章）

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。如果乙方在投标文件及谈判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) 乙方应按招标文件、投标文件及乙方在谈判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: (投标文件售后承诺等)

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

合同文本一式四份,采购单位、供应商、各一份,政府采购监管部门二份,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)

投标人法人代表: (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(主要技术指标需与投标文件相一致)(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 招标内容与技术要求

一、项目概况：

双鸭山市集约化云平台的搭建将有助于与双鸭山市电子集约化从粗放式、离散化的建设模式向集约化、整体化的可持续发展模式转变，使政府管理服务从各自为政、相互封闭的运作方式向跨部门跨区域的协同互动和资源共享转变。省数据政府建设十四五规划对全市信息化基础设施服务能力提出了更高要求，一方面需要通过服务能力的提升，支撑实现城市运行的全面感知、领域应用协同、资源整合和信息资源的智能化利用；另一方面需要通过集约化的建设和应用，提升整体运行管理水平，降低建设成本，减少运行能耗。云计算模式是确保集约高效、促进标准化和共享协同的有力手段。政府领导对云计算的发展高度重视，多次进行实地调研并做出重要指示，提出云计算是新一代信息变革的重要组成部分，是双鸭山信息产业实现跨越式发展的重要机遇，要紧紧抓住这一宝贵契机，积极推动云计算在双鸭山有序、高效、健康发展。

合同包1（双鸭山市政府网站集约化平台和机房等保加固）

1.主要商务要求

标的提供的时间	合同签订后30个日历日内交货
标的提供的地点	采购单位指定地点
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50%，签订合同后，首付款支付比例为合同总金额的50%；签订合同后对中小企业首付款比例为合同总额的50%，对小微企业首付款比例为合同总额的70%。 2期：支付比例40%，9月25日前项目施工完成并经甲方验收合格，支付比例为合同总金额的40%；如中标企业为中小企业的，支付比例为合同总金额的40%；如中标企业为小微企业的，支付比例为合同总金额的20%。 3期：支付比例10%，项目施工完成并经甲方验收合格，满5年后，结清剩余款项。
验收要求	1期：满足采购单位所有参数要求。
履约保证金	不收取
其他	

2.技术标准与要求

序号	核心产品 （“△”）	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）	所属行业	招标技术要求
1		其他计算机设备及软件	双鸭山市政府网站集约化平台和机房等保加固	套	1.000	4,548,340.00	4,548,340.00	其他未列明行业	详见附件一

附表一：双鸭山市政府网站集约化平台和机房等保加固 是否进口：否

参数性质	序号	具体技术(参数)要求
		设备一：政务网核心交换机 政务网核心交换机技术要求

数量2台

- 1.整机交换容量 $\geq 384\text{Tbps}$ ，转发性能 $\geq 72000\text{Mpps}$ ，业务板卡与交换网板采用完全正交设计，交换网板 ≥ 5 个；
- 2.配置主控引擎数量 ≥ 2 ，业务插槽数 ≥ 6 ，交流电源 ≥ 4 个；万兆光接口 ≥ 48 个，配置万兆光模块 ≥ 10 个；
- 3.支持防火墙、入侵防御系统等安全板卡扩展；
- 4.单槽位40G端口密度 ≥ 32 个；
- 5.支持40G/100G端口切换，切换后流量正常转发，不丢包。
- 6.多虚一技术(N:1)，支持4框虚拟化技术；
- 7.支持远程端口扩展，作为控制设备（Controlling Bridge,CB）实现对端口扩展模块（Port Extender, PE）的集中控制；
- 8.支持MACsec加密技术；支持MPLS Segment Routing 功能；
- 9.支持融合 AC 功能，无需额外配置单独硬件，在交换机上实现对AP 的接入控制和管理，有线无线用户的统一认证管理，最大 AP 上线数量为 12K，最大 Client 上线数量为 60K；
- 10.支持PC终端、哑终端、网络设备等连接元素的准入控制和权限划分，确保网络的可信可控；
- 11.支持Telemetry流量可视化功能；
- 12.支持 IPv4 Portal、IPv6 Portal 及 Portal 双协议栈功能，最大 Portal 认证用户数量可达 256K。

设备二：政务网数据中心交换机

政务网数据中心交换机技术要求

数量2台

- 1.整机交换容量 $\geq 36\text{Tbps}$ ，包转发能力 $\geq 2000\text{Mpps}$ ；
- 2.配置万兆光接口 ≥ 24 个，100GE光接口 ≥ 6 个，Console口 ≥ 1 个；热插拔风扇模块 ≥ 3 个，前后或后前通风；模块化电源 ≥ 2 个；万兆光模块 ≥ 16 个；40G电缆 ≥ 1 个；
- 3.支持融合AC功能，可管理AP数 $\geq 1\text{K}$ ；
- 4.支持二层、三层Vxlan网关和BGP EVPN特性；
- 5.支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议；
- 6.支持跨设备链路聚合技术，端口转发时延小于2微秒；
- 7.支持sFlow 支持RoCE v2无损网络；
- 8.支持服务链Service chain功能；
- 9.支持黑洞MAC、动态ARP检测、ARP防攻击；
- 10.支持零配置技术，配置自动下发。

设备三：分布式块存储软件

分布式块存储软件技术要求

数量1套

- 1.采用分布式的软件定义存储架构，在通用服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点，使用管理平台统一管理，无需在计算虚拟化平台上部署存储控制器；
- 2.配置 ≥ 4 节点服务器全部物理CPU分布式块存储授权软件；
- 3.支持厚/精简配置；厚配置根据业务需求分配固定的物理存储空间、精简配置根据应用实际写需要时才分配相应的物理存储空间；
- 4.支持包括iscsi, RBD多种块存储协议,块存储支持快照功能，可支持创建可写快照；

5.支持混合磁盘分区特性，可将集群内所有SSD盘跨节点做一个快存储池，所有类型不同性能磁盘均可支持分区，包含SSD，SAS，SATA，NL-SAS等。

设备四：分布式文件存储软件

分布式文件存储软件技术要求

数量1套

1.采用分布式的软件定义存储架构，在通用服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点，使用管理平台统一管理，无需在计算虚拟化平台上部署存储控制器；

2.配置≥4节点服务器全部物理CPU分布式文件存储授权软件；

3.支持FTP、CIFS、NFS、HTTP等文件存储协议；

4.提供多种NAS权限管理、快照管理(WORM)、共享目录管理等；NAS服务可以采用多服务节点高可用，并支持负载均衡增值服务功能；

5.支持通过B/S管理界面对存储基础架构进行集中的配置，如存储资源池、集群、集群节点、磁盘等资源进行合理的划分和配置。

设备五：计算虚拟化软件

计算虚拟化软件技术要求

数量1套

1.配置≥4节点服务器全部物理CPU计算虚拟化授权软件；

2.在管理平台管理界面上提供虚拟机启动、暂停、恢复、休眠、重启、关闭、克隆、迁移、删除、快照等功能批量操作；

3.在管理平台管理界面上提供集群HA（高可用），DRS（动态资源调度）等功能配置，无需界面跳转；

4.具有合理的内存调度机制，能够实现内存的过量使用，保证内存资源的充分利用；

5.支持根据业务需求设置不同的虚拟机磁盘缓存模式，包括直接读写、一级缓存、二级缓存等；

6.提供热添加CPU、内存、磁盘、网卡的功能，无需中断或停机即可实现虚拟资源的在线添加；

7.提供虚拟机回收站功能，统一管理被删除的虚拟机，防止因虚拟机误删除导致数据丢失，支持设置回收站文件保存周期，超期的文件将被自动删除；

8.支持批量修改虚拟机的配置参数，包括：I/O优先级、启动优先级、是否自动迁移、CPU调度优先级、CPU个数、内存大小、自动启动、VM启动设备、启用VNC代理、tools自动升级等；

9.具有存储精简配置能力（Thin Provisioning），减少存储容量的需求；

10.支持虚拟机IP和虚拟网卡绑定，以防止地址篡改导致的审计问题；

11.支持将多个物理服务器组成集群，可基于CPU、内存、网络流量、存储容量、磁盘IO等资源利用率动态资源调度功能；

12.支持设置虚拟机磁盘IOPS及I/O速率的读写限制；

13.提供虚拟机快照功能，支持设置手工和定时快照将虚拟机磁盘文件和内存状态信息保存到镜像文件中；

14.虚拟机支持在线克隆为模板，模板制作过程中对业务运行无影响，同时虚拟机模板支持完整性验证与

来源追溯，避免虚拟机模板文件被篡改的可能性，并追踪虚拟机模板的来源以及虚拟机模板部署的记录；

15.虚拟化软件内置备份模块，无需单独安装备份软件即可实现虚拟机全量、增量、差异备份功能。

设备六：政务网区智能加速卡

政务网区智能加速卡技术要求

数量1套

- 1.支持虚拟化的网络和存储IO都卸载到此硬件或者配置额外服务器；
- 2.提供两个10G端口，支持RDMA，Rocev2，支持聚合，采用专用的ASIC处理芯片和内存或者额外服务器实现，可以释放物理节点网络和存储消耗的CPU资源，提升CPU资源的利用率；
- 3.计算虚拟化支持智能加速，虚拟交换机在智能网卡或者额外服务器上卸载，且支持虚拟机热迁移HA配置要求，配置相应的CPU授权许可；
- 4.支持128字节转发性能达到10G以上（10G端口）；
- 5.支持网络二层直通和存储IO硬件加速，不消耗CPU资源；
- 6.可以在主CPU使用率低于2%的情况下提供分布式存储和网络功能。

设备七：政务网区云主机安全软件

政务网区云主机安全软件技术要求

数量1套

- 1.支持虚拟网络安全功能，可以提供公网IP、vLB、vFW、vRouter等功能，并支持部署虚拟NFV网元；
- 2.配置 ≥ 4 节点服务器网络安全虚拟化授权软件，不限制虚拟机数量；
- 3.支持公网IP地址池，支持公网IP和私网IP绑定，支持软件负载均衡；
- 4.提供虚拟网络设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性；
- 5.分布式防火墙基于监测虚拟机IP地址和端口进行东西向流量隔离控制；
- 6.虚拟负载均衡支持HTTP、HTTPS、TCP等监听协议支持配置均衡算法（轮转算法，最小连接算法，源地址算法），支持健康检查，可配置检查间隔、超时时长、重复次数等；
- 7.在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。

设备八：政务网区云主机杀毒软件

政务网区云主机杀毒软件技术要求

数量1套

- 1.配置虚拟化linux服务器杀毒授权 ≥ 300 点，虚拟化Windows服务器杀毒授权 ≥ 300 点，含3年软件版本升级服务和远程技术支持服务；
- 2.支持虚拟化内核集成虚拟化安全防护功能模块，无需单独占用虚拟机资源安装安全防护功能模块；内置安全杀毒，无代理方式部署；
- 3.虚拟化管理平台支持批量对虚拟机开启杀毒功能；
- 4.支持主机防病毒补丁安装检测功能，能够检测所有主机防病毒补丁安装状态、IP地址、安装进度等，并可进行卸载，一键安装防病毒功能模块。

设备九：政务网区管理交换机

政务网区管理交换机技术要求

数量2台

- 1.整机交换容量 ≥ 3.36 Tbps；包转发率 ≥ 126 Mpps； ≥ 24 个千兆电口， ≥ 4 个千兆光口， ≥ 4 个千兆多模光模块；
- 2.支持CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；

- 3.支持虚拟化功能；包括堆叠链路冗余，负载分担、单点管理等功能；
- 4.支持零配置启动，CPU保护功能，支持设备内存及Flash容量查询功能；支持跨设备链路聚合，单一IP管理，分布式弹性路由；
- 5.支持802.1x认证，支持集中式MAC地址认证；
- 6.支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；
- 7.支持RRPP功能，支持OSPF FRR功能；最多8个端口聚合；支持最多128个聚合组；
- 8.支持链路聚合功能；
- 9.支持基于第二层、第三层和第四层的ACL；整机提供ACL条目数 ≥ 1 K条。

设备一十：政务网区带外管理交换机

政务网区带外管理交换机技术要求

数量1台

- 1.整机交换容量 ≥ 3.36 Tbps；包转发率 ≥ 126 Mpps； ≥ 24 个千兆电口， ≥ 4 个千兆光口， ≥ 4 个千兆多模光模块；
- 2.支持CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；
- 3.支持虚拟化功能；包括堆叠链路冗余，负载分担、单点管理等功能；
- 4.支持零配置启动，CPU保护功能，支持设备内存及Flash容量查询功能；支持跨设备链路聚合，单一IP管理，分布式弹性路由；
- 5.支持802.1x认证，支持集中式MAC地址认证；
- 6.支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；
- 7.支持RRPP功能，支持OSPF FRR功能；支持最多8个端口聚合；支持最多128个聚合组；
- 8.支持链路聚合功能；
- 9.支持基于第二层、第三层和第四层的ACL；整机提供ACL条目数 ≥ 1 K条。

设备一十一：互联网核心交换机

互联网核心交换机技术要求

数量2台

- 1.整机交换容量 ≥ 384 Tbps，转发性能 ≥ 72000 Mpps，业务板卡与交换网板采用完全正交设计，交换网板 ≥ 5 个；
- 2.配置主控引擎数量 ≥ 2 ，业务插槽数 ≥ 6 ，交流电源 ≥ 4 个；万兆光接口 ≥ 48 个，配置万兆光模块 ≥ 10 个；
- 3.支持防火墙、入侵防御系统等安全板卡扩展；
- 4.单槽位40G端口密度 ≥ 32 个；
- 5.支持40G/100G端口切换，切换后流量正常转发，不丢包；
- 6.多虚一技术(N:1)，支持4框虚拟化技术；
- 7.支持远程端口扩展，作为控制设备（Controlling Bridge,CB）实现对端口扩展模块（Port Extender, PE）的集中控制；
- 8.支持MACsec加密技术，支持MPLS Segment Routing 功能；
- 9.支持融合 AC 功能，无需额外配置单独硬件，在交换机上实现对AP 的接入控制和管理，有线无线用户的统一认证管理，最大 AP 上线数量为 12K，最大 Client 上线数量为 60K；
- 10.支持PC终端、哑终端、网络设备等连接元素的准入控制和权限划分，确保网络的可信可控；
- 11.支持Telemetry流量可视化功能；

12.支持 IPv4 Portal、IPv6 Portal 及 Portal 双协议栈功能，最大 Portal认证用户数量可达 256K。

设备一十二：互联网数据中心交换机

互联网数据中心交换机技术要求

数量2台

- 1.整机交换容量 $\geq 36\text{Tbps}$ ，包转发能力 $\geq 2000\text{Mpps}$ ；
- 2.配置万兆光接口 ≥ 24 个，100GE光接口 ≥ 6 个，Console口 ≥ 1 个；热插拔风扇模块 ≥ 3 个，前后或后前通风；模块化电源 ≥ 2 个；万兆光模块 ≥ 16 个；40G电缆 ≥ 1 个；
- 3.支持融合AC功能，可管理AP数 $\geq 1\text{K}$ ；
- 4.支持二层、三层Vxlan网关和BGP EVPN特性；
- 5.支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议；
- 6.支持跨设备链路聚合技术，端口转发时延小于2微秒；
- 7.支持sFlow，支持RoCE v2无损网络；
- 8.支持服务链Service chain功能；
- 9.支持黑洞MAC、动态ARP检测、ARP防攻击；
- 10.支持零配置技术，配置自动下发。

设备一十三：分布式块存储软件

分布式块存储软件技术要求

数量1套

- 1.采用分布式的软件定义存储架构，在通用服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点，使用管理平台统一管理，无需在计算虚拟化平台上部署存储控制器；
- 2.配置 ≥ 4 节点服务器全部物理CPU分布式块存储授权软件；
- 3.支持厚/精简配置；厚配置根据业务需求分配固定的物理存储空间、精简配置根据应用实际写需要时才分配相应的物理存储空间；
- 4.支持多种块存储协议，包括iscsi，RBD块存储协议，块存储支持快照功能，可支持创建可写快照；
- 5.支持混合磁盘分区特性，可将集群内所有SSD盘跨节点做一个快存储池，所有类型不同性能磁盘均可支持分区，包含SSD，SAS，SATA，NL-SAS等。

设备一十四：分布式文件存储软件

分布式文件存储软件技术要求

数量1套

- 1.采用分布式的软件定义存储架构，在通用服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点，使用管理平台统一管理，无需在计算虚拟化台上部署存储控制器；
- 2.配置 ≥ 4 节点服务器全部物理CPU分布式文件存储授权软件；
- 3.支持通过B/S管理界面对存储基础架构进行集中的配置，如存储资源池、集群、集群节点、磁盘等资源进行合理的划分和配置；
- 4.提供多种NAS增值服务功能，包括：权限管理、快照管理(WORM)、共享目录管理等；NAS服务可以采用多服务节点高可用，并支持负载均衡；
- 5.文件存储支持协议包括：FTP、CIFS、NFS、HTTP。

设备一十五：计算虚拟化软件

计算虚拟化软件技术要求

数量1套

- 1.配置 ≥ 4 节点服务器全部物理CPU计算虚拟化授权软件；
- 2.在管理平台管理界面上提供虚拟机启动、暂停、恢复、休眠、重启、关闭、克隆、迁移、删除、快照等功能批量操作；
- 3.在管理平台管理界面上提供集群HA（高可用），DRS（动态资源调度）等功能配置，无需界面跳转；
- 4.支持根据业务需求设置不同的虚拟机磁盘缓存模式，包括直接读写、一级缓存、二级缓存等；
- 5.具有存储精简配置能力（Thin Provisioning），减少存储容量的需求；
- 6.提供热添加CPU、内存、磁盘、网卡的功能，无需中断或停机即可实现虚拟资源的在线添加；
- 7.提供虚拟机回收站功能，统一管理被删除的虚拟机，防止因虚拟机误删除导致数据丢失，支持设置回收站文件保存周期，超期的文件将被自动删除；
- 8.支持批量修改虚拟机的配置参数，包括：I/O优先级、启动优先级、是否自动迁移、CPU调度优先级、CPU个数、内存大小、自动启动、VM启动设备、启用VNC代理、tools自动升级等；
- 9.具有合理的内存调度机制，能够实现内存的过量使用，保证内存资源的充分利用；
- 10.提供虚拟机快照功能，支持设置手工和定时快照将虚拟机磁盘文件和内存状态信息保存到镜像文件中；
- 11.支持将多个物理服务器组成集群，可基于CPU、内存、网络流量、存储容量、磁盘IO等资源利用率进行动态资源调度功能；
- 12.支持设置虚拟机磁盘IOPS及I/O速率的读写限制，虚拟机IP和虚拟网卡绑定，以防止地址篡改导致的审计问题；
- 13.虚拟机支持在线克隆为模板，模板制作过程中对业务运行无影响，同时虚拟机模板支持完整性验证与来源追溯，避免虚拟机模板文件被篡改的可能性，并追踪虚拟机模板的来源以及虚拟机模板部署的记录；
- 14.虚拟化软件内置备份模块，无需单独安装备份软件即可实现虚拟机全量、增量、差异备份功能。

设备一十六：互联网区智能加速卡

互联网区智能加速卡技术要求

数量1套

- 1.支持虚拟化的网络和存储IO都卸载到此硬件或者配置额外服务器实现；
- 2.提供两个10G端口，支持RDMA，Rocev2，支持聚合，采用专用的ASIC处理芯片和内存或者额外服务器实现，可以释放物理节点网络和存储消耗的CPU资源，提升CPU资源的利用率；
- 3.支持128字节转发性能达到10G以上（10G端口）；
- 4.支持网络二层直通和存储IO硬件加速，不消耗CPU资源；
- 5.计算虚拟化支持智能加速，虚拟交换机在智能网卡或者额外服务器上卸载，且支持虚拟机热迁移HA配置要求：配置相应的CPU授权许可；
- 6.可以在主CPU使用率低于2%的情况下提供分布式存储和网络功能。

设备一十七：互联网区云主机安全软件

互联网区云主机安全软件技术要求

数量1套

- 1.支持虚拟网络安全功能，可以提供公网IP、vLB、vFW、vRouter等功能，并支持部署虚拟NFV网元；
- 2.配置 ≥ 4 节点服务器网络安全虚拟化授权软件，不限制虚拟机数量；
- 3.支持公网IP地址池，支持公网IP和私网IP绑定，支持软件负载均衡；

- 4.提供虚拟网络设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性；
- 5.虚拟负载均衡支持HTTP、HTTPS、TCP等监听协议支持配置均衡算法（轮转算法，最小连接算法，源地址算法）。支持健康检查，可配置检查间隔、超时时长、重复次数等。
- 6.分布式防火墙基于监测虚拟机IP地址和端口进行东西向流量隔离控制；
- 7.在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。

设备一十八：互联网区云主机杀毒软件

互联网区云主机杀毒软件技术要求

数量1套

- 1.配置虚拟化linux服务器杀毒授权 ≥ 300 点，虚拟化Windows服务器杀毒授权 ≥ 300 点，含3年软件版本升级服务和远程技术支持服务；
- 2.支持虚拟化内核集成虚拟化安全防护功能模块，无需单独占用虚拟机资源安装安全防护功能模块；内置安全杀毒，无代理方式部署；
- 3.虚拟化管理平台支持批量对虚拟机开启杀毒功能；
- 4.支持主机防病毒补丁安装检测功能，能够检测所有主机防病毒补丁安装状态、IP地址、安装进度等，并可进行卸载，一键安装防病毒功能模块。

设备一十九：互联网区管理交换机

互联网区管理交换机技术要求

数量2台

- 1.整机交换容量 ≥ 3.36 Tbps；包转发率 ≥ 126 Mpps； ≥ 24 个千兆电口， ≥ 4 个千兆光口， ≥ 4 个千兆多模光模块；
- 2.支持CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；
- 3.支持虚拟化功能；包括堆叠链路冗余，负载分担、单点管理等功能；
- 4.支持RRPP功能，支持OSPF FRR功能，最多8个端口聚合；支持最多128个聚合组；
- 5.支持零配置启动，CPU保护功能，支持设备内存及Flash容量查询功能；支持跨设备链路聚合，单一IP管理，分布式弹性路由；
- 6.支持链路聚合功能；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；
- 7.支持802.1x认证，支持集中式MAC地址认证；
- 8.支持基于第二层、第三层和第四层的ACL；整机提供ACL条目数 ≥ 1 K条。

设备二十：互联网区带外管理交换机

互联网区带外管理交换机技术要求

数量1台

- 1.整机交换容量 ≥ 3.36 Tbps；包转发率 ≥ 126 Mpps； ≥ 24 个千兆电口， ≥ 4 个千兆光口， ≥ 4 个千兆多模光模块；
- 2.支持CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；
- 3.支持虚拟化功能；包括堆叠链路冗余，负载分担、单点管理等功能；
- 4.支持RRPP功能，支持OSPF FRR功能，最多8个端口聚合；支持最多128个聚合组；
- 5.支持零配置启动，CPU保护功能，支持设备内存及Flash容量查询功能；支持跨设备链路聚合，单一IP

管理，分布式弹性路由；

6.支持链路聚合，支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；

7.支持802.1x认证，支持集中式MAC地址认证；

8.支持基于第二层、第三层和第四层的ACL；整机提供ACL条目数≥1K条。

设备二十一：运维管理交换机

运维管理交换机技术要求

数量2台

1.整机交换容量≥6.88Tbps；包转发率≥297Mpps；

2.配置≥24个千兆电口，≥4个万兆光口，≥4个万兆多模光模块，冗余电源、风扇；

3.支持静态路由、RIPv1/v2，RIPng、OSPFv1/v2，OSPFv3、BGP4，BGP4+ for IPv6、IS-IS，IS-IS v6、VRRP/VRRPv3、支持等价路由，策略路由；

4.实现ERPS功能，能够快速阻断环路，链路收敛时间≤50ms；

5.支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；

6.支持RSTP功能：收敛时间≤50ms；

7.实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；

8.支持出方向ACL，以便于灵活实现数据包过滤，支持802.1x认证，支持集中式MAC地址认证；

9.最大VLAN数(不是VLAN ID)≥4094。

设备二十二：政务网出口入侵防御软件

政务网出口入侵防御软件技术要求

数量2套

1.提供≥5年入侵防御特征库升级软件；

2.提供≥5年防病毒特征库升级软件；

3.提供≥5年行为审计特征库升级软件；

4.系统定义超过8000+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型；并支持在线升级和手动升级

5.支持基于常见协议进行异常检查，包括但不限于：HTTP、HTTPS、DNS、SMTP、POP3、FTP；检查内容支持自定义，包括但不限于：url长度、请求长度、目录长度、host字段、version字段、字符检测、文本长度、文件名长度、命令参数长度，支持针对每个协议设置处置动作和事件等级。

6.支持IPS日志聚合，可按照源IP、目的IP、防护规则和源目的IP等维度进行聚合，方便管理员快速进行攻击事件统计和回溯。

7.支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户。

8.支持弱密码扫描能力，可针对IP、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。

设备二十三：互联网出口入侵防御软件

互联网出口入侵防御软件技术要求

数量2套

1.提供≥5年入侵防御特征库升级软件；

2.提供≥5年防病毒特征库升级软件；

- 3.提供≥5年行为审计特征库升级软件；
- 4.系统定义超过8000+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型；并支持在线升级和手动升级
- 5.支持基于常见协议进行异常检查，包括但不限于：HTTP、HTTPS、DNS、SMTP、POP3、FTP；检查内容支持自定义，包括但不限于：url长度、请求长度、目录长度、host字段、version字段、字符检测、文本长度、文件名长度、命令参数长度，支持针对每个协议设置处置动作和事件等级。
- 6.支持IPS日志聚合，可按照源IP、目的IP、防护规则和源目的IP等维度进行聚合，方便管理员快速进行攻击事件统计和回溯。
- 7.支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户。
- 8.支持弱密码扫描能力，可针对IP、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。

设备二十四：互联网web应用防火墙设备

互联网web应用防火墙设备技术要求

数量1台

- 1.整机应用层吞吐量≥3Gbps，最大并发数≥100W；≥6个千兆电口，≥4个千兆光口；
- 2.支持自动发现网络环境中存在的Web业务系统，记录服务器的IP、Port、域名等信息
- 3.支持对HTTP请求关键字段进行合规性的检测（包括Host字段、User-Agent、Content-type字段等）
- 4.在单个服务器通过相同的IP地址为多个HTTPS域名提供服务时，WAF可以通过启用SNI，准确确定域名与证书的对应关系。
- 5.支持对跨站脚本(XSS)和注入式攻击（包括SQL注入、命令注入、代码注入、文件注入、LDAP注入、SSI注入等）的检测防护。
- 6.支持源地址识别，部署在SSL网关后面，能够解析到真实的访问者IP，并能对真实的IP进行防护和阻断。
- 7.支持透明串接和旁路反向代理下的HTTPS业务的安全防护。
- 8.支持ipv4/ipv6双协议栈。
- 9.支持集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS。
- 10.支持客户端安全防护，插入特殊的HTTP报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受Clickjacking攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）、X-XSS-Protect（用于当检测到XSS攻击时，指示浏览器停止加载页面）、Content-Security-Policy（用于降低浏览器上的XSS风险和注入攻击）

设备二十五：互联网web应用防火墙软件

互联网web应用防火墙软件技术要求

数量1套

- 1.提供≥5年WAF特征库升级软件；
- 2.能够检测防止服务器导致的信息泄露行为，包括：目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等信息泄露行为
- 3.内置安全规则可有效识别Acunetix、nessus、WebScan、Webdump、AppScan、等扫描器的扫描行为

4.支持多种盗链识别算法能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问

5.支持Cookie自学习支持Cookie防篡改、防劫持支持Cookie防篡改、防劫持

6.可基于时间设置对客户端IP放行、阻断或检测。

设备二十六：流量探针

流量探针技术要求

数量1台

1.≥20GE RJ45 Ports 2GE RJ45 or SFP Shared Ports;

2.吞吐量≥7.0G，并发会话数≥200W；

3.支持网关部署、透明部署、旁挂部署；流量镜像；

4.支持自带终端识别特征库，可识别设备的系统、主机名称等；

5.自带IPS、AV应用特征库，可自动威胁情报中心更新特征，可识别攻击流量，形成攻击日志，支持https证书卸载。

设备二十七：互联网上网行为管理与审计机

互联网上网行为管理与审计机技术要求

数量1台

1.硬件接口要求：≥12个千兆电口，≥12个千兆光口，≥2个万兆光口；应用层吞吐量≥15Gbps；

2.应用特征不少于7000个，移动应用不少于2200个。

3.支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持DNS域名学习模式，可引用数据包特征中的目标域名或指定域名。

4.支持IPv6策略路由、OSPFv3、静态路由、IPv6隧道，包括IPv6手工隧道、ISATAP、6to4等隧道模式；支持IPv6网络下的DHCPv6、DNSv6、SNMPv6、NTPv6、PPPoE等基础协议。

5.支持根据标签选择应用，预置标签分类至少包含安全风险、高带宽消耗、降低工作效率等11大类；支持根据标签选择一类应用做控制。

6.支持应用智能识别，有效识别P2P和迅雷行为，识别模式可选择严格、适中、宽松，支持排除扫描端口。

7.支持智能识别模式和快速识别模式，在智能识别模式下应用引擎尽可能地用各种方式识别网络流量，在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能。

8.支持针对搜索引擎、HTTP、网页内容进行关键字过滤并实时生成日志记录，日志级别包括但不限于紧急、告警、严重、通知、信息、调试、不记录等，方便管理员快速区分用户上网行为属性和定位日志级别。

9.支持针对虚拟账号进行黑白名单管理，设定允许登录的QQ账号白名单或禁止登录的QQ账号黑名单。

10.可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（ZIP、RAR、GZ、BZ2、Z、THZ、TBZ、7Z、CAB、BZ等）、应用程序、OFFICE系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。

11.内置URL分类库，支持≥56个URL分类，URL库可在线升级。

设备二十八：互联网上网行为管理与审计软件

互联网上网行为管理与审计软件技术要求

数量1套

1.提供≥5年应用识别特征库升级软件；

- 2.支持基于DNS前置技术实现在DNS解析阶段针对HTTP和HTTPS域名进行过滤，防止HTTPS域名过滤逃逸情况。
- 3.支持在设备旁路部署时针对违规上网行为进行阻断过滤。
- 4.支持配置解密策略，包括入接口、源地址对象、目的地址对象、HTTPS对象、域名排除等；支持HTTP S域名库，预定义域名以及自定义域名；支持针对SSL解密证书进行自动推送。
- 5.支持基于用户、地址、服务、应用、时间、VLAN等匹配条件进行流量控制；并支持配置保障带宽、最大带宽、每IP带宽、每用户带宽、带宽优先级等QoS动作。
- 6.支持至少8种认证方式，至少包含本地认证、短信网关认证、LDAP认证、AD域登录、微信公众号认证、IC卡认证、APP小程序认证、扫描二维码认证等多种认证方式。
- 7.支持通过解析HTTP流量包，可以获取用户名、IP地址和MAC地址信息等，进而实现无认证实名上线功能。

设备二十九：运维审计机

运维审计机技术要求

数量1台

- 1.机架式硬件架构，冗余交流电源， $\geq 4T$ 硬盘容量， ≥ 6 个以太网千兆电口， ≥ 4 个以太网千兆光口，支持 ≥ 1 个接口扩展槽位；
- 2.最大图形并发连接数 ≥ 200 ，最大字符并发连接数 ≥ 700 ，支持双因素组合认证， ≥ 2 个双因子认证授权。
- 3.支持 ≥ 500 个资产的管理能力。
- 4.支持集群部署模式，中心采用HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中查询、实时会话集中监控，以满足业务增长需求。
- 5.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。
- 6.支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据。
- 7.支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具。
- 8.支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出。
- 9.支持设备帐户和密码的自动登录、手工登录、二次自动登录模式。
- 10.持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能。
- 11.支持自动同步LDAP/AD用户，至少支持与吉大正元、LDAP和AD等系统进行联动，同步后可直接登录堡垒机。
- 12.支持可直接使用本地的运维工具等堡垒机，至少支持SecureCRT、winscp等客户端工具。

设备三十：漏洞扫描机

漏洞扫描机技术要求

数量1台

- 1.软硬件一体化产品，硬盘 $\geq 2T$ ，内存 $\geq 16G$ ，配备至少6个100/1000M自适应电口，USB口 ≥ 2 。
- 2.配置Web漏扫功能， ≥ 128 个IP扫描数量。
- 3.支持对各种网络主机、操作系统、网络设备(如交换机、路由器、防火墙等)、常用软件以及应用系统的识别和漏洞扫描。
- 4.支持云平台扫描，漏洞覆盖OpenStack、Kvm、VMware、Xen等主流的云计算平台，
- 5.用户可自定义扫描范围、定义扫描端口、扫描使用的参数集等具体扫描选项。

- 6.可以自定义扫描端口范围、端口扫描策略;
- 7.提供采用SMB、SSH、Telnet、RDP、SNMP等协议对Windows、Linux系统进行登录授权扫描。
- 8.具备弱口令探测功能,支持弱口令探测协议至少17种,至少包括SSH、TELNET、MSSQL、DB2、Oracle、MySQL、FTP、POP3、SMB、RDP、SMTP、IMAP、Sybase、Rlogin、Weblogic、Tomcat、SNMP等协议进行弱口令探测。
- 9.支持发现非默认端口启动的服务,支持服务的协议识别、版本。
- 10.支持对误报的漏洞进行修正,避免将误报结果导出。
- 11.端口扫描支持TCP CONNECT、TCP SYN、TCP FIN、TCP ACK、TCP Window等多种方式;
- 12.在资产管理页面可直接对单个资产或批量资产下发扫描任务。

设备三十一:漏洞扫描软件

漏洞扫描软件技术要求

数量1套

- 1.提供5年漏洞扫描特征库升级软件;
- 2.分布式部署可以随机分配扫描引擎,也可指定扫描引擎;
- 3.漏洞知识库支持自定义编辑,可编辑漏洞描述、修复建议、漏洞等级等内容,在扫描结果和导出报告中应展示编辑后的内容;
- 4.同IP不同端口同漏洞的结果应明确给予端口标识;
- 5.产品提供Web应用漏洞扫描功能,包括SQL注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、URL跳转、文件包含、文件上传、信息泄露等。支持OWASP TOP10等主流安全漏洞

设备三十二:安全态势感知平台系统软件

安全态势感知平台系统软件技术要求

数量1套

- 1.支持通过多种类型的安全、泛安全类数据接入采集,应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据;
- 2.支持通过流量采集设备采集接入全流量数据,包含流量中的请求包和返回包等信息,并可在数据检索中体现包信息;
- 3.支持SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode等6000种以上漏洞利用检测规则,可针对任意单条规则进行启用和禁用;
- 4.支持通过单条告警、聚合告警、归并告警添加白名单,快速过滤误报;支持通过配置模型名称、告警名称、IP、URL等告警字段生成白名单策略;
- 5.支持与不同品牌的网关类安全产品进行联动防护,防护策略支持设置每次阻断不同时长生效时间,时间设置包括10分钟,30分钟,24小时,72小时,7天,15天,30天,3个月,永久阻断,支持将安全策略同步下发至多台联动设备。
- 6.支持全网安全态势感知大屏幕展示功能,大屏幕内容应包含攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个视角,大屏不少于10块。
- 7.支持选择生成报告时间范围、显示TOP、导出文件类型、报告名称;支持自定义报告统计条件,包括统计业务范围、告警威胁等级、告警处置状态、告警结果等;
- 8.平台提供三权分立用户管理角色,配置员、用户管理员、操作审计员相互独立,支持根据不同角色分配平台功能权

设备三十三:安全态势感知探针

安全态势感知探针技术要求

数量2套

- 1.软硬一体化架构；五年服务；
- 2.支持通过原始网络流量分析异常流量事件；
- 3.支持异常流量事件统计；
- 4.支持按照威胁等级统计异常流量事件；
- 5.支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和IP，管理中心可实现告警统一管理；可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数；
- 6.支持自定义探测器配置项是否与管理中心保持同步。

设备三十四：网页防篡改软件

网页防篡改软件技术要求

数量1套

- 1.采用内核文件驱动、Web核心内嵌双重机制结合；
- 2.基于特征码、模糊Hash、脚本虚拟机动态检测Webshell；
- 3.一键启停所有对监控端的保护；
- 4.支持基于目录、进程、IP、用户等进行设置篡改规则；
- 5.支持各类网页文件的保护，包括静态和动态网页以及各类文件信息；
- 6.支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码；
- 7.将容器镜像内目录保护后，任何以该镜像创建的容器内的目录都将被保护；
- 8.支持设置子目录白名单和进程白名单。

设备三十五：安全隔离与信息交换机

安全隔离与信息交换机技术要求

数量1台

- 1.网口：内外网各≥6GE，2个接口卡扩展插槽；USB接口≥4个 USB2.0管理口≥2个 RJ45串口电源配置：双电源；双液晶屏
 - 2.支持接口冗余模式设置包括：轮询、热备、链路聚合协议、自适应均衡、选择均衡、广播模式、传输均衡。
 - 3.设备内、外主机与客户网络建立会话并提取通信数据，内部使用私有协议交换数据，屏蔽共有协议存在的风险。
 - 4.产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。
 - 5.支持SMB、FTP、NFS、FTPS、SFTP文件传输协议。
 - 6.支持基于私有文件传输协议的的主动文件交换功能，采用国密算法加密通信数据，支持优先级、文件并发数设置。
- 支持视频流多机负载均衡，可把视频流按算法分配给多台设备进行处理，解决物理带宽限制。
- 7.支持基于pSIP协议的警用数字集群通信，实现警用PDT对讲机与交换中心数据互通，支持语音呼叫、消息实时传输。
 - 8.支持TCP应用层数据单向传输的控制，保证TCP应用数据的0反馈，以满足二次防护对数据传输的安全性需求
 - 9.支持自定义的TCP、UDP协议的数据隔离交换，以用户定制的命令、参数等来限定隔离通道内的数据

内容。

10.支持带内管理，可通业务口进行网闸管理工作，用户可自行选择是否启用多口管理。

设备三十六：运维管理平台服务器

运维管理平台服务器技术要求

数量1台

1.配置≥2颗Intel CPU主频2.4GHz 10核；

2.内存配置容量≥128GB DDR4，最高速率2933MT/s，内存插槽可扩展不≥24个，官方支持最大内存容量≥3.0TB；

3.配置≥3个1.2T 10K SAS企业级热插拔硬盘，最大可配置硬盘数量≥40块；

4.配置缓存≥2GB，支持RAID0/1/10/5/6/50/60/1E，支持缓存数据保护，且后备保护时间不受限制；最高可选支持≥8GB缓存，支持超级电容保护；

5.配置≥4端口千兆接口；

6.提供≥3年维保服务；

7.标准机架式服务器，高度≥2U；

8.支持前置/内置NVMe硬盘，最高支持≥32块NVMe硬盘；

9.配置≥1G独立的远程管理控制端口，支持远程的开机、关机、重启、更新Firmware、虚拟光驱、虚拟文件夹等操作；

10.支持双宽GPU≥3块；支持机箱入侵检测，TCM/TPM安全模块；

11.可选配置PCIe防护模块，提供防火墙、防病毒等防护功能；

12.配置热插拔的冗余电源，功率≥550W，支持96%能效比的钛金级电源选项。

设备三十七：终端安全准入认证机

终端安全准入认证机技术要求

数量1套

1.硬件一体化专用设备，外观尺寸≥2U，最大支持≥20000点授权，实配≥100点终端认证授权；

2.支持802.1x、EoU、Portal、端口镜像、策略路由、设备指纹准入等多种控制方式，并可以混合使用，且支持无代理方式，适应有线、无线、远程分支机构接入、NAT等多种复杂网络环境；

3.支持系统内置账号认证、微软AD域帐号、LDAP帐号认证、邮件服务器账号认证、第三方Radius服务器认证、第三方扩展认证。

4.支持对接入设备指定相应的绑定规则，根据接入设备是否符合接入规则来决定允许或拒绝其接入，防止仿冒终端接入，如基于计算机IP/MAC、交换机端口、接入控制点设备等进行灵活绑定，并且可支持一对多、一对一、多对一、多对多进行绑定。

5.支持自动识别指定AD域和邮件服务器的PC，自动准入发现并下发权限控制策略。

6.支持对免检设备进行仿冒检查，可支持基于设备行为特征的仿冒检查，并可将仿冒设备隔离。

7.支持AD域环境，无需安装任何客户端。支持Windows设备安全检查，其中包括防病毒软件检查、终端是否加域检查、终端系统补丁检查、终端服务安装检查、终端软件及软件组检查。

8.支持Windows设备安全检查，其中包括防病毒软件检查、终端启用Guest账号检查、终端弱口令账号检查、终端是否加域检查、终端共享目录检查、终端系统补丁检查、终端系统版本检查、终端服务安装检查、终端防火墙检测和终端主机名检查。

9.支持Linux操作系统安全检查，其中包括防病毒软件检查、进程运行检查、软件、软件组配置检查、终端防火墙检查、屏保检查。

10.支持MacOS安全检查，其中包括防病毒软件检查、软件安装检查、终端是否加域检查、进程运行检

查、软件、软件组配置检查和屏保检查。

设备三十八：终端杀毒软件

终端杀毒软件技术要求

数量1套

- 1.须拥有完全国产自主知识产权杀毒引擎，防止产品后门和用户敏感信息外泄等隐患；
- 2.实际配置≥5年200点终端授权；
- 3.支持Windows/Linux/国产操作系统；
- 4.支持全盘扫描、快速扫描、自定义扫描等多种扫描方式；
- 5.支持目录白名单、文件哈希白名单；
- 6.提供外联检测机制，发现违规外联能够设置告警、断网等违规处理手段；
- 7.支持采集终端基础信息，包括终端名称、IP地址、MAC地址、健康状态、硬件架构、操作系统、组件等信息；
- 8.支持对引导区、内存、脚本、压缩包、宏病毒等进行威胁检测；
- 9.管理平台支持以组织架构的方式管理全网终端，能够显示终端基本信息（包括终端名称、IP、MAC、健康状态等）；终端资产支持显示终端详情包括性能、硬件、软件、进程、网络、漏洞等；包括策略分发、卸载、关机、重启、消息分发、隔离、取消隔离、误杀恢复等；
- 10.管理平台具备开放性接口，支持第三方态势分析平台接口联动。

设备三十九：政务服务网备份存储服务器

政务服务网备份存储服务器技术要求

数量1台

- 1.配置≥2个控制器；
- 2.处理器：配置≥4颗处理器；
- 3.缓存：：配置≥24GB缓存，存储系统掉电无需电池进行保护；
- 4.配置≥8个16G FC接口；
- 5.硬盘：配置≥10块8T 12G SAS硬盘；
- 6.硬盘类型：支持SSD、SAS、NL-SAS；
- 7.RAID 级别：支持RAID1、5、6、10。

设备四十：机柜

机柜技术要求

数量4台

- 1.机柜尺寸（高度×宽度×深度）≥2000×600×1200mm，容量≥42U；前门单开门，后门双开门。兼容19"国际标准；
- 2.机柜板材需采用强度A级及以上碳素冷轧钢板和镀锌板，网孔门材料≥1.2mm；立柱材料≥2.0mm；
- 3.机柜内部设备的有效安装深度≥750mm。PDU或插座不能阻挡服务器设备的安放；
- 4.机柜采用框架结构设计，整个柜体承重≥800KG，前后门采用网孔门设计，适应服务器高热密度的散热需求；
- 5.机柜表面颜色为黑色；整体防护等级应≥IP20；
- 6.外形尺寸偏差应符合JB/T6753.5-93所规定的A级及以上要求，机柜应方正、不歪斜，机柜六面互相垂直；
- 7.配置≥4条PDU，每个PDU含≥8个国标10A三脚插座和，同时PDU需配置总输入保护开关、防雷模块。

设备四十一：笔记本电脑

笔记本电脑技术要求

数量2台

显示器≥13.3英寸，内存≥16GB,净重≤1kg，电源续航≥8小时，CPU≥4核处理器；支持100W PD快充，支持8K视频输出或双路4K视频输出，搭配国产办公软件。

设备四十二：台式电脑

台式电脑技术要求

数量3台

显示器≥27英寸，内存≥16GB，硬盘≥512GB SSD固态硬盘，CPU≥12核处理器，操作系统win11，搭配国产办公软件。

设备四十三：打印一体机

打印一体机技术要求

数量1台

黑白激光多功能数码复合机 纸张尺寸：A5R-A3,纸张容量≥600张，预热时间≤20秒，复印类型：自动批量双面复印，可双面打印；（免费上门安装+保修）。

设备四十四：投影仪

投影仪技术要求

数量1台

语音遥控，支持3D功能，LED，桌上正投；吊装正投；吊装背投；桌上背投，80-120英寸，支持Wi-Fi连接，网络接口，支持幕布自适应，支持智能避障，腾讯，CIBN等。

设备四十五：智慧屏

智慧屏技术要求

数量1台

86寸智慧屏尺寸/背光类型:D-LED/屏幕扫描频率:60Hz/整机分辨率:7680 × 4320/亮度≥300nit/可视角:≥178°/色域(NTSC):85% NTSC (TYP) /低蓝光/钢化玻璃/全贴合/处理器≥4核；内存(RAM) ≥16GB;存储(ROM) ≥128GB。

设备四十六：辅助材料

辅助材料技术要求

数量1项

OM4 LC-LC 10光纤连接线≥50条、六类5米成品跳线≥50条、六类10米成品跳线≥50条、标签机≥1台、色带≥10个，绑带，网络工具箱≥1套，标配+108件工具箱 ≥1套。

四十七：安全运维内容

安全运维内容技术要求

数量1项

1.集约化平台运维内容

开展集约化平台系统更新升级、技术支持、系统维护、软件升级、补丁程序提供、故障检测、性能优化等工作。帮助用户诊断并解决其在使用产品过程中出现的有明显症状的，可能由产品导致的技术问题。定期进行功能维护，及时发现和排除潜在问题或故障隐患，保证系统的稳定运行。在运维期内提供产品升级。对集约化平台硬件设备运行状况、软件运行状况、备份系统状况等的故障检测。有序优化集约化平台系统架构和服务器资源配置，保障集约化平台软件及功能模块正常稳定安全高效运行，提升平台响

应速度。协助用户做好平台软件及功能模块和数据的日常备份。定期开展性能排查及调优。

2. 市政府机房安全运维内容

本次项目安全运维的内容指在实现市政府机房安全防护。投标人根据等级保护2?0安全框架下“一个中心三重防护”的理念，以公安部信息安全等级保护三级为标准进行平台安全建设，为云平台环境及云上业务应用系统提供完整的一站式安全方案，覆盖云安全管理平台，云安全能力（访问控制、入侵防御、恶意代码防范、运维审计、终端安全管理、虚拟机微隔离等），通过建设统一的安全资源池，为用户提供一个安全可视、可控、安全资源自动化部署、弹性扩展、平台开放的一体化安全资源方案，全方位构建事前预防、事中响应、事后审计的安全保障体系；建设安全态势感知平台，结合安全日志、威胁情报进行关联分析，实现网络安全通报预警、分析研判、攻击溯源、事件应急。在各项安保任务期间，协助用户做好安保任务期间信息系统保障方案，做好现场值守和远程技术支持，确保各项安保任务期间系统运行正常、稳定。定期开展系统巡检，重点检测平台安全设备性能、网络带宽性能、服务器承载性能等。定期对云平台的受管服务器设备及网络设备进行漏洞扫描、补丁升级等、安全设备防攻击、防病毒库进行升级等，记录发生的安全问题，对发现的安全隐患及时进行修补，对可能的安全问题进行预警，并提出安全规划建议。

3. 网络链路服务运维内容

保障市政府集约化平台和机房网络稳定性，并按照常规网站流量出口对网络带宽进行估算，支持互联网和政务外网的接入访问，保证在任何时刻的网络畅通。

四十八：安全运维指标

安全运维指标技术要求

数量1项

1. 中标方针对本项目成立专门的维护小组，建立考核标准和质量管理办法，保证运维工作的质量和水平，做到运维工作标准化、可管理、可监督。提供不少于10人的安全运维人员，其中至少2人员必须经过专业的培训和认证考试（如：CISP、CISSP等安全专业认证），至少不低于5年的工作经验，统筹和协助甲方处理安全事件及日常运维。
2. 为用户提供所涉及的硬件设施及软件的相关安全维护支持工作，帮助用户诊断并解决由于本次采购软硬件系统产品产生的任何故障，提供7×24小时的故障服务受理，半小时到达现场，到达后8小时内排除故障，恢复业务运行。若现场运维人员无法解决，将由技术专家赶赴现场或者远程解决，要求在发生故障时间点之后24小时内排除故障。
3. 建立突发事件应急管理措施，保证突发事件发生后半小时内人员到位并及时处理。参与/开展网络安全演练，并制定应急预案和应急处置机制，进而在真正的安全事件发生时实现有序处置。
4. 建立定期巡检制度，每季度巡检一次，保证平台正常使用。安排资深项目工程师进行巡检，对系统运行情况进行定期检查、优化，通过采取预防措施，对潜在的故障点进行分析诊断，达到预防目的。每次巡检后，向本项目使用单位提供《巡检报告》，巡检内容包含但不限于硬件状态、超融合软件状态、操作系统等。
5. 在重点安保任务期间，做好系统保障方案，加强专人值班值守，落实报备报告制度，保障机房各系统高效、安全、稳定运行；专人值守期间，同时要组织第三方技术单位落实技术值守支撑保障，提供7×24小时电话、远程等多种方式的技术支持，必要时提供技术人员驻场。
6. 中标方的运维工程师随时接听技术咨询电话，了解系统故障现象，远程帮助客户分析故障产生的原因，指导客户处理故障，并提出如何进行事故预防。解决客户的紧急技术需求问题。
7. 中标方配合用户做好云平台和各业务系统安全测评和安全整改、迁云等工作。

四十九：安全运维服务

安全运维服务技术要求

数量1项

- 1.提供免费的产品升级，包括产品的纠错性、适应性、预防性与完善性维护。对应用系统的产品部分，提供对程序BUG的修补，由于程序的问题，会在系统进行修补后随时向用户免费提供，并按照故障解决的时限性不断将问题提升，直至得到完全解决。针对集约化平台系统实际使用情况及相关要求提供系统软件功能的软件改进和升级，对产品的纠错性、适应性、预防性与完善性维护，提供具有新增功能的软件产品、提供主要维护版本的更新软件产品、提供软件修补包(PatchFixes)及替代方法(workarounds)。
- 2.提供包括对集约化平台各硬件运行状况、软件运行状况、备份系统状况等的故障检测。
- 3.提供全市性业务技术培训。
- 4.中标方所提供硬件设备需3年原厂维保；所提供系统软件需提供3年免费升级；所提供产品特征库需5年在线升级。

设备五十：政务网区云IaaS资源池设备

政务网区云IaaS资源池设备技术要求

数量1套

- 1.配置至少4节点服务器，单节点配置要求：X86机架式服务器，CPU物理核≥96核，主频≥2.3GHz；内存：≥256G DDR4；硬盘：≥3*480GB SSD，≥2*1.92TB NVMe SSD，≥6*8TB HDD；≥2G缓存RAID卡（含掉电保护模块）；≥4个万兆光接口（含4个万兆光模块），≥4个千兆电接口；冗余电源；提供三年原厂质保服务；
- 2.对硬件可靠性、系统可靠性、服务可靠性三大层面进行实时监控和分层监控，实现对计算、存储、网络、安全等资源的统一管理运维；
- 3.管理平台内置在线p2v、v2v迁移工具，支持业界主流的操作系统、公有云平台、虚拟化平台。包括但不限于VMware、华为、Hyper-V等平台的迁移功能，提升被迁移业务平台的普适性、降低业务上云的难度，降低运维工作量；
- 4.可视化实时监控中心，可视化实时监控中心从硬件可靠性（包括CPU、内存、磁盘、物理网卡和Raid卡）、系统可靠性（包括集群主机、分布式存储、集群网络配置状态和集群资源过载状态）、服务可靠（包括站点容灾、集群可靠性HA、应用HA、计算资源DRS、虚拟机运行状态和虚拟机备份）三大层面进行实时监控、分层展示，运维人员可以直观查看集群的整体运行情况，可以快速诊断集群的健康状态；
- 5.在统一的管理平台上即可实现对计算、存储、网络、安全等资源的统一管理运维，无需界面跳转即可实现全部操作，简化运维工作，降低运维成本；
- 6.虚拟化软件内置备份模块，无需单独安装备份软件即可实现虚拟机全量、增量、差异备份功能，备份时对业务运行无影响，支持按时间设置自动化备份策略，备份策略可细化到分钟级；
- 7.支持虚拟机迁移历史记录功能，记录中包含迁移的操作员、迁移方式、源主机、目的主机、开始时间、迁移耗时等信息，便于对虚拟机的迁移路径进行回溯；
- 8.当虚拟机Windows、Linux操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性。

设备五十一：政务网区云备份一体机

政务网区云备份一体机技术要求

数量1台

- 1.最大支持可用容量288TB，配置6*8T容量，实配可用容量32TB授权

- 2.配置≥2颗10核处理器；≥128GB以上内存，万兆光接口≥4个,千兆电接口≥2个
- 3.备份客户端支持部署在Windows、Linux、Solaris等操作系统，以及基于龙芯、飞腾、海光、兆芯、申威、华为鲲鹏处理器架构下的银河麒麟和统信UOS操作系统等国产操作系统
- 4.支持主流的数据库在线备份恢复，包括：Oracle、SQL Server、MySQL、Sybase、DB2、Caché、SAP HANA等主流数据库应用
- 5.支持在线备份Windows、Linux平台的操作系统及卷数据。支持Windows操作系统在裸机恢复过程中提供驱动程序更换界面，允许客户针对不同的硬件驱动程序做恢复现场的替换。支持Linux操作系统备份和裸机恢复，支持原机恢复和异机恢复
- 6.支持通过挂载方式实现Oracle、SQL Server、MySQL数据库的挂载恢复，挂载方式必须支持iSCSI、FC协议进行挂载
- 7.支持对Oracle、SQL Server、MySQL、DB2、达梦、人大金仓、神舟通用等主流数据库的备份数据进行定时容灾演练，符合等级保护的要求以检验备份集的可用性
- 8.支持Exchange、Exchange数据库可用性组的完全备份、增量备份、日志备份与恢复
- 9.支持VMware、Hyper-V、H3C CAS、OpenStack、CNware、RHV、腾讯云Tstack、浪潮云等虚拟化平台或云平台的备份恢复
- 10.主库支持数据库的物理备份与数据库复制功能同时启用。既保障数据库物理故障能启用备库应急，又保障逻辑故障时能使用备份数据进行恢复
- 11.支持对远程复制进行流量控制，合理控制带宽资源。支持对数据传输和存储进行加密，提升传输过程以及存储的安全性。具备断点续传特性，当远程复制过程中出现中断时，恢复正常后可基于上一次断点处进行续传
- 12.支持将对象存储的数据备份到本地存储中，实现O2D、O2T、O2O。支持完全备份、增量备份、合成备份与恢复，支持恢复到Linux、Unix、Hadoop分布式文件系统（HDFS）中，实现对象存储数据在不同文件系统中的转换恢复，并且支持单文件细粒度的备份和恢复。

设备五十二：互联网区IaaS资源池设备

互联网区云IaaS资源池设备技术要求

数量1套

- 1.配置至少4节点服务器，单节点配置要求：X86机架式服务器，CPU物理核≥96核，主频≥2.3GHz；内存：≥256G DDR4；硬盘：≥3*480GB SSD，≥2*1.92TB NVMe SSD，≥6*8TB HDD；≥2G缓存RAID卡（含掉电保护模块）；≥4个万兆光接口（含4个万兆光模块），≥4个千兆电接口；冗余电源；提供三年原厂质保服务；
- 2.对硬件可靠性、系统可靠性、服务可靠性三大层面进行实时监控和分层监控，实现对计算、存储、网络、安全等资源的统一管理运维；
- 3.管理平台内置在线p2v、v2v迁移工具，支持业界主流的操作系统、公有云平台、虚拟化平台。包括但不限于VMware、华为、Hyper-V等平台的迁移功能，提升被迁移业务平台的普适性、降低业务上云的难度，降低运维工作量；
- 4.可视化实时监控中心，可视化实时监控中心从硬件可靠性（包括CPU、内存、磁盘、物理网卡和Raid卡）、系统可靠性（包括集群主机、分布式存储、集群网络配置状态和集群资源过载状态）、服务可靠性（包括站点容灾、集群可靠性HA、应用HA、计算资源DRS、虚拟机运行状态和虚拟机备份）三大层面进行实时监控、分层展示，运维人员可以直观查看集群的整体运行情况，可以快速诊断集群的健康状态；
- 5.在统一的管理平台上即可实现对计算、存储、网络、安全等资源的统一管理运维，无需界面跳转即可

实现全部操作，简化运维工作，降低运维成本；

6.虚拟化软件内置备份模块，无需单独安装备份软件即可实现虚拟机全量、增量、差异备份功能，备份时对业务运行无影响，支持按时间设置自动化备份策略，备份策略可细化到分钟级；

7.支持虚拟机迁移历史记录功能，记录中包含迁移的操作员、迁移方式、源主机、目的主机、开始时间、迁移耗时等信息，便于对虚拟机的迁移路径进行回溯；

8.当虚拟机Windows、Linux操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性。

设备五十三：互联网备份一体机

互联网备份一体机技术要求

数量1台

1.最大支持可用容量288TB，配置6*8T容量，实配可用容量32TB授权

2.配置≥2颗10核处理器；≥128GB以上内存，万兆光接口≥4个,千兆电接口≥2个

3.备份客户端支持部署在Windows、Linux、Solaris等操作系统，以及基于龙芯、飞腾、海光、兆芯、申威、华为鲲鹏处理器架构下的银河麒麟和统信UOS操作系统等国产操作系统

4.支持主流的数据库在线备份恢复，包括：Oracle、SQL Server、MySQL、Sybase、DB2、Caché、SAP HANA等主流数据库应用

5.支持在线备份Windows、Linux平台的操作系统及卷数据。支持Windows操作系统在裸机恢复过程中提供驱动程序更换界面，允许客户针对不同的硬件驱动程序做恢复现场的替换。支持Linux操作系统备份和裸机恢复，支持原机恢复和异机恢复

6.支持通过挂载方式实现Oracle、SQL Server、MySQL数据库的挂载恢复，挂载方式必须支持iSCSI、FC协议进行挂载

7.支持对Oracle、SQL Server、MySQL、DB2、达梦、人大金仓、神舟通用等主流数据库的备份数据进行定时容灾演练，符合等级保护的要求以检验备份集的可用性

8.支持Exchange、Exchange数据库可用性组的完全备份、增量备份、日志备份与恢复

9.支持VMware、Hyper-V、H3C CAS、OpenStack、CNware、RHV、腾讯云Tstack、浪潮云等虚拟化平台或云平台的备份恢复

10.主库支持数据库的物理备份与数据库复制功能同时启用。既保障数据库物理故障能启用备库应急，又保障逻辑故障时能使用备份数据进行恢复

11.支持对远程复制进行流量控制，合理控制带宽资源。支持对数据传输和存储进行加密，提升传输过程以及存储的安全性。具备断点续传特性，当远程复制过程中出现中断时，恢复正常后可基于上一次断点处进行续传

12.支持将对象存储的数据备份到本地存储中，实现O2D、O2T、O2O。支持完全备份、增量备份、合成备份与恢复，支持恢复到Linux、Unix、Hadoop分布式文件系统（HDFS）中，实现对象存储数据在不同文件系统中的转换恢复，并且支持单文件细粒度的备份和恢复。

设备五十四：政务网出口防火墙

政务网出口防火墙技术要求

数量2台

1.采用标准机架式非X86多核架构，千兆电口≥12个、千兆光口≥12个，万兆光口≥2个

2.防火墙吞吐量≥15Gbps；并发连接数≥1500万，每秒新建连接数≥100万。

3.具有透明、路由、混合、旁路、虚拟线工作模式；支持端口镜像功能，支持入流量、出流量和双向流

量等维度镜像。

4.支持IPv4/v6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换。

5.支持链路负载均衡和服务器负载均衡，并支持会话保持和链路健康检查。

6.支持DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载。

7.支持DDNS功能，支持花生壳服务商的域名，将动态获取的IP地址映射为固定的域名。

8.支持标准IPsec VPN和快速IPsecVPN，标准IPsecVPN认证方式包括但不限于国密认证、数字证书和预共享密钥；同品牌设备快速IPsecVPN对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址

9.支持基于多元组的访问控制；并提供智能策略分析功能，支持策略命中分析、隐藏策略分析、冗余策略分析、冲突策略分析、可合并策略分析、过期策略发现、空策略发现、策略宽松度分析，并在web页面显示分析结果。

10.支持独立的Web防护模块，提供防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；支持HTTP协议的精确访问控制，可针对Method、Referer、User-Agent、Cookie、Url-args等字段设置内容。

11.支持非法外联学习和防护特性，可定义外联白名单地址和端口；需支持通过流量自学习获得服务器合法的外联行为，可实现检测流量中的异常访问流量，实现自动拦截；学习时长可选择多种学习时长。

12.支持针对IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能。

13.支持弱密码扫描能力，可针对IP、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。

14.支持与本方案所投的杀毒软件产品协同工作，实现终端在访问特定IP/网段时必须安装杀毒软件，否则拒绝访问并重定向杀毒软件的安装页面，加强终端安全检查管理。

设备五十五：政务网出口入侵防御设备

政务网出口入侵防御设备技术要求

数量2台

1.采用标准机架式非X86多核架构，千兆电口 ≥ 12 个、千兆光口 ≥ 12 个，万兆光口 ≥ 2 个

2.整机吞吐量 $\geq 15\text{Gbps}$ ；并发连接数 ≥ 1000 万，每秒新建连接数 ≥ 150 万；

3.提供 ≥ 5 年行为特征库升级；

4.系统定义超过8000+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型；并支持在线升级和手动升级

5.支持IPS日志聚合，可按照源IP、目的IP、防护规则和源目的IP等维度进行聚合，

6.支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户。

7.支持弱密码扫描能力，可针对IP、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。

设备五十六：互联网出口防火墙

互联网出口防火墙技术要求

数量2台

1.采用标准机架式非X86多核架构，千兆电口 ≥ 12 个、千兆光口 ≥ 12 个，万兆光口 ≥ 2 个

2. 防火墙吞吐量 $\geq 15\text{Gbps}$ ；并发连接数 ≥ 1500 万，每秒新建连接数 ≥ 100 万。
3. 具有透明、路由、混合、旁路、虚拟线工作模式；支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像。
4. 支持IPv4/v6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换。
5. 支持链路负载均衡和服务器负载均衡。
6. 支持DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载。
7. 支持DDNS功能，支持花生壳服务商的域名，将动态获取的IP地址映射为固定的域名。
8. 支持标准IPsec VPN和快速IPsecVPN，标准IPsecVPN认证方式包括但不限于国密认证、数字证书和预共享密钥；
9. 支持基于多元组的访问控制；并提供智能策略分析功能，支持策略命中分析、隐藏策略分析、冗余策略分析、冲突策略分析、可合并策略分析、过期策略发现、空策略发现、策略宽松度分析。
10. 支持针对IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能。
11. 支持弱密码扫描能力，可针对IP、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。

设备五十七：互联网出口入侵防御设备

互联网出口入侵防御设备技术要求

数量2台

1. 采用标准机架式非X86多核架构，千兆电口 ≥ 12 个、千兆光口 ≥ 12 个，万兆光口 ≥ 2 个
2. 整机吞吐量 $\geq 15\text{Gbps}$ ；并发连接数 ≥ 1000 万，每秒新建连接数 ≥ 150 万；
3. 提供 ≥ 5 年行为特征库升级；
4. 系统定义超过8000+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型；并支持在线升级和手动升级
5. 支持IPS日志聚合，可按照源IP、目的IP、防护规则和源目的IP等维度进行聚合。
6. 支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户。
7. 支持弱密码扫描能力，可针对IP、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。

设备五十八：互联网流量清洗防护机

互联网流量清洗防护机技术要求

数量1台

1. 流量清洗系统结构一体化，应采用B/S架构，运行与管理无需外置环境配合，所有功能操作均能够在设备内置的管理接口上完成；
2. 提供 ≥ 4 个千兆光口、 ≥ 4 个10/100/1000自适应电口；清洗容量 $\geq 4\text{Gbps}$ ；处理能力要求最大并发连接数 ≥ 1000 万，最大新建连接数 ≥ 30 万；
3. 提供产品需要支持 ≥ 1 路（2个）bypass接口；
4. 对欺骗与非欺骗等不同类型的SYN Flood攻击支持算法调整功能；
5. 对欺骗与非欺骗等不同类型的UDP Flood攻击支持组合防御，在监测到缺省算法无效或不佳时，可通过人工调整防御模式；

- 6.支持链接类型攻击组合防御，在监测到缺省算法无效或不佳时，人员可提取数据包中内容字符，对客户源进行访问频率和并发数量限制，并且能够自动加入动态黑名单；
- 7.提供数据包访问控制功能，能够基于“数据内容长度”、“数据内容字符”、“客户源IP”、“防护主机IP”、“协议类型”、“客户源端口”、“防护主机端口”等条件组合使用，并且能够输出匹配日志；
- 8.设备具备针对UDP53、TCP53及DNS提供专用的DNS Query Flood防护手段。

设备五十九：数据库审计机

数据库审计机技术要求

数量1台

- 1.机架式硬件架构， $\geq 2T$ 硬盘容量； ≥ 4 个千兆业务电口， ≥ 1 个接口扩展槽位
- 2.数据库吞吐量 $\geq 2Gbps$ ，SQL峰值处理能力 ≥ 4 万条/秒，日志存储数量 ≥ 9 亿条，实配 ≥ 4 个数据库实例；
- 3.支持IPv4/IPv6双栈审计；
- 4.支持和ES平台对接，将审计日志和告警日志存储在ES系统中，并支持通过页面查询日志；
- 5.支持在审计页面配置审计代理的最大CPU使用率、最大内存使用率、CPU使用率阈值、内存使用率阈值、流量接收端口、抓包过滤串；
- 6.支持在审计页面批量安装、卸载、重新安装审计代理
- 7.支持Oracle、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB等主流数据库审计；
- 8.支持PostgreSQL、GuassDB、HANA、greenplum、libA、graphbase、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、Redis审计；
- 9.支持MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Cassandra、greenplum、libA、graphbase、cache等数据库审计。
- 10.支持对数据库自动建模及智能对异常行为告警功能。

设备六十：智能运维管理软件

智能运维管理软件技术要求

数量1套

- 1.软件平台数据库：统一数据平台内置数据库，可根据不同数据类型选择不同的数据库，关系型数据库用于存储软硬件配置相关的信息；内存数据库用于将一些Web服务经常使用的数据缓存；时序数据库用于存储和时间有关的数据；
- 2.软件配置：网络设备管理数量 ≥ 50 点；服务器硬件管理数、数据库、操作系统、中间件、虚拟化主机、存储、应用监控数量 ≥ 50 ；数据可视化可视化大屏数量 ≥ 1 个；
- 3.服务器硬件管理:平台需具备全面性，支持通过IPMI、SNMP和RESTful协议带外方式对主流厂商服务器进行硬件层面的精细化管理，包括服务器序列号、硬件型号、产品ID、风扇状态/风速、温度、电源功率/状态/模式、处理器状态/缓存/速度、内存大小/状态/频率、网卡状态相关信息的监控；
- 4.软件基础平台:需要满足高性能、高可用，应采用微服务架构，容器底座，支持弹性扩展，自动伸缩，随着业务量的增加系统可自动新建容器，支撑业务的正常运行，单个模块的服务故障、升级等，不会影响其他业务。为保障架构稳定型与数据互通性及信息安全，软件产品及组件为国有自主研发统一产品，不得采用OEM第三方产品或组件；
- 5.软件基础平台架构：可基于资源和人员的归属机构映射，自动过滤数据和以树型结构的层次展示，以满足具有多层级组织结构企业的集中统一运维的要求。可实现多张网部署，支持大中小部署规模、监控对象分布在不同网络环境、多VPC内资源IP地址重复、定期修改操作系统密码等多样化部署需求；支持Proxy/Agent二级容错机制、断网容错、数据缓存；

6.存储监控:可通过SMI-S协议、SNMP协议或者RESTful协议对华为、HP、H3C、DELL、IBM等存储设备进行集中监控管理;

7.虚拟化监控:提供对虚拟化的全面监控,包括CAS、Hyper-V、VMware、FusionCompute。对ESX,Hyper-V服务器以及其上运行的VM的相关性能指标项进行数据采集并监控。

设备六十一:政务网云平台设备

政务网云平台设备技术要求

数量1套

1.部署环境采用集群架构:3台物理服务器或者3台虚拟机;

2.配置本次全部IaaS资源管理授权;

3.云管理平台基于云原生架构开发,通过容器化组件灵活扩展云服务功能,提供云计算服务目录;

4.云管理平台提供用户自助服务界面,用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作;

5.云管理平台能够提供X86云主机服务、密钥对服务、供镜像池服务、云硬盘服务、云防火墙服务、安全组服务、业务编排服务等;

6.云管理平台能够通过自服务门户为用户提供云主机、云硬盘、云防火墙、云负载均衡、公网IP、镜像、快照等服务;

7.支持通过云管理平台的图形化界面对已有的VMware虚拟化平台进行无缝纳管,并且支持虚拟机的批量纳管,纳管过程中虚拟机无需重启、用户业务不中断。提供VMware虚拟机的全生命周期管理和运维。支持VMware 5.5/6.0/6.5/6.7的标准版、企业版、企业增强版。对于已经纳管的虚拟机,也可以将虚拟机去纳管;

8.云管理平台中管理虚拟化平台的存储资源时可以根据SSD/SAS/SATA、IOPS等参数配置不同的存储资源池(如高速、中速、低速等类型),用户申请存储资源时可根据需要选择对应的资源池,达到云存储规格分级管理与使用的需要,不同资源池提供独立的资源规格和计费策略;

9.云管理平台能够提供X86云主机服务,用户通过自助服务门户申请所需操作系统、CPU核数、内存、硬盘以及相应网络IP,云管理员也可以将已存在的云主机指定给某一个用户;

10.云管理平台支持多租户划分,为不同的租户分配资源配额,配额包括CPU、内存、云主机、路由器、网卡、防火墙、负载均衡、安全组、公网IP个数等;

11.支持对OpenStack计算节点的CPU、内存、存储容量和虚拟化平台相关存储卷的存储容量进行统计展示及阈值告警设置,当监控到实际资源使用达到设定阈值时发出告警通知;

12.支持用户使用图形化界面通过拖拽的方式编排自己的VDC,用户可以通过拖拽的方式指定云主机、云网络、云路由器、云防火墙、云负载均衡等云资源的逻辑连接关系,当部署成功后,生成的云主机、云网络、云路由器、云防火墙、云负载均衡等云设备之间的连接关系应与编排时保持一致;

13.支持根据计算资源的硬件配置、虚拟化类型乃至地理位置等信息将计算资源划分到不同的可用域中,从而保证不同的组织能以最优的方式使用计算资源。

设备六十二:互联网云平台设备

互联网云平台设备技术要求

数量1套

1.部署环境采用集群架构:3台物理服务器或者3台虚拟机;

2.配置本次全部IaaS资源管理授权;

3.云管理平台基于云原生架构开发,通过容器化组件灵活扩展云服务功能,提供云计算服务目录;

- 4.云管理平台提供用户自助服务界面，用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作；
- 5.云管理平台能够提供X86云主机服务、密钥对服务、供镜像池服务、云硬盘服务、云防火墙服务、安全组服务、业务编排服务等；
- 6.云管理平台能够通过自服务门户为用户提供云主机、云硬盘、云防火墙、云负载均衡、公网IP、镜像、快照等服务；
- 7.支持通过云管理平台的图形化界面对已有的VMware虚拟化平台进行无缝纳管，并且支持虚拟机的批量纳管，纳管过程中虚拟机无需重启、用户业务不中断。提供VMware虚拟机的全生命周期管理和运维。支持VMware 5.5/6.0/6.5/6.7的标准版、企业版、企业增强版。对于已经纳管的虚拟机，也可以将虚拟机去纳管；
- 8.云管理平台中管理虚拟化平台的的存储资源时可以根据SSD/SAS/SATA、IOPS等参数配置不同的存储资源池（如高速、中速、低速等类型），用户申请存储资源时可根据需要选择对应的资源池，达到云存储规格分级管理与使用的需要，不同资源池提供独立的资源规格和计费策略；
- 9.云管理平台能够提供X86云主机服务，用户通过自助服务门户申请所需操作系统、CPU核数、内存、硬盘以及相应网络IP，云管理员也可以将已存在的云主机指定给某一个用户；
- 10.云管理平台支持多租户划分，为不同的租户分配资源配额，配额包括CPU、内存、云主机、路由器、网卡、防火墙、负载均衡、安全组、公网IP个数等；
- 11.支持对OpenStack计算节点的CPU、内存、存储容量和虚拟化平台相关存储卷的存储容量进行统计展示及阈值告警设置，当监控到实际资源使用达到设定阈值时发出告警通知；
- 12.支持用户使用图形化界面通过拖拽的方式编排自己的VDC，用户可以通过拖拽的方式指定云主机、云网络、云路由器、云防火墙、云负载均衡等云资源的逻辑连接关系，当部署成功后，生成的云主机、云网络、云路由器、云防火墙、云负载均衡等云设备之间的连接关系应与编排时保持一致；
- 13.支持根据计算资源的硬件配置、虚拟化类型乃至地理位置等信息将计算资源划分到不同的可用域中，从而保证不同的组织能以最优的方式使用计算资源。

说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。
----	-------------------------------------

第五章 投标人应当提交的资格、资信证明文件

投标人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，并作为其投标文件的一部分，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。如投标人是企业（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”；如投标人是事业单位，要提供有效的“事业单位法人证书”；投标人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；如投标人是个体工商户，要提供有效的“个体工商户营业执照”；如投标人是自然人，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.投标人应符合《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.信用记录查询

(1) 查询渠道：通过“信用中国”网站(www.creditchina.gov.cn)和“中国政府采购网”(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；

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。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并将相关截图存档。

4.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投标人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人作无效投标处理。

5. 按照招标文件要求，投标人应当提交的资格、资信证明文件。

第六章 评审

一、评审要求

1. 评标方法

双鸭山市政府网站集约化平台和机房等保加固：综合评分法,是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。(最低报价不是中标的唯一依据。)

2. 评标原则

2.1 评标活动遵循公平、公正、科学和择优的原则,以招标文件和投标文件为评标的基本依据,并按照招标文件规定的评标方法和评标标准进行评标。

2.2 具体评标事项由评标委员会负责,并按招标文件的规定办法进行评审。

2.3 合格投标人不足三家的,不得评标。

3. 评标委员会

3.1 评标委员会由采购人代表和有关技术、经济等方面的专家组成,成员人数为5人及以上单数,其中技术、经济等方面的评审专家不得少于成员总数的三分之二。

3.2 评标委员会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,与投标人存在劳动关系,或者担任过投标人的董事、监事,或者是投标人的控股股东或实际控制人;

(2) 与投标人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) 与投标人有其他可能影响政府采购活动公平、公正进行的关系;

3.3 评标委员会负责具体评标事务,并独立履行下列职责:

(1) 审查、评价投标文件是否符合招标文件的商务、技术等实质性要求;

(2) 要求投标人对投标文件有关事项作出澄清或者说明;

(3) 对投标文件进行比较和评价;

(4) 确定中标候选人名单,以及根据采购人委托直接确定中标供应商;

(5) 向采购人、采购代理机构或者有关部门报告评标中发现的违法行为;

(6) 法律法规规定的其他职责。

4. 澄清

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

4.2 投标人的澄清、说明或者补正应当采用书面形式,并加盖公章,或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

4.3 评标委员会不接受投标人主动提出的澄清、说明或补正。

4.4 评标委员会对投标人提交的澄清、说明或补正有疑问的,可以要求投标人进一步澄清、说明或补正。

5. 有下列情形之一的,视为投标人串通投标

5.1 不同投标人的投标文件由同一单位或者个人编制;(不同投标人投标文件上传的项目内部识别码一致);

5.2 不同投标人委托同一单位或者个人办理投标事宜;

5.3 不同投标人的投标文件载明的项目管理成员或者联系人员为同一人;

5.4 不同投标人的投标文件异常一致或者投标报价呈规律性差异;

5.5 不同投标人的投标文件相互混装;

5.6不同投标人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投标人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投标人直接或者间接从采购人或者采购代理机构处获得其他投标人的相关情况并修改其投标文件或者响应文件；

6.2投标人按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件；

6.3投标人之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

6.4属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同参加政府采购活动；

6.5投标人之间事先约定由某一特定投标人中标、成交；

6.6投标人之间商定部分投标人放弃参加政府采购活动或者放弃中标、成交；

6.7投标人与采购人或者采购代理机构之间、投标人相互之间，为谋求特定投标人中标、成交或者排斥其他投标人的其他串通行为。

7.投标无效的情形

7.1详见资格性审查、符合性审查和招标文件其他投标无效条款。

8.废标的情形

8.1出现下列情形之一的，应予以废标。

(1) 符合专业条件的投标人或者对招标文件作实质响应的投标人不足3家；（或参与竞争的核心产品品牌不足3个）的；

(2) 出现影响采购公正的违法、违规行为的；

(3) 投标人的报价均超过了采购预算；

(4) 因重大变故，采购任务取消；

(5) 法律、法规以及招标文件规定其他情形。

9.定标

9.1评标委员会按照招标文件确定的评标方法、步骤、标准，对投标文件进行评审。评标结束后，对投标人的评审名次进行排序，确定中标人或者推荐中标候选人。

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的，视为投标文件未实质性响应（或未响应）招标文件该部分要求的，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。如所投设备属于《节能产品政府采购品目清单》中强制采购产品范围的（如台式计算机，便携式计算机，平板式微型计算机，激光打印机，针式打印机，液晶显示器，制冷压缩机，空调机组，专用制冷、空调设备，镇流器，空调机，电热水器，普通照明用双端荧光灯，电视设备，视频设备，便器，水嘴等为政府强制采购的产品），供应商应提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则其投标文件无效。

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（双鸭山市政府网站集约化平台和机房等保加固）

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	20%	货物由小微企业制造，即货物由小微企业生产且使用该小微企业商号或者注册商标时，给予6%-20%价格扣除C1，即：评标价=投标报价×(1-C1)；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，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投标人属于小微企业的应填写《中小企业声明函》；监狱企业须投标人提供由监狱管理局、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：投标人应当认真填写声明函，若有虚假将追究其责任。投标人可通过“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/>）对投标人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提供投标人的《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。依据法律法规和招标文件的规定，对投标文件中的资格证明文件等进行审查，以确定投标投标人是否具备投标资格。（详见后附表一资格性审查表）

1.2符合性审查。依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标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.投标报价审查

2.1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，应当要求其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；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

3.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。

4.核心产品同品牌审查

4.1采用最低评标价法的采购项目，提供相同品牌产品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，按技术指标的优劣顺序排列获得中标人推荐资格，技术指标相同的，由采购人确定获得中标人推荐资格。

4.2使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人确定一个投标人获得中标人推荐资格。

5.详细评审

综合评分法：分为投标报价评审、商务部分评审、技术部分评审（得分四舍五入保留两位小数）。（详见后附表三详细评审表）

最低评标价法：投标文件满足招标文件全部实质性要求，且进行政府采购政策落实的价格扣除后，对投标报价进行由低到高排序，确定价格最低的投标人为中标候选人。

6.汇总、排序

6.1综合评分法：评标结果按评审后总得分由高到低顺序排列。总得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的，按技术指标的优劣顺序排列确定，以上均相同的由采购人确定。

6.2最低评标价法：投标文件满足招标文件全部实质性要求，且进行政府采购政策落实的价格扣除后，对投标报价进行由低到高排序，确定价格最低的投标人为中标候选人。价格相同的，按技术指标优劣顺序排列确定，上述均相同的由采购人确定。

表一资格性审查表

合同包1（双鸭山市政府网站集约化平台和机房等保加固）

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	提供承诺函。

具有良好的商业信誉和健全的财务会计制度	提供承诺函。
履行合同所必须的设备和专业技术能力	提供承诺函。
参加采购活动前3年内，在经营活动中没有重大违法记录	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）提供承诺函。
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）。提供承诺函。
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。提供承诺函。
落实政府采购政策需满足的资格要求	无

表二符合性审查表：

合同包1（双鸭山市政府网站集约化平台和机房等保加固）

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：

双鸭山市政府网站集约化平台和机房等保加固

评审因素	评审标准
分值构成	技术部分52.0分 商务部分18.0分 报价得分30.0分

技术 (2.0分)	互联网及政务网出口防火墙支持防病毒功能，支持对压缩文件进行解压查杀，压缩层级 ≥ 20 级。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得2分，部分提供或未提供不得分。
技术 (3.0分)	web应用防火墙需支持虚拟补丁功能，支持将Appscan扫描结果导入后自动生成虚拟补丁。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得3分，部分提供或未提供不得分。
技术 (3.0分)	web应用防火墙需支持HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得3分，部分提供或未提供不得分。
技术 (3.0分)	流量探针需支持NGAP、PFCP、GTP等5G协议解析和审计。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得3分，部分提供或未提供不得分。
技术 (3.0分)	运维审计机需支持自带运维客户端，该运维客户端自带运维工具，可不依赖本机的mstsc /xshell/Securecrt等工具进行运维操作。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得3分，部分提供或未提供不得分。
技术 (3.0分)	运维审计机需支持对数据库的会话记录进行图形审计及命令提取。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得3分，部分提供或未提供不得分。
技术 (3.0分)	漏洞扫描需支持分布式部署，可以进行随机分配扫描引擎，也可指定扫描引擎。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得3分，部分提供或未提供不得分。
技术 (2.0分)	安全态势感知需支持内置包括关联模型、规则模型、情报模型、统计模型、AI模型等不少于5类安全分析模型。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得2分，部分提供或未提供不得分。
技术 (2.0分)	安全态势感知需支持对安全日志里200个以上字段进行任意形式的逻辑与非形式组合建模。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得2分，部分提供或未提供不得分。
技术 (3.0分)	安全态势感知支持内置不少于4种机器学习分析场景模型，可检测发现网络会话数异常、流量异常、网址访问失败异常、域名请求数异常等特定场景条件下的安全态势异常。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得3分，部分提供或未提供不得分。

技术部分	技术 (2.0分)	安全态势感知平台支持登录分析、访问关系、Web服务分析、挖矿主机分析、勒索病毒分析、隐蔽隧道、邮件分析、数据安全、DGA域名检测、加密攻击检测等内置安全分析场景，基于场景特性进行默认条件的数据聚合分析，展示统计排序信息，支持分析结果导出。并且可以自由开关场景分析。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得2分，部分提供或未提供不得分。
	技术 (2.0分)	安全态势感知探针需支持一键登录到排错平台，对系统进行深度配置和排错，支持一键故障检测、表分区检查、表检测、配置核对、信息收集等功能。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得2分，部分提供或未提供不得分。
	技术 (2.0分)	安全态势感知探针支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示。提供产品功能证明材料(包括但不限于测试报告、生产制造商官方网站和功能截图等)，并加盖生产制造商公章；全部提供得2分，部分提供或未提供不得分。
	技术 (3.0分)	政务云及互联网核心交换机支持40G/100G端口灵活切换功能，且切换后流量转发正常，ping包无丢包。提供第三方检测报告等证明材料并加盖厂家公章；全部提供得3分，部分提供或未提供不得分。
	技术 (3.0分)	保证IaaS资源池管理平台内置在线p2v、v2v迁移工具，支持业界主流的操作系统、公有云平台、虚拟化平台。包括但不限于VMware、华为、Hyper-V等平台的迁移功能，提升被迁移业务平台的普适性、有效降低上云迁移的难度，降低运维工作量。需提供CNAS认可的检测机构出具的检测报告检测结果及检测结果截图页加盖厂家公章作为证明材料，全部提供得3分，部分提供或未提供不得分。
	技术 (3.0分)	互联网及政务网IaaS资源池设备具备对整个平台虚拟设备统一管理的功能，虚拟化WEB管理平台可以完成构建网络拓扑，完成自助逻辑编排各类虚拟设备，支持在管理平台上连接、开启、关闭各类虚拟设备，拓扑呈现业务流量信息，所画即所得，方便运维管理。需提供CNAS认可的检测机构出具的检测报告检测结果及检测结果截图页加盖厂家公章作为证明材料，全部提供得3分，部分提供或未提供不得分。
	技术 (3.0分)	备份一体机具备良好兼容性，支持对Oracle、SQL Server、MySQL、DB2、PostgreSQL、Informix、Sybase、达梦、人大金仓、神舟通用等主流数据库的备份数据进行定时容灾演练，符合等级保护的要求以检验备份集的可用性。要求提供软件截图证明并加盖厂家公章；全部提供得3分，部分提供或未提供不得分

	技术 (3.0分)	互联网及政务网交换机确保核心设备级冗余保护，实现流量负载分担，同时提高系统的安全性、可靠性、管理简易性，政务云及互联网核心交换机支持多虚一技术(N:1)，支持4框虚拟化技术,提供第三方检测报告等证明材料并加盖厂家公章；全部提供得3分，部分提供或未提供不得分。
	技术 (4.0分)	投标人需深入了解招标内容，设计出具有先进性、安全性、可靠性、可扩展性并且符合招标人实际的总体设计方案，满足本项目建设要求。设计方案应包括但不限于如下内容：机房安全防护解决方案、云平台建设方案、集成管理方案、政务服务网存储扩容解决方案。完全满足要求且方案合理得4分，每提供一项得1分，未提供或提供不满足本项目要求内容的该项不得分。
商务部分	企业资质 (3.0分)	在企业服务能力上，投标方或其所属总公司需具备信息系统建设和服务能力等级证书，投标文件中提供证书复印件并加盖投标方公章，能力达到优秀级（CS4）及以上的得3分；CS3级得1分；低于CS3级或没有不得分。
	企业资质 (3.0分)	在企业维护能力上，投标方或其所属总公司需具备ITSS信息技术服务资质（运行维护服务）二级及以上资质。投标文件中提供证书复印件并加盖投标方公章，满足一级资质得3分，满足二级资质得1分，二级以下不得分，未提供不得分。
	企业资质 (3.0分)	在企业安全运维能力上，投标方或其所属总公司需具备CCRC信息安全服务资质（信息系统安全运维）二级及以上资质。投标文件中提供证书复印件并加盖投标方公章，满足一级资质得3分，满足二级资质得1分，二级以下不得分，未提供不得分。
	人员要求 (2.0分)	投标方需组建一支不少于5人的项目团队，团队成员需具备不少于1名高级信息系统项目管理师、不少于1名高级系统架构设计师、不少于1名高级弱电工程师、不少于1名CISS P信息系统安全专家、不少于1名高级网络规划设计师。全部提供得2分，每提供一项得0.4分，未提供不得分。（须提供以上人员资质证书复印件、身份证复印件及联系方式，并加盖投标方公章）
	人员要求 (1.0分)	投标方的项目团队负责人要求具备中级以上职称，具备信息系统项目管理师证书或PMP证书，具备得1分，不具备或没有不得分。（须提供证书复印件、劳动合同复印件、身份证复印件及联系方式并加盖投标方公章）。
	运维服务要求 (2.0分)	保证设备均为原厂原装，具备在中国境内的合法使用权，且出厂前均经过厂家的检验合格，承诺提供3年免费质保服务,并提供终身维修服务。完全满足的得2分，部分满足或未提供不得分。
	运维服务要求 (2.0分)	提供运维服务方案，包括但不限于市政府网站集约化平台和政府机房安全运维服务内容；运维人员不少于10人。满分2分，每提供一项得1分，未提供不得分。
	运维服务要求 (2.0分)	提供系统链路保障方案，方案内容包括但不限于本地运营商针对本项目涉及的链路保障服务承诺，服务承诺内容包括但不限于故障响应时限、故障处理时限、服务团队人员数量、资质等，根据内容完整性、清晰程度及质量进行综合评分，完全满足的得2分，部分满足或未提供不得分。

投标报价	投标报价得分 (30.0分)	投标报价得分= (评标基准价/投标报价) ×价格分值【注：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。】最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。
------	----------------	--

第七章 投标文件格式与要求

投标人提供投标文件应按照以下格式及要求进行编制，且不少于以下内容。

投标文件封面

(项目名称)

投标文件封面

项目编号：**[230501]SZCG[GK]20220012-1**

所投采购包：第 包

(投标人名称)

年 月 日

投标文件目录

- 一、投标承诺书
- 二、资格承诺函。
- 三、法定代表人授权书
- 四、主要商务要求承诺书
- 五、技术偏离表
- 六、中小企业声明函
- 七、监狱企业
- 八、残疾人福利性单位声明函
- 九、分项报价明细表
- 十、联合体协议书
- 十一、项目实施方案、质量保证及售后服务承诺等
- 十二、项目组成人员一览表
- 十三、投标人业绩情况表
- 十四、各类证明材料

格式一：

投标承诺书

采购单位、双鸭山市政府采购中心：

1.按照已收到的 项目（项目编号： ）招标文件要求，经我方（投标人名称）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。我方完全接受本次招标文件规定的所有要求，并承诺在中标后执行招标文件、投标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.我方同意招标文件关于投标有效期的所有规定。

3.我方郑重声明：所提供的投标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.我方将按照招标文件、投标文件及相关要求、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) 不按照招标文件要求提交履约保证金；
- (5) 要求修改、补充和撤销投标文件的实质性内容；
- (6) 要求更改招标文件和中标结果公告的实质性内容；
- (7) 法律法规和招标文件规定的其他情形。

详细地址：

邮政编码：

电话：

电子函件：

投标人开户银行：

账号/行号：

投标人_____ (加盖公章)

法定代表人_____ (签字)

授权委托人_____ (签字)

年 月 日

格式二：

《投标资格承诺函》

双鸭山市政府采购中心：

我公司作为本次采购项目的投标人，根据招标文件要求，现郑重承诺如下：

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投标人、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。

4.我公司未违反“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。”的情形。

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。

投标人（单位盖章）：

日期:

格式三:

法定代表人授权书

本人_____ (姓名) 系_____ (投标人名称) 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、修改招标项目投标文件、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:

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。

如有优于招标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。

投标人名称: (加盖公章) 法定代表人 (或授权代表) 签字或盖章

年 月 日

格式五: (工程类项目可不填写或不提供)

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. 投标人应当如实填写上表“投标人提供响应内容”处内容，对招标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招标文件要求。

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。如直接复制招标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。

格式六：（不属于可不填写内容或不提供）

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（工程、货物、服务）；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（工程、货物、服务）；制造商为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

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

企业名称（盖章）：
日期：

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

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（工程、货物、服务）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（工程、货物、服务）行业；承建（承接）企业为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

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

企业名称（盖章）：
日期：

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

格式七：（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。

格式八：（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：

格式九：

分项报价明细表（网上开评标可不填写）

注：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，若在投标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：（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，进行合同谈判活动，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招标文件、投标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

格式十一：

（未要求可不填写）

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。

格式十二：

项目组成人员一览表（未要求可不填写）

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						
.....						

按招标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.如投标人中标，须按本表承诺人员操作，不得随意更换。

格式十三：

投标人业绩情况表（未要求可不填写）

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

投标人根据上述业绩情况后附销售或服务合同复印件。

格式十四：

各类证明材料（未要求可不填写）

- 1.招标文件要求提供的其他资料。
- 2.投标人认为需提供其他资料。