**招　标　文　件**

**项目名称：南京市江宁医院信息安全项目（四）**

**项目编号：JSZC-320115-JZCG-G2024-0201**

**（非专门面向中小企业）**

**南京市公共资源交易中心江宁分中心**

**2025年 02月**

**总 目 录**

1. 投标邀请……………………………………
2. 投标人须知…………………………………
3. 合同文本……………………………………
4. 采购需求……………………………………
5. 评标方法与评标标准………………………
6. 投标文件格式………………………………

第一章 投标邀请

受南京市江宁医院（采购单位）委托，南京市公共资源交易中心江宁分中心（以下简称“交易中心”）就南京市江宁医院信息安全项目（四）（项目名称）项目进行公开招标采购，欢迎符合条件的供应商投标。

一、项目基本情况

1.项目编号：JSZC-320115-JZCG-G2024-0201

2.项目名称：南京市江宁医院信息安全项目（四）

3.预算金额： 312万元

4.本项目最高限价：312万元。

5.采购需求（简介）：项目包括增加设备冗余，超融合平台扩容，网络安全运维服务，视频监控安全。项目针对现有信息系统进行安全加固，提升整体安全运维能力，保证现有信息系统安全有效的运行。 （详细内容见本招标文件第四章）

6.合同履行期限：交付期自合同签订之日起45天内，质保期为自交货验收合格之日起3年。

7.本项目不接受进口产品投标。

8.本项目不接受联合体投标。

二、申请人的资格要求

（一）通用资格要求

1.满足《中华人民共和国政府采购法》第二十二条规定，并提供下列材料：

1.1供应商信用承诺函（格式见第六章）。

2.落实政府采购政策需满足的资格要求：无

（二）本项目特定资格要求:无。

（三）拒绝下述供应商参加本次采购活动

1.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。

2.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，不得参加本项目的采购活动。

3.供应商被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）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。

三、获取招标文件

1.时间：自招标文件公告发布之日起。

2.方式：在“江苏政府采购网”免费下载。

四、提交投标文件截止时间、开标时间和地点

1.提交投标文件截止时间、开标时间2025年3月7日14点00分（北京时间）。

2.地点：江苏省政府采购交易系统（以下简称“苏采云系统”）网上开标大厅。

五、公告期限

招标公告及招标文件公告期限为自本公告发布之日起5个工作日。

六、其他事宜

1.本次招标不收取投标保证金。

2.本项目不组织集中勘察及答疑。

3. 供应商通过苏采云系统参与政府采购项目，需要办理江苏省政府采购数字证书及电子签章，具体详见苏采云系统登录页“新CA办理指南”。投标人按《苏采云系统投标人操作手册》要求进行注册，并制作上传电子投标文件（“苏采云”南京地区客服热线025-83633744、025-83633743）。江苏省政府采购管理交易系统投标人操作指南，下载地址：http://www.ccgp-jiangsu.gov.cn/jiangsu/zlxz/ee/ee3a4bc5a3454aa2b0d9312230633ce9.html。

4.有关本次招标的事项若存在变动或修改，请及时关注“江苏政府采购网”（www.ccgp-jiangsu.gov.cn）更正公告。

七、本次招标联系方式

1.采购人信息

名 称：南京市江宁医院

地 址：南京市江宁区湖山路169号

联系人：王雅庆

联系电话：15950530382

2.代理机构信息

名 称：南京市公共资源交易中心江宁分中心

地　址：　南京市江宁区杨家圩路2号A区三楼

联系人：　高嘉佳

联系电话：　025- 69613983

第二章 投标人须知

一、总则

1.招标方式

1.1 本次招标采取公开招标方式，本文件仅适用于招标公告中所述项目。

2.合格的投标人

2.1 满足招标公告对供应商资格要求的规定。

2.2 满足招标文件规定的实质性要求和条件。

3.适用法律

3.1 本次招标及由此产生的合同受中华人民共和国有关的法律法规制约和保护。

4.投标费用

4.1 投标人应自行承担所有与参加投标有关的费用，无论投标过程中的做法和结果如何，交易中心在任何情况下均无义务和责任承担这些费用。

4.2 本次招标交易中心和采购人不收取标书工本费与中标服务费。

5.招标文件的约束力

5.1 投标人一旦参加本项目采购活动，即被认为接受了本文件的规定和约束。

二、招标文件

6.招标文件构成

6.1 招标文件由以下部分组成：

（1）投标邀请

（2）投标人须知

（3）合同文本

（4）采购需求

（5）评标方法与评标标准

（6）投标文件格式

投标人应仔细检查招标文件是否齐全，如有缺漏请立即与交易中心联系。

6.2 投标人应认真阅读招标文件中所有的事项、格式、条款和规范等要求。按招标文件要求和规定编制投标文件，并保证所提供的全部资料的真实性，以使其投标文件对招标文件作出实质性响应，否则其风险由投标人自行承担。

7.招标文件的澄清

7.1 任何要求对招标文件进行澄清的投标人，应在投标截止期十日前按招标公告中的通讯地址，以书面形式通知交易中心。

8.招标文件的修改

8.1 在投标截止时间前，交易中心可以对招标文件进行修改。招标文件的修改将在原公告媒体发布更正公告，更正内容将作为招标文件的组成部分，并对投标人具有约束力。

8.2 投标人应在提交投标文件截止时间前，关注原公告媒体有关本项目的更正公告，根据更正公告内容自行决定是否需要重新制作和提交投标文件，并承担由此产生的相应责任。

8.3 交易中心有权按照法定的要求推迟投标截止日期和开标日期，并在原公告媒体发布更正公告。

三、投标文件的编制

9.投标文件的语言及度量衡单位

9.1 投标人提交的投标文件以及投标人与交易中心就有关投标的所有来往通知、函件和文件均应使用简体中文。

9.2 除技术性能另有规定外，投标文件所使用的度量衡单位，均须采用国家法定计量单位。

10.投标文件构成

10.1 投标人编写的投标文件应包括资格证明文件、符合性证明文件、投标分项报价表、响应及偏离表、其他证明文件、投标函、开标一览表等部分。

10.2 如标书制作工具中格式和内容与“江苏政府采购网”发布的招标文件不一致，以“江苏政府采购网”发布的招标文件为准。

11.证明投标人及投标标的符合招标文件规定的文件

11.1 投标人应按照法律、法规、规章和规范性文件以及招标文件要求提交证明文件，证明其投标标的符合招标文件规定。

11.2 招标文件对证明文件无明确形式要求的，证明文件可以以文字资料、图纸和数据等形式提交。

12.投标分项报价表（如有）

12.1 投标人应按照招标文件规定格式填报投标分项报价表。

12.2 投标文件中的单价和总价无特殊规定的采用人民币报价，以元为单位标注。招标文件另有规定的按规定执行。

13.响应及偏离表

13.1 投标人需对招标文件中的技术要求与商务要求逐项作出响应或偏离说明。

13.2 投标人可以在投标文件中提供认为需要的其他技术文件或说明。

14.投标函和开标一览表及核心产品品牌一览表

14.1 投标人应按照招标文件规定格式完整、正确填报投标函、开标一览表及核心产品品牌一览表。

14.2 对于采用货币报价的项目，开标一览表中的投标总报价应与投标分项报价表中的投标总报价一致，如不一致评标时以开标一览表中价格为准。

14.3 核心产品品牌一览表中所投核心产品品牌缺项的将视为无效投标。

15.投标有效期

15.1 投标有效期为招标公告规定的开标之日起六十天。投标有效期比规定短的将被视为未实质性响应招标文件而被拒绝。

16.投标有效期的延长

16.1 在特殊情况下，交易中心于原投标有效期满之前，可向投标人提出延长投标有效期的要求。这种要求与答复均应采用书面形式。投标人可以拒绝交易中心的这一要求而放弃投标。同意延长投标有效期的投标人既不能要求也不允许修改其投标文件，同时受投标有效期约束的所有权利与义务均延长至新的有效期满。

四、投标文件的递交

17.投标文件的递交

17.1 投标人应当按照《操作手册》规定，在招标公告规定的投标截止时间前制作并上传电子投标文件。

17.2 投标人应充分考虑网络环境、网络带宽等因素可能对投标产生的影响，如因投标人自身原因造成的电子投标文件上传不成功的，按照本招标文件第二章第25.1条规定做无效投标处理。

17.3 交易中心可以按照规定，通过修改招标文件酌情延长投标截止时间，在此情况下，投标人的所有权利和义务均以延长后新的截止时间为准。

18.投标文件的拒收

18.1 投标截止时间后上传的任何投标文件将被拒绝。

19.投标文件的撤回和修改

19.1 投标文件的撤回

19.1.1 投标人可在投标截止时间前撤回其电子投标文件，具体操作方法见《操作手册》。

19.1.2 投标人撤回电子投标文件，则认为其不再参与本项目投标活动。

19.2 投标文件的修改

19.2.1 投标人可在投标截止时间前对其电子投标文件进行修改，具体操作方法见《操作手册》。

19.2.2 投标截止时间之后，投标人不得对其电子投标文件作任何修改。

19.3 在投标截止时间至招标文件中规定的投标有效期满之间的这段时间内，投标人不得撤回其投标。

五、开标与评标

20.开标

20.1 交易中心在招标公告中规定的时间和地点组织公开开标。投标人按照《操作手册》规定参加开标活动，并在苏采云系统规定的时间内对投标文件进行解密。苏采云系统公布各投标人名称和投标价格。

20.2 投标人在开标过程中涉及到的投标文件解密、开标结果确认等工作，应按照《操作手册》规定执行。

20.3 投标人如果对开标过程和开标结果有疑义，应当根据《操作手册》规定提出，苏采云系统中《开标记录表》公布后5分钟内未提出的，视同认可开标结果。

21.评标

21.1 评标由依法组建的评标委员会（以下简称“评委会”）进行。

21.2 评委会由采购人代表和有关技术、经济或法律等方面的专家组成，且人员构成符合政府采购有关规定。

21.3 评委会独立工作，负责评审所有投标文件并推荐中标候选人，或根据采购人授权直接确定中标人。

22.评标过程的保密与公正

22.1 凡是与审查、澄清、评价和比较投标的有关资料以及授标建议等，采购人、评委、交易中心均不得向投标人或与评标无关的其他人员透露。

22.2 投标人不得以任何方式影响评标，否则其投标文件将被作为无效投标文件。

22.3 交易中心和评委会不向未中标的投标人解释未中标原因，也不公布评标过程中的相关细节。

22.4 采用综合评分法的项目，未中标的投标人可于中标结果公告期限届满之日起通过苏采云系统查看本单位的评审得分及排名情况。

23.投标文件的澄清

23.1 评标期间，评委会对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，有权要求投标人作出必要的澄清、说明或者补正。

投标人的澄清、说明或者补正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。

评委会并非对每个投标人都做澄清要求。

23.2 需要供应商进行澄清、说明和补正的，评委会将通过苏采云系统向投标人发出《澄清要求函》，接到《澄清要求函》的投标人应当按照要求在苏采云系统中提交《澄清响应函》并加盖电子公章。澄清、说明和补正的内容作为投标文件的补充部分，具体操作方式见《操作手册》。

23.3 接到评委会澄清、说明和补正要求的，投标人如未按规定作出澄清、说明和补正，其风险由投标人自行承担。

24.投标文件的审查

24.1 投标文件审查分为资格审查和符合性审查。

24.1.1 资格审查。依据法律法规和招标文件规定，由采购人对投标文件中的资格证明文件进行审查，并向评委会反馈审查结论。

采购人进行资格审查时，将在“信用中国”网站（www.creditchina.gov.cn）查询投标人的信用记录，以确定投标人是否具备投标资格，查询结果留存并归档。

接受联合体的项目，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。

24.1.2 符合性审查。依据招标文件的规定，由评委会从有效性、完整性和对招标文件的响应程度等方面对投标文件进行审查，以确定是否对招标文件的实质性要求作出响应。

24.1.3 未通过资格审查或符合性审查的投标人，交易中心将通过苏采云系统告知其具体原因，评标结束后不再接受有关询问。

24.2 评委会仅对实质性响应招标文件要求的投标文件进行详细评审。实质性响应的投标文件应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离或保留的文件。

所谓重大偏离或保留是指与招标文件规定的实质性要求存在负偏离，或者在实质上与招标文件不一致，而且限制了合同中采购人的权利或投标人的义务，纠正这些偏离或保留将会对其他实质性响应的投标人产生不公正的影响。重大偏离的认定由评委会按照少数服从多数的原则作出结论。评委会认定投标文件的响应性只根据投标文件本身的内容，而不寻求外部的证据。

24.3 如果投标文件实质上没有响应招标文件的要求，评委会将予以拒绝，投标人不得通过修改或撤销不合要求的偏离或保留而使其投标成为实质性响应的投标。

24.4 评委会将对确定为实质性响应的投标进行进一步审核，确定其是否有计算上或累加上的算术错误。修正错误的原则如下：

（1）投标文件中开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准；

（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；

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上错误的，按照前款规定的顺序修正。

24.5 评委会将按上述修正错误的方法调整投标文件中的投标报价，并通过苏采云系统告知投标人，调整后的价格对投标人具有约束力。如果投标人不接受修正后的价格，则其投标将被拒绝。

24.6 投标人在开、评标全过程中应保持通讯畅通，及时登录苏采云系统查阅、答复相关信息，并安排专人与交易中心及评委会联系。

25.无效投标和废标

25.1 无效投标情形

25.1.1 投标人在苏采云系统规定的时间内未成功解密电子投标文件。

25.1.2 投标人未按照招标文件要求上传电子投标文件。

25.1.3 同一投标人提交两个（含两个）以上不同的投标报价。

25.1.4 投标人不具备招标文件中规定资格要求。

25.1.5 投标人的报价超过了采购预算或最高限价。

25.1.6 未通过符合性审查。

25.1.7 不符合招标文件中实质性要求和条件（**本文件中斜体且有下划线部分，或者打“★”内容为实质性要求和条件**）。

25.1.8 投标人被“信用中国”网站（www.creditchina.gov.cn）列入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失信行为记录名单，或查询“信用中国”网站后发现投标人存在其他不符合《中华人民共和国政府采购法》第二十二条规定条件的信用记录。

25.1.9 投标文件含有采购人不能接受的附加条件。

25.1.10 评委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，有可能影响服务质量或者不能诚信履约的，将通过苏采云系统要求其在合理的时间内提供说明，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，评委会应当将其作为无效投标处理。

25.1.11 采购产品被财政部、国家发改委、生态环境部等列入“节能产品品目清单”强制采购范围，而投标人提供的产品不在强制采购范围内。

25.1.12 投标文件未按照招标文件要求加盖电子公章。

25.1.13 法律法规及本招标文件规定的其他无效投标情形。

25.2 废标情形

25.2.1 符合资格条件的供应商或者对招标文件作实质响应的供应商不足三家。

25.2.2 出现影响采购公正的违法、违规行为。

25.2.3 因重大变故采购任务取消。

25.2.4 评委会认定招标文件存在歧义、重大缺陷导致评审工作无法进行。

25.2.5 因苏采云系统故障造成开标不成功。

25.3 如出现投标截止时间后参加投标的供应商或者对招标文件作出实质性响应的供应商不足三家的情况，按政府采购相关规定执行。

六、定标

26.确定中标单位

26.1 中标候选人的确定原则和数量见招标文件第五章。

26.2 按以下第（1）种方式确定中标人：

（1）评委会直接确定排名第一的中标候选人为中标人；

（2）采购人在评委会推荐的中标候选人中按顺序确定中标人。

按第二种方式确定中标人的，交易中心自评审结束之日起两个工作日内将评审报告送达采购人，采购人自收到评审报告之日起五个工作日内，在评审报告推荐的中标候选人中按顺序确定中标人。

26.3 交易中心将在“江苏政府采购网”发布中标公告，公告期限为1个工作日。

26.4 **若有充分证据证明中标人有下列情况之一的，一经查实将被取消中标资格：**

26.4.1 提供虚假材料谋取中标。

26.4.2 向评审专家、采购人或交易中心工作人员行贿或者提供其他不正当利益。

26.4.3 与其他供应商、评审专家、采购人或交易中心工作人员恶意串通。

26.4.4 属于本文件规定的无效投标情形，但在评标过程中未被评委会发现。

26.4.5 采取不正当手段诋毁、排挤其他供应商。

26.5 **有下列情形之一的视为投标人串通投标，投标无效：**

26.5.1 不同投标人的投标文件由同一单位或者个人编制。

26.5.2 不同投标人委托同一单位或者个人办理投标事宜。

26.5.3 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。

26.5.4 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。

27.中标通知书

27.l 中标结果确定后，交易中心将向中标人发出《中标通知书》。中标人可在中标结果公告届满之日起三十日内，登录苏采云系统下载。

因系统存储空间有限，中标结果公告届满之日起三十日后，苏采云系统不再保证提供下载《中标通知书》服务，因未及时下载而造成的不利后果由中标人自行承担。

27.2 《中标通知书》是合同的一个组成部分，对采购人和中标人均具有法律效力。《中标通知书》发出后，采购人改变中标结果或者中标人放弃中标项目的，应当依法承担法律责任。

七、授予合同

28.签订合同

28.l 中标人应当在《中标通知书》发出之日起三十日内，按照招标文件确定的事项与采购人签订政府采购合同。采购人于合同签订后2个工作日内通过苏采云系统进行公示。

28.2 招标文件、中标人的投标文件及招标过程中有关澄清、承诺文件均作为合同附件。

28.3 签订合同后，中标人不得将合同标的进行转包。未经采购人同意，中标人也不得采用分包的形式履行合同，否则采购人有权终止合同。转包或分包造成采购人损失的，中标人应承担相应赔偿责任。

28.4 中标人因自身原因拒绝与采购人签订合同的，不得参加采购人重新组织的采购活动，且将可能被拒绝参加该采购人一年内的其他政府采购活动。

29.标的物的追加

29.1 合同履行中，采购人需追加与合同标的相同的货物（包含与货物相关的服务），在不改变合同其他条款的前提下，可以与中标人协商签订补充合同，但所有补充合同的金额不超过原合同金额的10%。

30.政府采购履约资金扶持政策

30.1 中标供应商可通过南京市公共资源交易平台网站“小企业融资平台”，选择相应的金融机构办理融资贷款。

30.2 依据《关于在全省政府采购领域推行电子履约保函（保险）的通知》（苏财购〔2023〕150号），需要缴纳履约保证金的，中标供应商可通过江苏政府采购网“政府采购电子履约保函（保险）综合服务平台”线上办理履约保函（保险）。

八、质疑

31.提出质疑的供应商应当是参与所质疑项目采购活动的供应商，潜在供应商依法获取其可质疑的采购文件的，可以对采购文件提出质疑。

32.供应商认为采购文件、采购过程和采购结果使自己的权益受到损害的，可以在知道或应知其权益受到损害之日起七个工作日内，按照第34条、第35条之规定以书面形式向采购人或交易中心提出质疑。**上述应知其权益受到损害之日是指**：

32.1 对采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日。

32.2 对采购过程提出质疑的，为各采购程序环节结束之日。

32.3 对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

33.供应商应当在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商如在法定期限内对同一采购程序环节提出多次质疑的，交易中心或采购人将只对供应商第一次质疑作出答复。

34.供应商提出质疑应提交《质疑函》原件，且尽可能通过邮寄方式送达，交易中心和采购人不接受无运单的快件。《质疑函》应按照本招标文件中《质疑函范本》的格式和内容填写。

供应商如组成联合体参加采购活动，《质疑函范本》中要求加盖公章之处，联合体各方均须按要求加盖公章。

35. **供应商（含潜在供应商）对采购方式、采购需求、供应商资格条件及审查结果、评标方法和评标标准、合同文本的询问、质疑向采购人提出，由采购人负责答复。**供应商对除上述事项以外其他事项的询问、质疑向交易中心提出，由交易中心负责答复。

**采购人质疑接收人为南京市江宁医院，联系地址：南京市江宁区湖山路169号3号楼7楼，联系人：王雅庆，联系电话：15950530382。**

交易中心质疑接收部门为业务受理科（快递运单上的收件人填写“业务受理科”即可），联系地址：南京市江宁区杨家圩路2号市民中心 A区3楼南京市公共资源交易中心江宁分中心A314业务受理科，联系电话：025-69634313。

**由采购人负责答复的质疑，采购人将《质疑答复函》抄送交易中心。**

36.以下情形的质疑不予受理：

36.1 内容不符合《政府采购质疑和投诉办法》第十二条规定的质疑。

36.2 超出政府采购法定期限的质疑。

36.3 以传真、电子邮件等方式递交的非原件形式的质疑。

36.4 未参加采购活动或在采购活动中自身权益未受到损害的供应商所提出的质疑。

36.5 供应商组成联合体参加采购活动，联合体中任何一方或多方未按要求签字或签章、加盖公章的质疑。

36.6 法律法规规定的其他不予受理情形。

37.供应商提出书面质疑必须有理、有据，不得捏造事实、提供虚假材料进行恶意质疑。否则，一经查实，交易中心或采购人有权依据政府采购的有关规定，报请政府采购监管部门对该供应商进行相应的行政处罚和记录该供应商的失信信息。

九、政策功能落实

38.促进中小企业发展

38.1 本项目中的货物全部由中小企业制造的，投标供应商享受中小企业扶持政策。

38.2 中小企业是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准（详见《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）、《国家统计局关于印发〈统计上大中小微型企业划分办法（2017）〉的通知》（国统字〔2017〕213号））确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

38.3 中小企业参加政府采购活动，应当出具《中小企业声明函》，否则不享受相关中小企业支持政策。

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

38.5 监狱和戒毒企业（简称监狱企业）视同小型、微型企业。按照《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）规定，监狱企业需提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件。

38.6 残疾人福利性单位视同小型、微型企业。按照《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定，残疾人福利单位需提供《残疾人福利性单位声明函》。

39.节能环保产品

39.1 执行节能环保产品优先采购和强制采购制度。节能产品是指列入财政部、国家发展和改革委员会制定的《节能产品政府采购品目清单》（财库〔2019〕19号），且依据国家相关标准的最新版本、国家能效标准中二级能效（水效）指标认证的节能产品；环境标志产品是指列入财政部、生态环境部制定的《环境标志产品政府采购品目清单》（财库〔2019〕18号），且依据相关标准的最新版本认证的环境标志产品。国家对品目清单进行调整的，按照最新的品目清单执行。

39.2 采购产品属于政府强制采购节能产品的，供应商应当选择依据国家能效标准中二级能效（水效）指标认证的节能产品投标，签订合同时提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书。

39.3 采购产品属于政府优先采购节能产品和环境标志产品的，对供应商提供的国家确定的认证机构出具的、处于有效期之内的节能产品或环境标志产品认证证书，评审时给予加分（详见第五章评标方法与评标标准）。

40.绿色采购

40.1 采购产品中涉及商品包装、快递包装要求的，应按照《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》（财办库〔2020〕123号）、《江苏省财政厅关于加强政府绿色采购有关事项的通知》（苏财购〔2023〕65号）文件执行。采购文件对商品包装和快递包装有具体要求的，政府采购合同中应当载明对供应商提供产品及相关快递服务的具体包装要求和履约验收相关条款，供应商须严格执行，必要时应按照要求在履约验收环节出具检测报告。

40.2 采购产品中涉及数据中心相关设备、运维服务的，应按照《关于印发〈绿色数据中心政府采购需求标准（试行）的通知》（财办库〔2023〕7号）、《江苏省财政厅关于加强政府绿色采购有关事项的通知》（苏财购〔2023〕65号）等文件执行。采购文件中涉及数据中心相关设备、运维服务的，采购人均以《绿色数据中心政府采购需求标准（试行）》提出的指标、标准为准。采购人应在政府采购合同中明确对相关指标的验收方式和违约责任，供应商应按合同约定提供设备或服务。

40.3 采购产品中涉及涂料、胶黏剂、油墨、清洗剂等挥发性有机物产品的，属于强制性标准的，供应商应当提供符合国家和江苏省相关VOCs 含量限制标准的产品。采购产品中涉及通用类货物、家具的，供应商应当优先使用低挥发性原辅材料，采购人将使用低VOCs含量的涂料、胶黏剂等纳入政府采购合同条款的，供应商必须严格执行。

40.4 采购产品中涉及数据库、操作系统、通用服务器、工作站、一体式计算机、便携式计算机、台式计算机的，供应商所投产品不得违反财政部、工业和信息化部印发的《需求标准》（详见财库〔2023〕29号、30号、31号、32号、33号、34号、35号文件）。采购人可以对《需求标准》中的指标提出更高要求，也可以根据实际需要增加《需求标准》以外的指标。采购人按照采购合同约定对供应商所提供的上述产品进行验收，必要时可以委托依法取得检测、认证资质的机构进行检测、认证。

41.创新产品采购

41.1 优先采购各级政府部门公开发布的有效期内的创新产品、首台套等《目录》内的创新产品。创新产品自进入《目录》起2年内视同具备相应销售业绩。

42.网络产品、市场准入类产品采购

42.1 本项目中如涉及网络关键设备或网络安全专用产品的，应严格执行国家互联网信息办公室、工业和信息化部、公安部、财政部和国家认证认可监督管理委员会2023年第1 号《关于调整网络安全专用产品安全管理有关事项的公告》及2023年第2号《关于调整<网络关键设备和网络安全专用产品目录>的公告》要求，所投设备或产品至少符合以下条件之一：一是已由具备资格的机构安全认证合格或安全检测符合要求；二是已获得《计算机信息系统安全专用产品销售许可证》，且在有效期内。采购人、中标供应商双方签订合同及验收环节，应包含上述网络安全要求的条款。

42.2 本项目中如涉及国家强制性产品认证证书（CCC认证证书）、电信设备进网许可证、无线电发射设备核准证等市场准入类资质的，应严格执行国家相关法律法规的要求。采购人、中标供应商双方签订合同及验收环节，应包含上述市场准入类资质要求的条款。

第三章 合同文本

以下为本项目的合同条款，合同双方不得对招标、投标文件内容作实质性修改。

政府采购合同（货物）

合同编号：

项目名称： 项目编号：

甲方：（买方）

乙方：（卖方）

甲、乙双方根据南京市公共资源交易中心组织的\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目公开招标结果，签署本合同。

一、合同内容

1.1 标的名称：

1.2 标的质量：按招标文件及投标文件执行。

1.3 标的数量（规模）：

1.4 履行时间（期限）：按招标文件及投标文件执行。

1.5 履行地点：采购人指定地点。

1.6 履行方式：按招标文件及投标文件执行。

1.7 包装方式：按招标文件及投标文件执行。

二、合同金额

2.1 本合同金额为（大写）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_圆（\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元）人民币。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供货物(包含与货物相关的服务)的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。保密期至保密内容按照相关法律法规规定，以合法方式和途径将其全部披露或本合同终止后5年为止，以两者孰长为准。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同货物（包含与货物相关的服务）或其任何一部分时不受第三方提出侵犯其专利权、著作权、商标权、工业设计权、商业秘密等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的货物（包含与货物相关的服务）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

6.1 本项目乙方无需缴纳履约保证金。

6.2 乙方可以采用银行、保险公司、担保公司等第三方机构出具的履约保函（保险）代替缴纳履约保证金，保函（保险）有效期届满且担保人按照约定履行了担保责任后自动失效。如乙方未按要求履行合同义务，由担保人按照合同约定对甲方承担赔偿责任。

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 除招标文件接受分包并经甲方同意，乙方可按分包意向协议分包情况外，乙方不得将合同标的分包给他人履行。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权终止合同。

八、合同款项支付

8.1 合同款项的支付方式及时间

8.1.1 合同签订后，甲方支付合同总价款的30%作为预付款。

8.1.2 供货结束并验收合格后,甲方支付合同总价款的70%。

8.1.3 满足合同约定支付条件的，甲方收到乙方发票后10个工作日内，将资金支付到合同约定的乙方账户。

8.2 根据工业和信息化部关于印发《保障中小企业款项支付投诉处理暂行办法》的通知（工信部企业〔2021〕224 号），甲方未按合同约定支付款项的，乙方可以向有关部门投诉。

8.3 当采购数量与实际使用数量不一致时，乙方应根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

九、税费

9.1 本合同执行中的相关税费均由乙方负担。

十、质量保修范围和保修期及售后服务

10.1 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

10.2 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商可按以下方式处理：

10.2.1 更换：由乙方承担所发生的全部费用。

10.2.2 贬值处理：由甲乙双方合议定价。

10.2.3 退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

10.3 如在使用过程中发生质量问题，乙方应在接到甲方通知后 4小时内到达甲方现场。

10.4 质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

10.5 质保期为自交货验收合格之日起3年，因人为因素出现的故障不在质保范围内。超过质保期的乙方负责终生维修，维修时只收取部件成本费。

十一、项目验收

11.1 甲方依法组织履约验收工作。

11.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案做好相应配合工作。

11.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

11.4 如有必要，甲方可邀请参加本项目投标的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收结论的参考。

11.5 甲方成立验收小组，按照采购合同约定对乙方履约情况进行验收。验收时间、验收标准见招标文件。验收时甲方按照采购合同的约定对每一项技术、商务要求的履约情况进行确认。验收结束后验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金退还挂钩。履约验收的各项资料存档备查。

11.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

十二、货物的包装、发运及运输

12.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。货物的包装应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的规定。

12.2 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

12.3 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备接货。

12.4 货物在交付甲方前发生的风险均由乙方负责。

12.5 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方货物已送达。

十三、违约责任

13.1 甲方无正当理由拒收货物的，应向乙方偿付拒收货物总价5%的违约金。

13.2 甲方无故逾期验收和办理货款支付手续的，应按逾期付款总额每日万分之五向乙方支付违约金。

13.3 乙方逾期交付货物的，应按逾期交货总额每日万分之五向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期10个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，应向甲方支付合同总价5%的违约金。

13.4 乙方所交付的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

13.5 甲乙双方任何一方违反本合同约定的，除应承担上述违约责任外，违约方还应当赔偿因此给守约方造成的一切直接和间接损失，包括但不限于守约方的实际损失、预期可得利益损失以及为实现债权而产生的费用（包括但不限于诉讼费、保全费、保全担保费、律师费、公证费、鉴定费、差旅费）。

十四、不可抗力事件处理

14.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

14.2 不可抗力事件发生后，应立即通知对方并寄送有关权威机构出具的证明。

14.3 不可抗力事件延续120天以上，双方应通过友好协商确定是否继续履行合同。

十五、解决争议的方法

15.1 甲乙双方因合同签订、履行而发生的一切争议，应通过友好协商解决。协商不成的由甲方住所地人民法院管辖。

十六、合同生效及其它

16.1 本合同经双方加盖单位公章后生效。

16.2 本合同未尽事宜，遵照《中华人民共和国民法典》《中华人民共和国政府采购法》有关条文执行。

16.3 本合同正本一式两份，具有同等法律效力，甲方、乙方各执一份。

甲 方：（公章） 乙 方：（公章）

地 址： 地 址：

法定代表人或授权代表： 法定代表人或授权代表：

联系电话： 联系电话：

签订日期：

《\*\*\*\*\*\*\*合同》补充协议（合同附件）

招标文件及合同未约定事项，双方可友好协商签订补充协议。

第四章 采购需求

一、项目属性：

货物类项目。

二、项目概况

（一）项目背景

在现代社会，网络安全越来越受到关注，因为随着信息技术的迅速发展，网络攻击和安全威胁日益增多。如威胁日益增加：随着网络的普及和数字化转型，网络攻击和安全威胁的数量和复杂性不断增加。这可能包括恶意软件、病毒、勒索软件、网络钓鱼等威胁，导致数据泄露、服务中断和金融损失等问题。还有数据安全和隐私保护：随着大量敏感数据存储在网络中，数据安全和隐私保护成为重要问题。医疗机构、金融机构、企业等都需要保护客户数据和机密信息，以免受到未经授权的访问和滥用。综合来看，网络安全项目的背景是多样的，但都与保护网络和信息系统的安全性、满足法规要求和业务需求等密切相关。通过实施网络安全项目，组织可以增强网络安全防护能力，降低网络风险，并为业务提供更可靠的支持。

（二）项目建设遵循标准

遵循国家、行业及地方现行的规范和标准。

1. 项目清单

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 数量 | 单位 | 单价上限（元 ） | 产品类型 | 所属行业类型 | 产品属性 | 政府强制采购节能产品 |
| 1 | 防火墙（内网专线区出口） | 1 | 台 | 127,500 |  | 工业 | 货物 | 否 |
| 2 | 防火墙（互联网出口区） | 2 | 台 | 127,500 |  | 工业 | 货物 | 否 |
| 3 | 互联网区WAF | 1 | 台 | 137,700 | 主要产品 | 工业 | 货物 | 否 |
| 4 | 防毒墙（内外网） | 2 | 台 | 285,600 | 主要产品 | 工业 | 货物 | 否 |
| 5 | 入侵防御(互联网区) | 1 | 台 | 158,100 | 核心产品 | 工业 | 货物 | 否 |
| 6 | 入侵防御(内网区) | 1 | 台 | 158,100 |  | 工业 | 货物 | 否 |
| 7 | 互联网区上网行为管理 | 1 | 台 | 150,000 |  | 工业 | 货物 | 否 |
| 8 | 安全资源计算池 | 1 | 套 | 100,000 |  | 工业 | 货物 | 否 |
| 9 | 网络安全运维服务 | 1 | 年 | 620,000 |  | 软件和信息技术服务业 | 服务 | 否 |
| 10 | 监控网出口防火墙 | 2 | 台 | 105,000 |  | 工业 | 货物 | 否 |
| 11 | 物联网(IPC)安全防护备-1 | 1 | 台 | 102,000 |  | 工业 | 货物 | 否 |
| 12 | 物联网(IPC)安全防护设备-2 | 1 | 台 | 270,000 |  | 工业 | 货物 | 否 |
| 13 | 物联网安全监控平台 | 2 | 套 | 130,200 |  | 工业 | 货物 | 否 |

四、拟采购标的需要满足的技术、商务要求

（一）技术要求

1、防火墙（内网专线区出口）

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **功能、性能、配置要求** |
| 1 | ★实质性要求 | 所供设备≧6个10/100/1000M千兆电接口及≧12个combo接口每个Combo口为一对互斥的千兆口，吞吐≧8G。并发连接数≧320万。默认支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及URL分类管理、流控和IPSecVPN模块；包含不少于3年IPS特征库、防病毒特征库、应用识别及URL分类库升级授权,不少于3年硬件质保。 |
| 2 | 非实质性要求 | 1.访问控制  支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。  2.流量控制  支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套的流控。  3.会话控制  支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每IP总连接数控制、每IP新建连接数控制。  4.SSL VPN  支持SSL VPN功能，无需额外授权，SSL VPN用户数无限制，TLS加密算法支持选择TLS1.0、TLS1.1、TLE1.2和TLS1.3，及国密TLS，客户端支持系统windows、mac、linux等平台。  5.威胁情报防护  1）支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。  2）支持IPv4和IPv6环境下威胁情报查询和实时防护。  6.防病毒  1）支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定。  2）支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于1000万。  3）支持IPv4和IPv6环境下病毒检测和过滤功能；  7.SDWAN  1）支持广域网双边优化，通过使用TCP动态拥塞控制、TCP窗口处理机制优化、TCP选择性应答、使用快速TCP协议传输以及数据压缩机制，实现对业务访问的有效加速。  2）支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线。 |

2、防火墙（互联网出口区）

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **功能、性能、配置要求** |
| 1 | ★实质性要求 | 所供设备电源≧2个；≧6个10/100M/1000M自适应千兆电接口、≧4个千兆SFP接口，≧2个SFP+万兆接口，及≧1个接口扩展槽，≧64G SSD硬盘；支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及URL分类管理、流控和IPSec VPN模块；开通IPS特征库、防病毒特征库、应用识别及URL分类库不少于三年升级服务，不少于三年软硬件升级服务。支持定制国密加密卡，吞吐≧20G，最大并发数≧280万，新建连接数≧20万/秒，IPSec VPN吞吐量 bps≧2G，IPSec VPN默认隧道数≧10000，提供不少于3年硬件质保。 |
| 2 | 非实质性要求 | 1.虚拟化  支持基于硬件Hypervisor技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的CPU、内存、接口等资源。  2.访问控制  支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。  3.入侵防御  支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。  4.威胁情报防护  1）支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护；  2）支持IPv4和IPv6环境下威胁情报查询和实时防护；  5.SDWAN  1）支持广域网双边优化，通过使用TCP动态拥塞控制、TCP窗口处理机制优化、TCP选择性应答、使用快速TCP协议传输以及数据压缩机制，实现对业务访问的有效加速。  2）通过WAN虚拟化技术实现多条链路捆绑，同一个session数据可以在多条链路上同时传输，加速大文件复制业务；  6.系统管理  1）支持SYSLOG和SNMPv3，SYSLOG日志支持同时发给多个日志服务器  2）支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的TOP10统计展示、基于具体威胁事件/威胁类型的TOP10统计展示等，统计展示的时间周期包括1小时/1天/7天/30天。 |

3、互联网区WAF

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 1.所供设备≧1个HA口，≧1个RJ-45Console口，≧1个10/100/1000Base-T带外管理口，≧6个业务电接口（≧2组Bypass）,≧4个业务光口，≧1个网络接口板扩展槽位，≧2个USB口，冗余电源，吞吐量≧12G，最大并发数≧300万，新建连接数≧5万/秒，提供不少于3年质保，不少于3年Web应用防护特征库升级授权。 |
| 2 | 非实质性要求 | 1.接入模式  支持透明、代理模式、单臂部署；  2.Web攻击防护  1）支持HTTPS应用防护；  2）支持SQL注入攻击的检测与防御能力；  3）支持XSS攻击的检测与防御能力；  4）支持爬虫、CGI、漏洞扫描检测检测与防御能力；  5）内置Web应用防护事件库，并提供定期升级，能够针对最新及热点Web攻击事件进行快速响应；  3.攻击防护功能  1）攻击防护功能；  2）支持网站一键关停功能；  3）支持源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响。 |

4、防毒墙（内外网）

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 所供设备≥1U标准机架式设备，板载自带接口：千兆电口≥2个，Bypass电口≥6个；网络层吞吐率≥8Gbps；防病毒吞吐率≥2Gbps；冗余电源；扩展插槽：≥2个；硬盘容量≥1TB;CPU6核≥1,内存≥32G,支持Bypass功能。软硬件不少于3年质保，质保内应当包括系统、特征库、病毒库的升级。 |
| 2 | 非实质性要求 | 1.安全可视化  **▲能够对威胁进行可视化展示，展示维度至少包括威胁类型统计、近30天威胁事件趋势、攻击源IP、受影响主机、勒索&挖矿事件拦截统计、热门威胁事件TOP5、自定义黑名单等，并且满足在界面对威胁类型统计数据提取威胁事件日志。**  2.防病毒能力  1）能够支持超过100种协议的解析,包括但不限于  HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/  RTMP/DNS/IRC等；  2）**▲支持两个的防病毒引擎同时工作，并能够按需开启，并且客户可根据需求自定义病毒文件扫描的大小，最大可支持2G，也可以针对超过20层的文件进行检查。**  3）能够与高级持续性威胁增强侦测模块联动，获取高级持续性威胁增强侦测模块侦测到的C&C黑名单，并阻止C&C违规外联，有拦截弹框提示且提供事件详情。此外，支持提交可疑文件、URL、IP及域对象至增强定制化沙箱模块做联动分析，并根据分析结果做进一步处理。  3.挖矿治理  产品需要具备在网络边界的挖矿检测和拦截能力，并能够直观展现拦截的挖矿事件。  4.威胁情报  1）能够支持威胁情报能力以覆盖更大范围的威胁检测。  2）支持用户自定义黑/白名单，支持URL黑/白名单设置、支持邮件收发件人黑/白名单设置、支持基于SHA1的文件黑/白名单设置。  6.安全性和可靠性  1）为确保管理安全，必须支持通过加密的SSL协议访问管理控制台。提供BYPASS功能，在故障时能自动实现直通功能。  2）支持手动软件bypass的能力，支持指定IP、端口设置bypass，支持设置会话数阈值。  3）支持手动清理主进程功能，并可对CPU、内存阈值进行设置，当超过该阈值，防毒墙主进程自动清理且不中断业务。 |

5、入侵防御(互联网区)

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 提供≧1个RJ-45Console口，≧1个管理口，≧1个HA口，≧4个具备BYPASS功能的10/100/1000Base-T接口，≧2个千兆光口，≧2个万兆光口，≧2个扩展插槽，≧2个USB口，最大IPS 吞吐量≧20G，最大并发连接数≧400万。包含不少于3年硬件质保，不少于3年特征库升级授权。 |
| 2 | 非实质性要求 | 1.入侵防御功能  1）系统应内置专业的入侵防御特征库，覆盖信息泄漏、权限绕过、未授权访问、文件上传、文件读取、文件下载、文件包含、SSRF、XXE、CSRF反字列化、代码执行、命令执行、XSS攻击、SQL注入等攻击类型，入侵防御特征数量至少在14000条以上。  2）为强化防御能力，应支持多种规则变更部署模式，至少包括自动防御模式、试运行模式和手动防御模式。  规则详情应至少包含影响系统、影响服务、影响应用、事件处理流程和判定，并支持攻击阶段、攻击结果、精确度、ATT&CK编号及概述措施。  3）规则应支持双向检测功能，根据双向流量检测攻击，输出检测结果包含正在利用、攻击成功，应支持HTTP请求/响应缓存。  3.部署方式  支持路由模式，至少包括：静态路由、策略路由、ISP和OSPF路由协议。  4.解码能力  **▲支持HTTP协议自适应解码、URL解码、UTF7解码、base64解码、XML解码、Unicode解码、十六进制转换、CHR解码、UTF-7解码，支持解析7层以上混合编解码能力，可实现对多层编码攻击的检测，支持格式文本解析JSON解析、html解析、multipart解析。**  6.高可用性  1）支持软件Bypass功能，通过CPU和内存阈值实现软件Bypass的开启。  2）支持重点资产和应用监控，当资产和应用出现异常时，通过syslog和邮件进行告警，并可以记录日志。 |

6、入侵防御(内网区)

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 1.提供≧1个RJ-45Console口，≧1个管理口，≧1个HA口，≧4个具备BYPASS功能的10/100/1000Base-T接口，2个千兆光口，≧2个万兆光口，≧2个扩展插槽，≧2个USB口，最大IPS吞吐量≧20G，最大并发连接数≧400万，冗余电源，不少于3年硬件质保，不少于3年特征库升级授权。 |
| 2 | 非实质性要求 | 1.入侵防御功能  1）系统应内置专业的入侵防御特征库，覆盖信息泄漏、权限绕过、未授权访问、文件上传、文件读取、文件下载、文件包含、SSRF、XXE、CSRF反字列化、代码执行、命令执行、XSS攻击、SQL注入等攻击类型，入侵防御特征数量至少在14000条以上。  2）**▲提供不少于11种规则集，至少包括严格检测模板、物联网检测模板、WEB服务器模板、僵木蠕虫检测模板等，规则应支持影响系统、攻击阶段分布、协议分布、动作分布可视化统计展示，规则响应动作应支持标记设备信息，重置报文携带设备信息。**  3）规则详情应至少包含影响系统、影响服务、影响应用、事件处理流程和判定，并支持攻击阶段、攻击结果、精确度、ATT&CK编号及概述措施。  4）规则应支持双向检测功能，根据双向流量检测攻击，输出检测结果包含正在利用、攻击成功，应支持HTTP请求/响应缓存。  2.部署方式  支持路由模式，至少包括：静态路由、策略路由、ISP和OSPF路由协议。  3.解码能力  支持HTTP协议自适应解码、URL解码、UTF7解码、base64解码、XML解码、Unicode解码、十六进制转换、CHR解码、UTF-7解码，支持解析7层以上混合编解码能力，可实现对多层编码攻击的检测，支持格式文本解析JSON解析、html解析、multipart解析。 |

7、互联网区上网行为管理

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 所供设备网络吞吐量≥10Gbps，应用层吞吐量≥1Gbps，支持用户规模≥5000人；配置≥6个千兆电口，≥2个万兆光口；设备需配置SSD硬盘，硬盘容量≥800GSSD；软硬件提供不少于3年原厂质保。 |
| 2 | 非实质性要求 | 1.多主模式  为提高产品冗余性，要求所投产品与现网的的上网行为管理必须支持两台及两台以上设备同时做主机的部署模式；  2.网页过滤  1）支持根据访问的URL和网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为；  2）支持在放行URL时，自动放行主域名的子链接中被禁止的网站，保证网页显示完整；  3.应用识别规则库  设备内置应用识别规则库，支持超过9000条应用规则数，支持超过6000种以上的应用，并保持每两个星期更新一次，保证应用识别的准确率；  4.P2P智能流控  支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。 |

8、安全资源计算池

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 所供设备配置≥2U标准机架式，配置CPU≥2颗CPU，每颗基础频率规格不低于2.4GHZ 16C,内存≥128GB,系统盘≥2块480GB SSD,缓存盘≥2块企业级960G SSD,数据盘≥8块8TBHDD,网络接口≥4个千兆电口、≥2个万兆光口;配置冗余电源;提供不少于3年原厂质保服务。 |
| 2 | 非实质性要求 | 1.知识产权要求  云平台为国内自主研发软件产品，禁止借用第三方合作伙伴软件整合，云平台不基于任何开源项目二次开发，平台核心代码开源，厂商掌握软件自主知识产权。  2.产品成熟度要求  1）云平台需支持对接主流存储类型，支持通过图形化添加本地存储、NFS、IPSAN、FCSAN和分布式存储等存储类型，且在同一集群中同时支持SAN和分布式存储、本地存储和分布式存储，不需要通过命令行进行对接。不同类型存储之间支持虚机跨存储冷迁移和热迁移。  3）**▲所投产品厂商需具备国产化适配能力，至少适配过6家国产芯片，支持同一管理平台下同时纳管2种以上芯片集群。**  3.计算虚拟化要求  1）云主机需支持WINDOWS、LINUX等操作系统，兼容常见的操作系统。必须包含对以下操作系统的支持：WindowsServer2016，WindowsServer2012，WindowsServer2008，WindowsServer2003，Ubuntu，Centos，kylinv10，UOS等。  2）云平台需支持OVF模板管理，支持上传vmdk格式镜像，支持通过OVF模板（ovf/vmdk/mf格式）导入云主机，支持导出ova格式云主机。需支持完整的云主机生命周期管理，提供云主机的创建、删除、修改、启动、重启、暂停、停止、恢复、关闭电源、更换操作系统、重置云主机等功能。云主机需支持定时器功能，可创建定时任务完成云主机启动、重启、停止、创建快照等操作；支持自定义执行时间、任务内容、执行周期等。云主机需支持热迁移，云主机无需停机即可将云主机从一台宿主机迁移到另一台宿主机上，保障业务连续性。  6）需支持弹性伸缩功能，根据业务需求和策略自动调整计算能力。可根据服务器的资源使用情况，自动的新增和缩减服务器实例数。  4.网络虚拟化要求  1）需支持软件定义云平台内部网络，无需借助外部网络设备，云平台通过软件定义网络创建二三层网络，提供VLAN、VXLAN等二层隔离技术。  2）需支持可视化方式展示云平台网络规划拓扑，帮助用户更高效地进行网络规划、管理。  5.调优功能  云平台需支持智能优化调优功能，通过一键全局设置，快速优化云平台能力，包括云平台性能调优、生产环境优化、高可用快速恢复和安全配置等。 |

9、网络安全运维服务

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 网络安全运维服务为壹年，自项目验收之日起算。服务内容投标人需依据医院要求在中标后列明服务内的周期及服务交付物。 |
| 2 | 非实质性要求 | 1.运维服务  在服务期内对安全设备进行常态化维护工作，包括设备运行安全监测、设备运行安全审计、设备及策略备份更新等工作。分析安全设备和态势感知的威胁日志与告警。  1）服务期内提供不少于1名驻场安全运营人员，具有PMP或CISP认证证书，有5年以上安全从业经验。  2）负责日常巡检、资产完善、设备安全策略梳理、配置、优化及备份、设备特征库升级、设备维护、日常安全监测分析和响应、配合完善安全管理制度流程等工作，提供5\*8小时驻场服务，重要节假日期间提供7\*8小时驻场服务。  3）提供1名非驻场项目服务经理，总体把控安全运营的进度、风险、质量、协调公司后台专家资源、专家级安全分析服务和项目指导。指导驻场产品专家运营工程师的项目工作，检查并审核工作内容，编辑安全月报，根据客户场景和月报分析提供安全建议，针对新的业务场景提供安全建议。  4）配备二线服务专家支持服务，提供7\*24小时远程服务，远程服务专家提供对驻场安全技术人员的工作指导和督查。  5）按照运营周期提供每周、每月、每年的《安全运营服务报告》  2.资产梳理服务（每季度至少提供1次）  配套自动化管理组件，具备资产发现、威胁管理，与态势感知、漏洞扫描进行配合，形成动态资产台账。动态资产台账依据资产的重要程度进行自动化分组（互联网暴露资产、内网业务资产及其他资产）。  3.基线核查服务（每季度至少提供1次）  对网络设备、安全设备、操作系统、数据库以及中间件的安全配置基线要求设定，并定期检查协助系统运维人员实施安全加固。  4.策略优化服务  针对已采购的网络安全设备、进行策略细粒度配置，细化为ip+端口+特定业务策略。编写各项模板记录与总结。  1）提供对网络安全工具、服务器及业务系统的安全基线定义及安全策略优化服务，定期巡查（至少1次/月）安全工制，评估影响并协助调整策略优化。  2）根据采购人实际需求持续提供安全策略优化服务，每次服务结束后，提供出具《南京江宁医院安全策略优化报告》《南京江宁医院安全策略优化确认单》以及《南京江宁医院安全策略优化记录》。  3）对南京江宁医院网络安全设备的控制策略是否起到作用、是否合理高效进行检查和改进，及时发现和控制风险。在安全服务的过程中，需要持续指导信息系统各个层面的安全策略进行优化。  4）通过持续优化网络及系统架构、设置调整网络防护策略，以实现有效提升防护质量、有效缩小暴露面。  5.重要时期保障服务  日常对态势感知进行分析和对探针的数据质量核验，输出每日风险报告，在重保时期进行增加一名安全服务远程专家进行安全值守。  6.风险评估服务（每季度至少提供1次）  运用漏洞扫描等技术手段，对所有网络、操作系统、数据库、应用等进行全量评估，发现潜在的安全漏洞，提交修复建议；  7.攻防演练服务（每年至少提供1次）  按需组建攻击方对业务目标进行模拟的演练攻击。检验已有的防御的有效性与流程便捷性；  8.基线加固服务（每季度至少提供1次）  针对端口开放多，配置不合理，终端防御缺失等问题，上门进行基线加固。针对系统、应用版本问题提出加固建议方案，指导应用厂商进行基线加固。  1）对南京江宁医院网络设备、安全设备、操作系统、数据库以及中间件的安全配置基线要求，结合安全评估结果，提出安全加固整改建议。  2）持续提供安全加固服务，提供安全加固的技术指导，提供监督检查，每次服务结束后，提供《南京江宁医院安全加固报告》。  3）结合威胁情报、专家指导意见、风险评估、内部安全检查、安全运营平台监测等安全加固线索，综合评估威胁影响级别、威胁影响范围等维度，制定安全加固方案，实施安全加固，检查安全加固结果，持续提供合理的安全加固措施，安全加固对象包括但不限于主机系统、数据库、WEB应用系统、微信小程序、移动APP等。  9.云端监测服务  服务工具可针对互联网开发业务，定期进行风险监测，监测包括网页篡改、暗链死链、敏感词、网站可用性、漏洞风险等监测满足院内服务站点要求。  10.网络空间威胁预警  **▲提供不少于300个授权，由网络空间威胁预警系统对客户内网各类终端设备进行监控，并自动分析网络中各类网络设备的威胁程度，提供TOP20威胁名单，并针对高危设备提供分析报告及处理预案。**  支持动态变换，虚拟IP不断变化；  支持虚拟组网，支持构建虚拟网络，用来迷惑和误导攻击者及快速定位攻击源。  支持虚拟响应，支持同网段虚拟响应，多网络虚拟响应；多种网络协议虚拟响应。  支持短时威胁评分，包括实时报警记录，最近七天的威胁评分折等。  支持端口威胁分析，包括攻击端口，端口分析等。  11.护网服务  提供不低于以下要求的软硬件系统租赁服务1年，不限于以下服务。  1）服务工具具备风险优先级排序能力，排序依据包括资产重要性、漏洞等级、弱口令、互联网暴露高危服务以及安全事件等级等多个维度；  2）流量分析处理具备以下能力≥10Gbps，万兆光口\*≥2,千兆电口\*≥2，标配交流冗余电源。  3）提供对抗时期的工作台，协助提供重保期间的守护流程和检测防御策略，包含工作台可展示待处理弱口令、新增外网暴露高危服务、新增站点、待处理漏洞等内容，对已发现的风险可以编辑处置状态。  4）可根据需求在服务工具上开启内网蜜罐实现内网攻击诱捕。  5）对研判的真实安全风险和事件通过服务组件或联动的方式进行快速阻断和处置，降低安全事件的风险影响，不限于IP或域名  6）支持基于源/目IP对监测到的攻击行为进行阻断、封禁，支持点对点封禁策略。支持服务工具与运营管理平台策略同步  7）溯源分析：对服务工具所发现的安全事件可以针对单个安全事件进行聚合分析，综合展示事件各维度的攻击链状况，提供自动化溯源分析能力。  8）支持与服务工具联动拦截，对安全事件链中分析的来源ip进行拦截。当发出拦截指令后，阻断系统将该来源ip地址加入其黑名单，阻止其访问接入的真实资产。  9）提供威胁检测看板，可根据用户需求自定义增加或删除安全数据分析小组件，支持可视化界面的自定义编辑。可直观查看风险检测汇总概览信息；提供可视化的ip资产台账管理列表、业务系统台账管理列表；可从弱口令、高危服务、漏洞、安全事件等维度查看详情；  10）支持在护网期间提供重保时段自动防御策略配置功能，可自定义配置拦截策略并实现无需人员值班自动阻断外部攻击行为；  12.应急响应服务  1）按需提供应急响应服务，每次现场应急处置结束后，提供《应急响应事件记录单》、《安全事件分析》、《安全事件处理总结报告》。  2）对南京江宁医院已发生网络安全事件进行响应，协助南京江宁医院检查所受影响的系统，对攻击事件进行溯源，找到问题的根源并提出解决方案，协助后续处理，提供应急响应报告。  3）在发生应急事件时，要求成交供应商在10分钟内响应，安全服务团队60分钟内到达现场，并在采购人要求时间内提出解决方案并解决。  4）需要提供7×24小时应急响应和处置服务，在发生网络安全事件时，可提供现场应急和远程应急等方式，迅速提供应急响应专家协助处置，协助进行事件原因调查，检查所受影响的系统，找出事件的根源、查出威胁的来源与安全弱点、找到问题正确的解决方案，快速恢复系统，根除隐患，判定事故的责任，提供应急响应报告。  13.安全培训服务  每年组织1次安全培训，培训内容包含但不限于技术研究类、攻防技能培训类、安全政策法规解读、安全热点事件深度剖析 |

10、监控网出口防火墙

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 1.提供≥1U设备,≥8个千兆电口,≥4个SFP千兆光口；≥1个可扩展插槽，吞吐率≥6Gbps，并发连接数≥150万，最大并发连接数（防火墙+APP+AV+IPS）≥100万，IPSEC隧道数≥500，SSL用户数≥100，不少于三年基础硬件保修和系统软件维保服务。IPS+AV+应用特征+URL库≥3年。 |
| 2 | 非实质性要求 | 1.虚拟化  **▲支持基于硬件Hypervisor技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的CPU、内存、接口等资源。**  2.访问控制  1）支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。  2）支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每IP总连接数控制、每IP新建连接数控制。  3.入侵防御  1）支持并开通网络入侵检测及防御功能，入侵防御事件库事件数量不少于3000条。  2）支持IPS抓包取证，可选择将产生IPS事件的会话所有报文进行存储，并与IPS日志关联一键导出。  4.防病毒  1）支持并开通对HTTP、FTP、SMTP、POP3、IMAP协议的病毒检测和过滤功能；  2）支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于200万。  5.资产防护  1）支持通过主动及被动探测方式，识别终端类型（至少包括：PC、网络打印机、网络摄像机、网络设备、防火墙、负载均衡等），支持多种资产异常告警选项包括MAC地址、操作系统、厂商、类别、指纹等。  2）支持资产行为画像，通过资产的连接关系、应用、应用流量、并发连接等的图形化展示；  3）支持对资产的行为学习，自动学习资产相关的流量以及网络连接关系，通过连接关系拓扑可以进行阻断、一键生成安全策略操作；  10.其他  2）支持链路质量实时探测,并基于链路的丢包、延迟、抖动等因素，进行智能选路功能。 |

11、物联网（IPC）安全防护设备-1

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 提供物联网（IPC）安全防护设备，冗余电源，配置千兆电口≥8个、万兆光口≥12个，最大处理能力≥2000路高清视频（4M码流）安全管控；不少于3年原厂质保服务。 |
| 2 | 非实质性要求 | 1.产品性能  **▲设备本身不能出现对视频业务产生如视频抖动、卡顿等现象，基于SIP的视/音频传输时延＜20微秒。**  2.安全准入  1）支持MAC认证功能，MAC地址在白名单中的终端能够通过设备进行正常访问，MAC地址不在设备白名单中的终端通讯会被阻断；支持IP认证功能，IP地址在白名单中的终端能够通过设备进行正常访问，IP地址不在设备白名单中的终端通讯会被阻断。  2）支持符合GB35114标准的终端接入检测功能，可对不符合GB35114的终端接入进行阻断并告警；  3.安全防护功能  1）支持DDoS攻击防护功能  2）支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断；  4.资产管理功能  1）支持全资产类型一机一档功能，资产类型包括IPC、PC、NVR、服务器、网络设备、诱导屏、信号灯、人脸识别、门禁等，同时支持一机一档按资产类型导入导出功能；  2）支持资产属性完整度检查功能，可查看到单个资产的属性完整度和整个类型属性完整度的统计信息；  3）支持基于多维度的资产在线率统计功能，可根据资产类型和属性进行分组在线率统计。 |

12、物联网（IPC）安全防护设备-2

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 提供物联网（IPC）安全防护设备，双电源，配置千兆电口≥8个、万兆光口≥12个，最大处理能力≥600路高清视频（4M码流）安全管控；不少于3年原厂质保服务。 |
| 2 | 非实质性要求 | 1.产品性能  设备本身不能出现对视频业务产生如视频抖动、卡顿等现象，基于SIP的视/音频传输时延＜20微秒；  2.安全准入  1）支持MAC认证功能，MAC地址在白名单中的终端能够通过设备进行正常访问，MAC地址不在设备白名单中的终端通讯会被阻断；支持IP认证功能，IP地址在白名单中的终端能够通过设备进行正常访问，IP地址不在设备白名单中的终端通讯会被阻断。  2）支持符合GB35114标准的终端接入检测功能，可对不符合GB35114的终端接入进行阻断并告警；  3）支持对扫描行为的识别与阻断功能，可对存在扫描行为的终端进行阻断并告警；  3.安全防护功能  1）支持DDoS攻击防护功能；  2）支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断；  4.资产管理功能  1）支持全资产类型一机一档功能，资产类型包括IPC、PC、NVR、服务器、网络设备、诱导屏、信号灯、人脸识别、门禁等，同时支持一机一档按资产类型导入导出功能；  2）支持资产属性完整度检查功能，可查看到单个资产的属性完整度和整个类型属性完整度的统计信息；  3）支持基于多维度的资产在线率统计功能，可根据资产类型和属性进行分组在线率统计；  5.自学习功能  支持对新入网终端进行资产识别，支持对未知业务协议特征自学习功能，支持对新入网业务延时阻断功能。 |

13、物联网安全监控平台

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 功能、性能、配置要求 |
| 1 | ★实质性要求 | 提供不少于3年软件升级服务 |
| 2 | 非实质性要求 | 1.资产管理功能  支持全资产类型一机一档功能，资产类型包括IPC、PC、NVR、服务器、网络设备、诱导屏、信号灯、人脸识别、门禁等，同时支持一机一档按资产类型导入导出功能；  支持资产属性完整度检查功能，可查看到单个资产的属性完整度和整个类型属性完整度的统计信息；  支持一机一档资产类型和属性自定义扩展功能，可对新添加的资产自定义新的类型，同时可对该类型资产自定义新的属性；  2.资产识别特征自学习功能  1）**▲默认终端特征库数量≥5000条。**  2）支持基于web特征自学习识别功能，支持基于端口特征自学习识别功能，支持基于型号特征自学习识别功能，支持基于流量特征自学习识别功能。  3.新业务入网功能  支持对新入网终端进行资产识别，将终端添加到资产库；支持对未知业务协议特征自学习功能，下发特征后不再产生告警日志；支持对新入网业务延时阻断功能。  4.配套硬件  配置≥10核≥2.4G，≥2千兆网口，≥1T硬盘，≥16G内存及HDMI线缆及分屏器。 |

★（二）商务要求

1、总体要求：

（1）供应商提供的货物（含配件）应是全新的、未使用过的原装合格正品，并保证所提供货物的开箱合格率为100%，外观和内在质量都不得有任何问题。采用的是最佳材料和第一流的工艺，并在各个方面符合合同规定的质量、规格和性能要求。设备经过检验、正确安装、合理操作和维护保养，在设备寿命期内运转良好。在规定的质保期内，中标供应商应对由于设计、工艺或材料的缺陷或故障负责。在未验收前，货物保管、安全均由中标供应商负责。

（2）所提供的技术资料（含软件）完整正确，数据和资料准确无误，包括：产品验收标准（含产品合格证验收清单等）；技术说明书；使用说明书；用户手册（中文）；设备安装调试资料；配置清单；备品备件易耗件清单及合同中要求的其他文件资料。能够保证设备按时正确地安装、调试和验收，并能满足正常运行和维修保养的需要。

（3）供应商负责将货物运到采购人指定地点，由供应商负责办理运输、装卸、安装、调试等，并协助采购人组织验收，检验不合格或不符合质量要求，供应商除无条件退货、返工外，还应承担采购人的一切损失。

（4）供应商要在提供完整、可靠设备的同时，还必须为整个系统提供规范、达标的安装工作。安装工程所需的仪器和专用工具由供应商自备。完工后，通过供应商提供的设备和安装服务，能满足采购人的要求。

（5）采购人使用该货物的任何一部分，当受第三方提出的侵犯其专利权、商标权或工业设计权的投诉时，一切后果由供应商负责。

（6）质保（维保）及售后要求

所有货物软硬件均提供三年原厂商质保服务。

①质保期内，每年维护保养1次，维护保养及更换损坏件的费用包含在投标总价中。

②质保期内，一旦产品发生质量问题，供应商接到报修请求，在2小时内响应，4小时内维修人员到达现场进行修理、更换或退货，费用由供应商负责。如供应商在接到通知后2小时内没有答复，则视为承认质量问题并承担由此发生的一切费用。质保期内家具的一切质量问题，更换部件及家具本身质量原因造成的直接经济损失全部由供应商负责。无法短时间完成维修的，应向采购人提供应急备用产品。

③质保期外，供应商提供终生服务，在货物的设计使用寿命周期内，供应商能保证采购人更换到原厂正宗的备件材料，确保产品的正常使用。

④质保期内维修（人为因素除外）费用包含在投标总价中，质保期外提供不高于市场价格的终身维护。中标后提供质保期外配件价格明细表。

2、本项目如需专业分包，必须经由采购人批准，未经批准，发现有转包或分包现象，立即终止合同，给采购人造成的损失，中标人应当予以赔偿，且承担相应的法律责任。

3、中标后实施要求：

（1）针对采购人业务特点阐述系统实施方法,包括但不限于项目管理、需求确认、平台建设、测试、试运行和最终验收等工作的实施方案。

（2）阐述项目实施的组织架构，并描述实施预期的时间进度表，提供具有明确里程碑的项目实施计划。

（3）要求投标人提供本项目中所有交付物清单(包括产品、技术文档等)。

（4）要求具有长期的本项目专属的技术支持人员，工作语言为中文，项目文档为中文。所有参与本项目实施的投标人人员，未经采购人许可,不得调换。

（5）投标人在本项目实施过程中，须服从采购人的管理，同时满足适用的法律法规和有关监管部门的监管要求。

（6）投标人须在本项目中为采购人提供的应用系统以及投标人为应用系统运行所提供的各类软件、中间件、插件，在项目使用范围内，均无授权许可数量和使用时间限制。如发生授权、许可或知识产权纠纷，由投标人承担所有责任，如造成不良影响和经济损失，由投标人负责赔偿。

4、综合管理和质量保证要求：

（1）负责制定项目计划，并按照采购人的要求进行必要的调整，监督和控制项目进度。

（2）负责管理安排项目资源。

（3）负责管理项目范围和需求变更，并配合采购人管理部门完成变更手续的签署工作。

（4）负责项目配置管理、交付物管理、项目质量管理、问题管理和风险管理等项目管理工作。

（5）负责与采购人沟通并按照要求进行工作汇报。

（6）投标人应保证提供的产品和服务，不得存在影响其交付系统满足采购人要求的任何缺陷，亦不存在实质性限制或影响其交付系统的性能、可靠性、稳定性或可扩展性的任何缺陷。

（7）投标人应保证提供的系统中不得包含或隐藏危害或可能危害采购人利益的计算机代码，包括但不限于后门程序、病毒、黑客程序、蠕虫、逻辑炸弹、时间炸弹等。

5、测试要求：

系统部署、安装完成后，按照系统要求的基本功能逐一测试。

单项测试：单项产品安装完成后，由投标人进行产品自身性能的测试。

网络联机测试：系统安装完成后，由投标人对所有部署、安装的产品进行联网运行，并进行相应的联机测试。系统运行正常，联机测试通过。

验收测试要求：

（1）编写服务验收计划和方案。

（2）按投标要求准备用户服务验收效果展示案例。

（3）配合执行用户验收测试或展示。

（4）负责服务平台或服务内容的修补。

（5）配合完成用户验收测试报告。

6、系统上线、试运行、最终验收要求：

（1）协助采购人完成系统上线。

（2）负责制定试运行方案、流程和策略。

（3）支持系统试运行工作。

（4）协助采购人完成最终验收。

7、组织实施及人员要求：

（1）投标人必须成立独立的项目组，安排不少于5人的专业技术人员参加本项目。项目经理或项目负责人需保证将全部工作时间投入本项目，不得在兼任其它项目负责人或项目经理；项目组主要成员需保证将80%以上的工作时间投入本项目。

（2）在项目组织机构中应明确各岗位的职责、任职资格，确保工程顺利实施。根据集成工作的业务性质，应分别配备有实际业务经验的项目经理承担本项目的管理工作。

项目组成员必须具有强烈的服务意识和高度的责任感。

项目组应建立健全保障项目顺利实施的各项规章管理制度和质量保证体系。

8、交付物要求：

按项目建设和采购人项目管理制度要求提交。

（1）应用成果

所有服务内容及相关技术成果版权均属于采购人，投标人未经采购人许可，不得转让、共享或提供给第三方。投标人承诺对采购人所有服务文档、数据资料和成果均负有保密责任。

（2）软硬件货物

应向采购人提供招标文件中所规定的货物。

（3）项目文档

投标人在完成项目建设过程中，须按项目建设和采购人项目管理制度要求提交各类文档。

9、培训要求：

（1）投标人应详细制定人员培训方案，培训方案包括培训目的、培训时间安排、人员层次、人数、次数、培训课程、主要内容、培训组织形式等；

（2）中标人应提供不少于2次的现场培训服务，培训内容、培训地点及培训时间由采购人指定。

（3）中标人应保证提供最有经验的教员，使业主单位相关人员在培训后能够独立地对无人机指挥和综合保障平台进行管理、使用、维护，而不需中标人的人员在场指导。

（4）培训内容应包括所提供产品的性能、使用、维护等各个方面。

（5）培训教材应使用标准中文。

（6）投标人负责培训相关的所有费用。

10、验收要求：

投标人需要满足以下的验收要求：

（1）投标人需按合同的约定，完成部署、安装、配置等建设任务；

（2）投标人需按合同和相关规定提交初步验收文档资料；

（3）投标人需提交初步验收申请，采购人签字认可。

（4）试运行时出现的问题均已被解决且采购人满意，并按照本项目合同和政府有关管理部门的规定提供了全部服务和对应资料。投标人需提交最终验收申请，采购人签字认可。

11、运维要求：

主要内容包括但不限于：

（1）技术支持服务

投标人就采购人在使用系统过程中所遇到的任何问题提供及时的反馈、解答及咨询服务。

对于本项目中所提供的系统软件，投标人应提供相应的软件升级版本，采购人有软件升级要求时，投标人还应提供升级服务和技术支持，费用包含在报价中。

（2）系统故障处理服务

系统出现故障时，投标人安排专业人员进行故障的排除和修复，使系统恢复正常运行状态。

（3）培训

投标人在保修期服务工作过程中，根据用户需要，提供与系统使用、管理、运维等有关的培训。

12、报价说明：

（1）报价为全包费用报价，最终投标报价应是本采购文件所包含确定的全部工作内容及本采购文件未说明但完成该项目必须包含的所有全包费用的价格体现。投标最终报价应包含但不限于设备采购安装费、备品备件费、现场办公费、场地费、交通费、劳务费、伴随服务费、专用工具等所有含税费用及项目实施过程中涉及到的一切费用。同时，还应包含支付给员工的工资和国家强制缴纳的各种社会保障资金，以及供应商认为需要的其他费用等。

（2）供应商的任何错漏、优惠、竞争性报价不得作为减轻责任、减少服务、增加收费、降低质量的理由。

13、付款条件

① 合同签订后，甲方支付合同总价款的30%作为预付款。

② 供货结束并验收合格后，甲方支付合同总价款的70%。

③ 满足合同约定支付条件的，甲方收到乙方发票后10个工作日内，将资金支付到合同约定的乙方账户。

14、交货时间、地点

1.交货时间：本项目交付期自合同签订之日起45天内，需在时间内完设备安装、调试、培训、验收。

2.交货地点：中标人按照采购人指定的地点进行设备及系统安装、调试，相关费用由中标人负责。由采购人组织验收，检验不合格或不符合质量要求，中标人除无条件返工外，还应承担采购人的一切损失。

（三）演示要求

1.视频文件的格式为\*.mp4或\*.avi，供应商须将视频文件分段压缩为\*.zip文件上传（单个文件不得大于50M，所有文件合计不得大于300M）。文件上传方式见《操作手册》，上传的演示视频将作为投标文件的组成部分。视频时长总计不超过15分钟。

2.演示内容详见“第五章 评标方法与评标标准”。

第五章 评标方法与评标标准

一、评标方法

1.采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的，按“三、评标标准中第2.1项”得分由高到低顺序排列。在投标文件满足招标文件全部实质性要求的供应商中，按照评审得分由高到低推荐3名中标候选人。

2.核心产品评审。多家供应商提供的核心产品品牌相同的，按一家供应商计算，评审后得分最高的同品牌供应商获得中标人推荐资格。

二、小微企业价格扣除

1.本项目全部货物制造商为小微企业的，对报价给予15%的扣除，用扣除后的价格参与评审。

2.残疾人福利性单位视同小型、微型企业，给予与小微企业相同的价格扣除，用扣除后的价格参与评审；监狱和戒毒企业视同小型、微型企业，给予与小微企业相同的价格扣除，用扣除后的价格参与评审。残疾人福利单位、监狱企业属于小型、微型企业的，不重复享受价格扣除。

**3.上述价格扣除政策仅适用于“非专门面向中小企业采购项目”**。

三、评标标准

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 评审因素 | 评审细则 | | 分值 | 分值  类型 | |
| **1.价格** | | | | | | |
| 1.1 | 价格分 | 采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算:投标报价得分=(评标基准价/投标报价)×30 | | 30 | 价格分 | |
| **2.技术** | | | | | | |
| 2.1 | 产品功能、性能、配置要求 | 产品技术参数全部满足招标要求的得满分14分；打★指标为必须满足项，如有负偏离将作为无效投标；打▲指标为重要指标，有1项负偏离扣2分；其余指标，有1项负偏离扣1分，扣完为止。 | | 14 | 客观分 | |
| 2.2 | 项目需求理解方案 | 投标人提供项目需求理解方案，包括对本项目建设的项目现状分析、建设背景等。  1、项目现状分析、建设背景等内容非常合理、针对性非常强，得5分；  2、项目现状分析、建设背景等内容比较合理、针对性比较强，得2分；  3、项目现状分析、建设背景等内容不够合理、针对性不强，得1分；  4、未提供的得0分。 | | 5 | 主观分 | |
| 2.3 | 总体技术  方案 | 评委根据投标人提供的对于本项目的总体技术方案（包括总体设计原则、建设思路、系统总体结构、设备兼容匹配符合规范）综合评分。  1、方案科学合理、符合性高，说明详实的得5分；  2、设计较合理、符合性较高，说明较详实的得2分；  3、设计不合理、符合性不高，说明不详实的，得1分；  4、未提供总体设计方案，或者方案与项目完全不符的，得0分。 | | 5 | 主观分 | |
| 2.4 | 实施方案 | 评委根据投标人提供的本项目整体实施方案（包括供货进度保证措施、质量保证措施、安装调试计划、进度安排控制、协调配合措施、应急措施、设备容错对接方案等内容）综合评分：  （1）方案阐述及提供的证明材料详细、合理，有很强的针对性，符合项目建设实际需求，得5分；  （2）方案阐述及提供的证明材料较为详细、合理，有较强的针对性，较符合项目建设需求，得2分；  （3）方案阐述及证明材料，基本符合项目建设需求，得1分；  （4）方案不合理、不符合项目建设需求或未提供方案的，不得分。 | | 5 | 主观分 | |
| 2.5 | 功能演示 | 评委根据投标人提供以下演示内容综合评分（每位投标人演示视频时长总计不超过15分钟）：  1、入侵防御(互联网区)功能  为确保规则库可靠，支持多种规则变更部署模式，至少包括自动防御模式、试运行模式和手动防御模式。  2、防火墙（互联网出口区）功能  为确保出口链路可靠，支持组建HA，例如主主模式、主备模式，其中主备模式下需支持按照设备的优先级进行主设备抢占，对于HA切换条件需要支持基于接口进行监控、网关监测。  3.网络安全运维服务  为满足运维管理需求，提供可视化大屏界面，支持采用空间立体化透视模式呈现攻击面，可360度自由旋转缩放透视查看，协助用户破除资产孤岛效应，洞察风险形式，直观快速掌握风险点。  4.网络安全运维服务  为了动态监测重要业务系统的安全情况，提供重要业务系统的探测与梳理能力，根据梳理出的业务系统资产信息分析出单位内部所使用的业务系统详情，梳理的维度包括但不限于业务系统关联的IP信息、关联站点信息、业务系统中存在的弱口令、高危服务、漏洞及提供的虚拟补丁数量；  以上每一项演示内容按理解程度完整、功能点展示全面，得2分；理解程度有偏差、功能点展示有缺漏的不得分；本项最多得8分。以上全部采用类似真实系统进行演示，如采用非类似真实系统（如DEMO、PPT等方式）进行演示的减半得分，最多得4分。  （未提供视频文件或因供应商自身原因视频文件无法打开或视频画面不清晰无法辨认的不得分。） | | 8 | 客观分 | |
| **3.服务** | | | | | | |
| 3.1 | 培训方案 | 评委根据投标人提供的对于本项目的培训方案（包含：培训计划、培训方法、培训质量控制等）综合评分：  （1）培训方案内容全面、详实可行，得 4分；  （2）培训方案内容较全面、较为详实可行，得 2 分；  （3）培训方案片面，方案可行性较差的，得 1 分；  （4）未提供方案或方案与项目完全不符的不得分。 | | 4 | 主观分 | |
| 3.2 | 运维服务方案 | 评委根据供应商提供的运维服务方案（包含但不限于服务内容、故障解决方案、专业技术人员保障等）进行综合评分：  1、供应商具备非常完善的运维服务方案，全面的服务内容、可行的故障解决方案、可靠的专业技术人员保障的，得5分；  2、供应商具备基本完善的运维服务方案，基本全面的服务内容、基本可行的故障解决方案、基本可靠的专业技术人员保障的，得2分；  3、未提供运维服务方案，得0分。 | | 5 | 主观分 | |
| 3.3 | 项目实施保障人员 | 投标人须针对本项目建立专门的实施交付团队，团队人员配置要求：  1、项目负责人：拟派项目负责人具有信息系统项目管理师证书、注册信息安全专业人员（CISP）证书、网络规划设计师证书，每有一项证书得2分，本项仅计项目负责人1人，最高得6分。  2、技术负责人：拟派项目技术负责人具有信息安全保障人员认证证书（CISAW）、系统集成项目管理工程师，每有一项证书得2分，本项仅计技术负责人1人，最高得4分。  除项目负责人、技术负责人以外的团队成员：拟派团队成员具有注册信息安全专业人员CISP证书、ITSS服务工程师、高级工程师证书（电子信息工程专业）证书，每提供一个证书得1分，最高得3分，一人多证最多得1分，不累计得分  投标人须上传项目负责人、技术负责人以及团队成员的相应证书原件扫描件及提供以上所有人员在投标单位2024年6月1日以来任意3个月缴纳社保的证明材料并加盖公章，不提供不得分。 | | 13 | 客观分 | |
| **4.履约能力** | | | | | | |
| 4.1 | 投标人业绩 | 投标人提供自 2021年1月1日以来（以合同签订时间为准）与本项目建设内容类似的（所提供案例要求至少包含防火墙或入侵检测或防毒墙等）的成功案例，每提供1个得2分，最高得4分（合同应能反映相关内容，合同盖章签字部分所在页等实质性内容须清晰，不清晰或未提供的不得分） | | 4 | 客观分 | |
| 4.2 | 软件著作权 | 供应商拟投入本项目的相关产品具有软件著作权证书（软件名称包含：“安全设备审计管理”“运维评价管理”“安全事件管理”“数字化运维平台”“网络运行监测”等关键字），每提供1个证书得1分，最多得5分，未提供不得分。  备注：所提供证书“软件名称”与评标标准约定名称不同时，应提供符合上述要求的内容（功能）说明及关键信息，否则不予认可。 | | 5 | 客观分 | |
| **5.节能环保** | | | | | | |
| 6.1 | 节能环保 | | 1.投标产品属于财政部、国家发改委公布的“节能产品品目清单”范围内的，投标人提供国家确定的认证机构出具的、处于有效期之内的该节能产品认证证书的，有1个得0.5分，最多得1分。投标产品属于政府强制采购节能产品或已在实质性要求中要求提供节能产品认证证书的，本项不得分。  2.投标产品属于财政部、生态环境部公布的“环境标志产品品目清单”范围内的，投标人提供国家确定的认证机构出具的、处于有效期内的该环保产品认证证书的，有1个得0.5分，最多得1分。 | 2 | | 客观分 |
| 合计 |  | | | 100分 | | |

第六章 投标文件格式

**投 标 文 件**

**项 目 名 称：**

**项 目 编 号：**

**投标人名称 ：（加盖电子公章）**

**日 期 ：**

投标文件目录

一、供应商信用承诺函

二、满足特定资格要求的证明文件（如有特定资格要求）

三、法人授权书

四、投标函

五、开标一览表

六、核心产品品牌一览表

七、投标分项报价表

八、技术要求响应及偏离表

九、商务要求响应及偏离表

十、中小企业声明函（如有）

十一、残疾人福利性单位声明函（如有）

一、供应商信用承诺函

供应商信用承诺函

南京市公共资源交易中心江宁分中心：

我公司 （供应商名称）郑重承诺：

我公司符合下列要求：

(一)具有独立承担民事责任的能力；

(二)具有良好的商业信誉和健全的财务会计制度；

(三)具有履行合同所必需的设备和专业技术能力；

(四)有依法缴纳税收和社会保障资金的良好记录；

(五)参加政府采购活动前三年内，在经营活动中没有重大违法记录。

如果我公司中标，将在中标结果公示后七个工作日内向采购人提供下列材料核验：

（1）营业执照副本或事业单位法人登记证书；

（2）参加本次政府采购活动前一年的经审计的财务报告（包括“四表一注”，法人成立满一年的提供）或参加本次政府采购活动前一年内的银行资信证明（法人或其他组织提供）或其他证明材料；

（3）履行合同所必需的设备和专业技术能力证明材料；

（4）参加本次政府采购活动前一年内至少一个月依法缴纳税收和社会保障资金的证明材料。

本公司对上述承诺内容的真实性、合法性、有效性负责，如有虚假，将依法承担相应责任。

供应商名称：（加盖电子公章）

日 期：

二、满足特定资格要求的证明文件

本项目申请人的特定资格要求中要求提供的材料。

三、法人授权书

法人授权书

本授权书声明： （投标人名称）授权 （被授权人姓名）作为我方参加编号为JSZC-3201XX-JZCG-G202X-XXXX项目采购活动的合法代理人，以本单位名义全权处理一切与该项目采购有关的事务。

本授权书自\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日起生效，特此声明。

被授权人身份证号码：

被授权人联系电话：（手机）

单位名称：（加盖电子公章）

单位地址：

日 期：

四、投标函

投标函

致：南京市公共资源交易中心江宁分中心

根据贵方编号为JSZC-3201XX-JZCG-G202X-XXXX的项目招标文件，我方正式提交投标函，并宣布同意如下内容：

1.按招标文件规定的各项要求，向买方提供所需货物（包含与货物相关的服务）。

2.我们完全理解贵方不一定将合同授予最低报价的投标人。

3.我们已详细审核全部招标文件及其有效补充文件，我们知道必须放弃提出含糊不清或误解问题的权利。

4.我们同意从规定的开标日期起遵循本投标文件，并在规定的投标有效期期满之前均具有约束力。

5.同意向贵方提供贵方可能另外要求的与投标有关的任何证据或资料，并保证我方已提供和将要提供的文件是真实的、准确的。

6.一旦我方中标，我方将根据招标文件的规定，严格履行合同的责任和义务,并保证在招标文件规定的时间完成项目，交付买方验收、使用。

7.我方为¨大型企业 ¨中型企业 ¨小型企业 ¨微型企业。（在对应¨内打“√”）

8.我方与本次投标有关信息

地 址：

邮 编：

电 话：

传 真：

开户行：

账 号：

投标人名称：（加盖电子公章）

日 期：

五、开标一览表

开标一览表

投标人名称：（加盖电子公章）

项目名称：

项目编号： 分包号：

|  |
| --- |
| 投标总报价 |
| 小写（元）： |

日 期：

六、核心产品品牌一览表

核心产品品牌一览表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品名称 | 产品品牌 | 规格或型号 |
| 1 |  |  |  |

投标人名称：（加盖电子公章）

**备注：供应商须按照表格要求明确填写所投“核心产品”的品牌，不得填报“/”“无”等内容，否则视为无效投标。**

七、投标分项报价表

投标分项报价表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 产品名称 | 品牌 | 规格或型号 | 交付期（天） | 数量 | 单位 | 单价 | 总价 |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| … | 投标总价（元）： | | | | | | | |

投标人名称：（加盖电子公章）

备注：

1.“投标总报价”应包括为完成整个项目所产生的所有费用，招标文件另有规定的除外。

2.《投标分项报价表》中“投标总价”应当与《开标一览表》中“投标总报价”一致。

3.供应商所投产品须与“第四章-项目清单”中的产品一一对应，如有缺项、漏项或者超出单价上限，视为无效投标。“项目清单”中分项仅为一项的，此表无需提供。

4.行数不够，可自行添加。

八、技术要求响应及偏离表

技术要求响应及偏离表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标文件要求 | 投标响应情况 | 正偏离、无偏离或负偏离 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

投标人名称：（加盖电子公章）

备注：

1.供应商必须对招标文件技术要求中的实质性要求（**斜体下划线内容或打“★”内容**）及其他要求做出明确响应。

2.技术要求中采购文件要求投标时提供证明材料的，供应商应按要求在此表下方提供。要求合同签订后提供证明材料的，中标供应商签订合同时应按招标文件要求和投标文件响应内容向采购人提供相应证明材料核验（如：白皮书、彩页、手册、网站截图、具有CMA标识的检测报告等）。中标供应商未按招标文件要求和投标文件响应内容提供相应证明材料或者提供的证明材料不符合招标文件要求的，视为提供虚假材料谋取中标，采购人将取消其中标资格。

3.供应商未对实质性要求作出明确响应的，或未按采购文件要求提供证明材料的，作无效投标处理。

4.行数不够，可自行添加。

九、商务要求响应及偏离表

商务要求响应及偏离表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标文件要求 | 投标响应情况 | 正偏离、无偏离或负偏离 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

投标人名称：（加盖电子公章）

备注：

1.供应商须对招标文件商务要求中的实质性要求（斜体下划线内容或打“★”内容）做出明确响应，否则视为无效投标。

2.行数不够，可自行添加。

十、中小企业声明函

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XXXXXXXXXXXXXXXXXXXXXXXXX（单位名称）采购编号为XXXXXXXXXXXXXXXXXXXXXXXXX项目（分包号：XXX）的采购活动，提供的货物全部由符合政策要求的中小企业制造。根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》(工信部联企业〔2011〕300号)的规定，相关企业（含联合体中的小微企业、签订分包意向协议的小微企业）的具体情况如下：

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

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

……

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：（加盖电子公章）

日 期：

备注：1.从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。2.在所属企业类型前的¨内打“√”。3.投标人如不提供此声明函，不得参加专门面向中小企业采购项目或者不得享受小微企业价格扣除政策。项目清单中列示的所有货物，投标人须在声明函中逐项列示并明确制造商的企业类型，如有缺失将按“不提供声明函”处理。此声明函将随成交结果同时公告，接受社会监督。4.货物采购项目中，货物的制造商应当为中小企业，不对其中涉及的服务的承接商、工程的承建商作出要求。

十一、残疾人福利性单位声明函

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，参加XXXXXXXXXXXXXXXXXXXXXXXXX（单位名称）采购编号为XXXXXXXXXXXXXXXXXXXXXXXXX项目（分包号：XXX）的采购活动，提供本单位制造的货物，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。

企业名称：（加盖电子公章）

日 期：

备注：

1.投标人如不提供此声明函，价格将不作相应扣除。

2.中标人为残疾人福利性单位的，此声明函将随中标结果同时公告，接受社会监督。

质疑函范本

一、质疑供应商基本信息

供应商名称：

地址： 邮编：

联系人： 联系电话：

授权代表： 联系电话：

二、质疑项目基本情况

项目名称：

项目编号： 分包号：

采购人名称：

三、质疑事项具体内容

质疑事项1：

事实依据：

法律依据：

质疑事项2：

……

四、质疑事项相关请求

请求：

签 字(签章)： 公 章：

日 期：

相关说明：

1.供应商提出质疑，应提交《质疑函》和必要的证明材料。

2.由授权代表负责质疑事宜的，《质疑函》附件中应提交由质疑供应商法定代表人签署的《授权委托书》。

3.质疑供应商针对项目的某一分包进行质疑的，《质疑函》中应明确分包号。

4.《质疑函》的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.《质疑函》的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，《质疑函》应由本人签字；质疑供应商为法人或者其他组织的，《质疑函》应由法定代表人、主要负责人，或者其授权代表签字或者签章，并加盖公章。

7.质疑供应商为联合体的，则《质疑函》中要求加盖公章之处，联合体各方均须按要求加盖公章。