**宁波大学附属妇女儿童医院信息安全提升项目**

**政府采购**

**公**

**开**

**招**

**标**

**文**

**件**

**采购编号：NBITC-202411414G**

**采购人：宁波大学附属妇女儿童医院**

**代理机构：宁波市国际招标有限公司**

**编制日期：2024年08月**

**温馨提醒**

**1、投标文件应按招标文件要求将“资格文件”、“商务和技术文件”、“报价文件”分别编制。**

**2、采购人可以对已发出的招标文件进行必要的澄清或者修改，将以“更正公告”的形式发布在政采云平台，供应商应及时登录政采云平台，进行浏览并下载，未及时浏览下载的责任自负。**

**3、如至开标现场，建议供应商自带电脑，以便于开标现场解密投标文件。**

**目录**

**[第一章 招标公告](#_Toc44162138)** [1](#_Toc44162138)

**[第二章 投标须知](#_Toc44162139)** [4](#_Toc44162139)

**[第三章 招标内容与技术需求](#_Toc44162152)** [37](#_Toc44162152)

**[第四章 商务条款](#_Toc44162153)** [61](#_Toc44162153)

**[第五章 评标办法及标准](#_Toc44162154)** [62](#_Toc44162154)

**[第六章 采购合同样本](#_Toc44162155)** [71](#_Toc44162155)

**[第七章 附件](#_Toc44162156)** [76](#_Toc44162156)

**第一章 招标公告**

发布时间：2024年08月13日

项目概况

宁波大学附属妇女儿童医院信息安全提升项目招标项目的潜在投标人应在政府采购云平台（www.zcygov.cn）获取（下载）招标文件，并于2024年09月03日14:00（北京时间）前递交（上传）投标文件。

一、项目基本情况

项目编号：NBITC-202411414G

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

预算金额（元）：1500000

最高限价（元）：/

采购需求：

标项1：

标项名称:信息安全提升

数量:1

预算金额（元）:1500000

简要规格描述或项目基本概况介绍、用途：具体详见招标文件第三章招标内容与技术需求。

备注：详细采购需求见本公告附件。

合同履约期限：标项1，合同签订后6个月内完成安装调试和试运行并通过采购人组织的验收。

本项目（否）接受联合体投标。

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单。

2.落实政府采购政策需满足的资格要求：无。

3.本项目的特定资格要求：无

三、获取招标文件

时间：2024年08月13日至2024年08月20日，每天上午00:00至12:00，下午12:00至23:59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

地点（网址）：政府采购云平台（www.zcygov.cn）

方式：1、供应商登录政府采购云平台（www.zcygov.cn）的注册账号后，进入政采云系统“项目采购”模块“获取采购文件”菜单，进行网上获取招标文件。如有疑问请及时咨询网站客服，咨询电话：95763。2、获取招标文件前，供应商应在“浙江政府采购网（zfcg.czt.zj.gov.cn）”上进行供应商注册申请，并通过财政部门的终审后登记加入到“浙江省政府采购供应商库”。中标供应商必须注册并登记加入“浙江省政府采购供应商库”。具体要求及注册申请流程详见浙江政府采购网“网上办事指南”的“供应商注册申请”。注册咨询电话：95763，如未注册的供应商，请注意注册所需时间。本招标公告附件中的招标文件仅供阅览使用，供应商应在规定的招标文件提供期限内在政采云平台登录上述供应商注册的账号后获取招标文件，未在规定的招标文件提供期限内或未按上述方式获取招标文件的，其投标均视为无效，并不得对招标文件提起质疑投诉。

售价（元）：0

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2024年09月03日14:00（北京时间）

投标地点（网址）：宁波市国际招标有限公司开标大厅（二）（宁波市江北区环城北路西段207弄19号世茂茂悦商业中心1号楼七楼招投标会议中心）、政府采购云平台（www.zcygov.cn）

开标时间：2024年09月03日14:00

开标地点（网址）：宁波市国际招标有限公司开标大厅（二）（宁波市江北区环城北路西段207弄19号世茂茂悦商业中心1号楼七楼招投标会议中心）、政府采购云平台（www.zcygov.cn）

五、公告期限

自本公告发布之日起5个工作日。

六、其他补充事宜

1.供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起7个工作日内，对采购文件需求的以书面形式向采购人提出质疑，对其他内容的以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、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作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

2.其他事项：（1）本项目实行网上投标，采用电子投标文件。若供应商参与投标，自行承担投标一切费用。（2）标前准备：各供应商应在投标截止时间前确保成为浙江政府采购网正式注册入库供应商，并完成CA数字证书办理。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。（供应商CA申领操作指南：https://help.zcygov.cn/web/site\_2/2018/11-29/2452.html，完成CA数字证书办理预计一周左右，请供应商自行把握时间）（3）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，不得参加同一标项号的投标。（4）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，不得再参加本项目的投标。（5）落实的政策：《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）、《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)、《关于环境标志产品政府采购实施的意见》（财库〔2006〕90号、《节能产品政府采购实施意见》的通知（财库〔2004〕185号）。

七、对本次采购提出询问、质疑、投诉，请按以下方式联系

1.采购人信息

名称：宁波大学附属妇女儿童医院

地址：宁波市海曙区柳汀街339号

传真：/

项目联系人（询问）：牟老师

项目联系方式（询问）：0574-87083382

质疑联系人：张老师

质疑联系方式：0574-87083300

2.采购代理机构信息

名称：宁波市国际招标有限公司

地址：宁波市江北区环城北路西段207弄19号世茂茂悦商业中心1号楼八楼

传真：/

项目联系人（询问）：王媛

项目联系方式（询问）：0574-87356230

质疑联系人：姜春辉

质疑联系方式：0574-87307605

3.同级政府采购监督管理部门

名称：宁波市财政局政府采购监管处

地址：/

传真：/

联系人：李老师

监督投诉电话：0574-89388042

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线95763获取热线服务帮助。

CA问题联系电话（人工）：汇信CA400-888-4636；天谷CA400-087-8198。

**第二章 投标须知**

**一、适用范围**

本招标文件仅适用于本采购项目所叙述的货物和服务的招标、评标、定标、验收、合同履约、付款等（法律、法规另有规定的，从其规定）。

**二、定义**

1、“采购人”系指宁波大学附属妇女儿童医院。

2、“代理机构”系指宁波市国际招标有限公司。

3、“供应商”或“投标人”系指向采购人提交投标文件的供应商。

4、“货物”系指供方按招标文件规定，须向采购人提供的一切设备、保险、税金、备品备件、工具、手册及其它有关技术资料和材料。

5、“服务”系指招标文件规定供应商须承担系统的升级、调试、运维、培训以及其他类似的义务。

6、“同级政府采购监管部门”系指宁波市财政局政府采购监管处。

7、“▲”系指实质性响应条款。

▲8、合格的投标货物或服务：

8.1应该是中国境内生产的货物或提供的服务。

若投标货物或服务是国家实行许可证制度或生产注册证制度的产品或服务，则应具备相应有效的证书。

招标文件允许采购进口产品的，若投标货物是进口产品，供应商应保证所投产品为可履行合法报通关手续进入中国关境内、在中国海关完税的可合法销售的货物。

8.2国家规定有标准及规范的，投标货物或服务应按有效的标准及规范执行，应符合国家及招标文件提出的有关技术、质量、安全标准。

8.3供应商应保证所提供的产品或服务免受第三方提出侵犯其知识产权（专利权、商标权、工业设计权及使用权等）的索赔或起诉，否则，由此可能产生的一切法律责任和经济责任均由供应商承担。

8.4**、合格货物来源：合格货物来源均为国产。**

▲**三、供应商的资格要求**

详见采购公告。

**四、投标费用**

4.1、无论投标过程和结果如何，供应商自行承担与投标有关的全部费用。

4.2、供应商可以自行前往现场踏勘，现场勘察所发生的费用由供应商自己承担。不论何种原因所造成，在勘察过程中，供应商自行对由此次踏勘现场而造成的死亡、人身伤害、财产损失、损害以及任何其它损失、损害和引起的费用和开支承担责任。

**五、投标报价**

5.1投标报价以人民币为结算货币。

5.2本项目投标报价为含税固定总价，包括不仅限于完成用户当前环境下系统正常运行所需的软件升级或改造、系统对接、测试、运输、安装调试、验收、培训、免费维保期的售后服务等全部费用。供应商须对其它认为必要的费用进行报价，如不报价则认为是中标人免费提供，以后不得在中标后项目实施过程中要求增加。如中标，除非业主方提出修改，中标人不得以任何理由要求增加费用。

5.3供应商应按招标文件要求填写《开标一览表》和《投标报价明细表》。

5.4供应商应详细列明各分项工作相关报价及依据，未列明的相关报价应视为已包含在已列明费用的报价中，采购人将不予单独支付。

5.5供应商应根据本招标文件规定的工作内容和计划工作量，结合市场及自身情况自行报价。

**六、投标有效期**

▲1、投标文件从开标之日起，投标有效期为90个日历日。投标有效期不能小于招标文件的要求。

2、特殊情况下，采购人可与供应商协商延缓投标文件的有效期，这种要求和答复均以书面形式进行。

3、供应商可拒绝接受延期要求。同意延长有效期的供应商不能修改投标文件。

**七、投标文件的形式和效力**

1、投标文件分为电子投标文件以及备份投标文件，备份投标文件为以U盘或光盘存储的电子备份投标文件。

2、电子投标文件，按“项目采购-电子招投标操作指南”及本招标文件要求制作，并加密。

投标文件制作说明：

（1）应按照本项目招标文件和政府采购云平台的要求编制、加密并递交投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政府采购云平台技术支持热线咨询，联系方式：95763。

（2）供应商通过政府采购云平台电子投标工具制作投标文件。电子投标工具请供应商自行前往浙江政府采购网下载并安装。

（3）以U盘或光盘存储的电子备份投标文件1份，即按“项目采购-电子招投标操作指南”制作的电子备份文件，以用于异常情况处理。

3、以U盘或光盘存储的电子备份投标文件，按“项目采购-电子招投标操作指南”制作的电子备份文件。

4、投标文件填写字迹必须清楚、工整，对不同文字文本投标文件的解释发生异议的，以中文文本为准。

5、投标文件的效力

投标文件的启用，按先后顺位分别为电子投标文件、以U盘或光盘存储的电子备份投标文件。在下一顺位的投标文件启用时，前一顺位的投标文件自动失效。

电子投标文件未能按时解密，供应商提供了电子备份投标文件的，以电子备份投标文件作为依据，否则视为投标文件撤回。电子投标文件已按时解密的，电子备份投标文件自动失效。

**八、投标文件的组成和份数（适用于所有标项）**

1、投标文件的组成：

**A、第一册：资格文件**

A1、关于资格的承诺函（格式见附件）；

A2、营业执照副本（或事业法人登记证副本或其他登记证明材料）扫描件加盖供应商公章（供应商如果有名称变更的，应提供由行政主管部门出具的变更证明文件扫描件加盖供应商公章）；

A3、供应商认为需要的其他资料（如有需提供）；

**B、第二册：商务和技术文件**

B1、投标书；（格式见附件）

B2、法定代表人身份证明；（格式见附件）

B3、法定代表人授权书（投标文件由授权代表签字的须提供）；

B4、供应商一般情况表；（格式见附件）

B5、用户需求响应表；（格式见附件）

B6、商务条款响应表；（格式见附件）

B7、第五章“评标办法及标准”中评分标准（兼评委打分表）要求提供的资料（如有需提供）；

7.1产品方案；

7.2实施方案；

7.3系统安全管理方案；

7.4项目实施人员配置情况；

7.5项目应急方案及措施；

7.6售后服务方案；

B8、综合评分打分表中需提供的评分资料（如有须提供）；

B9、供应商认为需要的其他资料（如有需提供）。

**C、第三册：报价文件**

C1、开标一览表；（格式见附件）

C2、分项报价表；（格式见附件）

C3、中小企业声明函；

C4、残疾人福利性单位声明函；

C5、供应商认为需要的其他资料（如有需提供）；

2、投标文件的份数：

本项目实行网上投标，供应商应准备以下投标文件：（备份投标文件不强制要求提交，但因电子投标文件未能按时解密或解密失败，供应商又未提交备份投标文件的，将被视为投标文件撤回，投标无效。）

2.1上传到政府采购云平台的电子投标文件（含资格文件、商务和技术文件、报价文件）1份。

2.2以U盘或光盘存储的电子备份投标文件（含资格文件、商务和技术文件、报价文件）1份。

▲**九、投标文件的签署盖章**

1、招标文件第七章“附件”中标明加盖公章或签字的，加盖公章部分采用CA签章，签字部分由法定代表人或授权代表签字后扫描上传或盖电子签章。授权代表签字的，还应附法定代表人签署的法定代表人授权书。

**十、投标文件的密封和标记**

1、电子投标文件：供应商应根据“项目采购-电子招投标操作指南”及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位。

2、以U盘或光盘存储的电子备份投标文件**用封袋密封后递交。**

3、电子备份投标文件须在封袋上注明：

（1）注 明： “电子备份投标文件” ；

（2）采购编号：NBITC-202411414G；

（3）项目名称：宁波大学附属妇女儿童医院信息安全提升项目；

（4）所投标项（如有多个标项须填写）：

（5）在 年 月 日（规定的开标日期和时间）前不准启封；

（6）供应商的名称： 。

供应商须在包封上加盖供应商公章或由其法定代表人（或授权代表）签字。

供应商未按上述要求标记的，采购人（代理机构）不承担错放或提前开封的责任。

**十一、投标文件的递交**

1、投标文件递交的具体要求：

（1）供应商应当于提交投标文件截止时间前将电子投标文件上传到政府采购云平台（https://www.zcygov.cn/），并应于提交投标文件截止时间前，将以U盘或光盘存储的电子备份投标文件密封，采用现场递交或邮寄送达方式递交。

方式一：现场递交方式，供应商可安排一名授权代表在投标截止时间前将投标文件送至开标地点：宁波市国际招标有限公司开标大厅（二）（宁波市江北区环城北路西段207弄19号世茂茂悦商业中心1号楼七楼招投标会议中心）。投标文件递交时须同时递交供应商的法定代表人（或其授权代表）联系方式，并保证投标期间联系方式畅通。

方式二：邮寄送达，送达地址：宁波市国际招标有限公司（宁波市江北区环城北路西段207弄19号世茂茂悦商业中心1号楼八楼015室），联系方式：王媛 0574-87307605。供应商邮寄后须将邮件单号发送至代理机构电子邮箱（电子邮箱：51518128@qq.com），并致电采购代理机构，以便采购代理机构查询物流记录。各供应商应当确保电子备份投标文件的密封包装在邮寄过程保持完好，并在邮寄包裹上注明项目名称、采购编号，因邮寄造成电子备份投标文件密封破损而不符合竞争性招标文件对投标文件的密封要求、或邮寄过程中导致电子备份投标文件未在投标截止时间前送达的，代理机构将拒绝其投标文件。各供应商自行考虑邮寄在途时间，投标文件送达时间以代理机构工作人员实际签收时间为准。

（2）开标时间后半小时内供应商可以登录政府采购云平台https://www.zcygov.cn/，用“项目采购-开标评标”功能进行解密投标文件。供应商按时在线解密投标文件的，以在线解密的投标文件作为评审依据，若供应商在规定时间内无法解密或解密失败，则以备份电子投标文件作为评审依据（若备份电子投标文件与政采云平台上传的投标文件被识别为不一致，视为投标文件撤回）。无论是否启用备份电子投标文件，备份电子投标文件均不退还供应商。

2、供应商未按上述要求密封的电子备份投标文件，代理机构不予受理。

3、逾期送达的或者未送达指定地点的，代理机构不予受理。

4、投标文件的补充、修改。

投标截止时间前，供应商可以对递交的投标文件进行补充、修改，补充、修改电子投标文件的，应当先行撤回原文件，补充、修改后重新上传，电子备份投标文件也应重新制作。在投标截止时间之后，供应商不得对其投标文件进行补充、修改。

**十二、开标**

1、代理机构在招标文件规定的时间和地点公开开标，并邀请所有供应商的法定代表人（或授权代表）准时参加。供应商的法定代表人（或授权代表）不参加开标的或迟到参加开标的，视同该供应商默认开标记录，不得事后对开标过程提出任何异议。

2、电子投标开标及评审程序：一阶段开标。

（1）宣布开标；

（2）本项目实行网上投标，采用电子投标文件。投标截止时间后，供应商登录政府采购云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密，在线解密电子投标文件时间为开标时间后半小时内。

（3）以下流程针对到达开标现场的供应商（未到现场供应商按政采云流程参与网上开标）

3.1介绍开标现场的人员情况；

3.2宣读递交投标文件的供应商名单、开标纪律、应当回避的情形等注意事项；

3.3供应商签署不存在影响公平竞争的《政府采购活动现场确认声明书》；

（4）在政府采购云平台开启供应商解密后的“资格文件”、“商务和技术文件”、“报价文件”，宣读供应商名称、报价文件中“开标一览表”内容，以及采购人认为必要的其他内容与记录，并做开标记录；

（5）开标记录在政采云网站确认；

（6）开标结束。休会，评标委员会对“资格文件”、“商务和技术文件”、“报价文件”进行评审；

（7）在政府采购云平台公布中标候选人名单及采购人最终确定中标供应商名单的时间和公告方式等。

3、特别说明：政府采购云平台如对电子化开标及评审程序有调整的，按调整后的程序操作。

本项目原则上采用政采云电子投标开标及评审程序，但有下情形之一的，按以下情况处理：

（1）若供应商在规定时间内无法解密或解密失败，代理机构将开启上述供应商递交的以U盘存储的电子备份投标文件，上传至政采云平台项目采购模块，以完成开标，电子投标文件自动失效。

（2）采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购人（或代理机构）可中止电子交易活动：

2.1电子交易平台发生故障而无法登录访问的；

2.2电子交易平台应用或数据库出现错误，不能进行正常操作的；

2.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

2.4病毒发作导致不能进行正常操作的；

2.5其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购人（或代理机构）可以待上述情形消除后继续组织电子交易活动。

**十三、评标**

1、采购人依据《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》等有关规定组建评标委员会。评标委员会由采购人代表和专家组成，负责本项目的评标工作。

2、评标活动遵循公开、公平、公正、科学和择优的原则。

3、评标委员会按照第五章“评标办法及标准”对投标文件进行评审。第五章“评标办法及标准”没有规定的方法、评审因素和标准，不作为评标依据。

**十四、招标文件的澄清和修改**

1、**采购人可以对已发出的招标文件进行必要的澄清或者修改，将以“更正公告”的形式发布在政采云平台，供应商应及时登录政采云平台，进行浏览并下载，未及时浏览下载的责任自负。**澄清或者修改的内容可能影响投标文件编制的，采购人应当在投标截止时间至少15日前，不足15日的，采购人应当顺延提交投标文件的截止时间；澄清或者修改的内容不影响投标文件编制的，则不受15日的期限限制。澄清或者修改的内容为招标文件的组成部分，对所有供应商具有约束力。

**十五、质疑与投诉**

1、供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应当在法定质疑期内一次性提出针对采购公告、采购文件、开标评标、采购结果等同一采购程序环节的质疑，第二次提出的质疑视为质疑无效，采购人、代理机构将不予受理（对于采购人、代理机构作出的澄清或者修改的内容提出质疑的除外）。

2、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。未依法获取采购文件的，不得就采购文件提出质疑；未提交投标文件的供应商，视为与采购结果没有利害关系，不得就采购响应截止时间后的采购过程、采购结果提出质疑。

3、供应商提出质疑应当提交质疑函和必要的证明材料，质疑函应当以书面形式提出，质疑函格式和内容须符合财政部《质疑函范本》、《投诉书范本》要求，供应商可到中国政府采购网自行下载财政部《质疑函范本》、《投诉书范本》。

4、供应商质疑实行实名制，质疑函应当署名，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，或者其授权代表（指代理人）签字或者盖章，并加盖供应商公章；代理人提出质疑的，应当提交供应商签署的授权委托书；以联合体形式参加政府采购活动的，其质疑应当由组成联合体的所有供应商共同提出。

5、采购人、代理机构接收质疑函的方式：只接收供应商以当面递交、邮寄、传真或电子邮件方式提出的质疑函，以其他方式提出的质疑不予接收。

采取邮寄方式的，提出质疑的时间为质疑函原件交邮的时间（以邮戳时间或快递收件时间为准）。

采取传真、电子邮件方式的，供应商应当在传真、电子邮件发出后将质疑函原件邮寄给被质疑人，提出质疑的时间为质疑函原件交邮的时间（以邮戳时间或快递收件时间为准）。

6、采购人、代理机构以实际收到质疑函原件之日作为收到质疑函的日期，将在收到质疑函后7个工作日内作出答复。

7、采购人、代理机构接收质疑函的联系人、联系电话和通讯地址等信息详见采购公告。

**▲十六、预算金额**

1、本次公开招标设有预算金额：150万元；投标报价超出对应预算金额的投标无效。

**十七、招标代理服务费**

1、本项目每标项招标代理服务费参照国家发改委发改办价格[2003]857号通知和原国家计委计价格[2002]1980号文件规定的代理服务收费标准90%向中标人收取，单个标项不足4000元按4000元收取。

2、中标供应商应在代理机构发出中标通知书5个工作日内向本代理机构支付招标代理服务费。

3、招标代理服务费收取银行票汇款、电汇款。

账户名称：宁波市国际招标有限公司

开户银行：上海浦东发展银行宁波分行江北支行

银行账号：94090154800000191

**十八、特别说明**

1、政府采购活动中有关中小企业的相关规定（采购进口产品的项目不适用）：

（1）中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。

符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

（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：

2.1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；

2.2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；

2.3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。

2.4中小企业参加政府采购活动，应当出具《政府采购促进中小企业发展管理办法》规定的《中小企业声明函》（格式见本采购文件附件），否则不得享受相关中小企业扶持政策。

采购活动过程中，对供应商的“中小企业”资格认定，以供应商提交的《中小企业声明函》为准，供应商必须实事求是地提交声明函，如有虚假，将依法承担法律责任。如果在采购活动过程中相关采购当事人对供应商“中小企业”资格有异议的，由货物制造商或者工程、服务供应商注册登记所在地的县级以上人民政府中小企业主管部门负责认定。

供应商提供声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

适用招标投标法的政府采购工程建设项目，供应商提供声明函内容不实的，属于弄虚作假骗取中标，依照《中华人民共和国招标投标法》等国家有关规定追究相应责任。

2.5《中小企业声明函》由参加投标的供应商提交，如供应商为代理商，须自行采集制造商的中小企业划分类型信息填入相应栏目并对其真实性负责。

2、执行财政部、司法部《关于政府采购支持监狱企业发展有关问题的通知》。监狱企业（监狱和戒毒企业）提供自己企业的产品（服务）参加投标视同小型、微型企业，享受政府采购促进中小企业发展的政府采购政策，监狱企业参加政府采购活动时，必须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，未能提供上述证明文件的不予认可。

3、执行《三部门联合发布关于促进残疾人就业政府采购政策的通知》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受政府采购促进中小企业发展的政府采购政策，残疾人福利性单位参加政府采购活动时，应当提供《残疾人福利性单位声明函》（格式见第七章附件），并对声明的真实性负责，未能提供的不予认可。

4、本项目不组织潜在供应商现场考察或者召开开标前答疑。

5、本文件未及事项，在签订合同时供需及使用方友好商定。

6、本招标文件解释权归采购人。

**第三章 招标内容与技术需求**

**一、采购内容**

宁波大学附属妇女儿童医院重要信息系统（基础支撑网络，关键应用系统）已按照等保三级的基本要求，进行相应的建设和不断整改，包括终端上的防病毒，网络边界处的防火墙、入侵防御、上网行为管理等安全软件和设备，在很大程度上已经对外部威胁能有一个基本的防护能力，但是如今的安全威胁和攻击手段日新月异，层出不穷，各种高危零日漏洞不断被攻击者挖掘出来，攻击的目标越来越有针对性，医院信息系统需在安全建设上进一步依靠国际先进技术增强主动防御，纵深防御的能力。

拟计划在原有信息化安全防护系统上进行安全系统产品升级，通过针对性的信息安全加固，让全院安全防护系统进一步做到安全控制和防护落实到等保要求和评测细节。

**二、采购产品清单如下：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 技术规格 | 数量 | 投标响应 |
| 1 | 互联网安全接入服务（SaaS服务） | 详见互联网安全接入服务（SaaS服务）技术规格要求 | 1项 |  |
| 2 | 零信任控制系统 | 详见零信任控制系统技术规格要求 | 1项 |  |
| 3 | HTTPS安全证书 | 详见HTTPS安全证书技术规格要求 | 1项 |  |
| 4 | CDP备份一体机系统（核心产品） | 详见CDP备份一体机系统技术规格要求 | 1项 |  |
| 5 | 数据发现和分类分级系统（核心产品） | 详见数据发现和分类分级系统技术规格要求 | 1项 |  |
| 6 | 防火墙（公卫网区域） | 详见防火墙（公卫网区域）技术规格要求 | 1项 |  |
| 7 | Web应用防火墙(北院WAF) | 详见Web应用防火墙(北院WAF)技术规格要求 | 1项 |  |
| 8 | 网闸（北院网络隔离） | 详见网闸（北院网络隔离）技术规格要求 | 1项 |  |
| 9 | 国密VPN系统 | 详见国密VPN系统技术规格要求 | 1项 |  |

**三、产品技术规格要求：**

**3.1互联网安全接入服务（SaaS服务）技术规格要求**

| **序号** | **类别** | **指标项** | **技术规格及配置要求** | **投标响应** |
| --- | --- | --- | --- | --- |
| 1 | 基础要求 | 产品数量 | 本项目需提供满足至少300个终端接入至少3年互联网安全接入服务，且后续能够按照授权增加扩容，扩容数量无上限约束 |  |
| 2 | 产品形态 | 纯SaaS服务，本地无需部署硬件设备 |  |
| 3 | 稳定性 | 全年服务可用时间占比≥99.999%  提供SLA服务承诺函，并加盖厂商公章 |  |
| 4 | 全局监控 | 仪表盘 | 支持首页仪表盘概览展示DNS查询与拦截情况、检出威胁域名、TOP受威胁主机、热点威胁、访问内容分析等内容，且每个统计信息均可下钻查看详情，可自主筛选时间查看，提供产品功能截图 |  |
| 5 | 支持以职场区域为划分，定向查看某职场的DNS查询情况、拦截情况、检出威胁域名、TOP受威胁主机、访问内容分析等内容，统计信息均可下钻查看详情 |  |
| 6 | ★实时监控全局DNS解析服务情况，DNS每秒处理量请求量动态变化，每秒处理量支持以职场维度筛选查看，提供产品功能截图，并加盖厂商公章 |  |
| 7 | DNS拦截防护能力 | 实时自动拦截能力 | 支持实时阻断内部受控主机或恶意终端域名通过DNS访问非法站点，阻断威胁对外连接建立，提升递归访问的安全性 |  |
| 8 | 内网威胁主机定位 | 可提供本地虚拟化探针，可对内部失陷主机IP进行定位，针对内网IP动态分配的情况，支持接入DHCP日志，定位到主机名与MAC地址。后续可跟进实际使用需求灵活扩充，定位工具支持软件部署，提供产品功能截图 |  |
| 9 | 日志溯源分析能力 | 部署定位工具后，可记录7天内内网主机IP访问DNS服务区的全量日志，支持搜索七天内任意内网IP的访问记录，或搜索某域名七天内访问的主机IP，定位工具支持软件部署。 |  |
| 10 | DNS隧道防护能力 | ★支持DNS隧道域名检测，自动计算生成DNS隧道地址列表，用户自主选择是否拦截对应的DNS隧道地址，DNS隧道告警支持IM、邮件通知，提供产品功能截图，并加盖厂商公章 |  |
| 11 | 新注册域名防护 | ★新注册域名代表whois信息在近期被注册的域名，这些域名通常被攻击者或攻击队用于实施恶意行为。可针对近7天、近30天新注册域名开启防护，支持仅检测、检测拦截两种模式，提供产品功能截图，并加盖厂商公章 |  |
| 12 | 主节点BGP路线 | 安全DNS提供的主节点为BGP路线，可自动识别用户所属区域和运营商，智能调度解析路线返回同运营商就近的最优解析IP |  |
| 13 | IPV6检测防护能力 | 具备IPv6检测与阻断能力，可新增注册IPV6网络出口节点，可配置IPv6地址进行安全解析，针对IPv6解析和威胁拦截进行数据展示 |  |
| 14 | 主机安全防护能力 | 授权数量 | 支持对项目要求的不少于300个终端提供威胁清除插件agent |  |
| 15 | 远程办公防护能力 | 无需与其他产品结合，平台自身的Agent工具能够为漫游终端提供实时威胁拦截的防护能力，并在云端控制台统计所有漫游终端的威胁防护情况,Agent支持Windows、统信、MACoS，提供产品功能截图，并加盖厂商公章 |  |
| 16 | 支持配置Agent策略，漫游终端设备回到企业内网后，默认使用内网DNS服务器 |  |
| 17 | 一键处置 | 安全DNS发现的告警，产品配套处置工具可直接定位问题终端、及恶意进程，处置工具根据威胁情况推荐处置动作，同时支持云端直接下发隔离进程、隔离终端、专杀工具任务，一键处置，提供产品功能截图，并加盖厂商公章 |  |
| 18 | 威胁扫描（杀毒） | 提供终端威胁清除工具，支持配置扫描策略，扫描支持快速扫描、全盘扫描、自定义扫描，对威胁清除中发现的恶意文件，支持自动处置，也能够配置仅上报告警信息不直接处置文件。 |  |
| 19 | 工具易用性 | 终端处置工具和威胁清除工具，应支持静默安装，静默运行，防退出，防卸载的能力 |  |
| 20 | 漫游终端防护工具、进程取证工具与威胁清除工具需为同一软件，无需重复安装，提供产品功能截图 |  |
| 21 | 网络行为访问控制 | 内容分类策略 | 支持识别超过50种分类千万级域名，包括色情暴力、违法内容、赌博、游戏、广告等敏感类别，用户可针对不同应用设置拦截策略 |  |
| 22 | 内容分类策略基于支持不同的工作时间段设置生效，例如支持全天、或工作日9:00-18:00生效，提供产品功能截图 |  |
| 23 | 自定义拦截或放行策略 | 支持按照职场维度自定义域名拦截及放行规则，支持配置多条拦截放行策略，可拖动修改优先级排序 |  |
| 24 | 职场级级自定义拦截页面 | 支持灵活的自定义拦截页面，默认拦截返回页面可自定义文字、企业名称、企业LOGO，支持跳转到指定的URL、或指定IP，提供产品功能截图，并加盖厂商公章 |  |
| 25 | 可基于不同拦截原因（威胁，内容，自定义名单）自定义不同拦截页面策略，例如威胁拦截返回默认拦截页自定义提示话术，内容分类拦截跳转到指定的URL，自定义黑名单拦截跳转到指定IP，提供产品功能截图，并加盖厂商公章 |  |
| 26 | 策略告警模式 | 威胁胁检测支持多种告警模式，用户可以自主选择仅告警不拦截、或告警并拦截模式 |  |
| 27 | 多种策略配置模式 | 可区分职场设置不同范围的策略配置，配置范围包括全局策略权限、某职场策略权限 |  |
| 28 | 配置管理功能 | 账号统一管理 | 采用WEB HTTPS方式进行SaaS服务集中管理 |  |
| 29 | 双因素验证 | 支持通过短信形式接受验证码完成二次验证后方可登录控制台，用户可自主选择是否开启双因素验证，提供产品功能截图，并加盖厂商公章 |  |
| 30 | 企业个性化配置 | 支持用户自定义控制台企业名称、企业LOGO，支持自定义Agent插件的名称和LOGO，提供产品功能截图 |  |
| 31 | 多级用户管理 | 提供多级账号的配置和管理能力，超级管理员账号用于全局视角，看到各分区职场的安全情况，同时支持设置区域管理员角色，根据账号权限设置不同范围的数据展示和策略配置权限 |  |
| 32 | 产品使用建议 | 根据用户使用安全DNS的行为和数据，自动生成使用建议，包括推荐开启敏感分类拦截策略、安装定位工具溯源、开启拦截策略等 |  |
| 33 | 多职场统一防护 | 支持至少接入100个分支机构出口DNS流量，分支职场支持多级架构，不限制下钻层级，职场管理页面可查看总部-一级-二级-三级到n级分支的架构关系，提供产品功能截图，并加盖厂商公章 |  |
| 34 | 动态出口接入 | 支持用户通过动态跟踪程序或者DDNS技术添加动态网络出口 |  |
| 35 | 终端Agent管理 | 终端Agent支持职场分组管理、登记人员、批量移动、批量删除、批量导入终端管理信息等管理能力，提供产品功能截图，并加盖厂商公章 |  |
| 36 | 终端Agent支持根据职场分组、终端信息、在线状态、隔离状态、操作系统、生效策略进行灵活筛选。支持快速筛选近24小时/7天/30天活跃终端，及超过30天未活跃的终端，提供产品功能截图 |  |
| 37 | 邮件通知管理 | 告警通知支持基于不同的威胁等级、事件类型设置灵活的告警通知，例如严重等级告警整点发送，APT事件有威胁检出立刻推送。 |  |
| 38 | 告警形式支持邮件，及钉钉、企业微信、飞书任意方式的IM通知推送 |  |
| 39 | API同步数据 | 可提供API能力，将指定时间拦截的恶意事件、网络出口数据、拦截或者放行策略等数据同步到本地已有系统和平台，提供产品功能截图 |  |
| 40 | 支持通过API的方式拉取阻断清单，添加和删除指定域名，通过安全DNS进行拦截防护，提供产品功能截图 |  |
| 41 | 数据分析展示能力 | 解析域名分析 | 根据企业各职场、各出口的访问，统计展示请求域名和拦截域名情况，支持按照时间、处置动作、检出原因、DNS查询类型、访问域名分类、出口IP等进行筛选，并支持下载 |  |
| 42 | 域名解析日志 | 支持查看24小时域名解析明细日志，展示请求时间、查询类型、处置动作、响应状态、解析结果、威胁等级等明细信息，支持多维度筛选与下载 |  |
| 43 | 安全事件分析 | 支持威胁事件视角、恶意地址视角、职场视角查看内网安全事件和检出趋势；可按照时间、请求职场、网络出口、威胁类型、事件名称、威胁域名、严重等级等进行筛选和分析 |  |
| 44 | 主机事件分析 | 支持按照失陷主机维度统计安全事件、以及失陷主机关联威胁事件展示 |  |
| 45 | 取证结果分析 | ★支持查看终端取证的进程分析，可按照时间、请求职场、严重等级、主机、事件名称等进行筛选，并支持取证报告下载，需提供产品功能截图，并加盖厂商公章 |  |
| 46 | 内容分类分析 | 支持针对上网请求的域名分类进行可视化分析，按照职场、时间段、敏感分类进行筛选，查看内容分类站点拦截情况，分析TOP内容分类访问趋势，敏感站点TOP访问时段、TOP访问职场等数据。 |  |
| 47 | 自定义报告生成 | 支持单次创建、定时周期创建报告，报告内容可充分自定义，包括：职场范围、威胁严重级别及报告名称等内容，支持排除无需展示的域名 |  |
| 48 | 报告类型支持综合分析报告、安全事件报告，威胁终端报告、检出情况列表等四种报告，定期生成月报、季度报、年报并发送指定邮箱，满足安全运营各种场景需求 |  |
| 49 | 威胁情报数据 | 失陷指标（IOC）情报 | 具备专业商用失陷指标（IoC）情报≥100万条，字段丰富度至少包括发现时间、域名、相关组织、严重程度、相关家族、置信度、针对行业、背景信息、关联样本、是否为APT攻击、通讯协议、应用协议、主机类型、情报类型、时间戳等 |  |
| 50 | 历史域名情报信息 | 网络基础数据至少包含Whois注册信息数据以及10年历史数据，PDNS数据以及5年历史数据 |  |
| 51 | ▲服务 | | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供至少三年原厂服务函原件，产品服务对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**3.2 零信任控制系统技术规格要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **类别** | **指标项** | **技术规格及配置要求** | **投标响应** |
| 1 | 配置要求 | 性能参数 | 最大加密流量≥350Mbps，最大理论并发用户数≥600，最大理论https并发连接数≥35000，理论https新建连接数（个/秒）≥90 |  |
| 2 | 硬件配置 | 内存大小≥16G，硬盘容量≥128G SSD，接口≥6千兆电口+2千兆SFP光口 |  |
| 3 | 授权 | 提供不少于200点并发接入永久授权 |  |
| 4 | 设备部署 | 网络部署 | 为了满足灵活部署的要求，产品应支持IPV4/IPV6双栈网络IP配置 |  |
| 5 | 高可靠性 | 为了提高系统可靠性，保障单台设备故障时系统仍可正常运行，产品应支持集群部署，且最少2台设备即可组建集群；本地集群组建时，集群中的节点可承载工作负载功能，不需要依赖其它外置设备 |  |
| 6 | 资源发布能力 | 隧道资源发布 | 可以支持基于TCP、UDP、ICMP等协议代理访问业务资源，支持发布IP、IP范围、IP段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面 |  |
| 7 | Web资源发布 | 可以支持基于http或https协议代理访问业务资源，支持发布IP或域名形式的后端服务器地址，可配置业务应用的具体访问URL路径 |  |
| 8 | WEB资源依赖站点 | 对于一些主要在主站点中点击使用的子站点WEB业务系统，且子站点跟主站点业务系统权限一致的场景，为简化管理员配置，应支持开启依赖站点功能。为方便业务快速上线，还应支持自动采集站点功能对依赖站点进行梳理 |  |
| 9 | 应用打开方式 | 支持配置点击工作台的业务应用即可直接拉起对应的C/S程序(如HIS)进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持Windows、macOS、统信UOS、麒麟kylin等主流操作系统；针对Windows系统，还应支持拉起C/S应用时自动访问管理员设定的地址 |  |
| 10 | 桌面云对接 | 为满足长期安全规划，提高远程访问时的安全性，要求产品支持将主流桌面云类资源发布成零信任的代理应用；并且为了提升终端用户使用的便利性，产品应支持跟桌面云进行单点登录对接，实现仅需在零信任进行认证即可直接进入桌面云进行业务办公，无需重复验证 |  |
| 11 | WEB水印 | 为提升业务应用的数据安全性，系统应支持针对发布的WEB应用开启WEB水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用，有效预防数据泄露 |  |
| 12 | 私有DNS解析 | 支持以私有DNS发布单位资源，无需额外购买DNS服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有DNS解析地址 |  |
| 13 | 终端接入能力 | 浏览器兼容性 | 为了保障用户的使用体验，不改变部分职工及人员在各种场景下的原有使用习惯，需支持以下主流浏览器访问WEB资源：IE8及以上版本、Chrome 69及以上版本、Edge、Firefox、Opera、Safari等其他主流浏览器、微信内置浏览器、钉钉内置浏览器、Android、iOS各大手机厂商的自带浏览器、支持国产操作系统浏览器 |  |
| 14 | 客户端兼容性 | 为了保障职工顺利访问经隧道模式代理的业务，客户端应兼容主流非国产终端，包括但不限于：Windows7（32位、64位）、Windows10（32位、64位）、Windows11（64位）、MacOS10、MacOS11、MacOS12、Android、iOS等非国产操作系统的终端 |  |
| 15 | 国产化终端兼容性 | 为了保障用户在国产化终端上的正常业务访问，客户端应兼容主流国产硬件CPU的国产操作系统终端，包括但不限于麒麟V10、统信V20等 |  |
| 16 | 客户端自带登录地址 | 为了尽可能简化员工登录操作难度，支持管理员配置是否允许用户在客户端下载安装后自动携带登录地址 |  |
| 17 | 密码找回 | 为了提升系统维护的便利性，管理员可配置是否允许用户通过短信验证码等方式自助找回密码。用户在PC端和手机端的登录页面均可通过点击忘记密码来重置密码 |  |
| 18 | 终端类型合规管控 | 可设置允许终端在线数为0，以禁止用户通过某类终端接入访问 |  |
| 19 | 多终端在线 | 支持不同平台的终端同时在线，管理员可分别设置可同时在线的PC或移动终端个数，当超过终端个数时，可以注销最早登录的终端，且被注销的终端有对应的注销提醒；支持用户自助查看在线或离线终端列表，并注销其他终端，避免账号盗用 |  |
| 20 | 认证管理 | 认证方式 | 为满足单位多样化安全便捷认证需求，需至少支持以下认证方式：本地账号密码认证、LDAP/AD认证、OAuth2.0标准协议的票据认证、CAS标准协议的票据认证、Radius账号认证、HTTPS帐号认证、证书认证、短信认证、标准Radius令牌认证、TOTP动态令牌认证等认证方式，并可与钉钉/浙政钉、企业微信结合实现扫码认证（要求至少提供钉钉、浙政钉扫码认证的功能截图证明） |  |
| 21 | 多因素认证 | 为了进一步保障用户身份安全，需支持多因素认证，支持管理员结合已对接的主认证和辅认证类型进行设置，可自由选择采用首次认证+二次认证+终端认证+增强认证等方式 |  |
| 22 | 自适应增强认证 | 为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等 |  |
| 23 | 单点登录 | 1、支持帐号密码代填的单点登录功能，支持智能识别登录页面的用户名和密码输入框，根据设置的用户名密码规则自动填写WEB业务系统的帐号密码并登录  2、在对接钉钉/浙政钉、企业微信等主流超级APP时，系统支持直接单点登录发布在钉钉/浙政钉、企业微信工作台的H5微应用，不改变用户原有访问习惯 |  |
| 24 | 用户管理 | 外部用户目录管理 | 产品支持与外部用户管理服务器进行对接，包括但不限于LDAP用户目录、AD域用户目录、企业微信用户目录、钉钉或浙政钉用户目录等。同步外部用户时，可配置的属性包括但不限于：用户过滤、用户名、外部ID、组织架构、所属角色、帐号状态、有效期、手机号码、电子邮箱等 |  |
| 25 | 业务访问安全能力 | 动态访问控制 | 支持配置动态访问控制规则，策略支持“与”、“或”条件嵌套，并可通过单一条件或条件组的方式灵活组合嵌套，可支持的条件变量应包括但不限于：应用类型、浏览器版本、客户端源IP、代理网关接入IP、应用访问的进程名称、终端名称、MAC地址、终端本地IP列表、操作系统版本、终端资产类型、终端标签类型、存在指定文件、操作系统安装的补丁、运行进程、运行指定杀毒软件、运行任一杀毒软件、客户端版本、安装指定软件、开启系统防火墙、用户接入城市、用户登录国家、用户登录时间、应用进程的信任状态、弱密码、授信终端、授信域环境等；可联动终端检测响应平台的检测评分作为策略条件； |  |
| 26 | 终端数据安全 | 手机SDK | 支持iOS、安卓手机APP集成SDK，从而实现安全接入、数据安全沙箱等功能，避免单独安装手机客户端，提升用户使用体验 |  |
| 27 | 终端沙箱 | 为了满足PC端数据防泄密需求，系统需支持在PC终端上基于沙箱技术生成隔离的安全工作空间（非容器类型），且无需再额外搭建服务端设备、组件。PC沙箱应支持Windows系统、macOS系统、统信UOS及麒麟Kylin等主流系统 |  |
| 28 | 安全特性 | 服务隐身 | 为了最大程度缩小网络、业务暴露面，平台需提供单包授权能力（SPA），支持UDP+TCP组合的单包授权技术，未授权用户无法连接设备，无法扫描到服务端口，不会出现敲门放大漏洞 |  |
| 29 | 分权管理能力 | 管理员账号 | 支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权 |  |
| 30 | 管理员分级分权 | 内容权限管理模块支持按应用和用户粒度划分权限，如指定某管理员仅能管理指定的应用和指定的用户 |  |
| 31 | 审计能力 | 日志记录 | 支持分别记录用户访问日志、管理员操作日志以及设备安全日志。应支持将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位 |  |
| 32 | 虚拟IP | 支持以虚拟IP方式，访问真实的业务系统，以配合其他对IP有要求的安全设备工作，以及便于流量分析类设备进行流量分析 |  |
| 33 | 系统运维 | 终端日志收集 | 支持用户在客户端自助进行日志收集，方便运维排查。为了方便快速运维排障，支持管理员在控制台远程获取在线终端的日志，若终端不在线时支持加入排队列表，排队列表中的终端上线后自动收集日志 |  |
| 34 | 账号安全检查 | 支持设备账号安全检查，包括但不限于：1、疑似管理员测试帐号的残留检查  是否开启找回密码功能检查；3、疑似用户测试账号的检查 |  |
| 35 | 监控中心 | 在线用户 | 支持查看当前在线用户终端总数；支持查看当前在线用户，用户信息至少包括用户名、组织架构、终端类型、浏览器类型、接入IP、最后接入时间、认证方式等；支持管理员对在线用户进行注销操作 |  |
| 36 | 国家商用密码 | 加密算法支持 | 支持中国商用密码标准，客户端接入及控制台访问均应支持SM1、SM2、SM3、SM4等加密算法，以及相应的 ECC\_SM4\_SM3、ECDHE\_SM4\_SM3、ECC\_SM1\_SM3、ECDHE\_SM1\_SM3等加密算法套件 |  |
| 37 | 支持使用商密密码卡进行加密；支持在控制台对密码卡进行管理（包括：激活、取消激活、密钥备份/恢复、管理KEY口令） |  |
| 38 | 开放集成 | API开放 | 为方便整合业务系统的工作流程，应支持通过OPEN API的方式将零信任系统的能力开放给第三方业务系统进行调用配置，如满足员工需要业务系统访问权限时可以直接通过OA办公系统的工单审批流程来申请的需求。支持通过限制访问OPEN API的IP接入地址、API密钥加密等方式来保障OPEN API的调用安全 |  |
| 39 | ▲服务 | | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供至少三年原厂质保函原件，设备产品序列号对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**3.3 HTTPS安全证书技术规格要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **技术规格及配置要求** | **投标响应** |
| 1 | 配置要求 | 1、证书类型：企业级OV通配符，保护所有二级子域名、不限子域名数量、有效期内随时新增子域名，最多250个子域名支持，支持可选RSA/SM2加密算法；  2、国产化产品，符合我国自主知识产权、安全可控；  3、保障应用站点的安全性，对应用站点用户与网站间的交互访问全链路数据进行加密, 实现传输数据的防劫持、防篡改、防监听；  4、符合国密局和工信部的合规性要求，证书签发机构具有国家密码管理局《电子认证服务使用密码许可证》、工业和信息化部《电子认证服务许可证》资质；  5、RSA证书根要求经过国际Webtrust认证；  6、SM2证书要求国内可信CA机构基于国家根体系，由国家密码管理部门制订规范；  7、证书支持360国密，齐安信，红莲花等国产浏览器使用；  8、支持所有主流操作系统及软件库iOS5+、Android4.0+、Windows 7+、Java1.6.15+，支持99.9%的主流浏览器；  9、可提供重新编译过支持国密SSL的Nginx，并进行了SM2服务器证书的部署验证；  10、遵循医院应用实施规范，清晰医院应用实施流程，具备医院应用实施、运维经验；  11、本地有常驻技术服务团队，可提供5\*8本地化上门服务，确保证书申请和使用过程中全程无忧；  12、通配符OV企业型证书，本次提供至少三年期服务。 |  |

**3.4 CDP备份一体机系统技术规格要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **技术规格及配置要求** | **投标响应** |
| 一 | 总体架构 | |  |
| 1 | 系统架构 | 采用B/S架构，全中文操作界面，支持主流浏览器，支持https/SSL等加密传输协议 |  |
| 2 | 用户权限 | 提供基于配置、授权、审计“三权”划分安全保密防护措施，系统内置安全管理员、安全保密员和安全审计员三种用户角色，整体保障平台基本权限安全；（提供产品功能截图）  支持用户管理、身份管理、角色配置、操作权限管理，实现用户角色自定义、操作权限安全可控；  支持数据权限组配置机制，针对拥有相同数据权限的用户组，进行数据权限的快速配置； |  |
| 3 | 安全性 | 支持对平台登录用户的密码复杂度（数字、大小写字母、特殊字符、密码长度等）、有效期、密码错误锁定策略等进行限制，有效期过后提供登录重置密码或禁止登陆需联系管理员处理2种处理方式，以确保平台自身账户的安全；  支持对访问身份进行强验证，验证因子包括生物特征-指纹、证书、OTP；  用户密码应采用加密算法进行存储和验证，服务报文采用对称加密方式加密，并具有校验机制；  提供详细有效的系统运行日志，支持一键下载，便于对故障、事件和错误等进行分析和定位，方便事件处理和审计追溯；  提供详细有效的用户使用日志，包括不限于：操作模块、浏览器类型和版本、设备类型、客户端IP、操作系统类型等，便于操作追溯和审计归档； |  |
| 二 | 灾备管控中心 | |  |
| 1 | 资产管理 | 支持跨网络域资产统一纳管；支持纳管应用、数据库、网络、中间件、负载均衡、消息队列、备份客户端、文件同步客户端、虚拟化平台等全业务级容灾资产；  支持对已纳管资产的自动化环境检测；支持容灾拓扑的自动检测和管理，并通过动态拓扑图进行可视化展示；支持按业务系统维度，进行资产归属管理；支持按数据中心维度，进行资产归属管理，平台内置数据中心拓扑模板； |  |
| 2 | 资产发现 | 支持自定义IP和端口方式，自动发现操作系统、数据库等资产；支持以报表形式批量导出发现的资产信息； |  |
| 3 | 脚本库 | 支持对用户的灾备脚本进行统一的管理；支持Shell、powershell、python等脚本语言；内置IHS、IBM MQ、WAS、Tomcat等主流应用脚本；（提供产品功能截图）  支持在线编辑、查看、下载脚本内容；支持脚本多版本管理，脚本新增和修改均需要发布； |  |
| 4 | 大屏可视化 | 提供运行监控大屏，支持多种大屏风格切换，支持自定义主标题和副标题，支持指标项数据自定义，支持监控频率的自定义； |  |
| 5 | 统一告警 | 支持容灾资源的可用性状态和延时（RPO）监控，可设定自定义规则进行告警；  支持自定义模板告警设置，并支持通过web监控页、短信、企业微信、邮件及其它方式进行告警通知；  通知内容支持降噪、分级、分类、内容过滤等自定义通知机制；（提供产品功能截图） |  |
| 6 | 工具箱 | ★内置丰富的灾备运维工具箱，包括但不限于RPA机器人、网络诊断、文件分发等能力； （提供产品功能截图） |  |
| 7 | 知识库 | 内置行业管理制度、政策法规、行业预案、脚本库等知识库； |  |
| 三 | 主机同步模块 | |  |
| 1 | 部署方式 | 支持单机或集群部署模式；  支持客户端在线安装、一键批量下发部署，可同时添加多个保护对象；内置服务器硬件驱动库，部署时自动匹配对应驱动；支持驱动在线自动更新或手动上传更新；（提供产品功能截图） |  |
| 2 | 资源管理 | ★支持计算资源、存储资源横向扩展，在资源不足时可以通过增加独立的计算或者存储节点扩展资源，而不是依赖原有一体机的硬件配置能力；扩展过程对业务无影响；（提供产品功能截图）  支持存储容量自动精简配置能力，可根据实际使用量分配空间； |  |
| 3 | 对象适配 | 支持对物理机、虚拟机、超融合主机、私有云主机和公有云主机资产进行整机保护；  支持对Windows、CentOS、Redhat、Ubuntu、Suse、Oracle Linux、麒麟、华为openEuler、统信V20、红旗Linux客户端进行整机保护；  支持Oracle RAC备份，只需配置集群内设备关系即可快速为集群内设备创建备份；支持以集群角度可视化集群设备的备份情况；支持Oracle RAC各个设备的验证、接管、恢复；支持自动识别共享盘； |  |
| 4 | 整机备份 | 支持基于磁盘块级别的持续数据保护，可精确到秒级，同时能够产生连续的秒级恢复点，可恢复到选定的任意时间点；（提供产品功能截图）  支持不需区分业务系统类型、部署方法、业务系统间的数据交互机制、数据结构、逻辑关系和数据库的品牌、版本等实现数据保护；  支持整机、磁盘、分区/卷级别的细粒度备份，且支持磁盘排除备份； |  |
| 5 | 备份策略 | ★支持系统内置多个备份策略，无需配置即可开箱即用；策略之间相互独立，可灵活定义数据保护模式、备份间隔、数据保留时间、策略执行时间、数据校验时间、备份性能模式、带宽速度等；（提供产品功能截图） |  |
| 6 | 数据传输 | 数据传输支持客户端级加密，支持任务级数据重删和断点续传； |  |
| 7 | 资源控制 | 支持选择业务优先、备份优先等多种备份模式；支持通过百分比方式限制源端存储资源占用；支持网络带宽限制； |  |
| 8 | 数据验证 | 支持同时对单台或多台客户端进行一致性验证，验证时间点支持实时、计划性实时或者自定义时间点；验证过程与生产环境隔离，不影响生产业务系统；  内嵌逻辑隔离网络环境，可根据实际网络情况，自定义配置验证网络，用于容灾演练、数据验证等场景。所有验证主机均运行在该独立的隔离网络中，无需配置复杂的网络信息，不会与现有业务发生冲突；  支持对单个客户端创建多个版本验证任务；  支持备份客户端可视化查看备份数据，无需任何配置；支持查看所有备份数据点文件；支持浏览后文件下载； |  |
| 9 | 数据恢复 | 支持生产系统操作系统、应用、数据一体化在线恢复，无需对恢复目标安装操作系统、配置软件、拷贝数据等操作；  支持接管恢复、备份恢复、实时恢复等多种恢复类型；支持整机恢复、磁盘恢复、分区/卷恢复等多种细粒度恢复； |  |
| 10 | 接管恢复 | 支持基于接管机的恢复，恢复过程接管机无需停机，不影响业务运行；恢复基于接管机，无需再次创建备份任务；恢复过程包含接管机运行后新增业务数据；（提供产品功能截图） |  |
| 11 | 实时恢复 | ★支持实时恢复功能，实时备份过程中，进行实时恢复，新增的备份数据会自动进行实时恢复，支持物理机、虚拟化主机、超融合主机、云主机间端到端的实时增量恢复，恢复目标机资源为原生架构资源，不是通过添加给CDP平台，嵌套虚拟化方式实现资源使用；（提供产品功能截图） |  |
| 12 | 应急接管 | 支持快速应急接管，可根据保护过程中收集源系统负载信息,自动匹配、自动构建接管虚拟网络、智能化自动分配接管资源，无需改变任何IP地址、MAC地址、机器名、服务启动状态等。接管主机环境保持与源主机完全相同，如磁盘分区结构、系统环境、程序配置信息等；  支持配置切换计划，参数配置支持与源设备一致或者自定义配置；接管时间点提供实时、故障前五分钟、十分钟、半小时、一小时等多种细粒度选择；切换方式支持系统切换、手动切换，系统切换支持配置网络链路检测、网络端口检测等不同切换条件，切换条件支持多次确认机制； |  |
| 13 | 远程复制 | ★支持基于远程复制调度计划，采用增量数据复制的方式，通过 IP 链路将本地产生的备份数据复制到远程容灾中心；调度策略支持分钟级别/小时级别/自定义日期；支持远程复制速度限制；（提供产品功能截图） |  |
| 14 | 授权数量 | 支持≥20T容量无限制主机数据实时保护功能授权，无限制节点容灾接管授权。 |  |
| 15 | 硬件配置 | 2U机架式设备；配置冗余电源；两颗64位16核处理器；内存≥256GB；12个热插拔盘位；配置6\*4T SATA 7200企业级硬盘；提供2个千兆以太网接口，2个双端口万兆以太网卡(SFP) 。 |  |
| 16 | 产品资质 | 产品具有自主知识产权，需提供软件著作权证书。 |  |
| 17 | 原厂资质要求 | 原厂商具有ISO27001信息安全管理体系认证证书；  具有ISO20000信息技术服务管理体系认证证书；  具有ISO9001：2008质量管理体系认证证书；  具有省级重点企业研究院证书。 |  |
| 18 | 原厂售后服务 | 本项目提供原厂项目管理和售后实施服务，要求项目经理同时具备PMP证书和OCM证书，实施工程师需要同时具备OCP和CISSP证书。提供相关证书原件复印件。 |  |
| 19 | 可以提供2小时以内的上门服务。提供营业执照等相关证明材料原件复印件。 |  |
| 20 | ▲服务 | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供至少三年原厂质保函原件，设备产品序列号对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**3.5 数据发现和分类分级系统技术规格要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **技术规格及配置要求** | **投标响应** |
| 1 | 性能指标 | 提供≥100张表/分钟的数据扫描性能 |  |
| 2 | 授权数量 | 提供≥5个资产授权，资产类型包括：数据库、大数据平台、文件等。  提供≥1000张表，且≥20000个字段的分类分级服务 |  |
| 3 | 架构部署 | 支持单机和集群部署模式 |  |
| 4 | 操作系统 | 支持麒麟V10、Linux红旗7、统信UOS |  |
| 5 | 可扩展性 | 提供完整的对接接口方案以及标准接口文档，能与其他系统进行交互 |  |
| 6 | 数据源适配 | 产品应支持目前主流关系型数据库、国产数据库、大数据平台和多类型格式文件  支持主流关系型数据库（Oracle，SQL Server，MySQL，DB2、PostgreSQL，Greenplum，informix，MariaDB，As400，TIDB，CACHE，OceanBase MySQL，Highgo，OceanBase Oracle，OpenGauss，Sequoiadb mysql，AntDB PostgreSQL，UXDB，OSCAR，ClickHouse，HotDB，StarRocks，Hana，Vertica、Teradata）  支持国产数据库（DM（达梦），Inspur K-DB（浪潮），Gbase（南大通用），KingBase（人大金仓），Gauss200（华为高斯），TRANSWARP INCEPTOR（星环/tdh））  支持大数据平台（Hive，hbase，TRANSWARP INCEPTOR，FusionInsight Hive，Presto，MaxCompute，Mongo DB，Hive HDP3，Elasticsearch）；  支持云数据库（阿里云RDS - MySQL，阿里云RDS - SQL server，阿里云RDS - PostgreSQL，ads，PolarDB MySQL，PolarDB Oracle）  支持文件扫描（txt、csv、xls、xlsx、元数据、json、xml、html） |  |
| 7 | 元数据管理 | 数据源管理，支持手工新增、批量导入、数据源发现三种方式添加数据源，可根据业务部门划分归属，页面支持查看数据源的关联用户、角色、权限 |  |
| 8 | 支持根据网段范围自动探测网络中的数据库，可扫描发现不限于Oracle、MySQL、SQL Server、DB2、TDSQL、postgresql、Sybase、 redis 、hbase、mongodb、informix等类型的数据库IP、端口、数据库类型等信息，支持仅对数据库常见的端口进行扫描以缩短扫描所用时间 |  |
| 9 | 支持对数据源进行元数据采集；支持对数据源的元数据变动进行采集；  支持定时执行数据源发现任务，可自定义定时周期和启动时间，启动时间可精确到小时、分、秒 |  |
| 10 | 支持展现数据源中的元数据清单，支持进行周期性扫描，并对其结果进行统计分析 |  |
| 11 | 资产发现 | 支持用户创建资产发现作业，支持按照库或者表选择需要发现的数据范围  支持选择发现模板自定义发现内容  支持自定义抽样行数范围、抽样行数（最小为10行）、输出命中率  支持定时开启资产发现作业  支持通过发现规则，语义内容分析和机器学习自动的识别数据含义  支持查看发现作业分析进度，并可以对每一步的结果进行修改和确认 |  |
| 12 | 资产关系梳理 | 支持用户根据库或表方式选择需要梳理关系的范围  系统自动化对于数据关系进行梳理，并以关系图谱的方式进行展现，提供产品功能截图  支持手动对待确定的数据关系进行确认，以及手动新增或删除数据关系 |  |
| 13 | 分类分级标准 | 内置分类分级标准，可支持数据的新增及分类分级配置，提供产品功能截图 |  |
| 14 | 类分级策略 | 支持表格分类分级配置，表格分类包括分类集合和就多原则两种分类策略，表格分级支持就高原则和加权计算两种分级策略 |  |
| 15 | 数据分析报告 | 系统提供完整、直观、内容丰富的分类分级结果报告，支持用户进行导出  资产发现报告：对数据资产、安全资产占比，基于源/库维度进行命中率分析排名，对源/库对应脏数据、空数据的统计排名，对于业务术语命中率排名等，支持PDF格式  资产分级报告：支持完成资产分级的相关统计分析，包括：安全数据分布、安全风险指数统计、重要数据/个人信息分布等，支持PDF、WORD等格式  安全合规报告：支持安全合规数据相关统计分析，包括：合规风险指数统计、群体数据统计，对重要数据源/库占比分析，对特定群体/行业主体/个人信息等进行分类统计，支持PDF、WORD等格式 |  |
| 16 | 分类分级结果 | 支持以分类分级目录形式查看数据资产自动发现的结果和分类分级情况。  支持提供全部数据资产梳理及可视化大屏展示  数据资产的盘点、数据分类分级概况、数据敏感分析、数据库差异分析等  资产分级驾驶舱展示，展示源/库/表/字段的统计。分别对分类命中率、数据分类，数据分级分布、数据敏感指数、敏感排名进行统计  大屏显示内容支持灵活配置 |  |
| 17 | 暗数据识别能力 | 支持用户维护和定义数据资产的业务标准，具备用户自定义业务术语  支持通过列内容匹配、列注释匹配、列名称匹配、函数分析等方式对数据语义内容进行自动识别，识别字段代表的业务术语 |  |
| 18 | NLP翻译 | 具备NLP翻译智能处理技术，实现语义发现，提高字段语义识别的准确性和效率  通过叠加特征NLP翻译技术，智能提升字段语义识别的效率和准确性，从而提升分类的效率和准确性 |  |
| 19 | 特征工程 | 备特征工程智能处理技术，实现字段识别，提高业务术语识别的准确性和效率  在基于内置业务术语发现规则（包括数据字典、正则、特定方法等）基础上，通过叠加特征工程技术，基于多维、高精度的特征比对，提供整体业务术语识别的准确性和效率  支持特征工程机器学习，梳理数据特征，并生成相应的数据发现规则，机器学习特征工程包含300+个特征维度 |  |
| 20 | LLM大模型 | 具备LLM大模型智能处理技术，实现语义推理，提供未知语义推理能力，进行智能数据分类 |  |
| 21 | 语义向量模型 | 具备语义向量模型智能技术，依托语义向量模型进行语义相似度的比较，实现数据分类，提高智能化分类的能力 |  |
| 22 | 重要数据特征库 | 重要数据特征库：支持根据内置的规则，包括数据量级和特殊群体定义识别数据资产中的重要和核心数据，包含1600+项重要数据特征规则 |  |
| 23 | 个人信息特征库 | 个人信息特征库：支持根据内置的规则，包括个人敏感信息、个人一般信息识别的数据，包含100+项个人信息特征规则 |  |
| 24 | 智能可视化大屏 | ★提供智能处理技术多维驾驶舱，支持智能策略提升效果的量化展示，展示当前作业状态分布及近7天数据源梳理情况的统计分析（提供产品功能截图）  提供智能处理对应源/智能化程度/源梳理情况/作业完成度的统计分析 |  |
| 25 | 安全策略联动 | 系统提供标准API，支持和现有数据安全产品系统联动，基于分类分级的结果定义制定数据安全策略 |  |
| 26 | 数据权限管理 | 支持按数据权限、功能权限和操作权限配置不同的角色。支持按数据源范围和数据样本权限进行权限管控 |  |
| 27 | ▲服务 | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供三年原厂质保函原件，产品序列号对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**3.6 防火墙（公卫网区域）技术规格要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **规格及配置要求** | **投标响应** |
| 1 | 基本要求 | 产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制 |  |
| 2 | 安全操作系统采用冗余设计，出于安全性考虑，多系统需在设备启动过程中进行选择不得在WEB维护界面中设置系统切换选项 |  |
| 3 | 2U,内存16G，机械硬盘不少于1T，不少于6个千兆电口，不少于2个千兆光插槽,不少于2个万兆光插槽，配置冗余电源,1个扩展槽位,防火墙吞吐12G，并发连接300万，每秒新建连接10万，应用层吞吐量10G，本次配置三年入侵防御、防病毒规则库升级许可 |  |
| 4 | 信息安全设备、系统软件的开发、生产符合TL9000-HSV标准，提供相关证明 |  |
| 5 | 网络接入 | 支持路由、交换、虚拟线、Listening、混合工作模式 |  |
| 6 | 支持RIP、OSPF、BGP4、QinQ、PIM-SM、PIM-DM |  |
| 7 | 支持策略略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由 |  |
| 8 | 支持手动和LACP链路聚合，可根据源/目的MAC、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法 |  |
| 9 | 支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作 |  |
| 10 | 支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换 |  |
| 11 | 防火墙作为DNS服务器可依据访问地址来源将服务器域名解析为内部地址或外部地址，同时支持通过配置多条转换策略，实现内网资源服务器的负载均衡 |  |
| 12 | 访问控制 | 支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、防代理、APT等功能配置,简化用户管理 |  |
| 13 | 支持域名控制，支持对多级域名进行控制，域名对象支持通配符 |  |
| 14 | 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址 |  |
| 15 | 提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果 |  |
| 16 | 提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度检索 |  |
| 17 | 安全防护 | 支持独立的入侵防护规则特征库，特征总数在5500条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库 |  |
| 18 | 规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，防护动作包括告警、阻断、记录攻击报文 |  |
| 19 | 支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义规则，自定义规则支持导入导出 |  |
| 20 | 支持对威胁事件、攻击来源、受威胁主机、威胁趋势等进行监控统计，并可进行可视化展示 |  |
| 21 | 支持针对IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP等协议进行DDOS防护；支持预定义和自定义策略模板 |  |
| 22 | 支持HTTP DDOS防护，采用阀值检查、源/目的限流、源认证、会话限制等方式综合进行HTTP FLOOD、HTTP URI CC攻击、HTTP连接耗尽等攻击防护 |  |
| 23 | 支持NTP DDOS防护，采用阀值检查、源/目的限流、源认证等方式综合进行NTP REQUEST FLOOD、NTP REPLY FLOOD攻击防护 |  |
| 24 | 支持病毒快速查杀和深度查杀模式，支持至少2种专业反病毒厂商的病毒特征库，病毒特征库规模超过400万 |  |
| 25 | 内置数据过滤功能，可对预置身份证号、护照号、银行卡号、手机号等敏感信息进行过滤 |  |
| 26 | 内置文件过滤功能，支持识别超过300种文件类型，对无法识别文件、更改文件后缀、缺失文件后缀等常见规避手段处理过的文件内容进行检查 |  |
| 27 | 内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测 |  |
| 28 | 系统管理 | 支持配置文件本地备份和回滚，支持＞3个配置文件备份，支持对访问控制策略、NAT策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计 |  |
| 29 | 支持系统温度、CPU温度、CPU利用率、内存利用率、电源故障等告警，支持CPU利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪 |  |
| 30 | ▲服务 | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供至少三年原厂质保函原件，设备产品序列号对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**3.7 Web应用防火墙(北院WAF)技术规格要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **技术规格及配置要求** | **投标响应** |
| 1 | 基本要求 | 2U,含交流冗余电源模块,2\*USB接口,1\*RJ45串口,2\*GE管理口。6\*GE电口 (BYPASS),4\*千兆光口，硬盘1T |  |
| 2 | 部署模式 | 串联代理、串联透传、单臂反向代理、旁路路由代理、反向代理集群部署，Nginx插件集群部署 |  |
| 3 | 高可用 | ★支持紧急模式：当并发连接数超过设置阀值时，WAF自动进入紧急模式，已经代理的连接正常代理，对新增的请求直接转发；当连接数恢复正常时，自动退出紧急模式。提供第三方测试报告，以及功能截图 |  |
| 4 | 访问控制 | HTTP自定义访问控制规则：可分别对请求、响应内容进行检测，包括对URI、URI-Path、host、参数（名&值）、头部（名&值）、cookie（名&值）、version、method、request-body、response-body等条件及条件组合，提供功能截图 |  |
| 5 | 内置PCI V3.2合规报表，能够结合当前防护站点的安全配置，按照PCI-DSS的合规要求对用户资产环境做出是否合规的判断，提供功能截图 |  |
| 6 | 解码能力 | 支持识别HTTP报文常见的编码和编码攻击：URL解码、Base64解码、HTML解码、JSON解析、XML解析、PHP反序列解析、UTF-8解码等，提供功能截图 |  |
| 7 | WEB安全 | 支持XML防护，包括XML基础校验、Schema校验以及SOAP校验。提供第三方测试报告，以及功能截图 |  |
| 8 | 防护 | 支持防护Java反序列化及基于Java的通用攻击 |  |
| 9 | 支持爬虫、扫描器等自动化工具的安全检测 能选择多种爬虫防护规则，并按照配置实例进行相应的动作，提供功能截图 |  |
| 10 | 支持非法下载防护，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等） |  |
| 11 | 支持暴力破解防护，支持GET/POST两种请求方法检测；支持Form/Ajax/JsonP三种验证方式；支持验证码机制，可有效防止误报 |  |
| 12 | 支持Cookie安全机制，通过cookie加密或cookie签名的方法对访问服务器后保留在客户端的cookie进行安全防护 |  |
| 13 | 支持扫描防护，通过应答样本的比例可以识别出扫描器的扫描行为，从而进行有效的扫描防护；通过算法统计请求量可以识别出扫描器的扫描行为，从而进行有效的扫描防护，提供功能截图 |  |
| 14 | ★会话追踪，通过浏览器标识和会话标识实现对会话的跟踪，记录完整的黑客攻击过程，做到场景复现。提供第三方测试报告，以及功能截图 |  |
| 15 | 防护ARP欺骗。提供功能截图 |  |
| 16 | 国密自适应，降低国密改造难度。同一域名/站点的SSL模块，同时支持国际标准https证书及国密证书，降低客户针对两种加密标准的国密改造难度。提供第三方测试报告，以及功能截图 |  |
| 17 | 策略配置 | 支持一键例外策略，降低误报。提供功能截图 |  |
| 18 | 提供虚拟站点配置，站点组全局策略提供安全基线；虚拟站点根据业务特点提供细粒度（IP+PORT+HOST+URI）的安全防护 |  |
| 19 | API防护 | ★支持API攻击防护，API资产自发现，影子API识别，API的OAS合规检查。提供第三方测试报告，以及功能截图 |  |
| 20 | BOT防护 | 通过人机识别、令牌认证、脚本配置、提交数据混淆、页面元素混淆、白名单配置等防护各种工具类的爬虫、扫描行为，降低数据泄露和资产漏洞暴露的风险，以及功能截图， |  |
| 21 | DDOS | 支持TCP Flood防护；支持基于阈值及算法配置的HTTP Flood防护。 |  |
| 22 | 防护 | 支持对慢速攻击的防护。支持流量算法防护，可有效区分客户正常访问与慢速攻击。依靠流量检测的方式，可兼容各种HTTP请求方式，提供功能截图 |  |
| 23 | 产品联动 | 智能补丁。定期自动获取专家级、个性化的《WEB漏洞扫描报告》，并转化为WAF可执行的、有针对性的WEB安全防护策略。提供功能截图 |  |
| 24 | 抗D联动。自身有TCP/HTTP Flood防护功能，并且支持与网络出口的绿盟Anti-DDoS设备联合防护大流量攻击。提供功能截图 |  |
| 25 | IP信誉。支持联动威胁情报，即时获取最新威胁情报；支持GEOIP，基于地理位置的源IP告警、动作以及封禁。 |  |
| 26 | 资质 | 产品生产厂商应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务安全开发类二级资质证书。提供资质证书证明。 |  |
| 27 | 产品产商参与起草了《标准信息安全技术 WEB应用防火墙 安全技术要求与测试评价方法》GB/T 32917-2016，提供截图证明。 |  |
| 28 | 具备能源管理体系ISO 23331-2020认证证书 |  |
| 29 | 具备中国信息安全测评中心颁发的国家信息安全测评信息安全服务安全开发类-二级认证证书 |  |
| 30 | 具备中国通信企业协会通信网络安全专业委员会颁发的通信网络安全服务能力评定证书-安全设计与集成二级认证 |  |
| 31 | ▲服务 | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供至少三年原厂质保函原件，设备产品序列号对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**3.8网闸（北院网络隔离）技术规格要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **技术规格及配置要求** | **投标响应** |
| 1 | ▲总体要求 | 需要和北院现有单台网闸TopRules（NR-51220）组成双机，无缝切换。 |  |
| 2 | 基本要求 | “2+1”系统结构，内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通。内外端机之间采用专用硬件和专用协议进行连接，不可编程。  硬件架构由内端机、外端机、专有隔离硬件三部分组成。内端机和外端机各自具有独立主板、独立总线、独立的存储和运算单元；内端机和外端机之间非网线、USB线、SCSI线等线缆直连，基于光隔离技术专有硬件进行隔离和数据交换 |  |
| 3 | 为保证系统软件设计全面性、保密性、完整性，要求招标产品系统遵从行业标准和政府法规，符合GB/T 18336信息技术安全性评估标准，提供信息技术产品安全测评EAL4+证书 |  |
| 4 | 2U,内外端机双侧液晶屏；内端机6个10/100/1000Base-T接口（含1个管理口），4个千兆光口插槽，2个万兆光口插槽；外端机6个10/100/1000Base-T接口（含1个HA口），4个千兆光口插槽，2个万兆光口插槽,冗余电源,网络吞吐量5Gbps，并发连接数30万，延时1ms，内外端机各16G内存，内外端机各1T机械硬盘 |  |
| 5 | 信息安全设备、系统软件的开发、生产符合TL9000-HSV 标准，提供相关证明 |  |
| 6 | 安全浏览功能 | 支持IP地址、端口、时间以及基于源用户身份的访问控制策略； |  |
| 7 | 支持访问控制日志记录和告警功能；支持最大活动会话数的控制和统计；支持IPV6扩展头的安全设置，提供功能截图 |  |
| 8 | ★支持http消息头、消息体，上下行方向，命令及关键字的管控，支持允许、阻断、告警三种处理方式，提供功能截图 |  |
| 9 | 支持50种以上文件类型特征识别，非扩展名过滤，包括可执行文件、文本文件、压缩文件、图片文件、多媒体文件等，支持上下行方向过滤单独控制，支持允许、阻断、告警三种处理方式 |  |
| 10 | 文件传输功能 | 提供基于FTP协议和TFTP协议的文件传输功能 |  |
| 11 | 支持代理、透明、路由三种接入方式 |  |
| 12 | 支持IP地址、端口、时间以及基于源用户身份的访问控制策略 |  |
| 13 | 无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口；有客户端方式可提供专用文件同步客户端安装在用户服务器上，提供安全的文件同步服务 |  |
| 14 | 提供有客户端和无客户端两种文件同步方式 |  |
| 15 | 支持文件名和文件类型的黑白名单过滤，文件类型过滤基于文件特征识别，非扩展名识别，且支持不小于50种文件类型识别。支持文件同步信息统计，包括每个任务的开始时间、同步数据量、同步成功数、同步失败数，并能够以图表的方式进行实时可视化展现，提供功能截图 |  |
| 16 | 支持FTP协议内部命令及数据层内容过滤，支持允许、阻断、告警三种处理方式 |  |
| 17 | 数据库功能 | 提供对多种主流数据库,如：MYSQL、SQLSERVER、ORACLE、DB2、SYBASE等系统的安全访问 |  |
| 18 | 内置数据库安全模块，支持内容过滤引擎，能够对数据库用户名、命令、关键字等内容进行管控，支持允许、阻断、告警三种处理方式 |  |
| 19 | 支持一对一、一对多、多对一方式的数据库同步；支持同构、异构数据库之间的同步，同步可具体设置到字段级别 |  |
| 20 | ★支持网闸同侧数据库之间的数据同步，网闸可旁路部署实现数据库同步，提供功能截图 |  |
| 21 | 快速配置支持全库表同步，可直接映射两个独立数据库进行同步，支持每策略映射表数量控制，支持每策略映射同步方向控制 |  |
| 22 | 支持实时同步和周期性同步方式，可分别控制插入、删除、更新的同步操作 |  |
| 23 | 系统管理 | 提供状态信息监控，以图表形式实时展现内外端机的CPU、内存、硬盘利用率，流量和会话数 |  |
| 24 | 提供在线用户监控，可实时展现内外端机在线用户名称、IP地址、认证服务器名称、客户端类型和在线时间信息，并可根据管理需要手动强制指定用户下线 |  |
| 25 | 支持日志审计功能，包括管理日志、系统日志、策略日志、同步日志和应用行为日志。支持日志记录查询、删除、导出，日志记录可导出文本文件和数据库文件两种格式 |  |
| 26 | ▲服务 | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供至少三年原厂质保函原件，设备产品序列号对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**3.9国密VPN系统技术规格要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **技术规格及配置要求** | **投标响应** |
| 1 | ▲专用的硬件和软件保障 | 产品必须为专业性VPN硬件设备，而非下一代防火墙\UTM 类设备集成的VPN模块，须符合国家商用密码产品认证证书 |  |
| 2 | 基本要求 | 2U机箱，默认配置4个SFP千兆插槽和6个10/100/1000BASE-T的接口，包括2个可插拨的扩展槽，标配模块化双冗余电源，国密IPSEC VPN最大吞吐率：400Mbps，国密IPSEC VPN最大隧道数：4000条，国密SSL VPN最大吞吐率：100Mbps，国密 SSL VPN最大建议并发用户数：1000，标配10个SSL并发用户许可，整机3年质保服务 |  |
| 3 | 产品设计 | 信息安全设备、系统软件的开发、生产符合TL9000-HSV 标准，（提供相关证明） |  |
| 4 | SSL VPN  功能 | 支持AES、DES、3DES、RC4、MD5、SHA1、RSA等多种算法；支持国家商密专用的SM2、SM3、SM4算法；支持国密、国际算法切换 |  |
| 5 | 客户端支持主流Windows、Mac OS、Linux操作系统 |  |
| 6 | 支持WEB转发、全网接入模式，支持FTP的WEB化访问 |  |
| 7 | 支持智能选路 |  |
| 8 | 支持HTML、JSP、ASP、JAVA APPLET、ACTIVE、Cookies等各种Web应用 |  |
| 9 | 支持对访问资源的健康检查 |  |
| 10 | 支持移动APP自动封装SSL VPN的SDK |  |
| 11 | 支持针对Android平台APP的VPN SDK自动打包 |  |
| 12 | 支持通过WebCache技术对web页面进行数据优化，支持智能压缩技术，减少不必要的数据传输 |  |
| 13 | IPSEC VPN  功能 | 符合国密局制定的《IPSEC VPN技术规范》，支持国家商用密码算法SM1、SM2、SM3、SM4； |  |
| 14 | 支持高效数据流压缩算法 |  |
| 15 | 支持虚拟路由、隧道转发 |  |
| 16 | 支持使用标准的X.509证书建立隧道 |  |
| 17 | 支持多机多隧道的负载均衡和备份 |  |
| 18 | 用户管理 | 支持SSL、IPSec使用一套用户认证，用户管理 |  |
| 19 | 支持管理员分级分权管理，根据不同管理可以管理不同的功能模块； |  |
| 20 | 支持基于用户、用户组、用户角色进行授权，实现用户可访问资源、可信接入和客户端杀毒策略 |  |
| 21 | 支持静态用户名口令、数字证书、短信、硬件特征码绑定、图形码、人脸识别认证方式 |  |
| 22 | 支持两种或两种以上组合认证方式 |  |
| 23 | 支持PC终端病毒检查功能 |  |
| 24 | 支持用户可自行配置终端类型，扫描级别等信息 |  |
| 25 | 系统管理 | 支持“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类 |  |
| 26 | 支持邮件、NETBIOS、声音、SNMP、控制台等多种组合报警方式 |  |
| 27 | 支持命令超时、历史命令、命令补齐、命令帮助、命令错误提示等功能 |  |
| 28 | 支持系统诊断管理 |  |
| 29 | 支持详细审计用户登录认证过程、各种认证授权错误、内网资源访问情况等信息 |  |
| 30 | 支持多级审计日志，可以灵活配置审计级别 |  |
| 31 | 支持将日志上传到外部日志服务器 |  |
| 32 | ▲服务 | 产品生产商需在国内设有400或800技术服务热线，提供原厂工程师安装调试服务及原厂企业级保修售后服务  中标后向用户提供至少三年原厂质保函原件，设备产品序列号对应最终用户：宁波大学附属妇女儿童医院  货物初次验收前有权要求提供样机进行上述功能要求的逐一测试验证，否则不予验收 |  |

**四、其他要求**

1、中标供应商中标后3个工作日内提供中标产品明细清单、详细参数、偏离表、明细价格表及采购文件要求提供的证明材料、认证证书；合同签订前提供以上所有资料，因中标人未及时提供以上资料导致采购人损失的，由中标人承担全部责任及损失。

2、所有产品必须保证为原厂原包装全新产品，产品的包装、运输与安装均由中标方负责，如在过程中产品有缺失、损坏或缺陷，医院可要求免费更换。

**第四章 商务条款**

|  |  |
| --- | --- |
| **序号** | **内 容** |
| **▲**1 | 服务地点：采购人指定地点。 |
| **▲**2 | 实施周期：合同签订后6个月内完成安装调试和试运行并通过采购人组织的验收。 |
| **▲**3 | 付款方法和条件：  1）适用中小企业：合同签订后，供应商应向采购人提交预付款保函。采购人在收到预付款保函、合同生效且项目具备实施条件七个工作日内支付合同金额的40%作为预付款；项目验收合格，支付合同价的60%。  注：签订合同时供应商明确表示无需预付款或者要求降低预付款比例的，采购人可在合同中另行约定。  2）适用大型企业：项目验收合格后支付合同价的100%。  3）采购人支付前，中标人须向采购人提供正规财务发票，否则采购人有权不予支付。 |
| 4 | 履约保证金：本项目不适用。 |
| 5 | 系统免费维护期≥1年，自系统验收通过之日起计算。 |
| 6 | 质量要求：满足招标文件规定的各项技术要求及国家、行业相关标准，并一次性验收合格。 |
| 7 | 验收要求： 采购人参照设备清单，进行产品品牌、型号、数量到货初验（所有货物一次性到安装场地），安装调试完成后根据招标文件里技术功能进行项目终验，发现产品达不到验收标准或合同规定的性能指标，供方必须立即调整或更换产品，采购人通过产品官方认证渠道，一经发现水货和串货的产品，立即终止合同，并且赔偿由此给用户造成的损失。 |
| 8 | 售后服务要求：  提供3年7x24小时现场技术服务；提供远程服务与现场服务相结合的方式，根据不同的故障级别采用不同的响应方案：电话及远程服务接到通报故障的电话或传真后的30分钟之内响应；对电话或远程无法排除的故障，在1小时之内到达现场，进行故障排除工作。一般非重大的故障保证系统在2小时之内修复，重大故障保证系统在8小时之内修复。对于无法修复的故障，提供相应的代用设备供用户应急使用，以确保系统的正常运行。  提供详细的售后服务方案，明确响应时间。 |
| 9 | 供应商应提供相应的培训计划并对采购人的操作人员、维修人员免费进行培训（培训时间由用户确定），包括但不仅限于原厂商工程师实施及提供设备相关的培训，并需提供产品的各项文档资料，包括但不仅限于部署文档、配置文档、试运行测试记录、用户使用手册等。提供详细的培训服务方案。 |
| 10 | 授予合同：按照招标文件的规定、中标人的投标响应及中标通知书确定的金额签订合同。 |
| 11 | 合同签订时间：中标通知书发出之日起30天内签订合同。 |

**第五章 评标办法及标准**

**一、评标办法**

1.1本项目评标采用综合评分法。

1.2综合评分法：采用百分制，总分100分。供应商的综合得分为商务和技术得分与报价得分之和。按综合得分由高到低的排序，推荐中标候选人。若供应商的综合得分相等，则投标报价低者列前；若投标报价也相同时，采取随机抽签的方式确定排序。

1.3本项目需要落实的政府采购政策：《关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）

**1.4本项目采购为非专门面向中小企业，采购标的对应的中小企业划分标准所属行业，属于软件和信息技术服务业，本次评标将对满足招标文件第二章第十八条第1、2、3款要求的货物制造商均为小微企业的价格给予10%的扣除，用扣除后的价格参与评审。价格扣除只用于评审过程，如中标，中标价格仍按照其投标价格进行公示。**

1.5评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。

二、**评标程序**

2.1初步审查：包含资格性审查和符合性审查。资格性审查是指采购人或代理机构根据“附表1资格性审查表”的要求对投标文件逐一进行评审。符合性审查是指评标委员会根据“附表2符合性审查表”的要求对投标文件逐一进行评审。**资格性审查和符合性审查中，有任意一项审查结论不合格的，作无效标处理。**

2.2比较与评价：评标委员会根据“附表3评分标准（兼评委打分表）”的要求，对照投标文件的应答进行比较，判定其偏差性质和程度，由评标委员会成员在分值范围内自行评分。供应商商务和技术得分为各评标委员会成员有效评分的算术平均值（小数点后保留二位数）。

2.3在评标过程中，发现的价格计算错误按下述原则修正：

（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。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经供应商确认后产生约束力，供应商不确认的，其投标无效。

非单一产品采购项目，多家供应商提供的核心产品品牌相同的，按上述规定处理。

2.2.3综合评估：经过初步审查、比较，评标委员会成员按照评分标准（兼评委打分表）规定的内容和分值设置以记名方式独立评定打分，汇总各评委对各供应商的评分，取算术平均值（小数点后保留二位数）即为各供应商的综合得分。

2.2.4推荐中标候选人：按综合得分由高到低的排序，推荐中标候选人。若供应商的综合得分相等，则投标报价低者列前；若投标报价也相同时，采取随机抽签的方式确定排序。

**2.3确定中标供应商**

评标委员会按综合得分由高到低的排序，向采购人推荐中标候选人。代理机构应当自评审结束之日起2个工作日内将评审报告送交采购人。采购人应当自收到评审报告之日起5个工作日内在评审报告推荐的中标候选人中按顺序确定，确定1名中标供应商。中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

**三、投标的澄清**

3.1评标委员会在对投标文件的有效性、完整性和响应程度进行审查时，可以要求供应商对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等做出必要的澄清。供应商的澄清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。

3.2政采云具体操作如下：

在评审过程中，如评标委员会对投标文件有疑问，由评标委员会组长将问题汇总后发函，或由采购代理机构代替发起。供应商在截止时间前，予以回复。此回复将作为投标文件内容的一部分，具有相应的法律效力。

路径：用户中心—项目采购—询标澄清

（1）政采云平台通过待办事项和短信提醒供应商在截止时间前完成澄清。

（2）供应商在“询标澄清-待办理”标签页下选择状态为“待澄清”的项目，点击操作栏【澄清】。

（3）查看函内容，在澄清截止时间前上传澄清文件并对澄清文件进行签章。（注：澄清文件必须以PDF格式上传，文件大小：50M）

（4）签章完成，文件名称处显示“已签章”，供应商可“撤回签章”修改澄清函和“查看文件”。

（5）确认澄清文件内容后，点击右上角【提交】；（注：供应商未对澄清文件签章，提交时，弹框提醒“澄清文件未签章，请进行签章操作”，如遇CA突发情况无法签章，供应商可点击【放弃签章并提交】提交澄清文件；反之则签章后再提交。）

（6）完成状态：供应商澄清文件提交成功后，在“询标澄清-全部”标签页下显示状态为“已澄清”。

3.3开标现场，供应商安排法定代表人或授权代表到场的，则由评标委员会组长将问题汇总后向供应商发出书面“采购响应文件问题澄清通知”，供应商应对需要澄清的问题作书面回答，该书面澄清应当由供应商的法定代表人或授权代表签字或者加盖供应商公章。书面澄清将作为投标文件内容的一部分，具有相应的法律效力。

3.4供应商未在截止时间前完成澄清，将被视作自动放弃。

**四、特别声明：价格是评标的重要因素之一，但最低价不是中标的唯一依据。**

**五、重新招标**

有下列情形之一的，采购人将重新招标：

5.1投标截止时间止，供应商少于:3个的；

5.2评标委员会评标过程中，有效供应商少于3个的；

5.3评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，应当停止评标工作，与采购人或者代理机构沟通并作书面记录。采购人或者代理机构确认后，应当修改招标文件，重新组织招标活动。

附表1：

**资格性审查表**

|  |  |  |
| --- | --- | --- |
| **序号** | **要求说明** | **审查要求** |
| 1 | 满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单。 | A1、关于资格的承诺函（附件一）；  A2、营业执照副本（或事业法人登记证副本或其他登记证明材料）扫描件加盖供应商公章（供应商如果有名称变更的，应提供由行政主管部门出具的变更证明文件扫描件加盖供应商公章）；  **代理机构将于开标当天通过“信用中国”网站查询供应商失信被执行人、重大税收违法失信主体信用记录，通过中国政府采购网查询供应商政府采购严重违法失信行为信用记录。若供应商被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单，其资格审查为不合格，其投标将被认定为无效投标。**  **若在开标当天因不可抗力事件导致无法查询且一时无法恢复查询的，可在中标公示期间对中标候选人进行事后查询。中标候选人被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的，采购人将依法取消其中标资格。** |
| **资格性审查结论** | |  |

**注：1、上述资格证明文件未按招标文件要求附入投标文件中的，资格性审查不合格。**

**2、上述审查项目中，任意一项不符合的，资格性审查不合格。**

附表2：

**符合性审查表**

|  |  |  |
| --- | --- | --- |
| **序号** | **要求说明** | **审查要求** |
| 1 | 投标有效期：符合第二章“投标须知”第六、1条的要求。 | 提供“投标书”。 |
| 2 | 法定代表人身份证明、法定代表人授权书。 | （1）投标文件由法定代表人签字的，提供“法定代表人身份证明”。  （2）投标文件由授权代表签字的，提供“法定代表人身份证明”和“法定代表人授权书”。 |
| 3 | 符合第二章“投标须知”第九、1条的要求。 | 投标文件的签署盖章。 |
| 4 | 对同个标项不允许提供两个投标方案。 | 是否有两个投标方案。 |
| 5 | 供应商不得在投标活动中提供任何虚假材料或从事其他违法活动的。 | 不得提供任何虚假材料或从事其他违法活动。 |
| 6 | 评标委员会经过审查，认定供应商虚假应标、串通投标的，有下列情形之一的，视为供应商串通投标：  （1）不同供应商的投标文件由同一单位或者个人编制；  （2）不同供应商委托同一单位或者个人办理投标事宜；  （3）不同供应商的投标文件载明的项目管理成员或者联系人员为同一人；  （4）不同供应商的投标文件异常一致或者投标报价呈规律性差异；  （5）不同供应商的投标文件相互混装； | 不得有所述情形。 |
| 7 | 符合法律、法规和招标文件中规定的其他实质性要求（实质性要求招标文件中“**▲**”标记） | 符合所述要求。 |
| 8 | 本项目不接受联合体投标。 | 供应商非联合体。 |
| 9 | 本次公开招标设有预算金额：150万元，投标报价超出对应预算价的投标无效。 | 提供“开标一览表”。 |
| 10 | 评标委员会认为供应商的报价明显低于其他通过初步审查的供应商的报价，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；供应商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。 | 符合所述要求。 |
| **符合性审查结论** | |  |

**注：1、上述审查项目中，任意一项不符合的，符合性审查不合格。**

**2、序号3-序号8、序号10在政采云上无须添加关联点。**

附表3：

**评分标准（兼评委打分表）**

**采购编号：NBITC-202411414G 适用于标项1**

| 供应商  分值 | | 分值 |
| --- | --- | --- |
| 技术分、商务分70分 | 1、对“第三章 招标内容与技术需求”响应性（28）  1）完全响应招标文件“第三章 招标内容与技术需求”所有指标的得28分，  2）每负偏离一条标“★”指标的扣1.8分。  3）每负偏离一条未标“▲”指标或“★”指标的扣1分。  4）本项最高得28分，当扣减分数≥28分时，作无效投标处理。  5）负偏离实质性条款（打“▲”）的，作无效投标处理。  （供应商请按照要求提供证明材料（如有），未提有效供证明材料视作对应条款负偏离。） | 28 |
| 2、项目负责人资质（2分）  拟派的项目负责人具有网络规划设计师或信息系统项目管理师证书的得2分，最高得2分。  （提供相关证书复印件及社保部门出具的供应商单位至少包括开标截止时间前三个月为上述人员缴纳社保的证明资料复印件加盖供应商公章，否则不得分。） | 2 |
| 3、业绩（3分）  供应商自2021年1月1日至今（以签订合同日期为准）同类项目业绩（合同内容含信息安全提升相关内容），每提供1个合同得1.5分，最多得3分。  （投标文件中须提供合同复印件并加盖供应商公章，否则不计分。同一用户不累计得分。） | 3 |
| 4、政策性因素加分（1分）：  投标产品为节能产品，提供有效期内节能产品认证证书的加0.5分；  投标产品为环境标志产品，提供有效期内环境标志产品认证证书的加0.5分。 | 1 |
| 5、根据供应商对现有安全信息系统与本项目信息安全提升的理解程度及分析、包括不仅限于对本项目现状、存在的问题、建设目标、建设任务、建设内容进行评议：（5分）  在针对本项目进行充分调研的基础上，能提出业务现状并提出符合实际信息化问题总结且方案全面、具体、表述清楚、针对性强的得5分；对项目背景较为了解，响应方案能与采购需求相结合，基本符合采购需求的得3分；对项目背景较为了解不足，方案不够具体、详细或部分内容有待补充、完善的得1分。无相应内容的不得分。 | 5 |
| 6、技术方案 |  |
| 1）根据供应商所提供的技术方案，包括整体系统架构、系统对接融合程度、系统描述，与项目实际情况的符合性等内容进行评议：（5分）  技术方案科学、安全、严密性、兼容性，具有可扩展性和前瞻性的得5分；系统设计方案简单且缺乏可行性，部分内容待补充完善的得3分；系统设计方案内容不全或有明显不合理之处的得1分；无相应内容的不得分。 | 5 |
| 2）根据供应商对本项目提供的所投产品整体性能描述，包括不仅限于产品选型专业性、安全性、系统功能技术实现与对本项目需求的契合度、配置情况情况等内容进行评议：（4分）  功能描述完善、质量技术水平高、技术指标领先于其他产品，可完全满足采购需求的得4分；质量技术水平较高、技术指标较先进，可较好满足采购需求的得3分；质量技术水平、技术指标均一般或存在缺陷的得1分；无相应内容的不得分。 | 4 |
| 7、评标委员会根据供应商提供的实施方案，包括不仅限于实施方案内容、管理运作流程设计、运作方式、项目管理目标、项目实施组织结构、协调方法以及项目实施重点关键环节阐述等内容进行评议：（5分）  实施方案内容完整全面、管理运作流程设计严谨、协调方法切实有效、执行度高，对重点关键环节分析全面、明确的得5分；实施方案内容完整，但缺少针对性，管理运作流程设计等各项内容齐全，但存在较少瑕疵、部分细节有待补充基本的得3分；实施方案内容未进行详细阐述，部分内容表述笼统、单一的得1分；无相应内容的不得分。 | 5 |
| 8、拟派项目团队人员配置方案，提供详细的团队清单及分工说明，提供的项目实施团队人员投入、人员技术力量（技术能力、资质证书、类似项目经验人员配置情况）情况进行评议：（5分） 团队人员组成结构合理、技术人员具备类似信息化、网络安全相关专业证书，团队人员中具备与本项目匹配实施经验的得5分；团队人员组成较为合理、能提供与本项目技术力量匹配的团队人员，但缺少与本项目匹配的实施经验或部分内容有待完善补充的得3分；团队人员分工或人员资质及工作经验缺乏或各项方案有明显不合理之处的得1分；无相关内容不得分。  （**投标文件中须同时提供相关专业证书复印件及社保部门出具的供应商单位至少包括开标截止时间前三个月为上述人员缴纳社保的证明资料复印件加盖供应商公章，否则不得分。**） | 5 |
| 9、供应商需提供项目应急方案以及是否能根据采购人信息安全实际环境提出的合理化建议，对项目各个阶段的实施过程中遇到应急情况有所预见和准备，包括：总体应急方案，完备的预防措施（如沟通协调、隐患排除、监督管理、事前准备、事后完善等），应急事件类型划分及针对性措施，应急人员保证和应急时间响应，应急工作责任主体和惩处方法等内容进行评议：（4分） 方案描述详细完善、能结合自身经验提供针对性的应急措施，确保有效解决可预见性问题，有规范处理流程和行之有效的处理办法、日常做好防范的措施，能提供切实有效的合理化建议的得4分；方案描述较为完善、应急措施基本合理可行、能提供合理化建议的得3分；方案内容不全、有明显不合理之处的得1分；无相关内容不得分。 | 4 |
| 10、根据供应商提供的培训方案，包括前端系统安装、系统应用、系统操作、系统运维指导、培训人员技术力量、培训时间安排进行评议：（3分）  培训内容合理完整、培训时间安排合理、培训内容涵盖本次货物所需技术需求、培训方式多样的得3分。培训时间安排基本可行但细节部分欠完整、培训内容基本可覆盖项目建设所需技术要求的得2分。培训方案内容简单、笼统，未进行细化的得1分。无相关内容不得分。 | 3 |
| 11、根据供应商需提供售后服务方案，包括售后服务机构、服务机构规模、售后服务响应时间、服务能力、服务保障及服务方案、维护收费承诺及其它优惠条件等内容进行评议：（5分）  售后服务方案详尽、明确，售后响应时间迅速，服务技术服务人员充足、售后服务方案详细完善、针对售后服务能提供优惠承诺的得5分；响应速度较快，技术服务人员满足本次采购需求， 售后服务方案完整但具体内容有所欠缺，针对售后服务能提供优惠承诺的得3分；响应速度无明显优势或技术服务人员投入少或售后服务方案有明显不合理之处或无优惠条件的不得分； | 5 |
| 价格分30分 | 参与评审的价格=评标价-小微企业价格扣除优惠值10%  评标基准价=满足招标文件要求且“参与评审的价格”中最低的价格为评标基准价  基准价得分为满分30分，其他供应商报价得分计算公式如下：  其他供应商报价得分=（评标基准价/参与评审的价格）×30%×100 | 30 |
| 合计 | | 100 |

注：1、各评委成员自行按以上参考分值评分，评分小数点后保留一位数。

2、表内要求提供的资料，未按要求提供的均不得分。

评委签名： 年 月 日

**第六章 采购合同样本**

**（本合同为合同样稿，最终稿由甲乙双方协商后确定）**

编号：

甲方： （以下简称甲方）

乙方： （以下简称乙方）

根据《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》、《政府采购货物和服务招标投标管理办法》等法律法规，项目名称 （项目编号： ）于 年 月 日进行公开招标，确定由乙方中标。按照《中华人民共和国民法典》的有关规定，在自愿、平等、公平、诚信的基础上，经双方协商一致，签订本合同。

1. **合同内容**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **产地品牌** | **单位** | **数量** | **单价（元）** | **合价（元）** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
| 合同总价（元） | | | | |  |  |

1. **实施周期**

年 月 日至 年 月 日

**三、合同金额**

**本合同为含税固定总价，合同金额为 元，**合同总价包括不仅限于完成用户当前环境下系统正常运行所需的软件升级或改造、系统对接、测试、运输、安装调试、验收、培训、免费维保期的售后服务等全部费用。即甲方不再另行支付其他任何费用。

**四、组成合同的文件**

（1）本合同协议书；

（2）中标通知书；

（3）投标书及其附件；

（4）招标文件；

（5）标准、规范及有关技术文件；

有关甲乙双方洽商、变更等书面协议或文件均视为本合同组成部分。

**五、软件保证与免责**

**（一）甲方保证**

1、甲方具有合法的权利能力签署并履行本合同项下的义务。

2、利益冲突：甲方签署和履行本合同或与本合同相关的文件将不会（1）与甲方的章程或其他适用于甲方的法律法规或判决等相冲突；（2）与甲方同第三人所签署的任何法律文件如保证协议、承诺、合同等中的义务相冲突或导致任何违约，或使乙方的权利受到约束。

**（二）乙方保证**

1、技术实力：乙方是一个具备较强开发能力的软件开发机构，且具有合法的权利能力签署和履行本合同项下的义务。

2、利益冲突：乙方签署和履行本合同或与本合同相关的文件将不会 （a）与乙方的章程或其他适用于乙方的法律法规或判决相冲突；（b）与乙方同第三人所签署的任何法律文件如保证协议、承诺、合同等规定的义务相冲突或导致任何违约，或使乙方的权利受到约束。

3、乙方保证：乙方履行本合同项下的义务。

4、在乙方所交付的软件系统中，不含任何可以自动终止或妨碍系统运作的软件。

**六、付款方式**

**七、履约保证金（如有）**

7.1履约保证金金额：

7.2履约保证金形式：

7.3履约保证金的退取：履约保证金在乙方完成项目终验后无息退还（但如乙方未能履行合同规定的任何义务，加分有权扣除相应履约保证金）。

**八、软件交付、软件领受与软件验收**

8.1交付

8.2交付内容

乙方应按照合同所约定的内容进行交付。

8.3领受

甲方在领受了上述交付件后，应立即对该交付件进行测试和评估，以确认其是否符合开发软件的功能和规格。甲方应在10个工作日内，向乙方提交书面说明以表示接受该交付件。如有缺陷，应递交缺陷说明及指明应改进的部分，乙方应立即纠正该缺陷，并再次进行测试和评估。甲方应于20个工作日内再次检验并向乙方出具书面领受文件或递交缺陷报告。甲、乙双方将重复此项程序直至甲方领受。

8.4软件系统试运行

8.4.1自软件交付通过之日起，甲方拥有30天的试运行权利。

8.4.2如由于乙方原因，软件在试运行期间出现故障或问题，乙方应及时排除该方面的故障或问题。

8.4.3乙方应在合理的期限内排除故障或处理问题。

8.5系统验收

8.5.1软件试运行完成后，甲方应及时按规定对该软件进行系统验收。乙方应以书面形式向甲方递交验收通知书，甲方在收到验收通知书的10个工作日内，安排具体日期，由甲、乙双方按照本合同的规定完成软件系统验收。

8.5.2如属于乙方原因致使软件未通过系统验收，乙方应排除故障，并可在甲方的同意下，适当延长试运行期限，直至软件系统完全符合验收标准。

8.5.3如属于甲方原因致使软件未通过系统验收，如属甲方原有计算机系统故障原因，甲方应在合理时间内排除故障，再进行验收。

**九、软件知识产权和使用权**

9.1知识产权： 甲方拥有开发软件的知识产权。乙方非经甲方同意，不得以任何方式向第三方披露、转让和许可有关的技术成果、计算机软件、技术诀窍、秘密信息、技术资料和文件。除本研发工作需要之外，未得到甲方的书面许可，乙方不得以任何方式商业性地利用上述资料。

9.2使用权： 甲方对软件具有使用权。

9.3本合同项下双方的任何权利和义务不因合同双方发生收购、兼并、重组、分立而发生变化。如发生上述情形之一，则本合同项下的权利和义务随之转移至收购、兼并、重组或分立之单位。如甲、乙双方在本合同项下的各项权利和义务由甲、乙双方之分立单位分别承受的，则甲、乙双方与甲、乙双方之分立单位分别享有和承担相关权利和义务。

9.4甲方与乙方在领受本合同项下的软件后，应严格遵守相关的知识产权及软件版权保护的法律、法规。

**十、软件维护和培训**

10.1软件的维护和支持：乙方同意在本合同规定的 年期限内，向甲方提供软件维护和支持服务。维护和支持服务期满后，如甲方继续聘请乙方提供上述服务，甲、乙双方将另行签订维护和支持协议。

10.2项目培训：乙方应及时对甲方的相关人员进行培训，培训目标为受训者能够独立、熟练地完成操作，实现依据本合同所规定的软件的目标和功能。

**十一、软件保密**

11.1信息传递在本合同的履行期内，任何一方可以获得与本项目相关的对方的商业秘密，对此双方皆应谨慎地进行披露和接受。

11.2保密获取对方商业秘密的一方仅可将该商业秘密用于履行其在本合同项下的义务，且只能由相关的工程技术人员使用。获取对方商业秘密的一方应当采取适当有效的方式保护所获取的商业秘密，不得未经授权使用、传播或公开商业秘密。

11.3非经甲、乙双方同意，在本合同实施过程中以及本合同履行完毕后的10 年内，双方均不得使用在履行本项目过程中得到的对方商业秘密，从事与对方有竞争性的业务。

11.4上述保密义务不适用以下情况

11.4.1法律强制披露；

11.4.2经披露方书面许可。

11.5信息安全：甲、乙双方同意采取相应的安全措施以遵守和履行上述条款所规定的义务。经一方的合理请求，该方可以检查对方所采取的安全措施是否符合上述规定的义务。

**十二、违约责任**

12.1交付违约

乙方应在合同所规定的时间内完成和交付本合同规定的项目。如开发工作延时在经过甲方同意后，可以给予乙方10日的宽限期，宽限期内不追究乙方的违约责任。如乙方在宽限期内仍未依据本合同的规定完成和交付本合同所规定的项目，甲方有权要求乙方作出补偿和采取补救措施，并继续履行本合同所规定的义务。

12.1.1每延期30天，乙方应向甲方支付合同总价5％的违约金。

12.1.2如延期时间超过100天，甲方有权终止合同，除前款所约定的违约金外，并要求乙方支付合同总价的30％作为对甲方的赔偿。如甲方由此终止本合同，乙方应在两个星期内返还甲方所支付的费用和报酬并依甲方的指示退还或销毁所有的基础性文件和原始资料。

12.2付款违约

12.2.1如甲方未按合同规定的期限付款，每延期30天，甲方应向乙方支付合同总价5％的违约金；

12.2.2如延期时间超过100天，乙方有权终止合同，除前款所约定的违约金外，乙方还可要求甲方支付合同总价的30％作为对乙方的赔偿；

12.2.3如合同继续履行，甲方除支付上述违约金外，仍应按照合同规定的金额付款，乙方履行本合同的日期相应顺延；

12.3保密违约

任何一方违反本合同所规定的保密义务，违约方应按本合同总价的10％支付违约金。

12.4其他条款违约：

任何一方违反本合同所规定的义务，除本合同另有规定外，违约方应按合同总价10％的金额向对方支付违约金。

12.5如发生违约事件，守约方要求违约方支付违约金时，应以书面方式通知违约方，内容包括违约事件、违约金、支付时间和方式等。违约方在收到上述通知后，应于15天内答复对方，并支付违约金。如双方不能就此达成一致意见，将按照本合同所规定的诉讼条款解决双方的纠纷，但任何一方不得采取非法手段或以损害本项目的方式实现违约金。

**十三、附则**

13.1因自然灾害等不可抗力因素造成本合同项目经济损失的，甲、乙双方共同协商妥善解决。

13.2本合同未尽事宜，以招标文件、乙方的投标文件及投标澄清和承诺或以双方签订的补充协议为准，均与本合同具有同等效力。

13.3本合同壹式 份，甲乙双方各执 份。

13.4本合同经甲、乙双方法定代表人或授权人签字后生效。

13.5诉讼：双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向合同签订地法院起诉。

甲方（盖章）： 乙方（盖章）：

法人代表人： 法人代表人：

委托代理人： 委托代理人：

签订时间： 年 月 日 签订时间： 年 月 日

**第七章 附件**

A.资格文件

**封面**

**正（副）本**

**宁波大学附属妇女儿童医院信息安全提升项目**

采购编号：NBITC-202411414G

标项号：（如有多个标项）

（资格文件）

**投标文件**

供应商全称：（加盖单位公章）

年月日

**A1、**关于**资格的承诺函**

致：采购人

我单位承诺：

我单位满足《中华人民共和国政府采购法》第二十二条 供应商参加政府采购活动应当具备的下列条件：

（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；

（六）法律、行政法规规定的其他条件。

特此承诺。

供应商（盖章）：

日期：

**A2、营业执照副本（或事业法人登记证副本或其他登记证明材料）扫描件加盖供应商公章（供应商如果有名称变更的，应提供由行政主管部门出具的变更证明文件扫描件加盖供应商公章）；**

**A3 供应商认为需要的其他资料（如有需提供）**

B.商务和技术文件

封面

**正本**

**宁波大学附属妇女儿童医院信息安全提升项目**

采购编号：NBITC-202411414G

标项号：（如有多个标项）

（商务和技术文件）

**投标文件**

供应商全称：（加盖单位公章）

年 月 日

**B1投标书**

致：宁波市国际招标有限公司

（供应商全称）　授权 （全名、职务） 为全权代表，参加贵方组织的宁波大学附属妇女儿童医院信息安全提升项目（采购编号：NBITC-202411414G）招标活动并投标，为便于采购人公正、择优地确定中标供应商及其服务，我方就本次投标有关事项郑重声明如下：

1、我方提交的所有投标文件、资料都是准确的和真实的。如有虚假或隐瞒，采购人愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

2、我方不是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。

3、我们已详细审查全部招标文件及有关的澄清/修改文件（若有），我们完全理解并同意放弃对这方面提出任何异议的权利。

4、保证遵守招标文件有关条款规定。

5、本项目的投标报价详见“开标一览表”。

6、投标文件有效期为自开标之日起 90 个日历日。

7、保证在中标后忠实地执行与采购人所签署的合同，并承担合同规定的责任义务。

8、完全同意招标文件中有关招标代理服务费的条款，保证在中标后按照招标文件规定的金额、时间和方式，向贵方一次性交纳招标代理服务费。采购人如逾期未交纳（含未足额）的，愿凭贵方开出的违约通知，按上述规定应交纳金额（含欠交纳）的200%交纳违约金和滞纳的银行利息。承诺在未交足上述违约金和利息前，同意不再参加贵方代理的其他项目，如果贵方不接受我们的投标，我们自愿放弃任何方式进行抗辩的权力。

9、与本投标有关的一切正式来往通讯请寄：

地址： 邮编：

电话： 传真：

供应商（盖章）：

日 期：

**B2法定代表人身份证明**

供应商名称：

单位性质：

地址：

成立时间： 年 月 日

经营期限：

姓名： 性别： 年龄： 职务：

身份证号码：

系（供应商名称）的法定代表人。

特此证明。

供应商（盖章）：

日 期：

后附：**法定代表人身份证复印件加盖供应商公章。**

**B3法定代表人授权书**

**（投标文件由授权代表签字的须提供）**

致：采购人

（供应商全称）法定代表人（法定代表人姓名）授权（授权代表姓名）为授权代表，参加宁波大学附属妇女儿童医院信息安全提升项目，采购编号为NBITC-202411414G，其在招投标活动中的一切活动本公司均予承认。

供应商（盖章）：

**法定代表人（签字或盖签章）：**

日 期：

附：

授权代表姓名：

授权代表身份证号码：

职务：

详细通讯地址：

电话：

传真：

后附：

**1、授权代表身份证复印件加盖供应商公章；**

**B4供应商一般情况表**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 单位名称： | | |
| 2 | 总部地址： | | |
| 3 | 当地代表处地址： | | |
| 4 | 电话： | 联系人： | |
| 5 | 传真： | 电子信箱： | |
| 6 | 注册地： | 注册年份： | |
| 7 | 公司的资质等级（请附上有关证书的复印件） | | |
| 8 | 公司（是否通过，何种）质量保证体系认证（如通过请附相关证书复印件，提供认证机构年审监督报告） | | |
| 9 | 从业人员数量 | |  |
| 10 | 营业收入 | |  |
| 11 | 其他需要说明的情况 | |  |

供应商（盖章）：

日 期：

**B5用户需求响应表**

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

项目编号：NBITC-202411414G

标项号：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标要求 | 投标响应 | 偏离说明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：须与“第三章招标内容与技术需求”逐项比较，如有偏离的，须在本表中列明，并提供详细的偏离说明。如供应商未在本表中列出偏离说明，即使其在投标文件的其他部分说明与采购文件要求有所不同或回避不答，亦视为完全符合采购文件中所要求的最佳值并写入合同。若中标供应商在定标及合同签订前，以上述事项为借口而不履行合同签订手续及执行合同，则视作其放弃中标资格。

供应商（盖章）：

日期：

**B6商务条款响应表**

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

项目编号：NBITC-202411414G

标项号：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标要求 | 投标响应 | 偏离说明 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |

注：1、须与“第四章商务条款”逐项比较，如有偏离的，须在本表中列明，并提供详细的偏离说明。如供应商未在本表中列出偏离说明，即使其在投标文件的其他部分说明与采购文件要求有所不同或回避不答，亦视为完全符合采购文件中所要求的最佳值并写入合同。若中标供应商在定标及合同签订前，以上述事项为借口而不履行合同签订手续及执行合同，则视作其放弃中标资格。

供应商（盖章）：

日期：

**B7、第五章“评标办法及标准”中评分标准（兼评委打分表）要求提供的资料（如有需提供）；**

7.1对现有安全信息系统与本项目信息安全提升的理解及分析；

7.2技术方案；

7.3实施方案；

7.4项目实施人员配置情况；

7.5项目应急方案以及是否能根据采购人信息安全实际环境提出的合理化;；

7.6培训方案；

7.7售后服务方案；

**B8、综合评分打分表中需提供的评分资料（如有须提供）。**

**B9、供应商认为需要的其他资料（如有需提供）。**

**。**

**部分格式如下：**

**拟投入项目实施人员名单**

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

项目编号：NBITC-202411414G

标项号：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **姓名** | **本项目拟任岗位** | **性别** | **年龄** | **学历** | **专业** | **职务**  **/职称** | **工作年限** | **经验及业绩** | **从业资格证书编号或上岗证编号** | **备注** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

**备注：**以上人员一经确认，不得随意更换，如需更换，必须征得采购人同意。擅自更换或不到位属违约行为。

供应商（盖章）：

日 期：

**业绩表**

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

项目编号：NBITC-202411414G

标项号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **用户单位** | **合同内容** | **签订合同时间** | **联系人及方式** | **合同扫描件所在页码** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**注：投标文件中同时提供合同扫描件加盖供应商单位公章。**

供应商（盖章）：

日 期：

**证书情况表**

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

项目编号：NBITC-202411414G

标项号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **证书名称** | **颁证机构** | **证书有效期**  **（起止年月）** | **证书扫描件所在页码** | **备注** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**注：后附证书扫描件加盖供应商公章。**

供应商（盖章）：

日 期：

C.报价文件

封面

**正（副）本**

**宁波大学附属妇女儿童医院信息安全提升项目**

采购编号：NBITC-202411414G

标项号：（如有多个标项）

（报价文件）

**投标文件**

供应商全称：（加盖单位公章）

年 月 日

**C1****开标一览表**

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

项目编号：NBITC-202411414G

标项号：

|  |  |  |  |
| --- | --- | --- | --- |
| **子包** | **项目名称** | **投标报价** | **备注** |
| 1 | 宁波大学附属妇女儿童医院信息安全提升项目 | 人民币（大写） 元  （￥ 元） |  |

注: （1）以上报价合计应与“分项报价表”中的“投标报价”相一致。

（2）投标文件中开标一览表内容与政采云系统“开标一览表”中录入的报价内容不一致的，以上传的签字盖章版投标文件中开标一览表为准；

供应商（盖章）：

日 期：

**C2分项报价表**

项目名称：宁波大学附属妇女儿童医院信息安全提升项目

项目编号：NBITC-202411414G

标项号：

货币单位：人民币元

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **编号** | **建设/改造内容** | **产地品牌** | **规格型号** | **数量/单位** | **综合**  **单价** | **合价** |
| 1 | 互联网安全接入服务（SaaS服务） |  |  | 1项 |  |  |
| 2 | 零信任控制系统 |  |  | 1项 |  |  |
| 3 | HTTPS安全证书 |  |  | 1项 |  |  |
| 4 | CDP备份一体机系统（核心产品） |  |  | 1项 |  |  |
| 5 | 数据发现和分类分级系统（核心产品） |  |  | 1项 |  |  |
| 6 | 防火墙（公卫网区域） |  |  | 1项 |  |  |
| 7 | Web应用防火墙(北院WAF) |  |  | 1项 |  |  |
| 8 | 网闸（北院网络隔离） |  |  | 1项 |  |  |
| 9 | 国密VPN系统 |  |  | 1项 |  |  |
| ... | ... |  |  |  |  |  |
| 投标报价 | | | | | |  |

**注：1、本表中的投标报价应与开标一览表中的投标报价一致。**

2、供应商可根据实际情况自行填写，但必须注明具体的细目内容，栏目不够可自行添加。

供应商（盖章）：

日 期：

**C3、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. 互联网安全接入服务（SaaS服务） （标的名称），属于 软件和信息技术服务业 行业；制造商为\_\_\_\_\_\_\_\_（企业名称），从业人员   人，营业收入为   万元，资产总额为  万元，属于（中型企业、小型企业、微型企业）；

2. 零信任控制系统 （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

3. HTTPS安全证书 （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

4. CDP备份一体机系统 （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

5. 数据发现和分类分级系统 （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

6. 防火墙（公卫网区域） （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

7. Web应用防火墙(北院WAF) （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

8. 网闸（北院网络隔离） （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

9. 国密VPN系统 （标的名称），属于 软件和信息技术服务业 行业；制造商为 （企业名称），从业人员   人，营业收入为   万元，资产总额为   万元，属于（中型企业、小型企业、微型企业）；

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

注：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。

供应商：（盖单位公章）

日期： 年 月 日

**C4、残疾人福利性单位声明函（如有需提供）**

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。

供应商（盖章）：

日 期：

**注：**

**享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：**

**（一）安置的残疾人占本单位在职职工人数的比例不低于25%（含25%），并且安置的残疾人人数不少于10人（含10人）；**

**（二）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；**

**（三）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；**

**（四）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；**

**（五）提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。**

**前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1至8级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或者服务协议的雇员人数。**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **中小微行业划型标准规定（根据工信部联企业〔2011〕300号制定）** | | | | | | | | | | |
| **行业** | **中型企业** | | | **小型企业** | | | **微型企业** | | |
| 从业人员X（人） | 营业收入Y  （万元） | 资产总额Z  （万元） | 从业人员X（人） | 营业收入Y  （万元） | 资产总额Z  （万元） | 从业人员X（人） | 营业收入Y（万元） | 资产总额Z（万元） |
| 1、农林牧渔业 |  | 500≤Y＜20000 |  |  | 50≤Y＜500 |  |  | Y＜50 |  |
| 2、工业 | 300≤X＜1000 | 2000≤Y＜40000 |  | 20≤X＜300 | 300≤Y＜2000 |  | X＜20 | Y＜300 |  |
| 3、建筑业 |  | 6000≤Y＜80000 | 5000≤Z＜80000 |  | 300≤Y＜6000 | 300≤Z＜5000 |  | Y＜300 | Z＜300 |
| 4、批发业 | 20≤X＜200 | 5000≤Y＜40000 |  | 5≤X＜20 | 1000≤Y＜5000 |  | X＜5 | Y＜1000 |  |
| 5、零售业 | 50≤X＜300 | 500≤Y＜20000 |  | 10≤X＜50 | 100≤Y＜500 |  | X＜10 | Y＜100 |  |
| 6、交通运输业 | 300≤X＜1000 | 3000≤Y＜30000 |  | 20≤X＜300 | 200≤Y＜3000 |  | X＜20 | V＜200 |  |
| 7、仓储业 | 100≤X＜200 | 1000≤Y＜30000 |  | 20≤X＜100 | 100≤Y＜1000 |  | X＜20 | Y＜100 |  |
| 8、邮政业 | 300≤X＜1000 | 2000≤Y＜30000 |  | 20≤X＜300 | 100≤Y＜2000 |  | X＜20 | Y＜100 |  |
| 9、住宿业 | 100≤X＜300 | 2000≤Y＜10000 |  | 10≤X＜100 | 100≤Y＜2000 |  | X＜10 | Y＜100 |  |
| 10、餐饮业 | 100≤X＜300 | 2000≤Y＜10000 |  | 10≤X＜100 | 100≤Y＜2000 |  | X＜10 | V＜100 |  |
| 11、信息传输业 | 100≤X＜2000 | 1000≤Y＜100000 |  | 10≤X＜100 | 100≤Y＜1000 |  | X＜10 | Y＜100 |  |
| 12、软件和信息技术服务业 | 100≤X＜300 | 1000≤Y＜10000 |  | 10≤X＜100 | 50≤Y＜1000 |  | X＜10 | Y＜50 |  |
| 13、房地产开发经营 |  | 1000≤Y＜200000 | 5000≤Z＜10000 |  | 100≤Y＜1000 | 2000≤Z＜5000 |  | Y＜100 | Z＜2000 |
| 14、物业管理 | 300≤X＜1000 | 1000≤Y＜5000 |  | 100≤X＜300 | 500≤Y＜1000 |  | X＜100 | Y＜500 |  |
| 15、租赁和商务服务业 | 100≤X＜300 |  | 8000≤Z＜120000 | 10≤X＜100 |  | 100≤Z＜8000 | X＜10 |  | Z＜100 |
| 16、其他未列明 | 100≤X＜300 |  |  | 10≤X＜100 |  |  | X＜10 |  |  |
| 说明　1、企业类型的划分以统计部门的统计数据为依据。  2、个体工商户和本规定以外的行业，参照本规定进行划型。  3、本规定的中型企业标准上限即为大型企业标准的下限。 | | | | | | | | | | |