****

**台州学院网络安全教学实训数字化建设项目**

**公开采购文件**

**（线上电子招投标）**

项目编号：ZGTZZB2024-0813

采购人：台州学院

采购代理机构：中冠工程管理咨询有限公司

二〇二四年 九 月

**目录**

**[第一部分 采购公告 1](#_Toc6474)**

**[第二部分 投标资料表 7](#_Toc13292)**

**[第三部分 投标须知 12](#_Toc17817)**

**[第四部分 评标办法及评分标准 26](#_Toc3915)**

**[第五部分 采购内容及要求 32](#_Toc2999)**

**[第六部分 拟签订的合同文本 68](#_Toc21037)**

**[第七部分 格式与表格 74](#_Toc6437)**

**第一部分 采购公告**

项目概况

台州学院网络安全教学实训数字化建设项目的潜在投标人应在政采云平台获取采购文件，并于2024年10月09日09点00分（北京时间）前递交投标文件。

**一、项目基本情况**

项目编号：ZGTZZB2024-0813

项目名称：台州学院网络安全教学实训数字化建设项目

预算金额（元）：2795200

最高限价（元）：2795200

采购需求：详见采购文件第五部分“采购内容及要求”

**标项一：**

标项名称：台州学院网络安全教学实训数字化建设项目

数量：1批

预算金额（元）：2795200

最高限价（元）：2795200

简要规格描述或项目基本概况介绍、用途：具体内容详见采购文件第五部分“采购内容及要求”。

交货期：合同签订后30日历天内交货。

本项目（否）接受联合体投标。

本项目（否）接受分包。

**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。

4、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；为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后不得再参加该采购项目的其他采购活动。

**三、获取采购文件**

时间：/至2024年10月09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）：政采云平台（https://www.zcygov.cn/）

方式：本项目采购文件实行“政府采购云平台”在线获取，不提供采购文件纸质版。供应商获取采购文件前应先完成“政府采购云平台”的账号注册；

潜在供应商登陆政采云平台，在线申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件；仅需浏览采购文件的供应商可点击“游客，浏览采购文件”直接下载采购文件浏览）；

采购公告附件内的采购文件仅供阅览使用，供应商只有在“政府采购云平台”完成获取采购文件申请并下载了采购文件后才视作依法获取采购文件（法律法规所指的供应商获取采购文件时间以供应商完成获取采购文件申请后下载采购文件的时间为准）。

**注：请供应商按上述要求获取采购文件，未依法获取采购文件的供应商不得对本项目提起质疑、投诉，不得参加本项目的投标活动；如未在“政采云”系统内完成相关流程，引起的投标无效责任自负。**

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10月09日09:00（北京时间）

**投标地点（网址）：**通过政采云平台（www.zcygov.cn）”实行在线投标响应（电子投标） 。

**开标时间：**2024年10月09日09:00

**开标地点（网址）：**台州市市府大道777号台州市公共资源交易中心3楼一号开标室。

**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起**（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）**7个工作日内，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）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）、《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）。

（2）电子招投标的说明：

①电子招投标：本项目以数据电文形式，依托“政府采购云平台（www.zcygov.cn）”进行招投标活动，不接受纸质投标文件；

②投标准备：注册账号--点击“商家入驻”，进行政府采购供应商资料填写；申领CA数字证书---申领流程详见“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”；安装“政采云电子交易客户端”----前往“浙江政府采购网-下载专区-电子交易客户端”进行下载并安装；

③采购文件的获取：使用账号登录或者使用CA登录政采云平台；进入“项目采购”应用，在获取采购文件菜单中选择项目，获取采购文件；

④投标文件的制作：在“政采云电子交易客户端”中完成“填写基本信息”、“导入投标文件”、“标书关联”、“标书检查”、“电子签名”、“生成电子标书”等操作；

⑤采购人、采购代理机构将依托政采云平台完成本项目的电子交易活动，平台不接受未按上述方式获取采购文件的供应商进行投标活动；

⑥对未按上述方式获取采购文件的供应商对该文件提出的质疑，采购人或采购代理机构将不予处理；

⑦不提供采购文件纸质版；

⑧投标文件的传输递交：投标人在投标截止时间前将加密的投标文件上传至政府采购云平台，并在投标截止时间前递交备份投标文件1份。备份投标文件的制作、递交详见采购文件第二部分“投标资料表”第9条；

⑨投标文件的解密：投标人按照平台提示和采购文件的规定在半小时内完成在线解密。通过“政府采购云平台”上传递交的投标文件无法按时解密，投标供应商递交了备份投标文件的，以备份投标文件为依据，否则视为投标文件撤回。通过“政府采购云平台”上传递交的投标文件已按时解密的，备份投标文件自动失效。投标人仅提交备份投标文件，没有在电子交易平台传输递交投标文件的，投标无效；

⑩具体操作指南：详见政采云平台“服务中心-帮助文档-项目采购-操作流程-电子招投标-政府采购项目电子交易管理操作指南-供应商”。

**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：台州学院

地址：浙江省台州市椒江区市府大道1139号

传真：/

项目联系人（询问）：梁老师

项目联系方式（询问）：0576-88660897

质疑联系人：吴老师

质疑联系方式：0576-88660896

2、采购代理机构信息

名称：中冠工程管理咨询有限公司

地址：浙江省台州市椒江区东海大道378号4楼

项目联系人（询问）：陈金泉、戴艳燕、王莎莎

项目联系方式（询问）：0576-81810227、18968407875

质疑联系人：唐虹波

质疑联系方式：0576-81810270

3、同级政府采购监督管理部门

名称：台州市财政局政府采购监管处

地址：浙江省台州市椒江区纬一路66号

传真：/

联系人：陈老师、李老师

监督投诉电话：0576-88206705 、88206731

**八、中标人如有融资需求，可使用以下服务**

**政采贷联系方式**

|  |  |  |  |
| --- | --- | --- | --- |
| **银行** | **贷款年利率** | **联系人** | **联系电话** |
| 中国工商银行 | 3.8%起 | 卢嘉诚 | 13867658508 |
| 中国农业银行 | 3.8%起 | 龚盛 | 15858682216 |
| 中国建设银行 | 3.8%起 | 梅晶晶 | 88525339、13736585303 |
| 中国银行 | 3.75%起 | 王海 | 13857677798 |
| 浦发银行台州分行 | 4.05%起 | 王渊 | 13616676319 |
| 浦发银行椒江分行 | 4.05%起 | 孙瑞华 | 13857688081 |
| 交通银行台州分行 | 3.75%起 | 周翔宇 | 13867697018 |
| 招商银行台州分行 | 4.32%起 | 王海玲 | 13566413827 |
| 浙商银行台州分行 | 5.01%起 | 章涉漪 | 81880185、13606681262 |
| 中信银行台州分行 | 4.15%起 | 陈金园 | 13586052161 |
| 华夏银行台州分行 | 4.5%起 | 邱明达 | 81871518、13736252233 |
| 泰隆银行开发区支行 | 5.6%起 | 梁宛莉 | 13306869100 |
| 民泰银行椒江支行 | 5.8%起 | 陈慧珠 | 13857699669 |
| 绍兴银行台州分行 | 5.1%起 | 郭庭斌 | 15958633119 |
| 温州银行台州分行 | 4.55%起 | 王晓波 | 15824005475 |
| 平安银行台州分行 | 6.53%起 | 李俊丽 | 15906861035 |
| 宁波银行台州分行 | 4.35%起 | 戴莉丽 | 13566627207 |
| 金华银行台州分行 | 4.05%起 | 金雪婷 | 81886670、15968661569 |
| 台州银行 | 5.6%起 | 洪婷 | 15858624999 |
| 邮储银行台州分行 | 3.85%起 | 董庆 | 81888982、18957683757 |

**合同履约保函联系方式**

|  |  |  |  |
| --- | --- | --- | --- |
| **保险公司名称** | **保费率** | **联系人** | **联系电话** |
| 中国人寿财产保险股份有限公司台州中心支公司 | 年费率1%，最低保费500元 | 徐凌 | 13905168070 |
| 永诚财产保险股份有限公司台州分公司 | 年费率1%，最低保费1000元 | 尹刚强 | 13750668184 |
| 华泰财产保险有限公司台州中心支公司 | 年费率0.5%，最低保费1000元 | 王灵芳 | 88869818、13586123199 |
| 中国大地财产保险股份有限公司台州中心支公司 | 年费率1.5%，最低保费1000元 | 徐小明 | 88552788、13968603112 |
| 阳光保险台州中心支公司 | 年费率1%，最低保费500元 | 林高明 | 15888682693 |
| 中华联合财产保险股份有限公司台州中心支公司 | 年费率2%，最低保费500元 | 王仙高 | 13858600221 |
| 中国人民财产保险股份有限公司台州中心支公司 | 年费率0.3%，最低保费1000元 | 王仙春 | 13515769179 |
| 永安财产保险股份有限公司台州中心支公司 | 年费率0.3%，最低保费1000 | 王春宇 | 13676675331 |

**预付款保函联系方式**

|  |  |  |  |
| --- | --- | --- | --- |
| 保险公司名称 | 保费率 | 联系人 | 联系电话 |
| 中国人寿财产保险股份有限公司台州中心支公司 | 年费率3%，最低保费500元 | 徐凌 | 13905168070 |
| 阳光保险台州中心支公司 | 年费率1%，最低保费500元 | 林高明 | 15888682693 |
| 天安财产保险股份有限公司台州中心支公司 | 年费率1%-2%，最低保费500元 | 罗赛 | 13736605643 |

**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。**

**第二部分** **投标资料表**

| **序号** | **内 容** | |
| --- | --- | --- |
| **1** | 采购人：台州学院  联系人：梁老师；联系电话：0576-88660897  地址：浙江省台州市椒江区市府大道1139号 | |
| 采购代理机构：中冠工程管理咨询有限公司  联系人：陈金泉、戴艳燕、王莎莎  电话：0576-81810227、18968407875  地址：浙江省台州市椒江区东海大道378号4楼 | |
| **2** | 经批准的本次采购人式：公开招标 | |
| **3** | 投标人的资格要求：详见“第一部分 采购公告”。 | |
| **4** | 资格审查：本项目采用资格后审。 | |
| **▲5** | 商务条款资料部分：见“第五部分 采购内容及要求” | |
| **▲6** | 投标报价：  **1、最高限价：279.52万元。报价超过最高限价的，其投标将作无效投标处理。**  2、投标报价应是采购文件所确定的采购内容及要求内全部工作内容的价格表现。其应包含实现标书的所有功能，采购人不再另外增加费用，其应包括（但不限于）所有软硬件货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用。  3、不论中标结果如何，投标人均应自行承担所有与投标有关的全部费用。 | |
| **▲7** | 投标有效期：开标之日起90日历天。 | |
| **8** | 投标文件的制作和投标：  请投标供应商在投标前仔细阅读“政府采购项目电子交易操作指南”。  1、投标文件的制作：投标供应商按照本项目采购文件和政采云平台的要求,通过“政采云电子交易客户端”编制、加密并递交投标文件（下载网址：https://zfcg.czt.zj.gov.cn/download/index.html）。  2、投标：投标供应商应当在投标截止时间前完成投标文件的传输递交，逾期上传的投标文件恕不接受。补充或者修改投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成上传的，视为撤回投标文件。  3、投标文件解密：投标供应商应在开标后30分钟内完成解密。  4、中标供应商中标后需提供纸质投标文件给采购人作为备案存档，纸质投标文件系电子投标文件纸质版，两者内容应一致；数量为：资格证明文件2份；资格及商务技术文件2份；报价文件2份。 | |
| **9** | 投标文件组成与份数：  1、上传到政府采购云平台的电子加密投标文件（含资格证明文件、技术商务文件、报价文件）1份。  2、电子备份投标文件（含资格证明文件、技术商务文件、报价文件）1份。备份投标文件是通过政采云电子交易客户端制作投标文件产生的备份文件，请投标供应商自行妥善保管。  （1）使用前提：投标供应商自行在线解密操作失败无法按时寻求技术人员帮助解密，或者投标供应商寻求技术人员帮助仍无法按时完成解密。  （2）递交截止时间：同投标截止时间。  （3）投递邮箱：**[zgtzfgs@163.com](mailto:zgtzfgs@163.com)。**  （4）备份投标文件由供应商自行确定是否提交，因备份投标文件未加密而造成失密等情况，采购代理机构概不负责。未在系统上提交投标文件而仅提交备份投标文件的，其投标无效。 | |
| **10** | 采购公告与中标公告发布网站：浙江政府采购网（www.zcygov.cn）。 | |
| **11** | 信用信息查询渠道：信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）。 | |
| **12** | 1、踏勘现场时间及地点：不组织，各投标单位根据自己需要，自行前往勘察现场和周围环境，所产生的费用由投标单位自理。  2、节能产品、环保产品：无要求；  3、样品：无  **4、视频演示：**A不组织。  组织：（1）本项目评分标准中的视频演示，供应商通过政采云“视频评审”系统进行远程在线演示，每次只邀请一家供应商进入评审室，供应商演示完成后应自动退出评审室。供应商自行准备演示的设备并提前测试耳麦、麦克风是否正常运行。   1. 视频演示备份文件：供应商可于提交投标文件截止时间前将视频演示备份文件以介质（U盘）存储的形式密封，采用现场递交或邮寄送达方式递交。   **方式一：现场递交方式**，供应商可安排授权代表在投标截止时间前将视频演示备份文件送至开标地点：台州市公共资源交易中心三楼开标大厅。视频演示备份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：台州市椒江区东海大道378号4楼，联系方式：陈金泉、王莎莎，18968407875。供应商邮寄后可将邮件单号发送至中冠工程管理咨询有限公司电子邮箱（电子邮箱：zgtzfgs@163.com），以便查询物流记录。各供应商应当确保视频演示备份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、项目编号，因邮寄造成视频演示备份文件密封破损而不符合采购文件对视频演示备份文件的密封要求、或邮寄过程中导致视频演示备份文件未能在投标截止时间前送达的，代理机构将拒绝其视频演示备份文件。各供应商自行考虑邮寄在途时间，视频演示备份文件送达时间以代理机构工作人员实际签收时间为准。 逾期送达的或者未送达指定地点的，代理机构不予受理。  **（3）视频演示备份文件不强制要求提交，但供应商远程在线演示时因自身设备原因无法演示又未递交视频演示备份文件的，视为供应商未提供视频演示。** | |
| **13** | 进口产品 | 🗹本项目不允许采购进口产品。  🞎可以采购进口产品**，**优先采购向我国企业转让技术、与我国企业签订消化吸收再创新方案的供应商的进口产品；但如果因信息不对称等原因，仍有满足需求的国内产品要求参与采购竞争的，采购人及其委托的采购代理机构不对其加以限制，将按照公平竞争原则实施采购。 |
| **14** | 项目属性与核心产品 | 🗹A货物类，核心产品为： 网络安全竞技系统 。  🞎B服务类。 |
| **15** | 采购标的对应的中小企业划分标准所属行业 | 1. 标的：虚拟化防火墙，属于软件和信息技术服务业行业； 2. 标的：虚拟化上网行为管理，属于软件和信息技术服务业行业； 3. 标的：虚拟化WEB应用防火墙 ，属于软件和信息技术服务业行业； 4. 标的：虚拟化入侵防御系统，属于软件和信息技术服务业行业； 5. 标的：虚拟化漏洞扫描与防护，属于软件和信息技术服务业行业； 6. 标的：CTF竞赛解题实战课程资源包，属于软件和信息技术服务业行业； 7. 标的：网络安全攻防技术实战课程资源包，属于软件和信息技术服务业行业； 8. 标的：企业网及服务建设课程，属于软件和信息技术服务业行业； 9. 标的：WEB安全综合实战课程资源包，属于软件和信息技术服务业行业； 10. 标的：Linux操作系统安全课程资源包，属于软件和信息技术服务业行业； 11. 标的：入侵检测基础课程资源包，属于软件和信息技术服务业行业； 12. 标的：网络安全技术基础课程资源包，属于软件和信息技术服务业行业； 13. 标的：网络安全应急响应课程资源包，属于软件和信息技术服务业行业； 14. 标的：逆向工程技术实战课程资源包，属于软件和信息技术服务业行业； 15. 标的：企业网渗透测试课程，属于软件和信息技术服务业行业； 16. 标的：密码学算法编程课程资源包，属于软件和信息技术服务业行业； 17. 标的：网络安全竞技系统（提供账号、队伍、角色权限管理，并提供系统配置、审计日志、系统版本管理。系统提供竞赛创建、竞赛中管理、竞赛结果导出、题库管理、工具管理、竞赛展屏。可支撑个人赛、团体赛2种参赛方式；理论赛、解题赛、攻防赛3种竞赛形式，并配有1000道选择类题目。150道解题赛题目(题库包含CRYPTO、MISC、WEB、PWN、Revers方向)，20道攻防赛题目，并配有解题思路。   可支撑用户自主刷题，查看解题思路，并统计训练人次、通过率、训练题目分类、题目占比等数据），属于软件和信息技术服务业行业；   1. 标的：边界防火墙认证模块，属于工业行业； 2. 标的：上网行为管理认证模块 ，属于工业行业； 3. 标的：IPS认证模块，属于工业行业； 4. 标的：WAF认证模块，属于工业行业； 5. 标的：日志审计系统认证模块，属于工业行业； 6. 标的：数据库审计系统认证模块，属于工业行业； 7. 标的：堡垒机认证模块，属于工业行业； 8. 标的：态势感知认证模块 ，属于工业行业； 9. 标的：网络准入控制认证模块，属于工业行业； 10. 标的：核心交换机，属于工业行业； 11. 标的：聚会交换机，属于工业行业； 12. 标的：网络机柜，属于工业行业。 |
| **16** | 履约保证金：本项目不收取履约保证金。 | |
| **17** | 代理服务费：  1、代理费金额：本项目招标代理费用参照下表中货物类计算标准乘以39.8%计算（差额定率累进法），按照中标通知书确定的中标金额，向成交供应商收取招标代理服务费。   |  |  |  |  | | --- | --- | --- | --- | | 服务类型  费率  中标金额（万元） | 货物招标 | 服务招标 | 工程招标 | | 100以下 | 1.5% | 1.5% | 1.0% | | 100-500 | 1.1% | 0.8% | 0.7% |   2、中标人应在接到代理机构通知之日起5个工作日之内向采购代理机构支付代理服务费。  3、收费账号：  开户银行：中国农业银行股份有限公司台州经济开发区支行  户名：中冠工程管理咨询有限公司台州分公司  账号：19900101040031566 | |
| **18** | 带“▲”的条款是实质性条款。 | |
| **19** | 本采购文件解释权属于采购人和采购代理机构。 | |

**第三部分 投标须知**

**一 、总 则**

**1、适用范围**

适用于本次项目的招标采购、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

**2、定义**

2.1、“采购代理机构”指组织本次招标采购的中冠工程管理咨询有限公司。

2.2、采购人：是指委托集中采购机构/采购代理机构采购本次项目的国家机关、事业单位和团体组织。

2.3、投标人：是指向采购代理机构提交投标文件的单位或个人，应该是符合《投标资料表》的报名条件，符合、承认并承诺履行本采购文件各项要求的具有独立法人资格的中国境内企业或组织。

2.4、货物：是指各种形态和种类的物品，包括原材料、燃料、设备、产品等。

2.5、服务：是指除货物和工程以外的政府采购对象，包括各类专业服务、信息网络开发服务、金融保险服务、运输服务，以及维修与维护服务等。

2.6、“书面形式”包括信函、传真等。

2.7、“▲”系指实质性要求条款。

**3、投标费用**

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用（有相关规定除外）。

**4、特别说明**

4.1、投标人在投标活动中提供任何虚假材料,其投标无效，并报监管部门查处；中标后发现的,根据《中华人民共和国政府采购法》第七十七条第一款第一项之规定，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任。

4.2、投标人被列入“黑名单”的，采购组织单位将根据《浙江省政府采购供应商注册及诚信管理暂行办法》第四十六条之规定，在处罚有效，资格审查时不予通过。

4.3、投标人不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害采购人或其他投标人的合法权益，投标人不得以向采购人、评标委员会成员行贿或者采取其他不正当手段谋取中标。

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

4.5、投标文件格式中的表格式样可以根据项目差别做适当调整,但应当保持表格样式基本形态不变。

4.6、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。

4.7、本项目不允许分包。

4.8、本采购文件中关于电子招投标内容、流程如与政采云系统中最新的内容、操作不一致的，以政采云系统中的要求为准。

**5、 质疑与投诉**

5.1、投标人认为、采购过程和中标、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七个工作日内，以书面形式向采购人、采购代理机构提出质疑**（注：投标人须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）**。潜在投标人的书面质疑或澄清要求均应加盖单位公章，署明日期。投标人未按规定要求提出的，则视同认可，但法律法规及规范性文件有明确规定的除外。供应商对采购代理机构的质疑答复不满意或者采购机构未在规定时间内作出答复的，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。

5.2、对于受理的质疑，采购代理机构将以书面形式或其他适当方式进行答疑，必要时将书面答复发送所有取得本项目采购文件的投标人。若采购代理机构所作的答疑不引起相应条款的实质性改变，则不应视作对采购文件的修正或更正。

5.3、采购代理机构发送的答疑文件是采购文件的组成部分，对投标人具有约束力。

5.4、未尽事宜，见《政府采购质疑和投诉办法》（中华人民共和国财政部令第94号）。

**二、采购文件**

**6、采购文件构成**

6.1、采购文件包括目录所示内容及采购文件的澄清或修改。

6.2、除上述所列内容外，采购人和采购代理机构的任何工作人员对投标人所作的任何口头解释、介绍、答复，只能供投标人参考，对采购人、采购代理机构和投标人无任何约束力。

6.3、采购文件是招标过程进行的有效依据，也是成交后签订合同的依据，对双方均具有约束力，凡不遵守采购文件规定或对采购文件的实质性内容不响应的，将可能被拒绝或以无效标处理。

6.4、本采购文件由采购人或采购代理机构依据相关法律、法规、规章、省市规定及采购文件进行解释。

**7、采购文件的澄清或修改**

7.1采购人或者采购代理机构可以对已发出的采购文件进行必要的澄清或者修改，但不得改变采购标的和资格条件。澄清或者修改应当在原公告发布媒体上发布澄清公告。澄清或者修改的内容为采购文件的组成部分。

澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构应当在投标截止时间至少15日前，以书面形式通知所有获取采购文件的潜在投标人；不足15日的，采购人或者采购代理机构应当顺延提交投标文件的截止时间。

7.2采购代理机构必须以书面形式答复投标人要求澄清的问题，并将不包含问题来源的答复书面通知所有获取采购文件的投标人；除书面答复以外的其他澄清方式及澄清内容均无效。

7.3采购文件澄清、答复、修改、补充的内容为采购文件的组成部分。当采购文件与采购文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

7.4采购文件的澄清、答复、修改或补充都应该通过本代理机构以法定形式发布，采购人非通过本机构，不得擅自澄清、答复、修改或补充采购文件。

**8、关于分公司投标**

除金融、保险、通讯等特定行业外，法人的分支机构由于不能独立承担民事责任，不能以分支机构的身份参加政府采购，只能法人身份参加。

**9、关于知识产权**

9.1供应商必须保证，采购人在中华人民共和国境内使用投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向采购人提出侵犯其专利权、商标权或其它知识产权的主张，该责任应由供应商承担。

9.2投标报价应包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。

9.3系统软件、通用软件必须是具有在中国境内的合法使用权或版权的正版软件，涉及到第三方提出侵权或知识产权的起诉及支付版税等费用由供应商承担所有责任及费用。

**三、投标文件**

**投标人应认真阅读采购文件中所有的事项、格式、条款和技术要求等。如果投标人没有按照采购文件要求和规定编制投标文件及提交全部资料，或者投标人没有对采购文件中各方面作出实质性响应，其风险应由投标人自行承担。**

**10、投标文件的组成**

投标人接到后，按照采购代理机构的要求提供：资格证明文件、商务与技术文件和报价文件。

【特别提示：如有要求提供各项证书、合同、报告等证明的，请将原件清晰扫描做入投标文件。】

**▲10.1、资格证明文件的组成：**

（1）符合参加政府采购活动应当具备的一般条件的承诺函（格式见附件)；

（2）法人或者其他组织的营业执照等证明文件，自然人的身份证明；

（3）本项目的特定资格要求（如果有，提供采购公告中符合供应商特定条件的有效资质证书扫描件)，以及供应商认为有必要提供的其他资格证明资料。

注：采购人或采购代理机构在资格审查时，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询供应商在投标截止日之前的信用记录并保存。投标人若被列入失信被执行人或重大税收违法失信主体或政府采购严重违法失信行为记录名单的，则否决其投标。若开标当天因不可抗力事件导致无法查询且一时无法恢复的，可在中标通知书发出前对中标人进行查询，如中标人被列入失信被执行人或重大税收违法失信主体或政府采购严重违法失信行为记录名单的，则取消中标资格。

**10.2、商务与技术文件的组成：**

（1）商务技术自评表(格式见附件)；

（2）投标函（格式见附件）；

（3）授权委托书或法定代表人（单位负责人、自然人本人）身份证明（格式见附件）；

（4）供应商基本情况表（格式见附件）；

（5）供货清单（格式见附件）；

（6）技术规范偏离表（格式见附件）；

（7）商务偏离表（格式见附件）；

（8）相关项目实施业绩一览表（格式见附件件）；

（9）供货方案；

（10）评分标准或采购文件需要提供的其他技术商务材料；

（11）供应商认为有必要提供的其他技术商务文件资料。

**10.3、报价文件的组成**

（1）开标一览表（格式见附件）；

（2）报价明细表（格式见附件）；

（3）中小企业声明函**（如有，可提供，格式见附件）**；

（4）投标人认为需提交的其他报价文件资料。

**11、投标文件的制作、封装及递交要求**

**11.1、投标文件的制作要求**

投标人应按照投标文件组成内容及项目采购需求和浙江政府采购云平台要求制作投标文件，不按投标文件组成内容及项目采购需求和浙江政府采购云平台要求制作投标文件的将视情处理（拒收、扣分等），由此产生的责任由投标人自行承担。

**电子投标文件部分：投标人应根据“政采云供应商项目采购-电子招投标操作指南”及本规定的格式和顺序编制电子投标文件并进行关联定位。**

备份电子投标文件：通过“政采云”平台电子投标工具制作投标文件所产生的备份文件

（2）投标人应对所提供的全部资料的真实性、有效性承担法律责任，电子投标文件中所须加盖公章部分均采用CA签章。

（3）投标文件以及投标人与采购代理机构就有关投标事宜的所有来往函电，均应以中文汉语书写。除签字、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的投标文件视同未提供。

（4）投标计量单位，已有明确规定的，使用规定的计量单位；没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元）。

（5）若投标人不按的要求提供资格审查材料，其风险由投标人自行承担。

（6）与本次投标无关的内容请不要制作在内，确保投标文件有针对性、简洁明了。

**11.2、投标文件的编制、递交要求**

（1）投标人须按照采购文件和政采云平台的要求编制并加密投标文件。在投标文件递交截止时间以前完成投标文件的传输递交。

（2）备份电子投标文件必须在规定时间前发送至指定邮箱。备份电子投标文件在截止时间后提交，采购代理机构将拒绝接收。

（3）如有特殊情况，采购代理机构延长截止时间和开标时间，采购代理机构和投标人的权利和义务将受到新的截止时间和开标时间的约束。

**11.3、投标文件的补充、修改和撤回**

补充或者修改投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。

**11.4投标文件的有效期**

（1）自投标截止日起90天投标文件应保持有效。有效期不足的投标文件将被拒绝。

（2）在特殊情况下，采购人可与投标人协商延长投标文件的有效期，这种要求和答复均以书面形式进行。

（3）中标人的投标文件自开标之日起至合同履行完毕均应保持有效。

**四、开标**

**12、开标事项**

12.1、采购代理机构在“采购公告”规定的时间和地点公开开标。

12.2、评标期间，投标供应商代表应在线操作，并关注政采云有关信息公布、澄清等情况。投标供应商的法定代表人或其授权代表未按时签到登记的，视同放弃开标监督权利、认可开标结果。

**13、 开标程序：**

13.1、开标时间到后，采购代理机构项目负责人准时组织开标。

13.2、投标人登录政采云平台，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30分钟内。**投标文件解密结束，投标供应商通过电子邮件形式将经授权代表签署的《政府采购活动现场确认声明书》（格式见最后一页内容）的扫描件或（图片）发至采购代理机构邮箱：zgtzfgs@163.com。开评标活动结束之前投标供应商拒不发送《政府采购活动现场确认声明书》的，由此产生的一切风险责任由供应商自行承担。**

13.3、开启《报价响应文件》后并在线公布开标一览表有关内容，投标供应商应在线签字确认（不予确认的应说明理由，否则视为无异议）。

13.4、公布开标结果。

13.5、特别说明：本项目原则上采用政采云电子招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）若投标人在规定时间内无法解密或解密失败，采购代理机构将开启该投标人递交的备份电子投标文件，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）**开评标细则按政采云电子评标流程进行。特别说明：政采云公司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。**

（3）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：

①电子交易平台发生故障而无法登录访问的；

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；

③电子交易平台发现严重安全漏洞，有潜在泄密危险的；

④病毒发作导致不能进行正常操作的；

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，也可以决定某些环节以纸质形式进行。

（4）未开启的备份投标文件现场不予以退还。

**五、评标和定标**

**14、评标委员会**

14.1受采购人的委托，采购代理机构根据《中华人民共和国政府采购法》、财政部第87号令的规定和有关的法律法规组建评标委员会，评标委员会负责评标工作。评标委员会由采购人代表和评审专家组成。评审专家将在开标日之前在管理部门的评审专家库中随机抽取。评标委员会成员名单在评标结果公告前应当保密。

14.2评标委员会将遵循公平、公正、科学、廉洁的原则和规定的程序进行评标，并且只依据投标文件本身对采购文件的响应情况进行评审，不考虑投标人在开标后提交的任何的补充声明、修正方案。

14.3评委依法独立评审，并对评审意见承担个人责任。对明显畸高、畸低的评分（其个人主观打分偏离所有评审小组成员主观评分平均分30%以上的），评标委员会主任委员提醒相关评审人员进行复核或书面说明理由。评委对需要共同认定的事项存在争议的，按照少数服从多数的原则做出结论。持不同意见的评委应当在评审报告上签署不同意见并说明理由，否则视为同意。

14.4评标委员会将核对投标价格和服务内容，对发现的价格计算错误按下述原则处理：

（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）投标文件的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，以单价金额计算结果为准。

**（5）客户端填写的报价与以pdf格式上传文件中的报价不一致的，应以pdf格式上传文件中的报价为准。**

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

14.5评标委员会根据采购文件的《评标办法》及在《投标资料表》和《采购内容及要求》中所列的具体标准，对投标文件进行评审和比较。

**15、****澄清问题的形式**

15.1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，可以要求投标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。投标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。

15.2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。投标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）投标供应商在“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）

（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：投标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”。

15.3投标供应商未在截止时间前完成澄清，将被视作自动放弃。

**16、评标办法**

16.1本项目采用综合评分法。本次招标采购采用的评标方法具体说明载明在采购文件“评标办法”部分中。

16.2综合评分法：

投标文件满足采购文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

**17、评标程序和原则**

17.1评标程序：遵循初步审查、澄清有关问题、比较与评价、推荐中标候选人的程序依次进行。

17.2初步审查：包含资格性审查和符合性审查。初步审查不合格者不进入澄清有关问题及后续的评标程序。

（1）资格性审查：

依据法律法规和采购文件的规定，采购人或采购代理机构对其资格证明文件齐全性和有效性等方面进行审查，以确定投标人是否具备投标资格。

（2）符合性检查：

依据采购文件的规定，评标委员会从投标文件的有效性、完整性和对采购文件的响应程度进行审查，以确定是否对采购文件的要求作出实质性响应。

17.3澄清有关问题：按第15条规定进行。

17.4比较与评价：

（1）技术商务评价：按照采购文件的要求和《评标标准》对照投标文件的响应进行技术商务评价，评定其偏差程度，并计算其相应的技术商务评分分值。

（2）综合评价：对经过技术商务评价的投标，按《评标标准》规定的评价办法进行综合评价，并按以下原则进行评审计算：

综合评分法的最终得分计算：综合得分=报价得分+技术商务评审得分

综合评价结束，按照上述第16条规定，列出进入最终评审各投标人排序次序。

17.5推荐中标候选人：按18条规定推荐中标候选人。

**18、推荐中标候选人**

**评标委员会根据各投标人的综合得分由高到低排定顺序，推荐本项目的中标候选人，推荐两名中标候选人。**

**19、采购人式转换**

公开招标数额标准以上的采购项目，投标截止后投标人不足3家或者通过资格审查或符合性审查的投标人不足3家的，除采购任务取消情形外，按照以下方式处理：

19.1采购文件存在不合理条款或者招标程序不符合规定的，采购人、采购代理机构改正后依法重新招标；

19.2采购文件没有不合理条款、招标程序符合规定，需要采用其他采购人式采购的，采购人依法报财政部门批准。

**20、评标过程的监控与保密**

20.1本项目评标过程实行全程录音、录像监控，投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

20.2开标后到中标通知书发出之前，所有涉及评标委员会名单以及对投标文件的澄清、评价、比较等情况，评标委员会成员、采购人和采购代理机构的有关人员均不得向投标人或其他无关人员透露。

**21、确定中标人、评标结果公示与质疑**

21.1采购代理机构在评标结束后2个工作日内将评标报告交采购人确认，采购人在收到评标报告之日起5个工作日内在评标报告确定的中标候选人中按顺序确定中标人，采购人在收到评标报告之日起5个工作日内未按评标报告推荐的中标候选人排序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

21.2代理机构自中标人确定之日起2个工作日内，在发布采购公告的网站上对中标结果进行公示，中标结果公告期限为1个工作日。如果中标人自动放弃中标资格或因质疑或是投诉被取消中标资格的，可视情况报经财政部门同意后，按本次评标供应商得分排序结果依次替补或重新组织。

21.3投标人若对评标结果有异议，可在中标公告期限届满之日起七个工作日内向采购人提出书面质疑，质疑书应该有质疑人名称、地址、公章、法定代表人签名盖章、联系人姓名、联系电话、传真以及被质疑人名称及联系方式，被质疑采购项目名称、编号及采购内容，具体的质疑事项及事实依据，认为自己合法权益受到损害或可能受到损害的相关证据材料，提出质疑的日期，否则视为无效质疑。本采购代理机构将受采购人委托在收到质疑文件之日起7个工作日内书面答复。不受理无效的任何质疑。

**六、无效投标认定**

**22、实质上没有响应采购文件要求的投标将被视为无效投标。**

22.1在资格审查时，不具备采购文件中规定的资格要求的，或者资格证明文件不全的，投标文件将被视为无效。

22.2在符合性审查时，如发现下列情形之一的，投标文件将被视为无效：

（1）投标文件未按采购文件要求签署、签章的；

（2）投标有效期不满足采购文件要求的；

（3）明显不符合采购文件要求的，或者与采购文件中标注“▲”的条款发生实质性偏离的；

（4）投标文件中含有采购人不能接受的附加条件的；

（5）投标声明书无法定代表人签名，或委托人未提供法定代表人授权委托书、填写项目不齐全的；

（6）投标文件格式不规范、提供资料不齐全或者内容虚假的；

（7）投标文件的实质性内容未使用中文表述、表述不明确、前后矛盾或者使用计量单位不符合采购文要求的（经评标委员会认定并允许其更正的笔误除外）；

（8）投标文件的关键内容字迹模糊、无法辨认的，或者投标文件中经修正的内容字迹模糊难以辨认或者修改处未按规定签署、盖章的；

（9）法律、法规和采购文件规定的其他无效情形。

22.3在技术商务评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）未提供或未如实提供投标货物的技术参数，或者投标文件标明的响应或偏离与事实不符或虚假投标的；

（2）明显不符合采购文件要求的规格型号、质量标准；

（3）投标技术方案不明确，存在一个或一个以上备选（替代）投标方案的。

22.4在报价评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）报价超过采购文件中规定的预算金额或者最高限价的；

（2）未采用采购文件要求的报价形式报价的；

（3）投标报价具有选择性的；

（4）投标人的报价明显低于其他通过符合性审查供应商的报价，评标委员会认为有可能影响产品质量或者不能诚信履约要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料，投标人不能证明其报价合理性的；

（5）采购文件规定的其他无效情形。

22.5被拒绝的投标文件为无效。

**七、合同签订及其他**

**23、签订合同**

23.1中标人在本采购代理机构发出中标通知书的30日内，应与采购人按照采购文件和中标人的投标文件的约定内容签订书面合同。中标人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人，也可以重新开展政府采购活动。同时，拒绝与采购人签订合同的供应商，由同级财政部门依法作出处理。

23.2采购文件、中标人的投标文件及在评标过程中提交的澄清文件均应作为合同附件。

23.3采购人应当自政府采购合同签订之日起2个工作日内，在省级以上财政部门指定的政府采购信息发布媒体及相关网站上公告。

**24、履约保证金（如有）**

24.1签订合同后，中标人应根据采购文件确定的履约保证金的金额交纳履约保证金。

24.2签订合同后，如中标人不按双方合同约定履约，则没收其全部履约保证金，履约保证金不足以赔偿损失的，按实际损失赔偿。

24.3采购人负责对中标人的履约行为进行验收，验收标准为本项目的采购文件以及中标人的投标文件，要求验收必须符合相关政策法规和地方标准。

**八、履约验收**

25、采购人负责对中标供应商的履约行为进行验收。政府向社会公众提供的公共服务项目，验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告。

**九、代理服务费**

**26、代理服务费**

中标人应向本采购代理机构支付代理服务费。代理服务费的收费依据及相关规定载明在采购文件《投标资料表》中。

**十、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）**

**27、**本项目非专门面向中小企业采购。

**28、本项目对应的中小企业划型标准所属行业：详见第二部分 投标资料表。**

29、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。

国务院批准的中小企业划分标准：具体见工信部联企业[2011]300号。

30、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，可享受小型、微型企业（以下简称小微企业）的价格扣除：

（1）在货物采购项目中，货物由小微企业制造，即货物由小微企业生产且使用该小微企业商号或者注册商标；

（2）在工程采购项目中，工程由小微企业承建，即工程施工单位为小微企业；

（3）在服务采购项目中，服务由小微企业承接，即提供服务的人员为小微企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

31、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，不享受的小微企业价格扣除。

32、根据《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》（财库〔2014〕68号）规定，监狱企业视同小型、微型企业。监狱企业参加政府采购活动时，应当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。

33、根据《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，在政府采购活动中，残疾人福利性单位视同小型、微型企业。残疾人福利性单位参加政府采购活动时，提供《残疾人福利性单位声明函》。

34、按规定享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

35、供应商按照《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46号）规定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。

**[第四部分 评标办法及评分标准](file:///F:\\微信\\WeChat%20Files\\a29023143\\FileStorage\\File\\2021-11\\台州市公安局特警支队最小作战单元装备建设采购项目10.28.docx" \l "●评分标准)**

一、采购组织机构将组织评标委员会，对投标人提供的投标文件进行综合评审。

二、本次招标项目的评标方法为综合评分法，总计100分，其中资格及商务技术文件分值70分，投标报价分值30分。评标标准按评分细化条款及分值进行评审。

（一）商务技术文件中的评分项由评标委员会在规定的分值内单独评定打分（小数点后保留1位）。

（二）各投标人资格及商务技术文件得分按照评标委员会成员的独立评分结果汇总后的算术平均分计算（小数点后保留2位），计算公式为：

资格及商务技术文件得分=评标委员会所有成员评分合计数/评标委员会组成人员数。

（三）投标报价得分采用低价优先法计算（小数点后保留2位），即满足采购文件要求且投标价格最低的投标报价为评标基准价，其报价得满分。其他投标人的投标报价得分按下列公式计算：

投标报价得分=(评标基准价／投标报价)×30%×100 。

（四）投标人综合得分＝资格及商务技术文件得分＋投标报价得分。

（五）政府采购政策及优惠：

（1）根据财政部、工业和信息化部发布的《政府采购促进中小企业发展管理办法》【财库（2020）46号】和《财政部关于进一步加大政府采购支持中小企业力度的通知》【财库（2022）19号】有关规定，货物和服务项目中未预留份额专门面向中小企业采购的，以及预留份额项目中的非预留部分采购包，采购单位、采购代理机构应当对符合规定的小微企业报价给予10%的扣除，用扣除后的价格参加评审。

接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合体协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，采购单位、采购代理机构应当对联合体或者大中型企业的报价给予6%的扣除，用扣除后的价格参加评审。

组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

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。

投标文件中须同时出具《政府采购促进中小企业发展管理办法》【财库（2020）46号】规定的《中小企业声明函》，否则不得享受价格扣除。

**本项目对符合规定的小微企业（含小型企业）报价给予10%的扣除。**

（2）根据《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）的规定，供应商如为监狱企业且所投产品为小型或微型企业生产的，其投标报价扣除10%后参与评审。

投标文件中须同时提供：供应商的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，未提供完整证明材料的，投标报价不予扣减。

（3）残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》（见附件），并对声明的真实性负责。

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：

①安置的残疾人占本单位在职职工人数的比例不低于25%（含25%），并且安置的残疾人人数不少于10人（含10人）；

②依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

③为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

④通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

⑤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。

注：得分以系统计算为准，保留2位小数。

三、在最大限度地满足采购文件实质性要求前提下，评标委员会按照采购文件中规定的各项因素进行综合评审后，推荐两名合格的中标候选人，并按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

四、如综合得分相同，投标报价低者为先；如综合得分且投标报价相同的，货物类采购项目以技术性能得分较高者为先，服务类采购项目以实力信誉及业绩得分较高者为先。

五、核心产品提供相同品牌产品的不同投标人参加同一合同项下投标的，按一家供应商认定：（1）采用最低评标价法的采购项目，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由评标委员会集体确定一个投标人参加评标，其他投标无效。（2）使用综合评分法的采购项目，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由评标委员会集体推荐一个投标人作为中标候选人，其他同品牌投标人不作为中标候选人。

六、本次评分具体分值细化条款如下表：

**评分标准**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评分项目** | **评分细则** | **分值** |
| **1** | **技术指标（23分）** | 专家结合投标产品各项技术参数与招标文件要求的偏离情况综合打分，每1条带★号的技术参数不满足招标需求的扣2分，每1条一般参数不满足招标需求的扣1分，扣完为止。**注：如采购文件技术需求参数中注明需提供承诺书或功能截图或检测报告或其它相关证明材料的，未提供将视为负偏离。** | 23分 |
| **2** | **项目分析**  **（3分）** | 根据投标人对现状分析、项目需求、项目背景、项目目标的理解程度进行打分：   1. 分析透彻、理解充分深入、合理的得2.1-3分； 2. 分析基本透彻、理解基本充分、合理的得1.1-2分； 3. 分析不够透彻、理解不合理的得0.1-1分 4. 未提供不得分。 | 3分 |
| **3** | **技术方案的完整性和科学性**  **（3分）** | 根据投标人提供的方案内容的全面完整程度及科学性、针对性、可操作性进行综合打分：   1. 内容完整、功能性强、科学合理的得2.1-3分， 2. 内容相对完整、功能性一般、基本科学合理的得1.1-2分， 3. 内容欠缺、功能性较差、不够科学合理的0.1-1分； 4. 未提供不得分。 | 3分 |
| **4** | **演示要求**  **（16分）** | 为保障课程的真实性及所采购资源的版权合法性，以及网络安全竞技平台的功能的真实性，投标时需提供课程资源及网络安全攻防竞技平台的录屏演示，演示时间控制在20分钟内，只提供PPT、图片演示不得分。  1、企业网及服务建设实训课程演示：以项目式的工作流程进行教学，包含①实验手册、②实验拓扑、③实验拓扑不少于18个网络节点、④可在线一键开启拓扑环境。以上4项功能每满足一项得1分，最高得4分；  2、企业网渗透测试实训课程演示：以项目式的工作流程进行教学，包含①实验手册、②实验拓扑、③实验拓扑不少于18个网络节点、④可在线一键开启拓扑环境。以上4项功能每满足一项得1分，最高得4分；  3、攻防竞技竞赛管理中心功能演示：  （1）平台支持①准备模式、②全通模式、③解题模式、④解题+加固模式、⑤加固模式、⑥攻防模式的网络控制；以上6项功能每满足一项得0.5分，最高得3分。  （2）各模式之间一键配置，分别对平台、题目进行访问控制、环境隔离控制。该项功能完全满足得1分，否则不得分；  4、攻防竞技竞赛管理中心功能演示：平台支持①网络控制、②动态flag、③随机附件随机flag、④虚拟机动态密码、⑤服务检测、⑥Writeup、⑦终端IP段验证、⑧提交间隔时间限制等多种防作弊手段。以上8项功能每满足一项得0.5分，最高得4分。 | 16分 |
| **5** | **技术支撑能力**  **（6分）** | 1.本次项目平台交付质量要求较高，要求网络安全竞技系统生产厂商具备CIC信息化建设及数字化能力评价证书、ISO27701隐私信息管理体系认证证书，以及ISO28000供应链安全管理体系认证证书，提供一项证书得1分，最高得3分。**须提供证书的扫描件并加盖投标人公章，编入投标文件中，否则不得分。**  2.为更好传授漏洞挖掘相关实战经验，培养学生的漏洞挖掘实战能力，要求网络安全竞技系统生产厂商具备较强的漏洞挖掘能力：在2023年向国家信息安全漏洞共享平台提供漏洞个数超过10000个，得0.5分，超过20000个得1分，超过30000个 得1.5分，不满足不得分；在2022年向国家信息安全漏洞共享平台提供漏洞个数超过10000个，得0.5分，超过20000个得1分，超过30000个 得1.5分，不满足不得分；本项最高得3分。**须提供相关证明材料并加盖投标人公章，编入投标文件中，否则不得分。** | 6分 |
| **6** | **同类产品 销售业绩（2分）** | 投标人自2021年7月1日以来（以合同签订日期为准）具有同类项目业绩的，每提供一份有效证明材料得1分，最高得2分。  注：需提供合同扫描件并加盖电子公章，不提供不得分。 | 2分 |
| **7** | **拟投入项目组人员情况**  **（9分）** | 拟派的项目负责人：具备信息系统项目管理师证书、信息安全工程师、高级大数据技术应用证书的，每提供一个得1分，最多得3分。  **注：须提供以上人员证书及自投标截止日前三个月内任意一个月的在投标人单位缴纳的社保证明的扫描件并加盖公章，编入投标文件中，否则不得分。** | 3分 |
| 拟派的技术负责人：具备高级大数据分析师证书、高级网络信息安全工程师的，每提供一个得1分，最多得2分。  **注：须提供以上人员证书及自投标截止日前三个月内任意一个月的在投标人单位缴纳的社保证明的扫描件并加盖公章，编入投标文件中，否则不得分。** | 2分 |
| 项目成员 (不含项目负责人、技术负责人):团队成员应具备数据中心（机房）运维管理工程师(高级)、综合布线工程师证书(高级)、高级人工智能应用工程师证书、高级信息系统运维管理工程师；每具备一本得1分，本项满分4分，一人多证或同类证书多人均不重复计分。  **注：须提供以上人员证书及自投标截止日前三个月内任意一个月的在投标人单位缴纳的社保证明的扫描件并加盖公章，编入投标文件中，否则不得分。** | 4分 |
| **8** | **售后服务**  **（2分）** | 根据投标人提供的售后服务体系完善程度及对招标文件服务要求的响应进行综合评估。 （1）根据售后自有网点数量、售后维护方案及承诺，售后自有网点较多、有完整、可行、合理的售后维护方案得1.1-2分；  （2）售后自有网点一般，有较完整、较可行、较合理的售后维护方案得0.1-1分；  （3）未提供不得分。  **注：需提供售后服务网点相关证明材料，否则不得分** | 2分 |
| **9** | **服务质量保证措施（2分）** | 提出完善的服务质量保证措施和体系，以及详细的应急保障措施、风险控制措施以及故障响应机制等措施。  （1）有较完整、较可行、较合理的服务质量保证措施得1.1-2分；  （2）内置质量较一般的服务质量保证措施得0.5-1分；  （3）缺失、不匹配、不合理的服务质量保证措施得0.1-0.4分；  （4）未提供不得分。 | 2分 |
| **10** | **相关培训（2分）** | 投标人提供的可行合理的培训方案及培训计划：含培训方式、培训参加人员、培训内容、日程、课程安排等：  （1）培训方案措施明确、培训人员安排非常周到、培训内容非常丰富、课程安排非常合理的得1.1-2分；  （2）培训方案措施比较明确、培训人员安排比较周到、培训内容比较丰富、课程安排比较合理的得0.1-1分；  （3）未提供不得分。 | 2分 |
| **11** | **投标人资质及信誉(2分)** | 投标人具备足够的实力，根据投标人的实力能力情况进行评分。  投标人具有有效期内的ISO20000信息技术服务管理体系认证证书、ISO27001信息安全管理体系认证证书、ISO22301业务连续性管理体系认证证书、商品售后服务评价体系十二星证书；每提供1本证书得0.5分，最高得2分，不提供的不得分。  **注：上述证书需提供有效期内证书原件扫描件及在国家认证认可监督管理委员会官方网站（http://www.cnca.gov.cn/）查询的认证结果截图扫描件并加盖投标人公章，未提供或缺项不得分。** | 2分 |
| **12** | **价格30分** | 以有效报价的最低价为基准价，其价格分为30分。其它投标人的价格分按照下列公式计算：投标报价得分=（评标基准价/投标报价）×30（小数点后保留2位小数）（注：对于小型和微型企业产品的价格给予10%的扣除，用扣除后的价格参与评审。小型和微型企业需填写《中小企业声明函》、并加盖单位公章）。 | 30分 |

**(注：以上需提供的合同、证书、报告等各项证明需将原件扫描上传至投标文件，并加盖电子印章。评委打分保留1位小数)**

**[第五部分](file:///F:\\微信\\WeChat%20Files\\a29023143\\FileStorage\\File\\2021-11\\台州市公安局特警支队最小作战单元装备建设采购项目10.28.docx" \l "●评分标准) 采购内容及要求**

**一、项目概况**

**（一）项目背景**

网络空间的竞争，归根到底是人才的竞争。随着国内外安全态势的深入发展，安全技术研究的逐步深化，整个网络安全的动态已逐渐从宣贯了解向实战研究转变。鉴于新形势下的网络安全严峻态势和国家对于优秀网络与信息安全人才的迫切需求，同时也是为贯彻国家关于加强一流网络安全学院建设的重要指示精神，落实《网络安全法》、《关于加强网络安全学科建设和人才培养的意见》明确的工作任务，在教育行业，高校教育作为国家培养安全人才的主力军，责无旁贷的要承担起网络安全人才的培养工作。

在网络安全保障工作中,人是最重要也是最活跃的因素。从我国现在网络安全保障工作的紧迫性来看,培养网络安全与信息化专业人才队伍更刻不容缓。

台州学院网络空间安全产业学院在过去的三年里取得了一定的成绩，从无到有，设计并装修完成教学实践场地，规划四个中心。为进一步强化台州学院网络空间安全产业学院建设和更好培养网络空间安全人才，需要进一步强化网络空间安全知识，通过体系化认证培训和攻防比武竞技等方式，进行基于攻击语境的信息安全教育与实操训练，培养适应当前的网络安全人才需求的复合型网络安全人才。

**（二）建设目标**

通过台州学院网络安全教学实训数字化项目，通过网络安全教学实训中心、网络安全攻防竞技中心、网络安全认证培训中心配套的设备建设，以丰富的实验模拟和虚拟实战等教学模式，提高学生的实操动手能力。同时结合攻防竞技，以安全技能比武的方式，以赛促学、以赛代练，提升学生的网络安全攻防技能；再以体系化的认证培训，为学生提供相应认证培训和考证工作，帮助学生评估和提高其网络安全水平

**二、招标项目一览表**

1.本次招标共1个标段，具体内容如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **标项** | **项目名称** | **规格型号** | **数量** | **单位** | **预算**  **（万元）** | **交货地点** |
| 1 | 台州学院网络安全教学实训数字化建设项目 | 详见技术需求 | 1 | 批 | 279.52 | 台州学院椒江校区 |

2.采购清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **建设项** | **建设子项** | **建设内容** | **技术要求** | **数量** |
| 1 | （一）网络安全教学实训中心建设 | 网络安全实训系统虚拟实验资源扩容 | 虚拟化防火墙 | 详见技术需求参数 | 1套 |
| 2 | 虚拟化上网行为管理 | 详见技术需求参数 | 1套 |
| 3 | 虚拟化WEB应用防火墙 | 详见技术需求参数 | 1套 |
| 4 | 虚拟化入侵防御系统 | 详见技术需求参数 | 1套 |
| 5 | 虚拟化漏洞扫描与防护 | 详见技术需求参数 | 1套 |
| 6 | 网络安全实训系统课程资源包扩容 | CTF竞赛解题实战课程资源包 | 详见技术需求参数 | 1套 |
| 7 | 网络安全攻防技术实战课程资源包 | 详见技术需求参数 | 1套 |
| 8 | 企业网及服务建设课程资源包 | 详见技术需求参数 | 1套 |
| 9 | WEB安全综合实战课程资源包 | 详见技术需求参数 | 1套 |
| 10 | Linux操作系统安全课程资源包 | 详见技术需求参数 | 1套 |
| 11 | 入侵检测基础课程资源包 | 详见技术需求参数 | 1套 |
| 12 | 网络安全技术基础课程资源包 | 详见技术需求参数 | 1套 |
| 13 | 网络安全应急响应课程资源包 | 详见技术需求参数 | 1套 |
| 14 | 逆向工程技术实战课程资源包 | 详见技术需求参数 | 1套 |
| 15 | 企业网渗透测试课程**资源包** | 详见技术需求参数 | 1套 |
| 16 | 密码学算法编程课程资源包 | 详见技术需求参数 | 1套 |
| 17 | (二)网络安全攻防竞技中心建设 | 网络安全竞技系统 | 提供账号、队伍、角色权限管理，并提供系统配置、审计日志、系统版本管理。  系统提供竞赛创建、竞赛中管理、竞赛结果导出、题库管理、工具管理、竞赛展屏。可支撑个人赛、团体赛2种参赛方式；理论赛、解题赛、攻防赛3种竞赛形式，并配有1000道选择类题目。  150道解题赛题目(题库包含CRYPTO、MISC、WEB、PWN、Revers方向)，20道攻防赛题目，并配有解题思路。  可支撑用户自主刷题，查看解题思路，并统计训练人次、通过率、训练题目分类、题目占比等数据。 | 详见技术需求参数 | 1套 |
| 18 | (三)网络安全认证培训中心增补 | 认证实训设备 | 边界防火墙认证模块 | 详见技术需求参数 | 2台 |
| 19 | 上网行为管理认证模块 | 详见技术需求参数 | 2台 |
| 20 | IPS认证模块 | 详见技术需求参数 | 2台 |
| 21 | WAF认证模块 | 详见技术需求参数 | 2台 |
| 22 | 日志审计系统认证模块 | 详见技术需求参数 | 1台 |
| 23 | 数据库审计系统认证模块 | 详见技术需求参数 | 1台 |
| 24 | 堡垒机认证模块 | 详见技术需求参数 | 1台 |
| 25 | 态势感知认证模块 | 详见技术需求参数 | 1台 |
| 26 | 网络准入控制认证模块 | 详见技术需求参数 | 1套 |
| 27 | 核心交换机 | 详见技术需求参数 | 1台 |
| 28 | 汇聚交换机 | 详见技术需求参数 | 2台 |
| 29 | 网络机柜 | 详见技术需求参数 | 2个 |

**三、技术需求参数**

**(一)网络安全教学实训中心**

**建设子项：网络安全实训系统虚拟实验资源扩容**

**1.虚拟化防火墙**

|  |  |  |
| --- | --- | --- |
| **项目** | **指标** | **指标要求** |
| 基础组网 | 兼容性 | 本次采购的虚拟化防火墙实验模块要求与我院现有信息安全实训平台无缝对接，构建虚拟化的实验环境，打破物理安全设备的局限性，提高教学、实训上课效率，实现更高效真实的攻防实训、仿真测试的需要，开展防火墙技术及应用的相关课程。**（投标时提供盖章承诺书）。** |
| 网络协议 | 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定**（提供功能截图）** |
| 所投产品必须支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能； |
| 路由协议 | 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） |
| 所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |
| 地址转换 | 所投产品必须支持全面的NAT转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL\_CONE模式和SYMMETRIC模式 |
| 所投产品必须支持在会话的源、目的地址同为IPv4地址时，可将目的地址转换至指定服务器地址 |
| 所投产品必须支持在源地址转换过程中，对SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过SNMP Trap、邮件等方式告警。**（提供功能截图）** |
| DNS代理 | 支持IPv4的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求 |
| 支持出站的DNS代理功能，支持在不更改内网终端设备DNS服务器地址设置的情况下，将DNS解析请求发送至指定的DNS服务器，并代理原DNS服务器返回解析结果 |
| 支持DDNS功能，支持Oray向日葵、Pubyun公云、Noip、Changeip提供的DDNS服务，将动态获取的IP地址映射为固定的域名 |
| 高可靠性 | 所投产品必须支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；支持链路探测。 |
| 访问控制 | ★访问控制 | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制。支持一种基于用户的安全访问控制的方法及装置的技术(投标时提供中国网络安全审查技术与认证中心或国家知识产权局或公安部第三研究所的相关证明文件)，并支持地理区域对象的导入以及重复策略的检查。 |
| 所投产品比如支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向。 |
| 应用识别与控制 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于200种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类**（提供功能截图）** |
| 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |
| 用户识别与认证 | 所投产品必须支持基于用户的访问控制，可与LDAP/Radius/证书/Active Directory/TACACS+/POP3等用户认证系统联动 |
| 所投产品必须支持802.1x认证，要求支持基于端口和MAC两种接入控制方式 |
| 邮件过滤 | 所投产品必须支持基于关键字的接收、发送或双向Email发件人、收件人过滤，并支持自定义RLB服务器地址配置，并可结合IP黑名单或白名单 |
| 文件过滤 | 所投产品必须支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件五种分类； |
| 所投产品必须支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等30种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别 |
| 流量管理 | 所投产品必须支持多调度类相互嵌套最大5级的带宽管理设置。支持设置每IP最大或最小带宽，支持对每IP进行带宽配额管理，可通过优先级实现多应用的差分服务。 |
| 攻击防护 | 网络攻击防护 | 所投产品必须支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护、增强防护、授权服务器防护等多种防护措施**（提供功能截图）** |
| 所投产品必须支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥 |
| 所投产品必须支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率 |
| 所投产品必须支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片等；并可在设备页面显示每种攻击类型的丢包统计结果 |
| 所投产品必须支持防御基于安全域的IP地址欺骗攻击，指定IP或网段必须从特定安全域流入 |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀； |
| 所投产品必须支持对最多6级的压缩文件进行解压查杀 |
| 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀**（提供功能截图）** |
| 入侵防御 | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护**（提供功能截图）** |
| 所投产品必须支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类; |
| 所投产品必须支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号。支持一种网络入侵行为检测系统及检测方法**(投标时提供中国网络安全审查技术与认证中心或国家知识产权局或公安部第三研究所的相关证明文件)。** |
| 所投产品必须支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围**（提供功能截图）** |
| VPN | IPSecVPN | 所投产品必须支持支持IPSec VPN功能，支持基于主模式（Main Mode）、积极模式（Aggressive Mode）、国密三种协商模式建立的网关-网关加密隧道； |
| 安全管理 | 网络异常感知 | 所投产品必须支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息。 |
| 所投产品必须支持用户自定义重点URL分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。 |
| 策略与处置 | 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。**（提供功能截图）** |
| 所投设备必须支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询 |
| 所投产品必须支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息**（提供功能截图）** |
| 运维管理 | 所投产品必须支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。**（提供历史配置文件＞2个设备截图）** |
| 所投产品必须支持三权分立管理 ，权限设置至少包括全部权限，仅具有策略变更权限和仅具有日志审计权限、仅具有账户配置权限、虚系统配置管理权限以及虚系统审计权限；并支持以读写、只读、无权限的方式自定义权限管理，权限管理的范围至少包括策略配置、对象配置、网络配置、系统配置、统计分析、威胁处置等 |
| 所投产品必须支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等；**（提供功能截图）** |
| 所投产品必须支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括流量、URL过滤、内容过滤、邮件过滤、行为、威胁等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试八种。 |
| 课程资源 | 《防火墙技术与应用》课程资源需包含课程大纲、教学ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足学校一个学期的理论和实验教学需求。以虚拟化防火墙系统为教学基准，主要介绍防火墙的基本知识、结构、配置方法。通过本课程能够学习防火墙系统的部署运维等。 |
| 教程编写能力 | | 为保证平台能够与教学深度融合，投标人所投品牌的厂商需具备网络安全教材编写能力，并通过正规出版社出版发行，需提供正式发行的书号。 |

**2.虚拟化上网行为管理**

|  |  |  |  |
| --- | --- | --- | --- |
| **指标项** | **指标要求** | | |
| 兼容性 | 本次采购的虚拟化行为安全管理实验模块要求与我院现有信息安全实训平台无缝对接，构建虚拟化的实验环境，打破物理安全设备的局限性，提高教学、实训上课效率，实现更高效真实的攻防实训、仿真测试的需要，开展行为安全管理的相关课程。**（投标时提供盖章承诺书）** | | |
| 设备部署 | 网关模式 | | 设备可部署在网络中提供路由转发和NAT功能，可连接ADSL线路和专线。 |
| 镜像模式 | | 设备可连接一条或多条镜像线路，获取网络信息，进行行为分析和审计。 |
| 网桥模式 | | 设备可直路串联在一条或多条原有网络线路上，进行行为分析、审计和控制。不改变网络拓扑，路由表项。 |
| Portal模式 | | 设备在部署时支持模式选择，可设置为Portal模式，实现Portal服务器功能；**（必须提供配置界面截图）** |
| 系统监控 | 首页行为风险面板 | | 可集中呈现上网行为风险等级和状态。 行为风险等级包括安全等级、业务防护等级、合规等级和数据防护等级。 行为状态包括管控效果、运行状态、安全状态、业务风险状态、外发状态和应用使用状态。 |
| 设备状态 | | 能够实时提供产品CPU、内存、磁盘使用率、网口状态、授权状态、系统情况等信息。 |
| 网络状态 | | 能够实时提供在线用户趋势、设备流速趋势、用户流量排名、应用流量排名、用户实时流量和应用实时流量等信息。 |
| 在线用户 | | 可监控到当前在线的用户信息并支持强制下线 |
| 安全管理 | 支持对病毒的云查杀 | | 至少应支持对以下几类网络应用传输的文件进行病毒云查杀：HTTP/FTP/IMAP/SMTP/POP3"**（提供功能截图）** |
| 支持失陷主机检测 | | 支持威胁情报、挖矿、间谍软件三种失陷特征识别 |
| 支持拦截请求并记录日志，阻塞IP并记录日志以及仅记录日志三种动作模式设置 |
| 应用管理 | 应用分类 | | 可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制。  为覆盖工作无关应用，移动应用不少于1000种，即时消息应不低于150种；  为规避外发类风险，论坛发帖应不低于3000种，网络存储不低于100种，代理隧道不低于100种。 |
| 内置应用标签 | | 设备内置常用应用标签，分类至少包含内容外发风险、期货行业合规、证券行业合规、高安全风险、影响工作效率、消耗带宽6大类； |
| 网安应用行为策略 | | 支持独立的网安应用行为审计策略，支持基于用户、时间、位置、工具进行策略设置。**（提供功能截图）** |
| 网页管理 | 搜索关键字审计与管理 | | 根据关键字管理搜索引擎访问；一条策略实现搜索关键字的阻断、记录、告警，方便维护； |
| 网址访问审计与管理 | | 根据URL库及URL关键字进行网址访问管理，一条策略实现阻断、记录、告警，方便维护； |
| 网页内容关键字过滤 | | 可根据网页内容关键字进行审计与过滤，一条策略实现阻断、记录、告警；每个关键字对象要求可至少录入500个关键字 |
| 发帖审计与管理 | | 对网站的发帖正文关键字进行管理，一条策略可同时实现控制、记录、告警、便于维护管理； |
| 广告推送 | | 支持基于用户、时间、网站分类或具体网站和搜索关键字推送广告。广告页面支持自定义和设置推送频率。 |
| 免监控域名 | | 支持配置免监控域名，用户在认证前即可访问免监控域名 |
| 邮件管理 | Webmail管理 | | 一条策略可实现Webmail以及SSL加密的Webmail基于发件人、收件人、主题、内容、附件名维度的记录、阻塞、告警； |
| 客户端邮件收发管理 | | 能够基于发件人、收件人、主题、内容、附件名维度进行过滤、记录、告警；能够支持SSL加密的SMTP邮件审计；**（提供功能截图）** |
| 能够对POP3、IMAP邮件接收进行审计 |
| 文件管理 | FTP文件外发管理 | | 支持FTP文件上传管理，可根据文件大小、文件名、扩展名、传输方向、内容关键字进行审计过滤；支持对帐号、命令的审计与过滤 |
| 网页文件管理 | | 可以对网页的文件，根据传输方向、文件名、扩展名、文件大小、网站域名进行控制管理，违规文件下载阻塞同时可以告警； |
| PC客户端文件外发关键字过滤 | | 支持对QQ、微信和百度网盘的PC客户端外发文件进行关键字过滤和封堵。**（提供功能截图）** |
| IM管理 | QQ审计与管理 | | 可针对QQ账号制定策略，对聊天、登录及登出的行为进行记录与控制；能够对QQ文件传输行为进行审计，并且能够对传输的文件进行备份留存；支持对QQ聊天内容进行审计。 |
| 数据库审计 | 数据库审计控制 | | 可审计、控制Oracle, MySql, SqlServer, PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等。**（提供功能截图）** |
| 协议审计 | Https审计 | | 通过HTTPS审计功能，可以针对网站分类、证书颁发者、证书所有者、证书有效期等进行审计，加以控制 |
| ftp审计 | | 通过设置FTP审计策略对使用ftp的用户、位置、命令、文件名/目录名进行审计和控制 |
| telnet审计 | | 通过设置telnet策略，对使用Telnet的用户、位置、登录名、命令等，实现对telnet使用的控制和审计 |
| DNS审计 | | 通过DNS审计策略对DNS通信内容进行审计和控制 |
| SNMP审计 | | 通过SNMP审计策略对SNMP通信内容进行审计和控制 |
| NFS审计 | | 通过NFS审计策略对NFS访问和传输文件进行审计和控制**（提供功能截图）** |
| NETBIOS审计 | | 通过NETBIOS审计策略对NETBIOS通信、登录名及文件、目录进行审计和控制 |
| 流控策略 | | 支持基于用户、时间、应用、源IP、目的IP和服务创建流量控制策略 |
| 连接限制 | | 支持基于连接数进行流量管理，可以每个人的并发/新建连接数量进行控制 |
| 每用户带宽限制 | | 可以指定每个人的最大上传、下载带宽 |
| 终端管理软件联动 | 终端管理软件联动 | | 能够与终端管理软件联动，设备检测到未安装终端管理软件的PC，可将其Web访问自动重定向到特定页面并提示下载；**（提供功能截图）** |
| 终端准入控制 | | 设备能够根据终端管理软件检测到的信息配置准入控制策略，准入规则应包括： 1、系统是否存在某个特定进程 2、注册表中是否含有特定内容 3、制定位置是否存在特定文件 4、操作系统类型和版本等 5、系统是否安装了特定的杀毒软件和特定版本 6、系统是否安装了特定的漏洞补丁 7、系统是否开启了文件实施防护功能 |
| 用户管理 | web认证 | | 支持本地、LDAP、Radius、邮件认证方式的WEB认证。支持在界面上通过配置，将一台设备作为独立的认证服务器配合审计设备使用，提升认证性能。 |
| 短信认证 | | 支持短信认证方式，用户输入手机号作为用户名，设备通过短信网关为用户手机发送密码。短信认证能够根据不同用户推送不同认证页面，该认证页面可自定义。支持白名单。支持完整短信认证功能，无需额外购买短信网关。 |
| 微信认证 | | 支持通过微信“扫一扫”二维码方式，快速连接Wi-Fi |
| 支持利用微信公众号进行网络接入的身份准入认证 |
| 认证策略 | | 可以基于IP、MAC等多因素进行用户认证、识别 |
| 用户识别 | | 支持对802.1X、华为controller、Kerberos、AD、POP3、Radius、数据库识别、PPPOE、城市热点、深澜计费等系统的单点登录。**（提供功能截图）** |
| 日志统计与报表 | 日志FTP导出 | | 支持通过FTP和SFTP方式将日志导出到指定服务器，日志支持SSL加密和ZIP压缩，支持自定义导出数据的时间段和数据定时上传的频率。支持定义导出日志数据的范围、用户、位置和工具。 |
| 系统管理 | 界面配置 | | 管理员登录支持登录失败次数配置和阻断时长配置 |
| 支持三权制衡管理机制 | | 支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端。 |
| 课程资源 | 《行为安全管理》课程资源需包含课程大纲、教学ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足学校一个学期的理论和实验教学需求。以上网行为管理系统为教学基准，主要介绍行为安全管理系统的基本知识、结构、配置方法。通过本课程能够学习上网行为管理系统的部署运维等。 | | |
| 教程编写能力 | | ★为保证平台能够与教学深度融合，投标人所投品牌的厂商需具备网络安全教材编写能力，并通过正规出版社出版发行，**需提供正式发行的书号。** | |

**3.虚拟化WEB应用防火墙**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 功能要求 | |
| ★兼容性 | 本次采购的虚拟化Web应用防火墙系统实验模块要求与我院现有信息安全实训平台无缝对接，构建虚拟化的实验环境，打破物理安全设备的局限性，提高教学、实训上课效率，实现更高效真实的攻防实训、仿真测试的需要，开展WEB应用防火墙的相关课程。**（投标时提供盖章承诺书）** |
| 基础防护 | 支持IPv4和IPv6双协议栈流量过滤防护 |
| 支持产品页面一键断网（禁止访问）功能，在特殊情况下，实现对特定网站的快速下线**（提供功能截图）** |
| 支持代理模式下对HTTP、HTTPS协议的单个连接允许请求数、长连接有效时间、最大空闲连接数和上传文件最大值等数据进行自定义配置 |
| 状态监控 | 支持对产品的CPU、内存使用率实时监控并以图形化方式展现 |
| 支持对产品的网络接口收发流量进行实时监控并以图形化方式展现 |
| 支持协议连接实时监控展示，可针对监控协议进行阻断以及加黑操作 |
| 支持系统状态实时展示，支持对CPU、内存使用情况实时呈现，设备信息呈现**（提供功能截图）** |
| 支持防护资产安全状态展示，可针对资产的TCP，UDP,ICMP/ICMP6，RAW-IP,HTTP,DNS等数据进行统计 |
| 态势感知 | 支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP并发请求及实时事件的动画统计**（提供功能截图）** |
| 访问控制防护 | 支持黑白名单策略，包括IP及URL黑白名单 |
| 支持IP访问控制，可根据源目的IP，端口，协议等进行访问控制处理，并可自定义访问过期时长 |
| 支持地域访问控制功能，支持根据国家、地区、城市等元素进行地域访问控制，并可自定义访问过期时长**（提供功能截图）** |
| 支持HTTP访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，支持设置HTTP 0.9/1.0/1.1/2.0版本和10多种http访问控制方法 |
| 安全防御 | 支持协议合规校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据 |
| 支持HTTP请求走私防护 |
| 支持SQL注入、XSS跨站攻击防御策略，支持特征检测与语义分析算法检测**（提供功能截图）** |
| 支持Web攻击防护功能，包括命令注入攻击，组件漏洞防护、Web扫描防护、XPATH注入防护、XML注入防护、SSI注入防护、JOSN注入防护、LDAP注入防护、webshell防护 |
| 支持Web业务控制防御功能，提供针对爬虫、黑链、盗链以及内网代理的防护功能 |
| 支持敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护 |
| 支持Web业务加固防御功能，提供弱密码检测、CGI安全、跨站请求伪造等防御功能 |
| 支持人机识别功能，可针对自动化攻击进行有效防护 |
| 支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护**（提供功能截图）** |
| 支持会话安全防护，Cookie加固、Cookie加密、会话固定等属性设置 |
| 支持业务流程控制，防止非法用户通过不合规流程请求，对web服务器进行攻击 |
| 支持自定义应用层攻击特征库，可在页面直接编写攻击特征写入设备 |
| 虚拟补丁 | 支持虚拟补丁功能，支持导入appscan和RayScan扫描器的扫描结果生成WAF的规则，对此类网站漏洞直接防护**（提供功能截图）** |
| 蜜罐防护 | 支持轻量级蜜罐防御功能，提供伪造的后台管理系统页面，主动诱使黑客进行攻击，记录攻击行为**（提供功能截图）** |
| 爬虫陷阱 | 支持爬虫陷阱防护**（提供功能截图）** |
| 智能封禁 | 支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间**（提供功能截图）** |
| 资产探测 | 支持资产探测功能，提供自动识别资产系统类型和开放端口**（提供功能截图）** |
| 支持周期性针对资产识别探测，支持自定义每天、每周、每月自动化探测功能 |
| 外联检测 | 支持非法URL外联检测功能，针对特定外联URL进行监控或阻断，并且支持自定义URL地址**（提供功能截图）** |
| 流量限速 | 支持流量限速功能，根据流量智能自动生成流量阈值 |
| 支持检测TCP并发链接数，TCP新建链接数，TCP带宽（c2s），UDP带宽（c2s），ICMP带宽（c2s），HTTP GET 速率，HTTP POST 速率，HTTP 其他请求速率，DNS 查询请求速率，并发IP数量等单用户和总量进行自定义阈值配置**（提供功能截图）** |
| 课程资源 | 《web应用防火墙技术与应用》课程资源需包含课程大纲、教学ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足学校一个学期的理论和实验教学需求。以虚拟化web应用防火墙系统为教学基准，主要介绍web应用防火墙系统的基本知识、结构、配置方法。通过本课程能够学习web应用防火墙系统的部署运维等。 |
| ★教程编写能力 | 为保证平台能够与教学深度融合，投标人所投品牌的厂商需具备网络安全教材编写能力，并通过正规出版社出版发行，需提供正式发行的书号。 |

**4.虚拟化入侵防御系统**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★兼容性 | 本次采购的虚拟化入侵防御实验模块要求与我院现有信息安全实训平台无缝对接，构建虚拟化的实验环境，打破物理安全设备的局限性，提高教学、实训上课效率，实现更高效真实的攻防实训、仿真测试的需要，开展入侵防御与入侵检测的相关课程。**（投标时提供的盖章承诺书）** |
| 网络配置 | [支持静态ARP配置以及动态ARP获取](#_支持静态ARP配置以及动态ARP获取);**（提供功能截图）** |
| 大屏展示 | 支持态势感知大屏展示，综合展示攻击风险情况 |
| IPS防护 | 支持根据攻击特征进行的攻击检测技术，对于攻击特征进行有效分类和组织便于用户管理和维护； |
| 支持自定义IPS特征； |
| [支持检测恶意活动，包括恶意SSL证书、钓鱼攻击、非法获取权限等](#_支持检测恶意活动，包括恶意URL证书、钓鱼攻击、非法获取权限等)；**（提供功能截图）** |
| [支持检测漏洞后门类攻击，包括漏洞利用、后门攻击、文件包含、缓冲溢出、目录遍历等](#表格8)；**（提供功能截图）** |
| [支持检测僵木蠕类攻击，包括木马、蠕虫病毒、僵尸网络等](#_支持检测僵木蠕类攻击，包括木马、蠕虫病毒、僵尸网络等)；**（提供功能截图）** |
| 支持检测Web攻击类攻击，包括注入攻击、跨站脚本、Webshell等； |
| [支持检测恶意软件类攻击，包括恶意软件、间谍软件等；](#_支持检测恶意软件类攻击，包括恶意软件、间谍软件等；) |
| 支持针对不同的策略设置例外规则 |
| IPv4和IPv6安全 | [支持IPv4和IPv6的双栈防护；](#_支持IPv4和IPv6的双栈防护；（要求提供界面截图证明）) |
| 外联检测 | 支持URL外联检测功能，针对特定外联URL进行监控或阻断； |
| 支持自定义URL过滤； |
| 攻击特征库和升级方式 | [内置入侵攻击特征库不少于15000条；](#_内置攻击特征库≥13000条；（要求提供界面截图证明）)**[（提供功能截图）](#_内置攻击特征库≥13000条；（要求提供界面截图证明）)** |
| 攻击特征库可支持本地、FTP服务器升级，同时支持在线更新和自动更新； |
| 管理维护 | [支持日志告警和内存告警配置，当设备达到设置阈值时会进行弹窗警报；](#_支持日志告警和内存告警配置，当设备达到设置阈值时会进行弹窗警报；（要求) |
| [支持手工备份和自动备份功能，可按每天、每周、每月自定义备份周期，并支持自动清除历史备份数据，保障数据和配置安全性;](#_支持手工备份和自动备份功能，可按每天、每周、每月自定义备份周期，并支持) |
| 支持一键诊断工具，一键完成系统信息收集； |
| 支持基于Web的在线运维工具，包括Webshell、Ping、tcpdump、traceroute等; |
| 课程资源 | 《入侵检测与防御技术》课程资源需包含课程大纲、教学ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足学校一个学期的理论和实验教学需求。以虚拟化入侵防御系统为教学基准，主要介绍入侵防御系统的基本知识、结构、配置方法。通过本课程能够学习入侵防御系统的部署运维等。 |
| 教程编写能力 | 为保证平台能够与教学深度融合，投标人所投品牌的厂商需具备网络安全教材编写能力，并通过正规出版社出版发行，需提供正式发行的书号。 |

**5.虚拟化漏洞扫描与防护**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 兼容性 | 本次采购的虚拟化漏洞扫描与防护实验模块要求与我院现有信息安全实训平台无缝对接，构建虚拟化的实验环境，打破物理安全设备的局限性，提高教学、实训上课效率，实现更高效真实的攻防实训、仿真测试的需要，开展漏洞扫描与防护的相关课程。**（投标时提供的盖章承诺书）** |
| 基本要求 | 系统应能提供4大独立扫描模块，包含系统扫描、Web扫描、数据库扫描、弱口令扫描的全面扫描能力，每个模块具备各自的配置项，可灵活修改每个模块的配置参数以满足不同场景下的扫描需求。**（提供功能截图）** |
| 采用B/S设计架构，SSL加密方式通信，无须安装客户端，用户可通过浏览器远程管理系统。 |
| 系统应支持部署在IPv4、IPv6环境下，且系统扫描、Web扫描、数据库扫描、弱口令扫描等各类型任务均支持添加IPv6扫描目标。 |
| 任务管理 | 系统应支持针对指定IP段，同时一键下发系统扫描、Web扫描、弱口令扫描任务，其中Web扫描能够自动发现该网段内的在线网站并开展扫描；弱口令扫描能自动发现该网段IP开放服务并自动开展弱口令扫描。**（提供功能截图）** |
| 系统应支持实时显示扫描进度及结果，能够在扫描过程中实时查看主机信息及漏洞信息。 |
| 系统应支持一键复制指定任务的配置，针对新的扫描目标创建相同配置的任务。 |
| 系统应支持自定义任务执行方式，支持立即扫描、定时扫描、周期性扫描等多种扫描方式，自定义周期扫描时间可精确到每天、每周或每月的某天、某时、某分； |
| 系统扫描 | 系统应支持检测的系统漏洞数不少于17万个，覆盖CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq多种漏洞标准。**（提供功能截图）** |
| 支持扫描通用操作系统，涵盖Windows系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris等；支持扫描交换路由设备，涵盖Cisco、Juniper、华为、F5、Checkpoint、锐捷在内的主流厂商的设备；支持扫描安全设备，涵盖Checkpoint、Cisco、Juniper、华为在内的主流厂商的防火墙等安全设备； |
| 系统应支持通过SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP、WMI、RSH、REXEC、WINRM、SNMP等协议对目标主机进行登录扫描。 |
| 系统应支持批量导入认证信息，能够批量验证登录认证信息是否正确。 |
| 支持中间件漏洞扫描，涵盖Apache、Resin、Nginx、Tomcat、BIND、DOMINO、WebSphere、IIS、Jboss等； |
| 系统支持大数据组件框架漏洞检测，如zookeeper、ElasticSearch、ActiveMQ 、Kibana、Hadoop等。 |
| 系统应支持不同维度的漏洞库视图，包含漏洞类别维度、操作系统维度、漏洞发现时间维度、服务维度、应用维度。 |
| 系统应默认内置多种不同的检测模式，包含但不限于标准扫描、快速扫描、完全扫描、深度扫描，不同检测模式默认对应不同的扫描任务策略及配置。 |
| 系统应提供高级漏洞模板过滤器，支持通过漏洞名称、漏洞编号（含CVE编号、CNNVD编号、CNVD编号）、漏洞级别、发现时间、操作系统类别、应用类别、服务类别过滤出满足需求的漏洞并创建漏洞模板。 |
| Web扫描 | 系统应支持Web漏洞扫描，支持检测OWASP Top10定义的常见10大类Web漏洞。 |
| 漏洞结果系统应支持展示详细的HTTP请求头信息。 |
| 系统应支持Web登录扫描，系统应支持Cookie认证、Form认证、Basic认证、NTLM认证、Session认证、Digest认证、SSL，并支持Web登陆验证，确保Web登录成功。**（提供功能截图）** |
| 系统应支持Web扫描代理检测，能够使用HTTP代理和SOCKS代理方式。 |
| 系统应支持自定义检测网站时爬虫爬取网站的页面深度。 |
| 系统应支持自定义检测方向设置，即爬虫在爬取网站树时，采用的先后顺序策略。 |
| 系统应支持自定义爬虫模拟提交时的表单填充内容。 |
| 系统应支持自定义例外URL、例外文件类型、例外特定检测参数。 |
| 系统应支持扫描并发线程数设置。 |
| 系统应支持大小写敏感或不敏感的检测方式。 |
| 系统应支持自定义最大类似页面数和同目录下最大页面数。 |
| 数据库扫描 | 系统应支持主流数据库漏洞的检测，应包括但不限于：Oracle、Sybase、SQLServer、DB2、MySQL、Postgres、Informix、达梦、南大通用、人大金仓、神通等。 |
| 系统应支持Oralce、Sybase、SQLServer、DB2、MySQL、Postgres、Informix数据库的登录扫描，包括数据库账号、密码，SYSDBA、SYSOPER、NORMAL认证，SID、数据库名称、实例名称及实例号等登录选项的设置，系统应支持数据库在线登陆验证。 |
| 弱口令扫描 | 系统应支持目前主流协议、数据库、中间件、HTTP web服务、HTTPS web服务、常用摄像头弱口令检测。**（提供功能截图）**  主流服务/协议弱口令包括：TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP  主流数据库弱口令包括：Oracle、REDIS、MySQL、PostgreSQL、MsSQL、DB2、MongoDB、Sybase 、Informix  主流中间件弱口令包括：Tomcat、WebLogic、JBoss、WebSphere、GlassFish  HTTP类型的web弱口令包括：http-get、http-get-form、http-post-form、http-head、http-post  HTTPS类型的web弱口令包括：https-get、https-get-form、https-post-form、https-head、https-post  主流摄像头弱口令包括：大华、华为、宇视、海康摄像头或相当于 |
| 系统应支持用户自定义口令字典。 |
| 系统应支持通过用户名字典、密码字典、用户名密码组合字典进行检测。 |
| 资产管理 | 系统应支持资产统一管理，支持按照IP、URL、网页编码、操作系统、MAC地址、所属资产组、资产标签、资产评分对资产进行高级检索和分析。 |
| 系统应支持对资产及资产检测结果进行备份恢复。 |
| 数据分析及报表管理 | 系统应支持漏洞数据高级检索及分析，系统应支持按照目标IP或URL、操作系统、MAC地址、资产评分、漏洞等级、漏洞名称、漏洞类别、漏洞评分、开放端口查看漏洞分布情况，并将检索结果导出。 |
| 系统应支持单个资产历史扫描结果变化趋势展示，并可对比任意两次扫描结果，查看新增漏洞和减少漏洞。 |
| 系统应提供对同一目标不同次任务扫描结果的对比分析功能，能够列出两次任务结果对比中新增和减少的漏洞信息。 |
| 系统应支持导出统计和详细两种类型的报表，并系统应支持设置报表压缩包密码，确保报表安全性。 |
| 系统应支持自定义导出报表模板，可定制指定漏洞等级（高危、中危、低危、信息）、指定漏洞状态（新增、误报、已修复）、指定报表标题以及章节内容的报表模板，并可在导出报表时灵活选择已经定义好的报表模板**（提供功能截图）** |
| 系统管理 | 系统能够对CPU、内存、磁盘、网络状态、设备授权到期及漏洞库升级授权到期进行告警，可以灵活配置告警要求。 |
| 系统支持自带诊断工具，包含端口探测、Tcpdump抓包、故障信息收集、一键诊断修复等工具。 |
| 课程资源 | 《漏洞扫描与漏洞防护》课程资源需包含课程大纲、教学ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足学校一个学期的理论和实验教学需求。以虚拟化漏洞扫描系统为教学基准，主要介绍漏洞扫描系统的基本知识、结构、配置方法。通过本课程能够学习漏洞扫描系统的部署运维。 |
| 教程编写能力 | ★为保证平台能够与教学深度融合，投标人所投品牌的厂商需具备网络安全教材编写能力，并通过正规出版社出版发行，**需提供正式发行的书号。** |

**建设子项：网络安全实训系统课程资源包扩容**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| **6、CTF竞赛解题实战课程资源包** | 1、本课程通过模拟企业构建信息系统及其支撑环境过程，学习和掌握支持企业信息处理的基本功能。通过对企业信息系统典型的信息输入、存储、处理、输出和控制过程的建设和管理，使得学生了解企业典型信息系统的建设思想，掌握信息系统建设过程中网络结构的规划和实施、信息服务的设计和部署，确保信息系统能够正常运行。  2、**项目实训任务要求包含：**  CTF竞赛解题实战- web  CTF竞赛解题实战- reverse  CTF竞赛解题实战- pwn  CTF竞赛解题实战- misc  CTF竞赛解题实战- crypto |
| **7、网络安全攻防技术实战课程资源包** | 1、本课程通过搭建主要业务应用系统的典型企业网络架构，让学生模拟攻击者的角色，在不了解企业环境内部拓扑和业务系统的情况下，通过企业对外服务业务的暴露途径考察学生对企业网络架构与应用的认知、脆弱性发现、漏洞利用。学生通过以上攻击过程，还原网络结构及发现网络中的脆弱点，最终形成渗透测试报告，其中发现的所有脆弱点及修复建议。含五年内课程资源包更新。  **2、项目实训任务要求包含：**  信息收集  漏洞分析  Web渗透测试  权限提升  权限维持  内网渗透代理  内网常见攻击  后渗透  痕迹清除 |
| **8、企业网及服务建设课程资源包** | 1、根据用户企业网安全建设的常见需求，分别从基础网络建设、网络服务搭建等方面设计该课程，通过课程的学习提高学生对企业网主流网络和业务架构的了解，可独立完成对企业网络架构和客户安全需求分析，掌握简单网络安全项目方案的设计思路，运用项目管理的方法管理项目过程，熟练掌握企业内部信息网络主流架构、网络、系统、服务等相关知识技能完成企业网络安全建设项目；  **2、项目实训任务要求包含：**  企业网络搭建；  企业服务搭建-DNS域名解析建设；  企业服务搭建-DHCP自动IP地址分配建设；  企业服务搭建-AD域建设；  企业服务搭建-FTP文件共享建设；  企业服务建设-Email建设；  3、该实训资源需与校内实训系统联动，以项目式的工作流程进行教学，包含实验手册、实验拓扑，实验拓扑不少于18个网络节点，可在线一键开启拓扑环境。 |
| **9、WEB安全综合实战课程资源包** | 介绍Web安全基础知识，掌握具备BurpSuite等常见工具的使用能力，具备MySQL注入、文件上传、命令执行、代码执行、XSS、SSRF、反序列化、中间件洞、数据库等漏洞的利用能力，以及基本的Web综合攻防能力。 |
| **10、Linux操作系统安全课程资源包** | Linux基本命令使用实验  Linux用户管理  Linux网络与服务管理  Linux文件系统管理  Linux下ftp服务器配置实验  Linux提权后获取敏感信息的方法与途径  Linux系统缺省的存取控制权限  samba服务器配置和管理  WEB服务器配置与管理  NFS服务器配置与管理  Iptables服务器配置与管理  Linux下修改OpenSSH服务端口号  Linux下MD5工具进行文件哈希签名  Linux系统日志清除 |
| **11、入侵检测基础课程资源包** | Snort基础环境安装配置  嗅探与数据包记录器  入侵行为检测  入侵检测规则编写  sfportscan预处理器  snort\_inline安装与配置  snort\_inline规则编写及应用  Snort与防火墙联动  barnyard2的安装配置  base的安装配置  Windows搭建SNORT+BASE入侵检测系统  WAF部署 |
| **12、网络安全技术基础课程资源包** | HTTP代理下HTTPS流量分析  DNS劫持  DNS劫持植入木马  主机探测与端口扫描  PGP加密技术  web安全  RST攻击  SYNflood攻击  iptables防火墙  入侵检测  蜜罐  综合实验 |
| **13、网络安全应急响应课程资源包** | 系统备份：  Windows备份  MySQL数据库备份与修复  安全加固：  windows安全加固2.0  IIs安全加固2.0  mysql安全加固2.0  网站篡改：网站篡改应急响应  勒索病毒：  勒索病毒应急响应\_wireshark安装  勒索病毒应急响应\_wireshark使用  勒索病毒应急响应-天擎控制台安装  勒索病毒应急响应-杀毒软件升级  勒索病毒应急响应-病毒查杀  勒索病毒应急响应 |
| **14、逆向工程技术实战课程资源包** | 逆向工程技术概述  逆向工程必备知识之操作系统及程序运行原理  逆向工程必备知识之IA-32寄存器及栈  逆向工程必备知识之汇编语言基础  逆向工程常用工具之动态调试工具  逆向工程常用工具之静态分析工具  “正向”学习逆向分析  逆向实战 |
| **15、企业网渗透测试课程资源包** | 1、本实训项目制课程通过搭建主要业务应用系统的典型企业网络架构，让学生模拟攻击者的角色，在不了解企业环境内部拓扑和业务系统的情况下，通过企业对外服务业务的暴露途径考察学生对企业网络架构与应用的认知、脆弱性发现、漏洞利用。学生通过以上攻击过程，还原网络结构及发现网络中的脆弱点，最终形成渗透测试报告，其中发现的所有脆弱点及修复建议。  2、**项目实训任务要求包含：**  登录www.qiye.com网站后台获取flag1（管理员用户的描述中）  通过www.qiye.com后台目录遍历漏洞，获取服务器tomcat管理页面的账号密码，并登录（获取管理页面中的flag2）  在www.qiye.com服务器的c盘根目录获取flag3  通过new.qiye.com网站某页面存在的Sql注入漏洞获取数据库中的flag4  登录news.qiye.com网站，提交网站后台首页中的flag5  读取news.qiye.com网站配置文件中的flag6  读取news.qiye.com服务器中/home目录下的flag7  登录blog.qiye.com网站的后台，提交网站后台草稿文章中的flag8  获取blog.qiye.com网站的配置文件中的flag9  获取blog.qiye.com数据库中flag表中的flag10  获取blog.qiye.com网站服务器/root目录下的flag11  找到存在redis服务的内网服务器的ip地址，提交格式flag12{ip地址}  读取存在redis服务的机器中redis服务所使用的配置文件的路径，提交路径flag13{文件全路径}  读取存在redis服务的机器中/root目录下的flag14  破解redis同网络中存在oa-web服务机器的admin用户的密码，提交格式flag15{密码}  发现和redis服务器同一网络中的ip为x.x.x.30服务器上的漏洞，并读取其/root目录中的flag16  网络中存在网络文件系统服务，读取存在用户目录的flag17  读取网络文件系统服务所在机器/root目录下的flag18  使用上一任务中发现的用户名登录网络中还存在此用户的机器，读取此用户目录下的flag19  读取任务十九机器中/root目录下的flag20  获取管理员电脑的administrator密码并提交，提交格式flag21{administrator密码}  找到网路中的用户区，获取网络管理员机器的权限，读取其电脑c:/flag22  获取域账号eviluser的密码，提交格式flag23{eviluser账号的密码}  读取域控服务器c:/flag24  4、该实训资源需与校内实训系统联动，以项目式的工作流程进行教学，包含实验手册、实验拓扑，实验拓扑不少于18个网络节点，可在线一键开启拓扑环境 |
| **16、密码学算法编程课程资源包** | 对称密码的工作模式  移位密码  置换密码  AES算法  DES密码  DSA签名算法  ECC算法  MD5算法  RC4算法  RSA算法  SHA-1算法  SM4密码  Vigenere密码  ZUC算法  仿射密码 |

1. **网络安全攻防竞技中心建设**

**17、网络安全竞技系统**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 系统管理中心 | 平台系统采用B/S架构，内置竞赛管理、训练管理、题目管理、工具管理、账号管理、队伍管理、系统管理等模块； |
| 平台支持数据展示功能，可针对系统的题目数量、虚拟机数量、竞赛数量、虚拟机启动数量进行展示； |
| 平台支持集群部署，并对服务器CPU使用率、内存使用率、硬盘使用率进行图表化展示，同时可对占用资源进行单一及批量释放； |
| 平台支持靶机网络自定义设置，支持默认网络、自配网络两种网络模式； |
| 平台支持审计日志管理，可查看用户增、删、改、查等操作，支持清空日志、按时间查询、搜索日志信息等操作； |
| 审计日志支持登录、登出、获取竞赛信息、创建竞赛、上传任务、获取权限、获取用户详情等多种行为统计； |
| 平台支持用户管理功能，提供账号管理、队伍管理、角色权限管理，管理员可对账户、队伍进行批量操作，包括导入、导出、新增、删除和禁用等操作； |
| 平台支持账号自定义，可对姓名、分类、队伍名称、队伍LOGO等信息进行设置，用户密码支持自定义、系统随机生成两种方式，并支持账号、密码等信息导出； |
| 平台支持自定义角色，除内置超级管理员、竞赛选手、普通用户角色外，管理员可根据需求自主创建创建裁判、管理员等角色； |
| 平台支持协作管理员、题目审核员角色账号创建，协作管理员有竞赛编辑、人员及题目关联、竞赛中过程管控等权限，题目审核员有题目的创建、编辑、验证等权限；**（提供功能截图）** |
| 竞赛管理中心 | 平台支持多场竞赛同时管理，支持对竞赛新建、编辑、搜索、发布、环境部署、竞赛中管理、竞赛结果等流程进行操作；★为使网络安全攻防竞赛管理中心更具备实战氛围，平台厂商需具备漏洞采集平台，漏洞平台具备自主知识产权、且平台上注册不少于100000人的白帽专家数量**（并能提供链接地址及证明材料)且同时提供软件著作权证书证明。** |
| 平台支持个人及团体参赛方式的理论赛、解题赛、攻防赛竞赛模式，并可根据需求进行竞赛形式自由组合； |
| 平台支持竞赛私有，竞赛创建者可通过关联协作管理员方式，实现竞赛管理权限的分配，协作管理员不限制数量； |
| 平台支持单账号赛前模拟测试，测试过程中管理员可在选手角色与管理员角色之间一键切换，无需多账号之间切换；**（提供功能截图）** |
| 平台支持竞赛一键重置，赛前模拟数据可一键清除，无需在模拟后再次创建新的竞赛； |
| 平台支持竞赛全阶段对题目进行单个/批量下发及回收操作； |
| 理论赛题目支持固定选题、全员随机、团队内分配三种选题下发策略，团队内分配可按题目类型、题目分类、初级、中级、高级进行设置，同时支持初级、中级、高级分值设置，以满足团队内成员题目不同但团队与团队之间题目相同的场景需求；**（提供功能截图）** |
| 平台支持题目、竞赛双策略计分规则，题目计分规则支持固定、动态、系数、零和多种方式，竞赛计分规则支持所得分值、所得分值/第一名所得分值两种基数计分方式；**（提供功能截图）** |
| 平台支持题目环境一键快速部署，根据队伍数量、题目类型自动分配虚拟机环境IP地址，并自动生成图形化拓扑及列表； |
| 平台支持解题赛题目环境、攻防赛题目环境分区域管理，管理员在竞赛阶段对各区域分别进行启动、关闭、还原操作； |
| 平台支持竞赛控制、题目控制、环境管理、环境检测、公告管理、答题详情、积分记录、实时排行榜等流程管理； |
| 平台支持准备模式、全通模式、解题模式、解题+加固模式、加固模式、攻防模式的网络控制，各模式之间一键配置，分别对平台、题目进行访问控制、环境隔离控制；**（提供功能截图）** |
| 平台支持终端IP段输入验证、登录绑定，从平台自有功能上实现各团队题目环境隔离；**（提供功能截图）** |
| 平台支持多方式竞赛运维策略，可对竞赛进行开始、暂停、重置、竞赛各阶段时间等信息进行配置； |
| 平台支持竞赛中环境管理，记录队伍启动、关闭、还原次数，支持题目的查看、启动、关闭、还原，攻防赛支持环境检测，记录服务异常情况，并支持对服务不可用队伍进行处罚； |
| 平台支持奖励及违规处罚，可对违规队伍分阶段进行扣分等处罚； |
| 平台支持公告管理，支持定向及不定向发布及取消公告，支持一般、中等、重要多级别公告管理，重要公告弹窗提醒； |
| 平台支持竞赛中题目答题详情、队伍答题详情的管理，支持具体分值、正确率、提交次数、答题进度、提交人次、被攻击次数、提交时间等数据展示； |
| 平台支持实时排行榜展示，分值默认由高到低展示，支持积分得失分数据及得失分原因统计； |
| 平台支持竞赛结果管理，统计个人榜单、团队榜单、过程数据，支持各榜单结果导出，各竞赛阶段成绩分开统计，统计最终排行、原始成绩等数据； |
| 平台支持题库管理，管理员根据实际需求新建、编辑、搜索、删除、导入、公开题目，支持理论赛题目、解题赛题目、攻防赛题目管理； |
| 平台支持docker虚拟化，可对虚拟机进行启动、关闭、查看等操作，支持可视化控制台； |
| 攻防赛题目支持自定义检测规则设置，根据需求可使用http、tcp检测协议从服务端口、期望输出、URL等方面设置； |
| 平台支持竞赛题库、训练题库统一化管理，题目归属一键转换； |
| 平台支持动态flag，可根据需求使用curl、脚本执行方式进行设置，解题赛题目支持多附件上传，支持附件题目的动态flag； |
| 平台支持网络控制、动态flag、随机附件随机flag、虚拟机动态密码、服务检测、Writeup、终端IP段验证、提交间隔时间限制、日志记录等多种防作弊手段；**（提供功能截图）** |
| 平台支持用户端Writeup上传，管理端Writeup查看、导出； |
| 平台支持解题赛、攻防赛实时3D可视化动态展示，展示数据主要有答题动态、攻击路径、排行榜、得分趋势、得分详情等，布局上适用不同队伍、不同题目分布，适配16:9及32:9分辨率； |
| 平台支持工具管理，可对工具进行上传、编辑、下载、删除、搜索等操作，后台上传工具会同步到用户端工具库，用户根据需求下载所需要的工具； |
| 训练管理中心 | 平台支持训练管理，统计训练总人数、训练通过率、训练题目数量、错题率等数据信息； |
| 平台支持训练统计分析功能，支持按日、周、月、年进行错题率分析，支持训练题目排名、通过率排名统计； |
| 平台支持自主刷题训练，并提供配套解题思路，帮助用户有效训练；支持训练题目收藏；支持我的队伍、竞赛、训练、收藏数据统计； |
| CTF竞赛题库 | 不少于270道CTF题目，其中不少于120道含详情解题思路；不少于30道攻防题目，其中不少于15道含详细解题思路。 |

**(三)网络安全认证培训中心增补**

**认证实训设备**

* + - 1. **边界防火墙认证模块**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 硬件要求 | 网络处理能力≥15Gbps，并发连接：≥200万，每秒新建连接：≥12万/秒，≥16个10/100/1000M自适应电、≥4个SFP光接口和≥4个SFP+光接口, ≥4T硬盘，冗余电源，含至少5年硬件质保。 |
| 访问控制 | 系统要求支持从用户视角的安全访问控制技术，要求提供信息产业信息安全测评中心或国家知识产权局等第三方权威机构出具的证明；支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 |
| 应用识别与控制 | 必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类。 |
| 文件过滤 | 所投产品必须支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等30种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别 |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；支持对最多6级的压缩文件进行解压查杀；支持设置例外特征，对特定的病毒特征不进行查杀； |
| 网络异常感知 | 所投产品必须支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断 |
| 所投产品必须支持用户自定义重点URL分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。 |
| 安全事件分析 | 所投设备必须提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素于为过滤条件且不少于35个维度进行数据钻取 |
| 安全联动要求 | 为提升产业学院整体网络的安全性，所投系统必须与产业学院现有的高级威胁态势感知平台进行联动，可上报网络活动产生的数据至网络威胁感知平台；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁。**（需要提供能够体现上述功能的截图）** |
| 为提升产业学院的终端威胁处置能力，所投系统须支持与产业学院现有终端安全管理系统进行联动，实现基于终端健康状态的访问控制；并支持阻断终端网络活动的同时，提示被阻断原因及重定向至自定义网址。 |
| 策略与处置 | 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 |
| 网元管理 | 所投产品支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如WAF安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品支持对网元进行健康检查，及故障bypass能力，健康检查至少包括链路探测、回环探测、接口探测能力 |
| 引流策略 | 所投产品支持引流策略的添加、删除、调序、清除命中数、刷新功能；支持引流策略的启用和禁用功能。 |
| 所投产品支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。 |
| 编排流量监控 | 所投产品支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 能力要求（需提供证书扫描件） | 产品具有高安全性可对抗高程度的威胁，国家信息安全测评信息技术产品安全测评证书（EAL4+级） |
| 产品具有中国信息安全测评中心颁发的自主原创证书 |
| 认证实训设备厂商属于CNNVD一级技术支撑单位 |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 |

* + - 1. **上网行为管理认证模块**

|  |  |  |
| --- | --- | --- |
| **技术指标** | **指标要求** | |
| 硬件规格 | 多核处理 | 采用国际先进的多核处理器硬件架构及多核并行处理系统 |
| 内置光Bypass接口 | 支持内置光Bypass接口，可通过系统开关或设备面板按扭实现光口Bypass，无需增加外置Bypass产品。 |
| 技术性能 | 带宽≥800M；最大并发连接数为≥60万；最大新建连接数：≥4万/秒；≥6个千兆电接口，≥1T硬盘，含至少5年硬件质保服务。 |
| 系统架构 | 一体化引擎 | 设备必须采用一体化引擎，避免在复杂应用场景开启多功能时的延迟损耗及性能衰减。 |
| 安全管理 | 支持对病毒的云查杀 | 支持配置病毒查杀策略，检查网络中传输的文件是否是病毒，支持记录日志、病毒过滤；  支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗；  至少应支持对以下几类网络应用传输的文件进行病毒云查杀：HTTP/FTP/IMAP/SMTP/POP3/SCP/SFTP。 |
| 支持对恶意URL的云查杀 | 支持基于云端大数据安全平台，对恶意URL访问进行封堵和记录日志。 |
| 支持失陷主机检测 | 支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志。**（提供功能截图）** |
| 至少支持拦截对外部威胁IP的访问请求和阻塞失陷主机IP两种控制策略。阻塞后支持向用户推送威胁情报阻塞提示页面。 |
| 应用管理 | 应用审计及控制 | 应用协议库包含的应用数量不低于12000种，应用规则总数不低于73000种。 |
| 应用分类 | 可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制； |
| 数据防泄漏 | 外发途径管控 | 支持基于大小的内容外发控制。不开启SSL，对终端影响小；仅对外发控制，不影响浏览和下载等行为；  可实现对网盘，webmail等的外发文件限制。 |
| 外发文件限制 | 支持基于文件后缀的文件类型识别；支持基于文件内容对归档文件、压缩文件、加密文件、脚本文件等170+文件类型识别。修改后缀名，压缩等方式均可以识别准确类型； |
| 业务审计 | 业务系统审计 | 支持业务系统访问及API接口进行双向扫描、通过敏感信息、安全漏洞、行为接口、自定义接口规则等识别并标识数据及传输风险。**（提供功能截图）** |
| 支持业务审计监控，可以查看最近某段时间内扫描到的业务系统访问数据的统计及排行； |
| 业务防护 | 入侵防护 | 支持对域名服务器、数据库服务器、文件服务器、邮件服务器、Web服务器等业务系统进行传输行为监测，能够及时中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。 |
| 共享接入 | 共享接入配置 | 可识别网络中的私接路由或共享wifi的网络行为并配置阻塞策略；  阻塞条件支持基于终端总数量、PC数量、移动终端数量分别配置；  阻塞条件只选择终端总数量时，支持例外名单配置，包含PC数量、移动终端数量； |
| 终端管理软件联动 | 终端管理软件联动 | 支持与现有的终端管理软件联动，设备检测到未安装终端管理软件的PC，可将其Web访问自动重定向到特定页面并提示下载。 |
| 能力要求（需提供证书扫描件） | 具备国家信息安全测评信息技术产品安全测评证书，EAL3+资质 | |
| 认证实训设备厂商具备ITSS运行维护符合性证书（二级及以上） | |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 | |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 | |

* + - 1. **IPS认证模块**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 自主可控要求 | 产品要求为专业入侵防御系统，拒绝下一代防火墙或UTM设备。 |
| 性能规格 | 网络层吞吐量为≥5Gbps，IPS吞吐量为≥2Gbps，最大并发连接数≥100万，每秒新建连接数≥5万/秒，千兆≥6个10/100/1000M自适应电口，5年硬件质保服务。本次IPS冗余部署，具备多系统切换技术，**要求提供信息产业信息安全测评中心或国家知识产权局等第三方权威机构出具的证明**。 |
| 部署模式 | 产品提供多种部署模式，支持路由、透明接入、虚拟网线等部署方案的工作模式 |
| 应用识别 | 产品具备应用识别特征库，提供P2P下载、网络电视、即时通讯、股票软件、流媒体、网络电话、手机应用等多种应用识别类型，特征库数量不少于3000 |
| 产品具备自定义应用协议，提供除五元组之外的应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度等多项设置 |
| 安全策略 | 产品具备一体化安全策略模板功能，通过单条策略既可完成多项策略设置，可以配置源目的地址、国家地区、源目的域、源目的MAC、时间对象、用户、虚拟身份、服务对象、URL分类等对象，同时可在同一策略下，调用入侵防护、一体化防病毒、文件控制、URL过滤、数据过滤防护、威胁情报、口令检测、挂马防护、僵尸网络等应用安全策略进行安全防护 |
| 配置向导 | 产品具备配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IPS、可视、概览等多项元素实现快速配置上线**（请提供截图证明）** |
| 入侵防护 | 系统采用自主研发的基于网络的入侵检测技术，要求提供信息产业信息安全测评中心或国家知识产权局等第三方权威机构出具的证明。具备检测防逃逸技术，提供缓冲区溢出、SQL注入、扫描刺探、间谍软件、拒绝服务、病毒、木马后门、漏洞攻击、潜在风险的入侵防御特征库。 |
| IPS特征库 | 产品提供入侵防御特征库，特征数超过10000条。并提供基于正则表达式匹配方式的自定义特征策略功能**（请提供截图证明）** |
| 大屏 | 具备安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对威胁趋势图、风险主机TOP10、威胁等级 、最新入侵事件 、设备运行状态 、资源监控、告警总数等信息统计展示**（请提供截图证明）** |
| 事件取证 | 产品具备事件取证分析功能，通过获取接口的报文文件保存在设备中留存为证据，取证文件支持导出功能 |
| 能力要求（需提供证书扫描件） | 产品具有《国家信息安全测评信息技术产品安全测评证书（EAL4+级）》 |
| 产品具有中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书》 |
| 认证实训设备厂商具备国测信息安全服务资质安全工程类三级及以上证书 |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 |

* + - 1. **WAF认证模块**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 性能规格 | 网络吞吐量为≥4Gbps，≥6个10/100/1000M自适应电口，≥2组bypass，5年硬件维修服务。 |
| 产品必须为专业性WEB应用防火墙设备，而非NGAF、NGFW、UTM设备 |
| 部署模式 | 支持透明流、透明代理、反向代理，旁路镜像检测模式及旁路镜像阻断模式 |
| 支持在旁路镜像阻断模式下，可配置多组阻断以及镜像口，对检测到的攻击进行旁路阻断，并可指定对端设备MAC地址 |
| 支持路由牵引部署模式，通过路由牵引、SNT回注方式对流量进行过滤 |
| 基础防护 | 支持IPv4和IPv6双协议栈流量过滤防护 |
| 支持产品页面一键断网（禁止访问）功能，在特殊情况下，实现对特定网站的快速下线**（要求提供产品截图）** |
| 态势感知 | 支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP并发请求及实时事件的动画统计**（要求提供产品截图）** |
| 安全防御 | 支持SQL注入、XSS跨站攻击防御策略，支持特征检测与语义分析算法检测 |
| 支持Web攻击防护功能，包括命令注入攻击，组件漏洞防护、Web扫描防护、XPATH注入防护、XML注入防护、SSI注入防护、JOSN注入防护、LDAP注入防护、webshell防护 |
| 支持敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护 |
| 支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护**（要求提供产品截图）** |
| 支持会话安全防护，Cookie加固、Cookie加密、会话固定等属性设置 |
| DDoS防护 | 支持智能分析DDOS防护，内置四个防护等级，并可自定义防护等级 |
| 支持检测并清洗的攻击类型：IP攻击，TCP攻击，UDP攻击，ICMP攻击，DNS攻击，HTTP攻击等20多种DDoS攻击类型，具备防SYN泛洪攻击的防御技术，**要求提供信息产业信息安全测评中心或国家知识产权局等第三方权威机构出具的证明。** |
| 入侵防护 | 支持入侵防护功能，并提供入侵防护特征库，特征库需要提供22种类型并提供至少14000条入侵检测特征库 |
| 支持检测Web攻击类攻击，包括注入攻击、跨站脚本、Webshell、目录遍历、恶意软件、间谍软件等 |
| 威胁情报 | 支持与第三方威胁情报中心联动功能，基于FTP或FTPS协议连接登录获取数据来源 |
| 虚拟补丁 | 支持虚拟补丁功能，支持导入Appscan和SecVSS扫描器的扫描结果生成WAF的规则，对此类网站漏洞直接防护 |
| 蜜罐防护 | 支持轻量级蜜罐防御功能，提供伪造的后台管理系统页面，主动诱使黑客进行攻击，记录攻击行为**（要求提供产品截图）** |
| 智能封禁 | 支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间 |
| 流量限速 | 支持检测TCP并发链接数，TCP新建链接数，TCP带宽（c2s），UDP带宽（c2s），ICMP带宽（c2s），HTTP GET 速率，HTTP POST 速率，HTTP 其他请求速率，DNS 查询请求速率，并发IP数量等单用户和总量进行自定义阈值配置 |
| 日志系统 | 支持日志快速响应功能，日志具备一键黑名单设置以及一键白名单排除功能 |
| 支持日志综合统计分析，可对源IP、目的IP、源地域、攻击类型、级别、处理动作、协议类型、客户端设备类型、客户端操作系统、客户端浏览器类型进行综合统计分析，并通过饼图、曲线图及柱图等对分析结果进行图形化统计 |
| 移动端管理 | 支持移动端管理功能，不需要安装APP和第三方插件，通过手机浏览器即可管理设备，并可查看设备CPU、内存使用情况 |
| 支持移动端对资产的一键断网功能，提供网站一键下线以及批量下线的应急措施**（要求提供产品截图）** |
| 高可用性 | 支持双机部署，支持主/主（双组vrrp）模式、主/备防护工作模式 |
| 能力要求（需提供证书扫描件） | 产品具有《国家信息安全测评信息技术产品安全测评证书（EAL3+级）》 |
| 认证实训设备厂商为ITSS运行维护符合性证书(二级及以上)。 |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 |

* + - 1. **日志审计系统认证模块**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 系统架构 | 为满足海量日志下，复杂计算和快速检索需求，要求系统基于大数据技术即ES技术，而非关系型数据库或文本型数据库架构。 |
| 硬件规格 | 6个千兆电口，1个Console接口，4T硬盘，5年硬件维保服务。 |
| 日志采集与转发 | 支持通过Syslog、SNMP Trap、Netflow V5、ODBC/JDBC、Agent代理(Windows/Linux)、WMI、(S)FTP、文件共享(SMB、NetBIOS)、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行。 |
| 资产管理 | 支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。 |
| 支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示。 |
| 支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理 |
| 日志归一化 | 系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。 |
| 日志解析字段内置130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等15种，可选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。 |
| 支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化。支持对日志的高性能处理技术，**投标时要求提供信息产业信息安全测评中心或国家知识产权局等第三方权威机构出具的证明。** |
| 对于枚举类型的范化字段，其字典表可根据需要自定义扩展；对于原始日志的枚举字段，能够将原始的枚举值映射为系统统一的枚举值 |
| 日志交互式分析 | 系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件； |
| 可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。 |
| 能够在世界地图上实时定位事件源/目的IP地址（内网IP）的地理位置； |
| 日志综合展现 | 仪表板支持自定义创建框架，用户根据需要在框架内添加不同的仪表板组件（数值、折线、面积、柱图、饼图、环状图、地图、组件、URL、文本、图片、列表等），支持组件位置自由摆放，组件大小自由拖曳等。 |
| 能力要求（需提供证书扫描件） | 认证实训设备厂商要求具备数据安全服务能力评定资格证书-数据安全建设能力 |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 |

* + - 1. **数据库审计系统认证模块**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 硬件规格要求 | 6个千兆自适应电口，5年维保服务。 |
| 内置4TB硬盘，采用一种安全产品的硬盘减震技术，加强硬盘运行稳定性，**投标时要求提供第三方机构出具的证明或相关检测报告；** |
| 处理性能 | 峰值事件处理能力不低于10000条语句/秒，日志存储最低5亿条。 |
| 网络环境支持 | 系统可同时支持IPv4和IPv6的网络环境下数据库的审计。 |
| 审计功能 | 支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、Caché、REDIS。 |
| 旁路阻断功能（非串联方式）。阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断。 |
| 可监控发现未知仿冒进程工具访问数据库，如通过非法第三方工具连接数据库进行风险操作的行为；可监控权限滥用行为，对超出用户权限范围的操作，可根据IP、MAC等五元组实时监控 |
| 对审计记录返回内容中的敏感数据能进行隐秘处理，防止二次泄露。 |
| 支持C/S架构COM、COM+、DCOM组件的三层审计，可提取应用层工号（账号）的身份信息，精确定位到人；支持框架：tomcat、apache、weblogic、jboss |
| 全面支持后关系型数据库Cache的审计，包括terminal、portal、studio、Sqlmanager、MedTrak等工具访问的审计，Portal可审计Sql语句、查询Global变量以及二者的返回内容，Terminal可审计M语句及返回内容，MedTrak可审计工号、操作报表以及二者的返回内容，studio可审计到编译、代码更改等操作，Sqlmanager可审计数据库账号和操作的sql语句。 |
| 审计策略 | 审计策略支持18种以上分项响应条件；可支持数据库操作命令（包括select、create等14个命令）；语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间（含开始结束日期）等 |
| 审计查询 | 支持全数据库检索，检索效率高达亿条数据秒级响应。 |
| 可根据包括时间范围、风险级别、保护对象、操作类型、进程名、应用账号、关键字、规则类型、规则名、规则组名、操作系统主机名、操作系统用户名、客户端MAC、客户端端口、服务器端口、数据库名、语句长度、语句回应、语句执行时间、返回行数、返回结果、处理状态、会话ID、记录编号等二十种条件进行精细化查询。 |
| 可根据事件的时间范围、客户端IP、关键字、进程名、应用账号、规则名、客户端端口号、返回内容等多种条件进行事件回放，回溯事件过程。 |
| 支持查询结果自定义报表，支持Word、PDF、xls格式报表导出 |
| 风险评估 | 支持对指定时间段风险数据按不同维度进行统计排行，统计维度包括:风险最多的类型、触发风险最多的保护对象、触发风险最多的IP、触发风险最多数据库账户、触发风险最多应用账户、触发风险最多工具； |
| 支持对统计数据进行下钻，获取更详细的风险数据； |
| 实时监控 | 提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信系统、短信猫告警等六种方式 |
| 系统管理与防护 | 备份数据支持弹性180天的时间，可上传至FTP服务器，或者其他网络转存方式备份日志信息 |
| 能力要求（需提供证书扫描件） | 认证实训设备设备厂商具备数据安全服务能力评定资格证书（数据安全建设二级） |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 |

* + - 1. **堡垒机认证模块**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 硬件规格 | 标准1U机架式，6个千兆电口, 4个千兆SFP接口，支持1个接口扩展槽位，支持现场扩展万兆接口，支持液晶屏； |
| 内置4TB硬盘； |
| 处理性能 | 支持150路图形会话或400路字符会话并发，≥100个授权许可，≥6个千兆电口，含5年标准售后服务。 |
| 资源管理 | 支持IPv6网络环境下的运维、操作审计 |
| 支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure云平台的资源 |
| 不限操作客户端系统类型，无需安装任何客户端插件，使用H5即可直接运维windows、Linux、网络设备等资源 |
| 通过群发命令、预置命令，实现同时运维多台资源设备 |
| 运维过程中支持会话协同，可邀请其他用户参与、协助操作 |
| 自动运维 | 支持从Linux服务器推拉账户，实现堡垒机与资源服务器的账户同步 |
| 支持在页面上批量执行命令，实时查看命令和脚本的输出结果。且按执行周期，将命令、脚本、文件批量传输设置自动化运维任务。 |
| 操作记录 | 支持用户水印功能，避免数据泄露无法追责 |
| 支持对运维操作中的详细操作命令、步骤、以及双人授权、协同用户、剪切板拷贝行为进行记录，并可以通过关键字搜索定位回放，审计日志内容支持导出 |
| 访问和命令控制 | 支持访问控制策略，可配双人授权，针对核心设备需要管理员现场审批才能操作 |
| 支持对MySQL和Oracle数据库的访问操作控制，可基于库、表、命令实现对数据库操作的细粒度访问控制 |
| 会话回放 | 页面直观展示操作指令，包括原始操作命令，命令输出、并可以通过命令关键字定位播放会话视频，视频回放，支持播放速度调整、拖动、暂停、停止、跳过空闲、重新播放等操作，会话视频可下载，使用通用播放器即可播放 |
| 改密计划 | 支持自动修改资源服务器账户密码，系统类型包括Windows/Linux/Unix/Cisco/Huawei/H3C，等网络设备，数据库类型包括MySQL、Oracle、SQL Server等。 |
| 支持随机生成不同、相同密码或者手动指定密码，改密日志内容包括改密账户总数，成功、失败和未修改数量。 |
| 能力要求（需提供证书扫描件） | 产品具备国家信息安全测评信息技术产品安全测评证书EAL3+证书 |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，中标公示期间需要提供同型号的样机进行上述功能要求的逐一测试验证，全部通过后执行合同流程，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 |

* + - 1. **态势感知认证模块**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **指标要求** |
| 硬件规格 | | 吞吐≥1Gbps，6千兆网口，1T 硬盘，5年标准维保服务 |
| 流量采集 | 网络协议 | 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs、ICMP、SSL、SSH等 |
| 文件协议 | 支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk、bin等）、压缩格式文件（RAR、ZIP、GZ、7Z、tar等）、文档类型文件（word、excel、pdf、rtf、ppt、txt等）、多媒体文件（flash、jpg、jpeg、png、flv、swf等）、脚本文件（html、htm、java、mhtml、mht等）等类型。 |
| 威胁检测 | 威胁情报 | 支持基于流量实时IOC匹配功能，设备具备主流的IOC，情报总量500+万条 |
| Web攻击检测 | 支持检测针对WEB应用的攻击，如SQL注入、XSS、系统配置等注入型攻击； |
| Webshell攻击检测 | 支持基于工具特征的WEBSHELL检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等 |
| 网络攻击检测 | 支持多种攻击检测，能更全面的从流量中发现威胁，如：SQL注入、XSS、信息泄露、间谍软件、协议异常、网络欺骗、黑市工具、代码执行、挖矿等 |
| 威胁情报检测 | 支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件 |
| 威胁检测 | 情报查询 | 支持与云端威胁情报中心联动，可对受害IP、攻击IP、IOC/规则ID、文件MD5进行一键搜索，查看基本信息、开源情报、相关样本、可视化分析、域名解析、注册信息、关联域名、数字证书等。 |
| 行为分析 | 支持告警的深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为。 |
| 检测能力扩展 | 支持根据攻击载荷自定义漏洞检测规则，可自定义载荷检测位置、检测字段、匹配方式（文本匹配/正则匹配）、匹配载荷内容，并且单条规则可指定多个检查项，同时可定义漏洞威胁级别、威胁分类、攻击结果、CVE编号、CNNVD编号、漏洞描述、漏洞危害、解决方案。为了保证在认证实训过程中可以更好体验漏洞挖掘和威胁检测的深度，**要求认证实训设备厂商需具备CNNVD颁发的高质量通报优秀贡献单位，并在投标文件中提供相关证明。** |
| 威胁检测 | 高级威胁检测 | 具备AI隧道检测、非TCP完整流、畸形包检测、数据包完整性检测、碎片重组检测、编码绕过检测、高级逃逸 AET 检测等防逃逸检测能力。 |
| 策略配置 | 文件还原 | 支持对HTTP、FTP\_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS等类型协议的流量进行文件还原 |
| 抓包分析 | 支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、IP地址、端口或协议类型 |
| 旁路阻断 | 支持基于攻击特征的旁路阻断;  支持基于URL、GET参数、POST参数、XFF、HOST等高级参数的旁路阻断;  支持基于IP地址的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断; |
| HTTPS威胁检测 | 支持旁路HTTPS解密、威胁检测 |
| 能力要求（需提供证书扫描件） | 具备IT产品信息安全认证证书，有“APT安全监测产品”字样 | |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 | |
| 产品测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 | |

* + - 1. **网络准入控制认证模块**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **指标要求** |
| 技术性能 | 硬件规格 | 含300个准入授权，6个千兆电口，4TB 硬盘，含5质保服务 |
| 部署方式及管理 | 管理架构 | 系统控制中心采用B/S架构，支持管理员分区分权管理模式，灵活配置管理权限，适应大型分级管理组织架构 |
| 集中管理 | 支持设备集中管理，可在同一管理平台集中管理所有设备，支持设备分组，权限管理，实现分布式部署、集中管理，满足大型网络环境下的部署要求。 |
| 流量复制 | 设备支持将收到的镜像流量做过滤并将镜像流量复制一份输出给其他流量监测类设备。**(提供功能截图证明)** |
| 准入控制 | 准入技术 | 产品支持多种认证控制方式，支持802.1x、portal、DHCP、MAB MAC、策略路由、旁路镜像、WebAuth等方式，支持无线和有线环境下的接入控制，适应复杂网络环境下的接入控制 |
| 引导部署 | 检测是否安装客户端，达到入网遵从条件，保障入网终端是安全可信的，未安装客户端的终端禁止访问，将被重定向到客户端安装页面快速引导部署；针对未认证或不合规的设备，当终端访问http、https网站时，支持对其网站访问重定向至引导页面进行身份认证或修复。 |
| 身份认证 | 支持使用客户端或portal方式进行设备身份认证，只有合法的用户才可接入网络 |
| 用户管理 | 系统内置用户身份管理系统，支持创建、导入或从第三方系统同步用户身份信息，以便进行身份认证、权限设置等操作 |
| 第三方认证源 | 支持LDAP、Email、Http认证源三种认证源配置，支持第三方认证源的高可用配置；支持在不修改第三方认证源中用户信息的前提下，临时限制特定账号的入网认证请求。 |
| 设备身份认证源 | 支持基于终端身份标识的设备身份验证方式；支持同时校验用户身份和设备身份的双重认证。 |
| NAT精度控制入网 | 通过小路由、VPN等场景接入的经过NAT转换后的终端必须安装客户端并经过身份认证后方可接入网络**(提供功能截图证明)** |
| 访问授权 | 动态授权 | 可基于用户、角色、设备类型、设备分组、设备标签、终端安检结果等动态下发VLAN、acl或厂家属性**(提供功能截图证明)** |
| 动态ACL | 支持基于不同设备类型定义访问控制规则，特定类型的设备仅允许访问指定的关键服务器，并只允许合法的协议通过  支持基于终端使用用户的用户组、用户角色定义访问控制策略，无论用户使用什么设备还是IP，均可执行对应的访问控制策略 |
| 合规检查（Windows客户端） | 客户端软件 | 基于不同用户规模与需求，提供轻量级准入客户端和终端安全一体化客户端的不同方案，支持Windows、Linux、信创操作系统 |
| 全静默认证 | 支持全静默的终端身份认证，无需人工参与，终端即可自动完成准入认证，整个过程无弹窗，不影响全屏进程。**(提供功能截图证明)** |
| 合规检查 | 支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络。 |
| 隔离处置 | 支持终端安全检查失败处置措施，可基于协议、特定端口、端口范围、特定地址、IP范围、URL来控制终端访问权限，从而无需操作交换机达到终端网络隔离目的，实现细粒度的访问控制管理 |
| 引导修复 | 支持对不合规的终端提供软隔离，不符合安全策略的计算机终端进行友好提示，提供终端修复向导，需支持引导修复和一键修复功能，并支持不同区域终端的修复区域定义。 |
| 进程检查 | 支持对终端所安装的软件、服务、进程检查，设置黑白名单，管理员可以自己编辑黑白名单，可以对进程进行签名校验，文件MD5检查，版本比较，并提供设定的下载链接引导安装 |
| 域检查 | 支持检查终端用户是否加入AD域，当前用户是否登录域，并能与AD域进行联动认证，便于用户统一管理 |
| 系统联动 | 数据输出 | 对外提供设备信息、资产信息、设备入网状态、设备合规状态API查询接口 |
| 准入联动 | 支持与流量分析软件、威胁情报分析平台等第三方安全分析系统联动，对于第三方平台发现的风险终端，提供准入阻断的能力 |
| 单点登录联动 | 准入认证用户数据支持与奇安信、深信服等主流上网行为管理联动身份认证数据，无需重复认证 |
| 能力要求（需提供证书扫描件） | | 具备IPv6 Ready Logo（Phase-2） |
| 认证实训设备厂商具备培养国内网络安全人才的能力，具有中国信息安全测评中心授权的CISP培训资格，**提供证明材料** |
| 服务 | | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品测试 | | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备过程中无法实现所需的功能，采购方保留产品功能测试的权利，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为，采购人有权要求中标方退回预付款，同时终止合同，并追求其责任。 |

* + - 1. **核心交换机**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **指标要求** |
| 技术性能 | 硬件规格 | 1. 一体化总装机箱； 2. 主控板\*2,交流电源\*2，48千兆光口\*1,48千兆电口\*1； 3. 交换容量：≥76.8/336Tbps，包转发率：≥57600Mpps； 4. 业务槽位数≥6，支持模块化风扇框，可热插拔，独立风扇框数≥2,支持颗粒化电源，电源槽位数：4，支持独立的硬件监控板卡, 控制平面和监控平面物理槽位分离，支持 1+1 备份，能集中监控风扇、电源等模块，能调节能耗； 5. 含原厂15对万兆多模光模块； 6. 含5年质保服务 |

* + - 1. **汇聚交换机**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **指标要求** |
| 技术性能 | 硬件规格 | 1. 包转发率：≥207Mpps； 2. 交换容量：≥672Gbps/6.72Tbps； 3. 固定端口：48 个 10/100/1000BASE-T 以太网端口，4 个万兆 SFP+，2 个专用堆叠口； 4. 电源模块支持1+1备份； 5. 支持静态路由、RIPv1/2、RIPng、OSPF、OSPFv3、ECMP、ISIS、ISISv6、BGP、BGP4+ ； 6. 双电源； 7. 含5年质保服务； |

* + - 1. **网络机柜**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **指标要求** |
| 技术性能 | 硬件规格 | 1. 尺寸：≥600\*1200\*2000mm； 2. 高密度平板通风孔单开前门及双开后门，扁六角通风孔设计，通风率至少达80%，具有最佳的自然空气流量，特别适合于装入服务 ； 3. 具有最佳的自然空气流量，特别适合于装入服务器等有源设备，有效解决服务器散热，机械防护，外部观察机器运行状态等问题 ； 4. 前后焊接框架拼装机柜，静载承重可达1300KG ； 5. 顶部前后、底部前后左右采用敲落孔设计，进线位置灵活 ； 6. 快开侧板,开启方便灵活 ； 7. 角规镀锌，主要部件预置接地铜柱，可快速形成机柜接地系统； 8. 加宽托盘设计，兼容所有主流服务器安装 ； 9. 可方便安装竖向PDU电源分配单元和走线板，800宽机柜可加装2000MM深超大容量带盖金属线槽； 10. 符合标准QNSI/EIQ RS-310-D,IEC297-2,DIN41491:PART1,DIN41491:PART7,GB/T3047.2-97ZN； 含同品牌PDU\*2（左右布置）；额定值：32A250VAC;输出：12位10A、4位16A国标三孔插座;带开关，防雷，接线盒，电源指示灯; 11. 含5年质保服务 |

**(四)系统集成**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 系统集成要求 | 1、本项目所提供的软、硬件产品按招标方的要求采购、集成、调试。  2、目实施期间发生的所有劳务支出、安全保险、住宿、运输、税金等一切费用都已包含在竞投报价中，由中标方自行负责。  3、中标方须提供实施7\*24小时技术支持。 |

**四、商务需求**

|  |  |
| --- | --- |
| 付款条件 | 合同签订后，甲方（台州学院，以下简称甲方）向乙方（中标供应商，以下简称乙方）支付50%的合同款项作为预付款；采购的货物到位后，乙方安装调试完成，经台州学院该项目验收小组组织验收，验收合格后，在乙方票证齐全，且符合甲方付款流程的前提下，甲方一次性付清剩余款项。 |
| 质保期 | （1）质保期： 5 年及以上； |
| 售后技术服务要求 | （1）合同生效后，制造商（或代理商）对安装产品的实验室工作条件应提出具体要求，并在安装前予以确认。  （2）提供的产品须为原装正品，相关的配套附件质量优良，数量齐全，并在标书中注明可选配件的价格。  （3）产品到达用户指定交货地点后，根据用户的时间安排，制造商（或代理商）在接到用户通知后30天内进行安装调试，直至通过验收。  （4）产品安装调试合格后，制造商（或代理商）负责对用户技术人员（至少2人）进行免费现场培训，培训内容包括产品的原理、操作、保养和维护等，培训日程视实际情况另定。  （5）质保期过后，制造商（或代理商）对产品提供终身维修服务，能提供广泛、即时、优惠的技术服务，并提供质量上乘、价格合理的各种配件。  （6）在国内有维修中心，有专职维修工程师和备品备件库。质保期内如有问题接电后2小时内给与答复，24小时内派员赶赴现场予以解决。质保期外，制造商（或代理商）应在4小时内作出响应，2个工作日内到达用户现场维修，一般故障应在24小时内修复，重大故障应在72小时内修复。  （8）制造商（或代理商）终身免费提供应用咨询及技术帮助，质保期内，易损件和外购件根据原厂家质保期和国家质保标准保修，属人为因素酌情收取材料费。质保期外实行有偿服务。 |
| 交货时间  及地点 | 时间：合同签订后30日历天内交货  地点：台州学院椒江校区 |

**五、相关说明**

**1、现场勘察：**无

**2**、▲所有软件和设备均采用人民币报价。本项目的成交报价应包含（但不限于）所有软硬件货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用。

**第六部分 拟签订的合同文本**

台州学院

\*\*\*\*\*\*\*\*\*\*项目

货物购买合同

甲方（采购人）： 台州学院

乙方（中标供应商）：

2024年\*\*月

项目名称：\*\*\*\*\*\*\*\*\*\*\*\*

项目编号：\*\*\*\*\*\*\*\*\*\*\*\*

标段信息：\*\*\*\*\*

甲方：（采购人）台州学院

所在地：浙江台州

乙方：（中标供应商）\*\*\*\*\*\*\*\*\*\*\*\*

所在地： \*\*\*\*\*\*\*\*\*\*\*\*

甲、乙双方根据台州学院关于 项目公开招标的结果，签署本合同。

一、货物内容及合同价格

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 品牌、产地 | 型号规格 | 数量 | 单价（元） | 总价（元） |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 合计： | | | | | |  |
| 合同总价（人民币大写）： | | | | | | |

注：1.以上货物内容不清楚的详见采购文件或附件清单。

2.以上合同总价包含货物送达用户并能正常使用所需的一切费用。

二、技术资料

1.乙方应按采购文件规定的时间向甲方提供使用货物的有关技术资料。

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。

三、知识产权

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。如果任何第三方向甲方提起侵权索赔，乙方应负责与之进行交涉，造成甲方损失的后果均由乙方承担。

四、产权担保

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等权利瑕疵，否则由乙方承担全部责任。

五、转包或分包

1.本合同范围的货物，应由乙方直接供应，不得转让他人供应；

2.除非得到甲方的书面同意，乙方不得将本合同范围的货物全部或部分分包给他人供应；

3.如有转让和未经甲方同意的分包行为，甲方有权解除合同，并追究乙方的违约责任。

六、质保期

质保期为 年。

七、交货时间、交货方式及交货地点

1.交货时间： 交货；

2.交货方式： ，运费、装卸费由乙方负责；

3.交货地点： 。

八、货款支付

1.付款方式。合同签订后，甲方向乙方支付50%的合同款项作为预付款；乙方设备安装调试完成，经台州学院该项目验收小组组织验收，验收合格后，在乙方票证齐全，且符合甲方付款流程的前提下，甲方一次性付清剩余款项。否则甲方有权拒绝付款，不视为违约。

2.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。

3.因进口货物无法办理免税手续的，甲方可以解除该货物的采购合同，并应当及时通知乙方，因此造成的损失由乙方承担。

九、税费

本合同执行中相关的一切税费均由乙方负担。

十、质量保证及售后服务

1.乙方应按采购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原装正品。

2.乙方提供的货物在质保期内非因人为原因发生故障，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，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶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）。

上述三种方式如协商不成，甲方有权直接自行选择上述三项处理方式任一项进行处理，乙方不得异议。

3.质保期内如在使用过程中发生质量问题，乙方在接到甲方通知后 小时内给与答复， 小时内派员赶赴现场予以解决。否则，应按每次500元支付甲方违约金。同一质量问题，如修理超过3次，甲方有权提出更换商品，乙方必须更换。否则，甲方因此支出的全部费用由乙方承担。质保期外，乙方应在 小时内作出响应， 个工作日内到达甲方现场维修，一般故障应在 小时内修复，重大故障应在 小时内修复。

4.在质保期内，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及责任。质保期过后，乙方提供终身维修服务，能提供广泛、即时、优惠的技术服务，并提供质量上乘、价格合理的各种配件。乙方保证供应货物质保期后3年内所需的备品、备件，并给出详细清单（品名、货号、生产厂家、数量、价格等）。

5.乙方终身免费提供应用咨询及技术帮助，质保期内，易损件和外购件根据原厂家质保期和国家质保标准保修，因人为因素出现的故障酌情收取材料费；质保期外实行有偿服务。

十一、调试和验收

1.甲方对乙方提交的货物依据采购文件上的技术规格要求和国家有关质量标准进行现场初步验收，外观、说明书符合采购文件技术要求的，给予签收，初步验收不合格的不予签收。

2.乙方交货前应对产品做出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3.乙方对安装仪器的实验室工作条件应提出具体要求，并在安装前予以确认。

4.货物到达甲方指定交货地点后，根据甲方的时间安排，乙方在接到甲方通知后 天内进行安装调试，直到符合技术要求，甲方才做最终验收。安装调试合格后，乙方负责对甲方技术人员（至少2人）进行免费现场培训，培训内容包括仪器的性能、原理、操作、保养和维护等，培训日程视实际情况另定。

5.对技术复杂的货物，甲方可请国家认可的专业检测机构参与初步验收及最终验收，并由其出具质量检测报告。

6.验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由乙方负责。如乙方拒不到场，视为其同意甲方之验收结果并不得异议。

7.因乙方人员在合同履行过程中造成甲方或其自身人身或财产损害，由乙方承担全部责任。

十二、货物包装、发运及运输

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。

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。

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。

4.货物在交付甲方前发生的风险均由乙方负责。

5.货物在约定的交付期限内由乙方送达甲方指定的地点，乙方同时需通知甲方货物已送达，并与甲方工作人员办理交接手续，否则视为未交付。

十三、违约责任

1.甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

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

3.乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，甲方可直接从待付货款中扣除。乙方逾期超过约定日期10个工作日不能交货的或有其他违约行为的，甲方有权解除合同，预付款返还甲方，并且乙方应向甲方支付合同总价20%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4.乙方所交的货物品种、型号、规格、技术参数、质量不符合合同约定及采购文件规定标准的，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，预付款返还甲方，并向甲方支付合同总价20%的违约金，如造成甲方的损失超过违约金的，乙方理应继续承担赔偿责任。

5.若发生纠纷，由违约方赔偿守约方因纠纷所支付的费用（包括但不限于律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）。

十四、不可抗力

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。

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。

3.不可抗力事件延续60天以上，双方应通过友好协商，确定是否继续履行合同。

十五、解决合同纠纷方式

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，依法向甲方所在地人民法院提起诉讼。

十六、合同生效及其它

1.合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2.本合同未尽事宜，遵照《民法典》及有关规定执行。

3.本合同一式柒份，甲方执伍份、乙方执贰份。本项目未尽事宜以采购文件、投标文件及澄清文件等为准。

甲方（公章）台州学院 乙方（公章）

法定代表人： 法定代表人：

委托代理人： 委托代理人：

联系电话：0576-88660896 联系电话：

开户银行：建行台州市分行 开户银行：

账号：33050166350000000852 账号：

地址：台州市椒江区市府大道1139号 地址：

签订时间： 2024年 月 日

**第七部分 格式与表格**

项目名称

**项目编号：**

投

标

文

件

（资格证明文件）

投标人名称（公章）：

投标人地址：

时 间：

**资格证明文件**

**目录**

1、符合参加政府采购活动应当具备的一般条件的承诺函………………………………（页码）

2、法人或者其他组织的营业执照等证明文件，自然人的身份证明……………………（页码）

3、本项目的特定资格要求（如果有，提供采购公告中符合供应商特定条件的有效资质证书扫描件)，以及供应商认为有必要提供的其他资格证明资料………………………………（页码）

………( 目录自行扩展)

**一、符合参加政府采购活动应当具备的一般条件的承诺函**

（采购人）、（采购代理机构）：

我方参与（项目名称）【招标编号：（采购编号）】政府采购活动，郑重承诺：

（一）具备《中华人民共和国政府采购法》第二十二条第一款规定的条件：

1、具有独立承担民事责任的能力（如投标人为金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构，以及个体工商户、个人独资企业、合伙企业，已经依法办理了工商、税务和社保登记手续，并且获得总公司（总机构）授权或能够提供房产权证或其他有效财产资料，承诺具备实际承担责任的能力和法定的缔结合同能力，可以独立参加政府采购活动）；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必需的设备和专业技术能力；

4、有依法缴纳税收和社会保障资金的良好记录；

5、参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6、具有法律、行政法规规定的其他条件。

（二）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、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

（三）不存在以下情况：

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参加同一合同项下的政府采购活动的；

2、为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后再参加该采购项目的其他采购活动的。

投标人名称（盖公章）：

法定代表人或授权委托代理人（签字或盖章）：

日期： 年 月 日

**二、法人或者其他组织的营业执照等证明文件，自然人的身份证明**

**三、本项目的特定资格要求，以及供应商认为有必要提供的其他资格证明资料**

（根据招标公告本项目的特定资格要求提供相应的材料；未要求的，无需提供）

（供应商认为有必要提供的其他资格证明资料，如果有，可提供）

项目名称

项目编号：

投

标

文

件

（商务与技术文件**）**

投标人名称（公章）：

投标人地址：

时 间：

**技术商务文件**

**目录**

1、商务技术自评表…………………………………………………………………………（页码）

2、投标函……………………………………………………………………………………（页码）

3、授权委托书或法定代表人身份证明……………………………………………………（页码）

4、供应商基本情况表………………………………………………………………………（页码）

5、供货清单………………………………………………………………………………（页码）

6、技术规范偏离表…………………………………………………………………………（页码）

7、商务偏离表………………………………………………………………………………（页码）

8、相关项目实施业绩一览表………………………………………………………………（页码）

9、供货方案…………………………………………………………………………………（页码）

10、评分标准或采购文件需要提供的其他技术商务材料…………………………………（页码）

11、供应商认为有必要提供的其他技术商务文件资料……………………………………（页码）

......( 目录自行扩展)

1. **商务技术自评表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **评审项目** | **评审细则** | **分值** | **自评分** | **投标文件对应页码** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**二、投标函**

致： （采购人）

（供应商全称） 授权 （被授权人姓名、职务） 为本公司合法代理人，参加贵方组织的 （项目编号、项目名称） 招投标活动，代表本公司处理招投标活动中的一切事宜。在此：

1、提供采购文件中“投标须知”规定的全部投标文件资料。

2、据此函，签字代表宣布并承诺如下：

（1）我们已详细审查全部“采购文件”，包括修改文件（如有）以及全部参考资料和有关附件，我们完全理解并同意放弃对这方面提出任何异议的权利。已经了解对于采购文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及相关渠道和要求。

（2）本投标自开标之日起90天内有效。

（3）保证遵守采购文件有关条款规定。

（4）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。保证在中标后按照采购文件的规定支付招标代理服务费。

（5）承诺应贵方要求提供任何与该项目投标有关的数据、情况和技术资料。

3、我们郑重声明：

我公司符合政府采购法规定的参加采购活动应当具备的条件：具有独立承担民事责任的能力；具有良好的商业信誉和健全的财务会计制度；具有履行合同所必需的设备和专业技术能力；有依法缴纳税收和社会保障资金的良好记录；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；法律行政法规规定的其他条件。

4、与本投标有关的一切往来通讯请寄：

地址：

邮编：电话：传真：

投标人名称（盖公章）：

法定代表人或授权委托代理人（签字或盖章）：

日期：年 月 日

**三、授权委托书或法定代表人身份证明**

**授权委托书(格式)**

本授权委托书声明：我 (填写姓名)系 （填写投标人单位全称）的法定代表人，现授权委托 （填写单位全称）的（填写姓名）为我公司授权代表，（填写身份证号码： ）。以本公司的名义参加 组织的 投标活动。授权代表在开标、评标、合同谈判过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

在撤销授权的书面通知以前，本授权书一直有效。全权代表在授权书有效期内签署的所有文件不因授权的撤销而失效。

授权代表无转委托权。特此委托。

授权代表姓名： 性别： 年龄：

单位： 部门： 职务：

办公地址： 联系电话： 传真：

供应商名称（电子签章）：

法定代表人（签字或盖章）：

**法定代表人及其授权代表身份证扫描件（正反面）**

日期： 年 月 日

**法定代表人身份证明(格式)**

投 标 人：

地 址：

姓 名：

身份证号码：

职 务：

系 （填写投标人名称）的法定代表人。

特此证明。

供应商名称（电子签章）：

日期：年 月 日

**法定代表人身份证扫描件（正反面）**

**四、供应商基本情况表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 单位名称 |  | | | 组织机构代码 |  |
| 注册地址 |  | | | 注册登记号 |  |
| 经营地址 |  | | | 税务登记证号 |  |
| 单位性质 |  | | | 注册资本 |  |
| 经营范围 |  | | | 营业期限 | 年 月- 年 月 |
| 资质情况 |  | | | | |
| 员工数量 | 共人，其中，高级职称人，中级职称人 | | | | |
| 联系电话 |  | | | 传真 |  |
| 主要业绩 |  | | | | |
| 法 定 代 表 人 基 本 情 况 | | | | | |
| 姓 名 |  | | | 身份证号码 |  |
| 职 务 |  | 职 称 |  | 学 历 |  |
| 备注： | | | | | |

**兹证明上述声明是真实、正确的，并提供了全部能提供的资料和数据，我们同意遵照贵方要求出示有关证明文件。**

投标人名称（盖公章）：

法定代表人或授权委托代理人（签字或盖章）：

日期： 年 月 日

**五、供货清单**

项目编号：

项目名称：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **品牌** | **规格型号** | **产地** | **数量** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**要求：**

1. 本表参照本采购文件第五部分“采购内容及要求”内容填制。
2. 在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

投标人名称（盖章）：

法定代表人或授权委托人(签字或盖章)：

日 期：2024年 月 日

**六、技术规范偏离表**

项目编号： 项目名称：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 《采购文件》中的技术要求 | 《投标文件》技术条款响应 | 说明 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 | …… |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| …… |  |  |  |

备注：

1、列明采购文件的技术要求与投标文件对应响应，并说明偏离状况（正偏离或负偏离）；

2、无偏离应在本表“说明”处醒目地注明“无条款偏离”的字样。

3、本表格供参考，投标人可根据项目实际情况自拟（增减）表格。

投标人名称（盖公章）：

法定代表人或授权委托代理人（签字或盖章）：

日期： 年 月 日

**七、商务偏离表**

项目编号： 项目名称：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 《采购文件》商务条款要求 | 《投标文件》商务条款响应 | 说明 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| …… |  |  |  |

备注：

1、列明采购文件的商务要求与投标文件对应响应，并说明偏离状况（正偏离或负偏离）；

2、无偏离应在本表“说明”处醒目地注明“无条款偏离”的字样。

3、本表格供参考，投标人可根据项目实际情况自拟（增减）表格。

投标人名称（盖公章）：

法定代表人或授权委托代理人（签字或盖章）：

日期： 年 月 日

**八、相关项目实施业绩一览表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 采购单位名称 | 合同金额 | 合同签订  时间 | 联系人/电话 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| … |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**注：需按评分标准要求附项目证明材料。**

投标人名称（盖公章）：

法定代表人或授权委托代理人（签字或盖章）：

日期： 年 月 日

项目名称

项目编号：

**报**

**价**

**文**

**件**

（报价文件）

投标人名称（公章）：

投标人地址：

时 间：

**报价文件**

**目录**

1. 开标一览表…………………………………………………………………………（页码）
2. 报价明细表…………………………………………………………………………（页码）

3、中小企业声明函（如有，可提供）………………………………………………（页码）

4、投标人认为需提交的其他报价文件资料…………………………………………（页码）

………( 目录自行扩展)

**一、开标一览表**

项目编号： 项目名称：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 采购内容 | 内容 | 备注 |
| 1 | 投标总价 | 大写： |  |
| 小写： |
| 合同履行期限 | |  | |

填报要求：

1.报价一经涂改，应在涂改处加盖单位公章或者由法定代表人或授权委托人签字或盖章，否则其投标作无效标处理；

2.投标报价应是采购文件所确定的招标范围内全部工作内容的价格表现。其应包含实现标书的所有功能，采购人不再另外增加费用，其应包括货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用。

投标人名称（盖公章）：

法定代表人或代理人（签字或盖章）：

日 期：

**二、报价明细表**

**项目编号: 项目名称：**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称**  **（采购标的）** | **制造商名称（全称）** | **是否是中小微企业** | **品牌、产地**  **（如有）** | **型号和规格** | **数量** | **单位** | **单价** | **总价** |
| 1 |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |
| 合计大写（人民币）： | | | | | | | | | ¥ |

1. 此表的合计总价应与开标一览表中投标报价总价一致。
2. 投标人需按本表格式填写，如无对应内容，则填写：“无或/”。

投标人名称（盖公章）：

法定代表人或代理人（签字或盖章）：

日 期：

**三、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（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. 虚拟化防火墙 ，属于（工业）行业；制造商为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元①，属于 （中型企业、小型企业、微型企业）；

2. 虚拟化上网行为管理 ，属于（工业）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。

供应商名称（电子签名）：

日期： 年 月 日

**注：**

**1.填写要求：①“标的名称”、“采购文件中明确的所属行业”依据招标文件第二部分供应商须知前附表中“采购标的对应的中小企业划分标准所属行业”填写，不得缺漏；②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；③中型企业、小型企业、微型企业等3种企业类型，结合以上数据，依据《中小企业划型标准规定》（工信部联企业〔2011〕300号）和《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》和《中国人民银行中国银行业监督管理委员会中国证券监督管理委员会中国保险监督管理委员会国家统计局关于印发〈金融业企业划型标准规定〉的通知》中的企业划型标准进行填报（**如国家颁布新的企业划型标准，则按最新标准执行。**）；④供应商提供的《中小企业声明函》与实际情况不符的或者未按以上要求填写的，中小企业声明函无效，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。**

**附件：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，且本单位参加\_（采购人）\_单位的\_（项目名称）\_\_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。

供应商名称（电子签名）：

日 期：

**(参加本项目采购活动的供应商须填写“政府采购活动现场确认声明书”，并在开标后30分钟内将扫描件发送至代理机构邮箱[zgtzfgs@163.com](mailto:zgtzfgs@163.com))**

**政府采购活动现场确认声明书**

中冠工程管理咨询有限公司：

本人经由（单位）法人代表（负责人）（姓名）合法授权参加项目（编号：）政府采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

1. 本单位与采购人之间□不存在利害关系□存在下列利害关系：

A.投资关系 B.行政隶属关系 C.业务指导关系

D.其他可能影响采购公正的利害关系（如有，请如实说明）。

二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位□与其他所有供应商之间均不存在利害关系□与 （供应商名称）之间存在下列利害关系：

A.法定代表人或负责人或实际控制人是同一人；

B.法定代表人或负责人或实际控制人是夫妻关系；

C.法定代表人或负责人或实际控制人是直系血亲关系；

D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系；

E.法定代表人或负责人或实际控制人存在近姻亲关系；

F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系；

G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况；

H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入50%以上）或重要财务往来关系（如融资）等其他实质性控制关系；

I.其他利害关系情况。

1. 现已清楚知道并严格遵守政府采购法律法规和现场纪律。
2. 我发现供应商 之间存在或可能存在上述第二条第项利害关系。

（供应商代表签名）：