

**政府采购**

**竞争性磋商文件**

**（电子招投标方式）**

项目编号： tzya2025-tz37

**采购项目：**信息安全运维服务项目

**采 购 人：**台州市中级人民法院

**采购代理机构：**台州永安工程咨询有限公司

二○二五年七月

**目 录**

1. **竞争性磋商公告**
2. **供应商须知**
3. **评审办法及评审标准**
4. **项目需求**
5. **政府采购合同主要条款**
6. **响应文件格式附件**

**第一章 竞争性磋商公告**

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》和《政府采购竞争性磋商采购方式管理暂行办法》等有关规定, 受**台州市中级人民法院**委托，现就其**信息安全运维服务项目**进行竞争性磋商采购，欢迎合格供应商前来磋商。

**一、项目编号：tzya2025-tz37**

**二、磋商内容：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **简要技术要求** | **数量** | **单位** | **预算**  **（万元）** | **最高限价（万元）** | **备注** |
| 1 | 信息安全运维服务项目 | 详见项目需求 | 1 | 项 | 67 | 66.8 |  |

**本项目采用“电子交易”的方式提交磋商响应文件（还可以提供备份磋商响应文件），请各供应商按照要求进行。**

**三、合格磋商供应商的资格条件：**

**（一）符合《中华人民共和国政府采购法》第二十二条及其他法律、行政法规规定的对投标主体的要求；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。**

**（二）本项目供应商特定资格要求**

**1、本项目不接受联合体投标。**

**（三）法律、行政法规规定的其他条件：单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加同一项目磋商；为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参与本项目磋商。（联合体参与磋商的，联合体各方均须满足该条款。）电子交易平台运营机构，以及与该机构有直接控股或者管理关系可能影响采购公正性的任何单位和个人，不得在该平台进行的政府采购项目电子交易中投标、响应和代理政府采购项目。**

**四、采购文件获取的方式、时间:**

**1、本项目采购文件实行“浙江政府采购网”（http://zfcg.czt.zj.gov.cn）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“浙江政府采购网”的账号注册。**

**2、获取方式：潜在供应商登录政府采购云平台，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，本项目采购文件不收取工本费；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）；**

**3、获取（公告）时间**：自本公告发布之日起至投标文件递交截止时间止；

4、**供应商网上报名操作指南：“浙江政府采购网-办事指南-省采中心-网上报名”（http://zfcg.czt.zj.gov.cn/bs\_other/2018-03-30/12002.html）。**

**5、供应商获取采购文件时须提交的文件资料：无；**

**6、提示：竞争性磋商公告附件内的采购文件（或采购需求）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，如未在“政府采购云平台”系统内完成相关流程，引起的投标无效责任自负。**

**五、招标答疑会**

无

**六、响应文件递交截止时间及磋商开始时间、地点：**

**1、递交磋商响应文件截止时间与地点**：2025年 月 日上午09:00整，地点：通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应

**2、磋商时间及地点**：2025年 月 日上午09:00整，地点：通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应

**3、解密截止时间**：2025年 月 日上午09:30整

**七、在线投标响应（电子投标）说明**

**1、本项目通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应（电子投标），供应商应先安装“政采云电子投标客户端”，并按照本采购文件和“政府采购云平台”的要求，通过“政采云电子投标客户端”编制并加密磋商响应文件。**▲**供应商未按规定加密的磋商响应文件，“政府采购云平台”将予以拒收。**

**“政采云电子投标客户端”请自行前往“浙江政府采购网-下载专区-电子交易客户端”进行下载；电子投标具体操作流程详见《供应商项目采购-电子招投标操作指南》；通过“政府采购云平台”参与在线投标时如遇平台技术问题详询95763。**

1. **为确保网上操作合法、有效和安全，投标供应商应当在提交磋商文件截止时间前完成在“政府采购云平台”的身份认证，确保在电子投标过程中能够对相关数据电文进行加密和使用电子签章。使用“政采云电子投标客户端”需要提前申领CA数字证书，申领流程请自行前往“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](http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12945.html" \o "CA驱动和申领流程)”进行查阅；**

**3、供应商通过政府采购云平台电子投标工具制作磋商响应文件，电子投标工具请供应商自行前往浙江省政府采购网下载并安装，（下载网址：https://zfcg.czt.zj.gov.cn/bidClientTemplate/2021-11-01/12975.html?utm=web-government-front.a2eab82.0.0.19c58540c14611ed94855fb6758c26ac），电子投标具体流程文档详见网址：[https://service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHx](https://service.zcygov.cn/" \l "/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHx)**

**lNdQ8Na?keyword=%E6%8A%95%E6%A0%87。**

**▲4、投标供应商应当在提交磋商文件截止时间前，将生成的“电子加密磋商响应文件”上传递交至“政府采购云平台”。提交磋商文件截止时间前可以补充、修改或者撤回电子投标响应文件。补充或者修改电子投标响应文件的，应当先行撤回原文件，补充、修改后重新传输递交。提交磋商文件截止时间前未完成传输的，视为撤回磋商响应文件。**

**5、供应商同时还可以提供经政采云平台加密处理的、以介质（U盘）存储的数据电文形式的备份磋商响应文件（不强制要求，未递交备份磋商响应文件的风险由供应商自行承担）。备份磋商响应文件应当在磋商截止时间前送达并按要求密封（备份磋商响应文件在密封袋的封口处应有磋商供应商公章或磋商授权委托代理人签字。封皮上写明项目编号、标段、招标项目名称、供应商名称，并注明“备份磋商响应文件”、“磋商时启封”字样）并建议采用顺丰邮寄（或直接递交）到台州市椒江区中环世纪6幢801室（交通银行台州分行楼上）收件人：俞雅琪；联系电话：15757696186，逾期寄达、到付或未按要求密封将被拒收。**

**6、▲通过“政府采购云平台”上传递交的“电子加密磋商响应文件”无法按时解密，投标供应商递交了备份磋商响应文件的，以备份磋商响应文件为依据，否则视为磋商响应文件撤回。通过“政府采购云平台”上传递交的“电子加密磋商响应文件”已按时解密的，“备份磋商响应文件”自动失效。▲磋商供应商仅递交备份磋商响应文件的，投标无效。**

**7、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，享受本办法规定的中小企业扶持政策： ①在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标； ②在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业； ③在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》 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，不享受本办法规定的中 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。**

**八、供应商信用信息查询渠道及截止时点、信用信息查询记录和证据留存的具体方式、信用信息的使用规则：**

1、查询渠道：“信用中国”（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）、“浙江政府采购网（www.zjzfcg.gov.cn）。

2、信用信息查询的截止时点：开标后评标前。

3、信用信息查询记录和证据留存的具体方式：由采购代理机构在规定查询时间内打印信用信息查询记录并归入项目档案。

4、信用信息的使用规则：对列入失信被执行人、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及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将被拒绝其参与政府采购活动。

**九、相关注意事项：**

1、《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》 (浙财采监〔2022〕3号)、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》(浙财采监〔2021〕22号))、《浙江省财政厅关于进一步加大政府采购支持中小企业力度助力扎实稳住经济的通知》 (浙财采监〔2022〕8号)已分别于2022年1月29日、2022年2月1日和2022年7月1日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

2、根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》 浙财采监〔2021〕22号)文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表；鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为:浙江政府服务网-政府采购投诉处理-在线办理。

3、本项目公告期限为3个工作日。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，以书面形式一次性向采购人和采购代理机构提出同一环节，后续就采购过程、采购结果提出质疑的，也应在同一环节一次性提出，以供应商线上提供质疑函的时间为提起质疑的时间。否则，被质疑人可不予接受。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。

4、未进行供应商资格报名或登记（含网上报名登记）的供应商，应视为未参加政府采购活动，一般不得提出质疑，但因供应商资格条件受到限制、报名时间设定不符合有关规定等原因使供应商不能参加报名或登记的除外。

5、请各磋商响应供应商及时办理浙江政府采购网“政府采购供应商注册”手续。

6、参与政府采购项目的注册供应商，需登录浙江政府采购网（http://zfcg.czt.zj.gov.cn）进行网上获取文件；尚未注册的供应商应当先在浙江政府采购网上申请注册，注册终审通过后再进行网上获取文件。

7、本项目所有公告发布网站：“浙江省政府采购网”（http:// [www.zjzfcg.gov.cn）。](http://www.zjzfcg.gov.cn）。)

8、采购文件发售截止时间之后有潜在供应商提出要求获取采购文件的允许其报名获取，但对采购文件有异议应按规定的时间提出，逾期提出的，采购组织机构可不予受理、答复。

**十、联系方式：**

**1、采购代理机构**

采购代理机构名称：台州永安工程咨询有限公司

联系人：林女士

联系电话：0576-88882270,15757696186

传真：0576-88882270；

质疑接收人：叶先生

联系电话：13857637980

地点：台州市椒江区中环世纪6幢801室（交通银行台州分行楼上）

**2、采购人**

采购人名称：台州市中级人民法院

询问联系人：林先生 询问联系电话：0576-88553020

质疑联系人：仇先生 质疑联系电话：0576-88553527

采购人地址：台州市椒江区市府大道399号

**3、同级政府采购监督管理部门**

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

联系人：陈老师，李老师

监督投诉电话：0576-88206705，0576-88206731

地址：台州市椒江区纬一路66号

**4、其余事项**

（1）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元 | 王春宇 | 13676675331 |

（2）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 |

（3）中标供应商如有融资需求，可使用以下银行的政采贷服务。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 | 88588246 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 | 15906861025 |
| 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  18957683735 |

**十一、采购（中标）公告发布媒体：**浙江政府采购网（[http://zfcg.czt.zj.gov.cn](http://www.zjzfcg.gov.cn/new/)）

**备注：请贵单位下载本次招标采购文件后，认真阅读各项内容，进行必要的准备工作，按文件的要求详细填写和编制响应文件，并按以上确定的时间、地点准时上传投标文件。**

台州永安工程咨询有限公司

二○二五年七月

**第二章 供应商须知**

**前 附 表**

|  |  |  |
| --- | --- | --- |
| **序号** | **项目** | **内容** |
| 1 | 项目说明 | 项目类别：服务类  采购标的所属行业：根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定，本项目采购标的对应的中小企业划分标准所属行业为（十二）软件和信息技术服务业。 |
| 2 | 供应商特定资格要求 | 符合竞争性磋商公告资格要求的供应商 |
| 3 | 答疑会或现场踏勘 | 无 |
| 4 | 磋商响应文件组成要求 | 本项目实行电子投标，供应商应准备电子磋商响应文件、还可以提供以介质（U盘）存储的数据电文形式的备份磋商响应文件。  1、电子磋商响应文件：指通过“政采云电子投标客户端”完成响应文件编制后生成并加密的数据电文形式的电子磋商响应文件。  2、备份磋商响应文件：是指“电子响应文件”同时生成的数据电文形式的电子文件（备份标书），以U盘形式提供。  以上两类响应文件均由资格证明文件、商务技术文件、报价文件三部分组成。 |
| 5 | 磋商响应文件有效期 | **▲**磋商有效期为90天，磋商有效期从提交磋商响应文件的截止之日起算。 |
| 6 | 电子投标响应文件的传输递交 | **截止时间：** **2025年 月 日上午09:00整**  ▲供应商应当在磋商截止时间前完成电子磋商响应文件的传输递交，磋商截止时间前可以补充、修改或者撤回电子磋商响应文件。补充或者修改电子磋商响应文件的，应当先行撤回原文件，补充、修改后重新传输递交。磋商截止时间前未完成传输的，视为撤回磋商响应文件。磋商截止时间后寄达的磋商响应文件，将被拒收。 |
| 7 | 备份磋商响应文件的递交 | 供应商同时还可以提供经政采云平台加密处理的、以介质（U盘）存储的数据电文形式的备份磋商响应文件（不强制要求，未递交备份磋商响应文件的风险由供应商自行承担）。备份磋商响应文件应当在磋商截止时间前送达并按要求密封（备份磋商响应文件在密封袋的封口处应有磋商供应商公章或磋商授权委托代理人签字。封皮上写明项目编号、标段、招标项目名称、供应商名称，并注明“备份磋商响应文件”、“磋商时启封”字样）并建议采用顺丰邮寄（或直接递交）到**台州市椒江区中环世纪6幢801室（交通银行台州分行楼上）收件人：俞雅琪**；联系电话：15757696186，逾期寄达、到付或未按要求密封将被拒收。▲如供应商未在磋商截止时间前完成电子磋商响应文件的传输递交，其备份磋商响应文件也将为无效磋商响应文件。  **截止时间： 2025年 月 日上午09:00整** |
| 8 | 备份磋商响应文件份数及密封要求 | 一份，以U盘形式提供。  备份磋商响应文件在密封袋的封口处加盖投标人公章、法定代表人代表或授权委托代理人印章或签字。封皮上写明项目编号、标项、招标项目名称、投标人名称，并注明“响应文件名称”、“开标时启封”字样。未按上述要求密封及加写标记将被拒收，采购代理机构对响应文件的误投和提前启封不负责任。  如电子磋商响应文件解密成功，则备份磋商响应文件不再拆封。 |
| 9 | 电子投标响应文件解密时间及地点 | 时间：2025年 月 日上午09:00-09:30（北京时间）  地点：政采云平台（www.zcygov.cn） |
| 10 | 实质性条款 | 带“▲”的条款是实质性条款，磋商响应文件须作出实质性响应，否则终止磋商。 |
| 11 | 其他要求 | 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：无要求；4、现场演示：无要求。 |
| 12 | 中小企业扶持政策 | 1、依据《政府采购促进中小企业发展管理办法》（财库【2020】46号）第十二条规定，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，否则按违约处理。 |
| 13 | 其他 | 1、各供应商自行在浙江政府采购网下载或查阅采购文件和相关更正公告等，不另行通知，如有遗漏采购人、采购代理机构概不负责。  2、两家或两家以上供应商提供的投标文件出自同一终端设备的，或在相同Internet主机分配地址（相同IP地址）报名或网上投标的，后果由供应商自行承担。  3、开标时间后30分钟内供应商须携带CA自备电脑登录“政采云”平台，用“项目采购-开标评标”功能解密投标文件，投标人未按时解密或解密失败的，其上传的电子投标文件自动失效。 |
| 14 | 解释权 | 本采购文件的解释权属于**台州永安工程咨询有限公司和采购人** |

**一、总则**

**（一） 适用范围**

本磋商文件适用于本次项目的磋商、评审、确定成交供应商、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

**（二）定义**

1、“采购组织机构”指采购人委托组织磋商的集中采购机构或采购代理机构。

2、采购人：是指委托集中采购机构或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。

3、磋商供应商：是指向采购组织机构提交磋商响应文件的单位或个人。

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。

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。

6、“书面形式”包括信函、传真等。

7、“▲”系指实质性要求条款。

**（三）磋商费用**

不论磋商结果如何，供应商均应自行承担所有与磋商有关的全部费用（磋商文件有相关规定除外）。

**（四）特别说明**

1、供应商磋商所使用的资格、信誉、荣誉、业绩与企业认证必须为本供应商所拥有。供应商磋商所使用的采购项目实施人员必须为本供应商员工。▲其中涉及资格条件的如非本法人所拥有，则投标无效。

2、供应商所标产品除磋商文件中明确规定要求“提供官网截图或相应检测报告的证明材料”以外，所有技术参数描述均以磋商响应文件为准。**磋商供应商对所标产品技术参数的真实性承担法律责任。**项目磋商结束后、质疑期限内，如有质疑供应商认为成交供应商所标产品、磋商响应文件技术参数与采购需求存在重大偏离、错误、甚至造假的情况，应提供具体有效的证明材料。

▲3、供应商在磋商活动中提供任何虚假材料,其响应无效，并报监管部门查处；成交后发现的,成交人须依照根据《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、供应商不得相互串通磋商报价，不得妨碍其他供应商的公平竞争，不得损害采购人或其他供应商的合法权益，供应商不得以向采购人、磋商小组成员行贿或者采取其他不正当手段谋取成交。

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

6、磋商响应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。

▲7、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。电子交易平台运营机构，以及与该机构有直接控股或者管理关系可能影响采购公正性的任何单位和个人，不得在该平台进行的政府采购项目电子交易中投标、响应和代理政府采购项目。

▲8、投标人在参与政府采购活动中所签署的一切文件，包括但不限于签到表、《政府采购活动现场确认声明书》等文件，特别是有关利害关系应如实填写、如实披露，投标人授权参与政府采购的人员视为应当知道与招标人、其他投标人之间的利害关系。如未如实披露，则视为提供虚假材料，由投标人承担不利后果。

▲9、本项目不允许转包、分包。

**二、磋商响应文件**

**（一）磋商响应文件的形式和效力**

本项目实行电子投标，供应商应准备电子磋商响应文件、还可以提供备份磋商响应文件。

1、电子磋商响应文件按政府采购云平台供应商项目采购-电子招投标操作指南（网址：https://helpcenter.zcygov.cn/document/#/document/detail?siteCode=beijing&manualId=359&topicId=1447）及本磋商文件要求制作、加密并递交。

2、备份磋商响应文件是指“电子响应文件”同时生成的数据电文形式的电子文件（备份标书），以U盘形式提供。

3、磋商响应文件启用顺序和效力：磋商响应文件的启用，按先后顺位分别为电子磋商响应文件、备份磋商响应文件。如果某位供应商的电子磋商响应文件无法按时解密的，可启用以介质（U盘）存储的数据电文形式的备份磋商响应文件。

▲未传输递交电子磋商响应文件，投标无效。

**（二）磋商响应文件的组成**

供应商应仔细阅读磋商采购文件的所有内容，按磋商采购文件的要求，详细编制磋商响应文件（包含电子响应文件和备份响应文件）。【特别提示：如有要求提供资料原件的，原件另行包装，并与磋商响应文件一起提交，磋商响应截止时间后所有原件不予接收。资料原件也可以用与原件相符的公证原件替代】

**▲1、资格证明内容的组成：**

（1）磋商声明书；

（2）授权委托书（法定代表人亲自办理投标事宜的，则无需提交)；

（3）法人或者其他组织的营业执照等证明文件，法定代表人和授权代表的身份证明；

（4）供应商认为需要说明的其他材料；

**2、商务与技术内容的组成：**

（1）供应商企业情况介绍；

（2）磋商响应方案描述：

A.项目需求的理解与分析(供应商对项目现状及需求的理解情况，对项目现状和需求描述的全面性、准确性、针对性，对项目重点、难点的把握，解决方案及合理化建议)。

B.项目组织实施方案（包括项目服务期、确保项目实施的措施或方案、项目实施进度安排、项目实施人员及项目负责人的资质、类似经验及社保证明等）。

C.验收方案（包括项目验收标准和验收方法等）和措施；

（3）商务及技术响应表。

（4）供应商通过的与本项目相关的认证证书或文件；

（5）类似项目的成功案例（供应商类似项目实施情况一览表、合同复印件及其相应的发票、用户验收报告等）；

（6）供应商认为需要提供的其他资料（包括可能影响供应商商务与技术内容评分的各类证明材料）。

（7）售后服务描述及承诺：

A.距采购人最近的服务网点详细介绍（包括地理位置、资质资格、技术力量、工作业绩、服务内容及联系电话等）。

B.针对本项目的售后服务措施及承诺（售后技术服务方案、人员配备、服务响应时间、技术培训方案等）。

**注：若磋商文件中有专门标注的某关联点，并要求供应商在电子投标系统中作出磋商响应的，如供应商未对关联点进行响应或者在响应文件其它内容进行描述，造成电子评审不能查询的责任由供应商自行承担。**

**3、报价内容的组成**

**（1）报价内容由开标一览表、报价明细表、中小企业声明函（如有），以及供应商认为其他需要说明的内容组成。**

▲（2）此报价为供应商针对本项目报出的唯一的首次报价，包含其它一切所要涉及到的费用，有选择、附条件的报价将被拒绝。

（3）投标报价为完成本项目的所有费用，包括所有人员的人工费、交通费、住宿费、伙食费、办公设施费、管理费、利润、税金、合同包含的所有风险责任等各项费用及不可预见费等所需的全部费用，全部费用已包含在投标报价中。

（4）政府采购优惠政策相关资料。

▲（5）相关报价表需打印或用不褪色的墨水填写， 磋商响应报价表不得涂改和增删，如有错漏必须修改，修改处须由同一签署人签字或盖章，未由同一签署人签字或盖章的修改无效。由于字迹模糊或表达不清引起的后果由供应商负责。

（6）报价有关表格应按采购文件中相关附表格式填写。

（7）最后的磋商报价低于首次报价，除磋商内容发生实质性变更，其报价明细表（如有）中各项报价需另行明确以外，各项报价均按比例下调。

**（三）磋商响应文件的制作、封装及递交要求**

**1、磋商响应文件的签署**

（1）电子磋商响应文件中须加盖供应商公章部分均采用CA签章，并根据“政府采购云平台供应商项目采购-电子招投标操作指南”及本采购文件规定的格式和顺序编制电子磋商响应文件并进行关联定位，以便磋商委员会在评标时，点击评分项可直接定位到该评分项内容。如对采购文件的某项要求，供应商的电子磋商响应文件未能关联定位提供相应的内容与其对应，则磋商委员会在评审时如做出对供应商不利的评审由供应商自行承担。

电子磋商响应文件如内容不完整、编排混乱导致磋商响应文件被误读、漏读，或者在按采购文件规定的部位查找不到相关内容的，由供应商自行承担。

（2）温馨提醒：CA签章上目前没有法定代表人或授权代表签字信息，需要供应商联系浙江杭州汇信科技有限公司等相应公司进行办理，或在磋商响应文件中涉及到签字的位置线下签好字然后扫描或者拍照做成PDF的格式亦可。

（3）▲磋商响应文件不得涂改，若有修改错漏处，须加盖单位公章或者法定代表人或授权委托人签字或盖章。磋商响应文件因字迹潦草或表达不清所引起的后果由供应商负责。

**2、磋商响应文件的制作要求**

（1）供应商应按照磋商响应文件组成内容及项目磋商需求制作磋商响应文件，不按采购文件要求制作磋商响应文件由此产生的责任由磋商供应商自行承担。

▲响应文件（包含电子磋商响应文件和备份磋商响应文件），其中电子磋商响应文件中所须加盖公章部分均采用CA签章。备份磋商响应文件按要求密封，否则其响应文件将可能被拒绝。

（2）▲供应商应对所提供的全部资料的真实性承担法律责任，磋商响应文件内容中有要求盖章或签字的地方，必须加盖磋商供应商的公章以及法定代表人或授权委托代理人的盖章或签字，其中所有证书类文件提供的复印件必须全部加盖单位公章且必须在有效期内的。

（3）磋商响应文件以及磋商供应商与采购组织机构就有关磋商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磋商响应文件视同未提供，如该文件未提供将影响投标有效性的，则视为投标无效。

（4）磋商计量单位，磋商采购文件已有明确规定的，使用磋商采购文件规定的计量单位；磋商采购文件没有规定的，▲应采用中华人民共和国法定计量单位（货币单位：人民币元），否则视同未响应。

（5）若磋商供应商不按采购文件的要求提供资格审查材料，其风险由磋商供应商自行承担。

（6）与本次磋商无关的内容请不要制作在内，确保磋商响应文件有针对性、简洁明了，同时节约纸张；磋商响应文件统一以A4纸大小双面打印并装订。

**3、磋商响应文件的封装要求**

（1）磋商文件的正本封面需注明“正本”字样。▲除报价文件外其余一律不准出现数字报价。如有不同标项，请按标项号分别编制。

（2）所有磋商响应资料按采购文件的组成所列内容及顺序装订成册，并逐页连续标注页码。因磋商响应文件内容不完整、编排混乱导致磋商响应文件被误读、漏读或者查找不到相关内容的责任由供应商自行承担。

（3）备份磋商响应文件请在密封袋的封口处应有磋商供应商公章或磋商授权委托代理人签字。封皮上写明项目编号、标段、招标项目名称、供应商名称，并注明“磋商响应文件名称”、“磋商时启封”字样，未按上述要求密封及加写标记将被拒收，采购组织机构对磋商响应文件的误投和提前启封不负责任。

（4）项目如分标段，各标段磋商响应文件必须分开编制。

（5）因密封不严、标记不明而造成失密、拒收、过早启封等情况，采购组织机构概不负责。

**4、磋商响应文件的递交要求**

（1）供应商同时还可以提供经政采云平台加密处理的、以介质（U盘）存储的数据电文形式的备份磋商响应文件（不强制要求，未递交备份磋商响应文件的风险由供应商自行承担）。备份磋商响应文件应当在磋商截止时间前送达并按要求密封（备份磋商响应文件在密封袋的封口处应有磋商供应商公章或磋商授权委托代理人签字。封皮上写明项目编号、标段、招标项目名称、供应商名称，并注明“备份磋商响应文件”、“磋商时启封”字样）并建议采用顺丰邮寄（或直接递交）到**台州市椒江区中环世纪6幢801室（交通银行台州分行楼上）收件人：俞雅琪；联系电话：15757696186**。备份磋商响应文件在截止时间后提交、到付或未按要求密封的，采购代理机构将拒绝接收。▲如供应商未在磋商截止时间前完成电子磋商响应文件的传输递交，其备份磋商响应文件也将为无效备份磋商响应文件。

**（2）电子磋商响应文件的相关说明**

供应商进行电子投标应安装客户端软件，并按照采购文件和电子交易平台的要求编制并加密磋商响应文件。▲供应商未按规定加密的磋商响应文件，电子交易平台将拒收。

▲供应商应当在磋商截止时间前完成磋商响应文件的传输递交，并可以补充、修改或者撤回磋商响应文件。补充或者修改磋商响应文件的，应当先行撤回原文件，补充、修改后重新传输递交。磋商截止时间前未完成传输的，视为撤回磋商响应文件。▲磋商截止时间后递交的磋商响应文件，电子交易平台将拒收。

供应商在电子交易平台传输递交磋商响应文件后，还可以在磋商截止时间前提交备份磋商响应文件，若供应商未提交备份磋商响应文件，其后果由供应商自行承担。

▲供应商仅提交备份磋商响应文件的，投标无效。

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

**5、磋商响应文件的补充、修改和撤回。**

▲（1）供应商应当在投标截止时间前完成电子磋商响应文件的上传、递交，并可以补充、修改或者撤回电子磋商响应文件。补充或者修改电子磋商响应文件的，应当先行撤回原文件，补充、修改后重新上传、递交。投标截止时间前未完成上传、递交的，视为撤回电子磋商响应文件。投标截止时间后递交的电子磋商响应文件，“政府采购云平台”将予以拒收。

（2）投标截止时间后，供应商不得撤回、修改磋商响应文件。

（3）在开标后规定的投标有效期内，供应商不能撤销磋商响应文件。

**（四）磋商响应文件的有效期**

▲1、自磋商响应截止日起90天磋商响应文件应保持有效。有效期不足的磋商响应文件将被拒绝。

2、在符合相关法律法规规定的情况下，采购人可与磋商供应商协商延长磋商响应文件的有效期，这种要求和答复均以书面形式进行。

3、磋商供应商可拒绝接受延期要求。同意延长有效期的磋商供应商不能修改磋商响应文件。

▲4、成交供应商的磋商响应文件自磋商之日起至合同履行完毕均应保持有效。

**三、磋商**

**（一）磋商事项：**

采购组织机构按照采购文件规定的时间通过电子交易平台组织磋商、开启响应文件，所有供应商均应当准时在线参加。

磋商时，电子交易平台自动提取所有响应文件，提示采购组织机构和供应商按采购文件规定的方式和时间在线解密。**给予供应商在线解密的时间为截止提交磋商响应文件后30分钟。**

▲响应文件未按时解密，供应商提供了备份磋商响应文件的，以备份磋商响应文件作为依据，否则视为响应文件撤回。响应文件已按时解密的，备份磋商响应文件不再拆封。

1. **磋商委员会或磋商小组**

磋商委员会或磋商小组（以下简称磋商委员会）成员由政府采购管理部门负责组织，对具备实质性响应的响应文件进行评估和比较。磋商委员会由招标人的代表、专家和其他有关方面的代表组成。

磋商委员会由采购人代表和评审专家共3人及以上单数组成，其中评审专家人数不得少于磋商小组成员总数的2/3。采购人代表不得以评审专家身份参加本部门或本单位采购项目的评审。采购代理机构人员不得参加本机构代理的采购项目的评审。

**（三）磋商程序**

1、采购组织机构将在“磋商公告”规定的时间和地点进行磋商，磋商采购会议由采购组织机构工作人员主持，所有供应商均应准时在线参加磋商采购会议。

2、 主持人宣布磋商采购会议开始，介绍磋商现场的人员情况，宣读提交磋商响应文件的供应商名单、磋商纪律、应当回避的情形等注意事项。

3、供应商登录政采云平台，用“项目采购-开标评标”功能对电子响应文件准备在线解密，在线解密电子响应文件时间为开启解密时间起30分钟内。

电子磋商响应文件未按时解密，供应商提供了备份磋商响应文件的，以备份磋商响应文件作为依据，否则视为磋商响应文件撤回。电子磋商响应文件已按时解密的，备份磋商响应文件不再拆封。

4、采购组织机构点击【开启标书信息】，进入资格审查及符合性审查环节。

5、磋商小组必须按照客观、公正、审慎的原则，根据磋商文件规定的评审程序、评审方法和评审标准进行独立评审。▲未实质性响应磋商文件的响应文件按无效响应处理，磋商小组应当告知提交响应文件的供应商。

（1）对响应文件的初审

A.资格性检查：依据法律法规和磋商文件的规定，对响应文件中的资格条件进行审查，以确定磋商供应商是否具备投标资格。

B.符合性检查：详细评标之前，磋商小组依据磋商文件的规定，对响应文件是否满足采购文件的实质性要求进行审查，以确定响应文件是否有效。

6、初审合格的供应商进入下一步的磋商活动。

7、磋商小组所有成员集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

8、在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。

9、磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组将要求所有实质性响应的供应商在规定时间内提交最后报价。最后报价是供应商响应文件的有效组成部分。

10、经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。

11、磋商小组根据综合评分情况，按照评审得分由高到低顺序确定成交候选供应商，编写评审报告。

12、采购组织机构对磋商小组专家成员进行评价；

13、主持人宣布磋商结果（含技术得分、最后报价、报价得分及总得分），磋商采购会议结束。

**（四）澄清问题的形式**

磋商供应商的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或授权委托代理人签字，并不得超出磋商响应文件的范围或者改变磋商响应文件的实质性内容。

**（五）错误修正**

磋商响应文件报价出现前后不一致的，除采购文件另有规定外，按照下列规定修正：

1、磋商响应文件中开标一览表内容与磋商响应文件中相应内容不一致的，以开标一览表为准。政采云平台开标一览表中填报的价格与上传的报价响应文件中开标一览表的报价不一致的，以上传的报价响应文件中开标一览表的价格为准，修正平台上的投标报价；

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。修正应当采用书面形式，并加盖公章，或者由法定代表人或授权委托代理人签字。修正后的报价经磋商供应商确认后产生约束力，磋商供应商不确认或未在规定时间内进行有效澄清的，将终止磋商。

▲**（六）磋商供应商存在下列情况之一的，响应无效，终止磋商**

1、磋商响应文件中的报价货物跟商务与技术内容中的供应货物出现重大偏差的；

2、不具备采购文件中规定的资格要求的。

3、磋商响应文件含有采购人不能接受的附加条件的。

4、供应商代表人未能出具身份证明或与法定代表人授权委托人身份不符的（受疫情期间影响供应商代表人无需现场参加磋商会议）；

5、磋商小组认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评审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，磋商小组应当与其终止磋商。

6、报价超过采购文件中规定的预算金额/最高限（单）价。

7、磋商参数未如实填写，完全复制粘贴招标参数的。

8、磋商响应文件提供虚假材料的。

9、不同供应商的磋商响应文件由同一单位或者个人编制；

10、不同供应商委托同一单位或者个人办理磋商事宜；

11、不同供应商的磋商响应文件载明的项目管理成员或者联系人员为同一人；

12、不同供应商的磋商响应文件异常一致或者报价呈规律性差异；

13、不同供应商的磋商响应文件相互混装；

14、不同供应商的电子投标（响应）文件上传计算机的网卡MAC地址或硬盘序列号等硬件信息相同且无法合理解释的；

15、上传的电子投标（响应）文件若出现使用本项目其他投标（响应）供应商的数字证书加密的，或者加盖本项目其他投标（响应）供应商的电子印章的；

16、不同供应商的投标（响应）文件的内容存在3处（含）以上错误一致的；

17、不同供应商联系人为同一人或不同联系人的联系电话一致的。

18、不符合法律、法规和采购文件中规定的其他实质性要求的（采购文件中打“▲”内容及被拒绝的条款）。

19、投标人的电子响应文件无法按时解密且本项目未达到启动备份文件条件的。

20、电子响应文件解密失败的，且未在规定时间内提交备份响应文件的；

21、电子响应文件未按规定要求提供电子签章的。

▲**（七）有下列情况之一的，本次磋商终止**

1、出现影响采购公正的违法、违规行为的；

2、磋商小组发现磋商文件存在歧义、重大缺陷导致评审工作无法进行，或者磋商文件内容违反国家有关强制性规定的；

3、因重大变故，采购任务取消的；

4、法律、法规和磋商文件规定的其他导致评审结果无效的。

**（八）磋商原则和方法**

1、磋商原则。磋商小组必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评审有关的内容；任何单位和个人不得干扰、影响评审的正常进行；磋商小组及有关工作人员不得私下与磋商供应商接触。

2、磋商办法。具体磋商内容及评分标准等详见《第三章：评审办法及评分标准》。

**（九）评审过程的监控**

本项目评审过程实行全程录音、录像监控，政府采购监管部门视情进行现场监督，供应商在评审过程中所进行的试图影响评审结果的不公正活动，可能导致其被拒绝磋商。

**（十）电子交易异常情形处理**

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，采购组织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。

出现以上规定情形，不影响采购公平、公正性的，采购组织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；影响或可能影响采购公平、公正性的，应当重新采购。

**四、磋商结果确定**

1、确定成交供应商。磋商小组根据采购人的《授权意见确认书》，推荐成交候选供应商或直接确定成交供应商。其中推荐成交候选供应商的，采购组织机构在评审结束之日起2个工作日内将评审报告送交采购人，采购人自收到评审报告之日起5个工作日内在评审报告推荐的成交候选人中按顺序确定成交供应商。

2、发布成交结果公告。采购组织机构应当在成交供应商确定后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成交结果，并将磋商文件随同公告。

3、发出成交通知书。采购组织机构在发布成交结果同时，向成交供应商发出成交通知书。

4、中标人在中标之后领取通知书之前，应向招标代理机构交纳招标代理服务费。若中标人未在约定时间内支付招标代理服务费，从逾期之日起按日利率千分之一承担违约金。若中标人未按上述规定办理，需承担招标代理机构为实现债权的所有费用（包括但不限于律师费、催讨车旅费、保全担保费等）。

5、招标代理费：按照中标通知书确定的中标金额，按下附表收费标准，采用差额累进算法向中标单位收取代理服务费。代理服务费结算不足陆仟元的，按定额陆仟元收取。该费用中标方须在领取中标通知书时一次性付清。（单位名称：台州永安工程咨询有限公司；人民币账号：530125998900015；开户行：台州银行黄岩工业园区支行）

**附表：招标代理服务收费标准**

|  |  |
| --- | --- |
| **服务**  **费　　类型**  **率**  **中标金额（万元）** | **服务招标** |
| 100以下 | 1.5% |
| 100-500 | 0.8% |
| 500-1000 | 0.45% |
| 1000-5000 | 0.25% |
| 5000-10000 | 0.1% |
| 10000-100000 | 0.05% |
| 100000以上 | 0.01% |

**五、合同签订及公告**

**（一）签订合同**

1、采购人应当自成交通知书发出之日起30日内，按照磋商采购文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量和服务要求等事项签订政府采购合同。

2、采购人不得向成交供应商提出超出磋商文件以外的任何要求作为签订合同的条件，不得与成交供应商订立背离磋商文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量和服务要求等实质性内容的协议。

3、成交供应商无故拖延、拒签合同的,取消成交资格。

4、成交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成交候选供应商名单排序，确定下一候选供应商为成交供应商，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。

5、询问或者质疑事项可能影响成交结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同（成交结果的质疑期为成交结果公告期限届满之日起七个工作日）。

**（二）合同公告及备案**

1、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。

2、采购人应当自政府采购合同签订之日起7个工作日内，将政府采购合同副本报同级人民政府财政部门备案以及采购组织机构存档。

**第三章 评审办法及评审标准**

一、采购组织机构将组织磋商小组，对供应商提供的磋商响应文件进行综合评审。

二、本次磋商项目的评审方法为**综合评分法**，总计100分，其中商务技术分值70分，投标报价分值30分。评审标准按评分细化条款及分值进行评审。

（一）商务技术文件中的客观分应由评审小组成员独立评审，但客观分打分应一致；客观分不一致时，由评审委员会复核或书面说明理由，其余在规定的分值内单独评定打分（小数点后保留1位）。

（二）各磋商供应商商务技术文件得分按照磋商小组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，四舍五入），计算公式为：

商务技术文件得分=磋商小组所有成员评分合计数/磋商小组组成人员数。

（三）综合评分法中的价格分统一采用低价优先法计算（小数点后保留2位，四舍五入），即满足磋商文件要求且最后报价最低的供应商的价格作为磋商基准价，其报价得满分。其他供应商的价格分统一按照下列公式计算：

磋商报价得分=(磋商基准价／最后磋商报价)×30%×100 。

（四）磋商供应商综合得分＝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、关于小型、微型企业（简称小微企业）磋商：①根据浙江省财政厅发布的《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》【浙财采监（2022）3号】规定，对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，采购人、采购代理机构应当对符合本办法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。②小微企业是指符合《中小企业划型标准规定》的供应商，通过磋商提供本企业制造的货物、承担的工程或者服务，或者提供其他小微企业制造的货物。本项所指货物不包括使用大、中型企业注册商标的货物；2、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，视同小型、微型企业，享受小微企业政府采购优惠政策；3、残疾人福利性单位在参加政府采购活动时，应提供《残疾人福利性单位声明函》（见附件），视同小型、微型企业，享受小微企业政府采购优惠政策。

具体优惠：对于非联合体投标，小型微型企业产品的价格给予10%的扣除，用扣除后的价格计算评标基准价和投标报价。对于联合体投标，小型、微型企业的协议合同金额占到联合体协议合同总金额30%以上的，可给予联合体6%的价格扣除。联合体各方均为小型、微型企业的，联合体视同为小型、微型企业享受扶持政策，对于小型微型企业产品的价格给予10%的扣除，用扣除后的价格计算评标基准价和响应报价。同一投标人（包括联合体），小微企业、监狱企业、残疾人福利性单位价格扣除优惠只享受一次，不得重复享受。

注：得分以系统计算为准，保留2位小数。

**\*以上证明材料不提供或提供不全的视为自动放弃优惠政策。**

三、在最大限度地满足磋商文件实质性要求前提下，磋商小组按照磋商文件中规定的各项因素进行综合评审后，以评审总得分最高的供应商为第一成交候选供应商，评审总得分次高的供应商为第二成交候选供应商，评审总得分第三高的为第三成交候选供应商。

四、如综合得分相同，最后报价低者为先；如综合得分且最后报价相同的，以商务分得分较高者为先，商务分得分也相同的则抽签决定。

五、中标候选人放弃中标、拒绝与采购人签订合同、因不可抗力提出不能履行合同的，采购人可以按照评审报告推荐的中标或者成交候选人名单排序，确定下一候选人为中标或者成交供应商，也可以重新开展政府采购活动。评标办法的解释权归招标人。

六、本次评分具体分值细化条款如下表：

**评标打分标准表**

|  |  |  |  |
| --- | --- | --- | --- |
| **评标因素** | | **评分标准** | **分值** |
| 商务分（13分） | 企业综合实力 | 投标人具有ITSS信息技术服务运行维护资质、信息安全服务资质的，每个资质证书得1分，本项最高得2分。  **（须提供相应的证书扫描件（相关证书应在有效期内）加盖投标人公章编入投标文件中，未提供的不得分）** | 2 |
| 投标人具有国家认证认可监督管理委员会批准认可的认证机构颁发的，且在有效期内的信息安全管理体系认证、信息技术服务管理体系认证的，每个认证证书得1分，本项最高得2分。  **（须提供相关证书扫描件及[全国认证认可信息公共服务平台](https://www.so.com/link?m=bgeKa5pUJ7jqGvX1HhllAJLNiphU7TZFNQwb4+7ZUZpVLH3/mqlCJ7rNGXZ5/YNpLh7l1an07AVpzdd+DNfDz03MHubLsbYxQOzT8llEFb57FaGuLm6gSmMhBy2lLDBrTFSNNDZqVzwQMcexMhSdw5Kuw+3MXS7HQcV4Anm9Fs1KmUyptcyDigHMKmFQMXtO7xSEBzzl+542xjBTD4X4Ft///zWSTHNTKcszTMLGSmT541nhMntevTSaKintmdBbT4YHZJEfW00MedhN8WiQ3A1LHjOM=" \t "https://www.so.com/_blank)网站截图并加盖投标人公章编入投标文件中，未提供或提供不全的不得分）** | 2 |
| 项目组人员配置情况 | 拟投入本项目的项目负责人：具有信息系统项目管理师（软考）证书、信息安全工程师（软考）证书、CISP认证证书的，每提供1个得1分，本项最高得2分。  **（须提供相应的证书扫描件（相关证书应在有效期内）和投标人为其缴纳的近3个月社保证明加盖投标人公章编入投标文件中，未提供或提供不全的不得分）** | 2 |
| 根据驻场服务技术人员（1名）的专业资质和从业经验情况进行打分。  1、专业资质优秀的得1分，资质一般的得0.5分，未提及此项不得分。  2、从业经验丰富的得1分，经验一般的得0.5分，未提及此项不得分。  本项最高得2分。  **（须提供投标人为其缴纳的近3个月社保证明加盖投标人公章编入投标文件中，未提供的不得分）** | 2 |
| 根据本地化服务团队支撑技术人员的专业资质和从业经验等情况进行打分。团队整体专业资质优秀，从业经验丰富的得2分，资质和经验一般的得1分，资质和经验有待加强的得0.5分，未提及此项不得分。  **（须提供投标人为相关人员缴纳的近3个月社保证明加盖投标人公章编入投标文件中，未提供或提供不全的不得分）** | 2 |
| 承接经验 | 投标人自2022年7月1日（以合同签订时间为准）以来，承接过类似项目的，每提供一个项目合同得1分，最高得3分。  **（须提供合同扫描件并加盖投标人公章编入投标文件中，未提供的不得分）** | 3 |
| 技术分（57分）  （54分） | 现状分析 | 根据投标人对项目现状了解的情况进行打分。  现状分析深入，内容全面准确，见解到位的得5分；  现状分析基本到位，内容基本全面准确的得4分；  现状分析内容一般，有欠缺的得3分；  现状分析基本提及的得1分；  未提及此项不得分。 | 5 |
| 项目建设思路 | 根据投标人对本项目建设思路的理解、重难点的把握进行打分。  思路清晰，重难点把握准确，理解深入的得5分；  思路基本清晰，重难点把握基本准确，理解基本深入的得4分；  思路模糊，重难点把握及定位不够准确的得3分；  建设思路基本提及的得1分；  未提及此项不得分。 | 5 |
| 技术方案 | 根据投标人技术方案与本项目需求的吻合程度进行打分。  方案详细、完善、科学合理，适用本项目需求的得5分；  方案比较详细完善，基本满足本项目需求的得4分；  方案内容欠佳，不够详细的得3分；  技术方案简单提及的得1分；  未提及此项不得分。 | 5 |
| 技术参数响应 | 根据投标人所提供的设备技术指标与需求全部满足采购文件要求的得满分18分，负偏离或不满足的一项扣1分，扣完为止。 | 18 |
| 根据投标人所提供的服务全部满足采购文件要求的得满分10分，负偏离或不满足的一项扣1分，扣完为止。 | 10 |
| 实施方案 | 根据投标人提供的组织实施方案，包括产品供货、验货、安装调试、调优、验收等内容进行打分。  方案详实、内容完整、供货安排操作性强，进度详细有保障，验收标准符合行业标准且有针对性的得5分；  方案基本详实、内容基本完整、供货安排操作性比较强强，进度安排基本合理，验收标准基本符合行业标准的得4分；  方案粗糙、内容缺漏、供货安排操作性一般，保障性和合理性有待加强的得3分；  实施方案简单提及的得1分；  未提及此项不得分。 | 5 |
| 培训方案 | 根据投标人针对本项目制定的培训方案的合理性、科学性、可行性等情况进行打分。  培训方案内容齐全，可操作性强的得4分；  培训方案内容基本齐全，可操作性比较强的得3分；  培训方案内容一般，可操作性一般的得2分；  培训方案不够周全、可操作性有待加强的得1分；  未提及此项不得分。 | 4 |
| 应急处置方案 | 根据投标人结合本项目的特点，对网络信息安全中可能出现的突发情况分析以及应急处置方案的完整性、合理性、针对性等因素进行打分。  方案说明详细、考虑齐全、科学合理，与本项目吻合的得5分；  方案说明内容一般，基本科学合理，基本满足需求的得4分；  方案说明内容欠佳，不够详细的得3分；  应急方案简单提及的得1分；  未提及此项不得分。 | 5 |
| 价格  （30分） | | 取投标合格供应商的投标最终报价最低价为评标基准价，基准价为30分。  投标报价得分=(评标基准价／投标报价)×30%×100 。（小数点后保留2位小数）。 | 30 |

**第四章 项目需求**

**一、采购项目一览表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **简要技术要求** | **数量** | **单位** | **预算**  **（万元）** | **最高限价（万元）** | **备注** |
| 1 | 信息安全运维服务项目 | 详见项目需求 | 1 | 项 | 67 | 66.8 |  |

**二、技术需求**

**（一）安全服务内容**

1、投标人以服务模式提供安全软硬件平台给采购方使用，采购方每年支付服务费用。

2、投标人提供安全软硬件平台的安装调试、试运行、设备维护、项目验收以及技术培训和售后现场技术服务等。

3、投标人需要根据本招标文件的要求为采购方提供安全运维服务：包括安全规划、漏洞扫描服务、渗透测试服务、安全系统配置、协助加固、安全巡检、安全培训、应急响应等，并协助采购方建立建全网络安全管理制度和应急响应制度。所提供的服务范围包括台州市中级人民法院及9个基层法院的信息系统。

▲**投标文件中可以使用网络拓扑示意图来阐述网络安全解决方案，但不允许出现采购人真实详细的网络拓扑图和IP地址。**

**（二）安全运维服务清单**

**服务清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务内容清单** | **数量** | **单位** |
| **互联网安全服务** | | | |
| 1 | 互联网出口安全防护服务 | 1 | 套 |
| 2 | 终端入网控制服务 | 1 | 套 |
| 3 | 上网行为管理服务 | 1 | 套 |
| 4 | 互联网大数据安全分析服务 | 1 | 套 |
| 5 | 互联网主机安全及管理服务 | 1 | 套 |
| **法院专网安全服务** | | | |
| 6 | 专网运维审计系统服务 | 1 | 套 |
| 7 | 专网综合日志审计系统服务 | 1 | 套 |
| 8 | 专网APT预警平台服务 | 1 | 套 |
| 9 | 专网大数据安全管理平台服务 | 1 | 套 |
| 10 | 专网数据库审计服务 | 1 | 套 |
| 11 | 威胁情报分析服务 | 1 | 套 |
| 12 | 威胁情报收集服务 | 1 | 套 |
| 13 | 安全准入服务 | 1 | 套 |
| **其他安全服务** | | | |
| 14 | 安全培训服务 | 1 | 年 |
| 15 | 应急演练服务 | 1 | 年 |
| 16 | 网络安全专项检查服务 | 1 | 年 |
| 17 | 漏洞扫描服务 | 1 | 年 |
| 18 | 基线核查服务 | 1 | 年 |
| 19 | 渗透测试服务 | 1 | 年 |
| 20 | 应用上线检查服务 | 1 | 年 |
| 21 | 安全运维服务 | 1 | 年 |
| 22 | 资产梳理服务 | 1 | 年 |
| 23 | 数据备份服务 | 1 | 年 |
| 24 | 网络入侵攻击监测分析服务 | 1 | 年 |
| 25 | 异常流量态势监测服务 | 1 | 年 |
| 26 | 安全隐患处置服务 | 1 | 年 |
| 27 | 重大事件应急响应服务 | 1 | 年 |
| 28 | 特殊时期的安全巡检和保障服务 | 1 | 年 |

**（三）具体清单**

**1．互联网出口安全防护服务**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基本要求 | | 设备最大吞吐量≥6 Gbps，HTTP吞吐量≥2.65 Gbps，IPS吞吐量≥800 Mbps，AV吞吐量≥700 Mbps，IPSec VPN性能≥1 Gbps，最大并发连接数≥200万，每秒新建连接数≥5万，IPSec VPN隧道数≥1024，SSL VPN接入数≥400。 |
| 标准1U专用千兆硬件平台，内置交流单电源，硬盘≥500GB HDD。 |
| 10\*GE电口，4\*Combo口；支持千兆接口总数≥14个。 |
| 部署模式 | | 支持网关模式、网桥模式、旁路模式、虚拟网线工作模式、混合模式；部署模式切换无需重启设备。 |
| 网络特性 | NAT | 支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换。 |
| 链路负载均衡 | 支持基于负载链路的出接口的DNS请求，主动完成DNS服务器替换，解决用户主机配置DNS解析结果与实际转发运营商链路解析结果有冲突，从而导致跨运营商访问慢的问题；支持进行DNS探测，针对探测失败情况，可选择禁用DNS-DNAT功能或禁用负载链路出接口。 |
| DNS | 支持DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载。 |
| 安全防护 | 入侵防御 | 系统定义超过8600+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型；以及对应IPS规则的攻击类型、严重程度、CVE编号、CNNVD编号、协议、操作系统、发布年份、漏洞厂商等详细信息。 |
| 支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者SYSLOG告警，不同告警规则可以发送给不同的用户。 |
| 病毒防护 | 支持对最多10级的压缩文件进行解压查杀。 |
| 威胁情报 | 支持与多个威胁情报中心订阅，帮助产品实现检测、预警和防御。 |
| 协同防御 | 支持与本方案所投的EDR产品协同工作，实现终端在访问特定IP/网段时必须安装EDR，否则拒绝访问并重定向EDR的安装页面；可实时阻断EDR同步的风险主机的访问；并在与EDR产品联动后，增强防火墙对木马特征、内网资产的识别能力。 |
| 支持与本方案所投的APT产品协同工作，实现将APT分析到的SMB远程溢出攻击、扫描行为、Web后门访问、隐蔽信道通信、暴力破解、挖矿、远控工具利用、Web特征攻击等外部攻击源IP同步到本设备，通过本设备的黑名单功能实现自动阻断。 |
| 应用缓存加速 | 支持文件缓存，缓存文件形式不限于视频、APP等；设备智能解析用户流量，针对域名或者文件请求，设备推送文件至终端，帮助用户缓解互联网出口压力，实现文件下载加速的效果。 | |

**2．终端入网控制服务**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基本要求 | | 支持500台以上无代理软件设备安全管理，同时支持瘦终端、IoT设备、ICS设备。 |
| 1U硬件设备，2核4线程，6个千兆电口，16GB。 |
| 准入控制方式 | | 支持802.1x、EOU、Portal、端口镜像、策略路由、设备指纹准入等多种控制方式，并可以混合使用，且支持无代理方式，适应有线、无线、远程分支机构接入、NAT等多种复杂网络环境。 |
| 网络准入控制 | 网络控制规则 | 支持自动识别指定AD域和邮件服务器的PC，自动准入发现并下发权限控制策略。 |
| 安全控件入网安全检查 | 支持Windows设备安全检查，其中包括防病毒软件检查、终端启用Guest账号检查、终端弱口令账号检查、终端是否加域检查、终端共享目录检查、终端系统补丁检查、终端系统版本检查、终端服务安装检查、终端防火墙检测和终端主机名检查。 |
| 支持对操作系统、设备信息、流量关系等进行识别，同时支持自定义添加资产指纹，可根据扫描到的资产字段添加资产指纹识别规则。 | |
| 支持以图表的方式展现IP资源的实际使用情况，包括已使用、未使用IP地址以及每个IP地址的终端类型，协助管理员对IP资源进行整体规划，快速完成IP地址资源分配和回收登记管理。 | |

**3．上网行为管理服务**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基本要求 | | 网络层吞吐量≥3Gbps，应用层吞吐量≥1 Gbps。 |
| ≥4\*GE电口。 |
| 路由支持 | | 支持基于入接口、源地址、目标地址、用户、服务、应用、时间、域名的策略路由，提供Web配置界面截图。 |
| 行为管理 | 应用识别 | 应用特征不少于5000个，移动应用不少于2000个。 |
| 支持智能识别模式和快速识别模式，在智能识别模式下应用引擎尽可能地用各种方式识别网络流量，在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能。 |
| 应用控制 | 支持针对搜索引擎、HTTP、网页内容进行关键字过滤并实时生成日志记录，日志级别包括但不少于紧急、告警、严重、通知、信息、调试、不记录等，方便管理员快速区分用户上网行为属性和定位日志级别。 |
| 可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（ZIP、RAR、GZ、BZ2、Z、THZ、TBZ、7Z、CAB、BZ等）、应用程序、OFFICE系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。 |
| 防私接路由 | 支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断；检测方式包括但不限于时间戳、UA识别、应用特征、Flash Cookie、微信长连接等。 |
| 针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。 |
| 数据分析 | 支持用户全天行为分析，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息。 |
| 流量管理 | 支持基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套；支持基于地址、用户、服务、应用、时间、终端型号、VLAN、DSCP等匹配条件进行流量控制；并支持配置保障带宽、最大带宽、每IP带宽、每用户带宽、带宽优先级等QoS动作。 |

**4．互联网大数据安全分析服务**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基本要求 | | CPU10核20线程 ，内存96GB，硬盘：16T，千兆电口\*4。 |
| 数据采集和处理性能≥5000EPS，每条数据大小>1KB；  10亿数据关键字查询结果响应时间<2秒。 |
| 大数据分析平台中的安全数据，包括告警数据、资产数据、工单等至少20种可共享给第三方系统，实现数据共享和交换。 |
| 安全检测能力 | 行为审计与可疑通信检测 | 支持违规操作、违规访问、违规应用、违规外发等300种以上行为审计检测规则，可针对任意单条规则进行启用和禁用。 |
| 扫描探查检测 | 支持端口扫描、服务扫描、Web扫描、扫描器指纹检测等300种以上的扫描探查检测规则，可针对任意单条规则进行启用和禁用 |
| 恶意文件检测 | 支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell等18000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。 |
| 安全检测能力 | 终端溯源 | 能够对威胁告警事件提供全面的可视化溯源能力。从事件关联的设备、涉及到的恶意进程的父子关系，到每个进程运行时间、详细路径、文件安全等级、网络访问关系、进程调用关系等清晰呈现，最终追溯到恶意事件根源，还原威胁真实目的、了解入侵路径、评估响应范围。 |
| 远程处置 | 支持多种终端处置动作，如进程隔离、文件隔离、进程结束、网络隔离等，支持命令行方式操作终端操作系统。 |
| 安全分析能力 | AI高级分析 | 平台内置不少于3种机器学习分析场景模型，可Web攻击检测分析、DGA域名检测分析、钓鱼邮件检测分析等特定场景条件下的安全态势异常。 |
| 威胁情报分析 | 支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等；支持对接第三方威胁情报平台，支持配置情报碰撞接口及查询接口，支持查看请求接口数、今日情报请次数、昨日命中情报数，支持设置接口请求频率阈值，进行接口请求限制。 |
| 威胁狩猎 | 实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持通过一键溯源进行威胁关系的自动拓展。 |
| 设备联动 | 支持对接同厂商EDR同步资产指纹信息及脆弱性信息，支持与EDR集成联动，一键查杀木马病毒，访问封禁。 |
| 可视化安全分析 | 安全态势可视化 | 支持立体、平面、球面等多种维度的网络实体关系透视，可在大屏上展示不同实体的标签属性，包括但不限于DNS服务器、监管单位、邮件服务器、黑客组织、WEB服务器等。 |
| 资产管理 | 支持通过流量无侵入式自动发现资产，支持发现终端、Web服务器、DNS服务器、邮件服务器、FTP文件服务器等类型≥5种，其中web服务器支持自动识别服务域名和服务站点名称。 |

**5．互联网主机安全及管理服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 授权要求 | 150台PC终端防护授权。 |
| 全网风险可视 | 支持当前待处理高危风险展示，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面；  支持查看当前top 5 风险资产、top 5 威胁ip、top 5 威胁区域。 |
| 系统性能监控服务 | 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断。 |
| 高级威胁防护服务 | 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。  识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。  对失陷后主机远控持久化行为进行检测（反弹Shell、远程控制），可阻断远控。  对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。  可对渗透的收尾阶段的数据清除行为进行识别和阻断。 |
| 系统安全性服务 | 支持防端口扫描，锁定恶意的端口扫描，并记录告警。  违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。  支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度（任意IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。 |
| 防病毒服务 | 支持多引擎设置，包括默认引擎、深度扫描引擎。  对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。  提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。  提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。同时支持白名单设置。  支持病毒立即处理，对于无法普通隔离的病毒文件进行处理并加入隔离区，或动态移动到信任区。  支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用。 |
| 文件推送 | 支持下发文件、安装应用程序、远程执行命令。 |
| 屏幕水印功能 | 支持对屏幕拍照泄密数据的行为进行溯源。 |
| 集中管控服务 | 能够通过统一的管理中心对多个服务器或主机进行监控。  支持通过web页面进行客户端推广部署，推广页面支持自定义。 |
| 用户管理服务 | 支持自定义创建用户角色以及权限。至少支持以下帐号管理功能：帐号创建、帐号授权、帐号属性修改和帐号删除。 |

**6．专网运维审计系统服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具基本要求 | 至少配备6个100/1000M自适应电口，CPU：≥4核4线程，内存：≥8GB，硬盘：≥2T\*2。 |
| 可管理设备数量≥500个，运维用户无限制。 |
| 单台堡垒机字符类并发会话≥500个、图形类并发会话≥100个。 |
| 设备采用旁路部署，不得影响业务环境；须支持HA主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障。 |
| 用户管理要求 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。 |
| 支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等。 |
| 身份认证要求 | 支持与get、post、soap发送方式的http短信网关平台进行联动，实现短信动态口令双因素认证机制。 |
| 支持手机APP动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定APP动态口令；支持AD、LDAP、RADIUS、吉大正元、北京CA、深圳CA认证系统联动登录堡垒机；支持多个AD域认证源；支持自动同步AD/LDAP用户。 |
| 内嵌动态令牌和usbkey认证引擎，可同时使用动态令牌和USBkey。 |
| 设备管理要求 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，支持本地资源的映射及私有协议传输。 |
| 支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出。 |
| 支持设备帐户和密码的自动登录、手工登录、二次自动登录模式。 |
| 自动改密要求 | 支持定期自动修改windows服务器、网络设备、安全设备、linux/unix等目标设备密码功能，支持自动密码恢复、手工验证密码、密码强度控制等。 |
| 支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；支持发送方式，包括邮件、FTP、SFTP等。 |
| 运维方式要求 | 支持通过堡垒机页面直接调用本地Windows系统里的plsql、sqlplus、toad、sqlwb、ssms、mysql.exe等数据库客户端工具。 |
| 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力。 |
| 支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量自动登录多台设备。 |
| 审计日志要求 | 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志，本机能保存半年以上日志。 |
| 支持保存SSH传输，SFTP/FTP，RDP传输的原始文件。 |
| 支持审计主流数据库（如DB2、oracle、mysql、sql server）运维中的SQL语句，可进行关键信息定位查询。 |
| 支持全局搜索审计日志，无需区分图形/字符/文件/应用类型，只需通过关键信息直接搜索定位。 |
| 安全策略要求 | **支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功。（提供截图证明）** |
| 支持自动推送脚本任务，如可自动备份交换机/路由器的配置信息、可自动执行周期任务；并将结果以邮件/FTP/SFTP的方式发送给相关管理员。 |
| 报表统计要求 | 内置丰富的报表统计模板，可点击柱状图、饼状图或曲线图进行数据钻取分析，且支持PDF、doc、html格式导出。 |
| 支持一键导出符合等级保护要求的综合分析报告。 |
| 内置根据运维人员和组生成各种维度的分析报表，维度包含总为运维次数、时长、活动时长、会话起止时间、会话大小、命令数、上传下载文件数，分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供非常有价值有意义的报表。 |
| 系统管理要求 | 支持自身审计，包括但不限于：系统状态检测、登录日志、用户配置日志、设备配置日志、授权配置日志、策略配置日志、运维访问日志、系统配置日志等。 |
| 支持和同品牌的SOC系统进行联动，对绕过堡垒机而登录主机的行为，SOC进行实时告警，并且与SOC进行日志关联性分析。 |
| 产品资质 | 产品通过中国信息安全认证中心检测并获得证书。 |

**7．专网综合日志审计系统服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具基本要求 | CPU规格：≥4核；内存容量：≥8GB\*2；硬盘接口：2T；网口类型：≥4个千兆电口，≥4个千兆光口(配2个多模SFP光纤模块)，1个console口，电源配置：双电源；日志源授权：≥1000个。 |
| 工作模式 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统。 |
| 审计工作不影响被审计对象的性能、稳定性或日常管理流程。 |
| 日志收集 | 包括且不限于Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP等常见的网络、操作系统、数据库、中间件等日志收集。 |
| 支持使用代理（Agent）方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。 |
| 支持的设备厂家包括但不限于：Cisco(思科)、Juniper、联想网御/网御神州、F5、华为、H3C、微软、绿盟、飞塔(Fortinet)、Foundry、天融信、启明星辰、天网、趋势、东软、Nokia、CheckPoint、Hillstone(山石)、安恒信息、珠海伟思、BEA、中国电信、安氏、帕拉迪、APC、Arbor、Clam、戴尔（Dell）、Digium等。 |
| 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| **▲须满足业主方实际日志源的收集需求。** |
| 日志分析 | 支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息。 |
| 具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。 |
| 内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景。 |
| 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 |
| 日志查询 | 支持B/S模式管理，支持SSL加密模式访问。 |
| 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询。 |
| 支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 应用性能监控  （APM） | 支持监控设备自身CPU、内存、磁盘等工作运行状况。 |
| **通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。（提供截图证明）** |
| 综合查询及报表管理 | 内置合规性报表。 |
| 内置完善的等级保护合规报表。 |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
| 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力。 |
| 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。 |
| 产品资质 | 产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》。 |

**8．专网APT预警平台服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具基本要求 | MTBF 大于65000，小时吞吐率：≥网络层5Gbps；WEB检测：≥HTTP最大并发数10万；秒邮件检测：邮件处理数: ≥200万封/24小时；文件检测：≥10万个/24小时；电源：1+1冗余电源；CPU：≥10核20线程；内存：≥64G硬盘容量：≥2T\*2，；接口类型：≥千兆RJ45网口\*4；≥千兆业务SFP光口\*4（配置千兆多模光模块\*2）。 |
| 部署方式 | 旁路镜像模式部署，不影响服务器处理性能和网络架构。 |
| 全流量检测 | 支持全流量检测。  支持双向流量审计，可对请求和响应内容进行审计。 |
| IPv4 & IPv6网络 | 支持IPv4和IPv6网络环境下的部署，可同时对IPv4和IPv6网络流量分析检测。 |
| 检测风险类别 | 支持检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问、行为分析、DGA域名请求、SMB远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP欺骗、密码明文形式传输等行为。 |
| 弱口令风险检测 | 支持对HTTP、IMAP、SMTP、POP3、Redis、Telnet、FTP、PostgreSQL、MQTT等协议的弱口令检测。  支持自定义弱口令规则配置（最短口令长度、最少字符类型数），自定义新增弱密码及其检测类型。  支持对HTTP协议请求头中用户认证弱口令、对JSON格式(逗号分割和冒号区分键值)的用户信息提取和弱口令、明文口令和MD5加密口令碰撞的弱口令、BASE64加密口令的弱口令等进行检测。 |
| WEB登录 | 支持自定义HTTP登录行为关键字，包括用户名和密码。 |
| 主机威胁分析 | 支持对内网主机进行主机威胁分析，详细展示具体的威胁等级、威胁次数、攻击开始时间、攻击结束时间、威胁性指数统计等可按攻击链阶段（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）详细展示主机相关事件数量。 |
| 流量异常监控 | 支持对流量大小进行监控，接入流量超过物理网络带宽上限时报警。  支持对流量中的数据包、会话连接、重传包、网络报文等状态进行检测，可对业务网络流量传输异常告警。 |
| 协议解析 | 支持 HTTP、HTTPS（需要导入服务器私钥证书）协议解析，检测WEB攻击 |
| 攻击检测 | 支持30个以上的深度检测模块，对流量进行二次分析，提高攻击检测的准确性 |
| WEBSHELL检测 | 支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功。 |
| 子文件扫描 | 对文件内部嵌入的子文件可进行二次扫描，分析安全性。 |
| 本地威胁情报 | 设备集成离线的高可用威胁情报库，支持离线环境下，根据威胁情报进行检测，增量威胁情报随策略升级包升级。 |
| 威胁情报检索 | 支持对IP、域名、恶意文件SHA256进行威胁情报检索，或跳转第三方链接（安恒情报分析、Whois、VirusTotal）进行检索。  支持在告警详情页面直接查询与告警IP、域名相关的威胁情报，获取样本通信记录、情报画像等信息。 |
| 代理服务 | 支持使用代理服务器访问云端；支持代理服务器认证。 |
| 可视化展示 | 攻击溯源：支持大屏展示风险较为严重的事件，并进行攻击溯源，包括攻击主机个数最多的情报事件TOP10、威胁情报告警类型分布、3D攻击关系图、威胁活动（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）；支持按IP搜索关联的攻击事件，包括攻击拓扑图、攻击者基本信息、被攻击者信息、攻击过程（攻击过程列表内容包括时间、攻击者、被攻击者、攻击链阶段、风险标签、攻击次数）。 |
| 告警与报表 | 告警可详细展示风险级别、发生时间、告警名称、客户端IP、服务器IP、ATT&CK矩阵、报文内容（URL、请求头、请求参数、请求内容）。 |
| KAFKA服务器配置支持SASL认证和Kerberos认证；KAFKA数据传输支持明文或SSL加密。 |

**9．专网大数据安全管理平台服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具基本要求 | 数据采集和处理性能≥15000EPS，每条数据大小>1KB；  10亿数据关键字查询结果响应时间<2秒。  CPU ≥12核\*2 ，内存 ≥256GB，总容量≥64TB；  网口要求：≥千兆电口\*4，≥万兆光口\*2。 |
| 工作台 | 工作台首页支持自定义个性化配置，支持以拖拽方式进行画布页面设置，页面可选组件包括原始告警、资产管理、组件管理、风险资产、安全事件、安全日志、平台概览、快速搜索、安全设备、SOAR、系统消息、通报预警、工单、告警监控等，可选组件不少于36个，每个组件均支持点击“收藏”按钮进行自定义收藏。 |
| 菜单管理 | 支持菜单栏一页全局预览，菜单名称支持匹配检索，用户可点击菜单“收藏”按钮自定义收藏菜单和查看最近访问的菜单以便快速访问。 |
| 安全态势可视化 | 支持立体、平面、球面等多种维度的网络实体关系透视，点击每个实体可展示资产名称、风险评级、告警TOP3、最近异常发生时间等，点击实体间的访问连线可展示实体间访问方向、访问类型、累计流量、最近访问时间等。 |
| 分析中心 | 应内置包括规则模型、关联模型、统计模型、情报模型等多种安全分析模型。 |
| 安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容。 |
| 支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，保留检索语句历史记录；检索语句可直接发布成统计指标、规则模型、关联模型、情报模型，对实时数据进行分析与告警。 |
| 响应中心 | 支持通过单条告警、聚合告警添加白名单，快速过滤误报；白名单配置可自定义过滤条件及作用的组织架构，白名单生效时间设置包括长期生效和定期生效，新建白名单策略可将最近7天告警标记为已处置-误报；支持白名单策略状态的开启、关闭，并统计策略本日匹配次数。 |
| 支持前端拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种策略编排动作，包括但不限于数据源、分析组件、处置响应等，可自动判断策略编排是否合理并弹窗提示。 |
| 支持通过任务看板查看自动响应任务的数量、状态、任务趋势；可查询并追踪每条自动化响应任务的运行阶段查看详细信息，任务执行过程中可加入安管人员查验环节，通过邮件、短信方式将告警和分析报告推送到对应用户。 |
| 支持钉钉、阿里云、腾讯云等进行消息通知。 |
| 运营中心 | 平台具有统一的安全运营门户，作为重点关注功能的统一入口，如集成态势感知、Sherlock网络星空、通报预警、联动策略、运行监测等多个功能模块，实现平台功能的快速跳转；支持用户配置个人专属的统一门户，可配置项包括门户名称、菜单名称、应用图标等，且菜单内容支持自定义编辑，可链接平台以外的域名地址。 |
| 资产中心 | 支持人工录入、流量自动发现、主动扫描、web自动发现、资产同步等不少于5种的资产数据接入方式；流量自动发现方式能自动识别资产类型，如Web服务器、DNS服务器、邮件服务器、FTP文件服务器等多种类型资产，支持web业务系统自动发现；支持批量确认流量发现的资产。 |
| 运维管理 | 大数据平台支持一键巡检功能，检查项包含但不限于数据健康、探针健康检查、大数据集群健康、实时流计算引擎健康、管理服务健康、服务器节点健康等多种维度检查，提供巡检处置建议，并能将巡检结果导出PDF格式分析。 |
|
|
| 支持对接入探针进行运行监控，包括探针注册时间、设备IP、版本信息、许可证信息、本日数据上送条数、CPU利用率、内存使用率、磁盘使用率、网络流量大小、数据上送条数等；支持导入许可及导出许可申请文件。 |
| 支持对接入探针进行统一管理，支持查看探针在线、离线、升级等状态，可对license已过期、即将过期探针进行预警，对内存长时间超出阈值、CPU长时间超出阈值探针进行预警；支持平台统一升级和配置探针，沙箱文件检测可配置安全文件大小、文件访问方向、检测配置、检测结果复用、真实格式识别、沙箱网络行为、沙箱操作系统配置等，流量探针可配置检测模式。 |
| 支持自定义消息订阅，订阅方式包括机器人、短信、邮件、钉钉方式，消息类型包括告警通知、数据接入异常、系统资源使用超限、系统组件状态异常、探针状态消息、联动设备状态异常、系统配置异常、系统更新、日常运维等类型。 |
| 支持系统消息声音播报，机器人弹窗提醒，支持按时间顺序及消息类型查看系统消息。 |
| 工单管理 | 支持按照组织架构进行绩效考核，总部管理员可查看全局或单个组织的工单处理情况，包括滞留工单情况、风险资产情况及风险资产概率等。 |
| 驾驶舱 | 支持驾驶舱功能，总部驾驶舱能够看到市法院内以及所有基层法院的安全资产威胁态势；同时基层法院具备自己的账号，能够独立展示基层法院自身安全威胁态势。 |

**10．专网数据库审计服务**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基本要求 | | 支持的数据库实例个数：≥50； 峰值SQL处理能力≥20000条/秒； 硬件最大吞吐量≥2000Mbps； 双向审计数据库流量≥200Mbps； 标配日志存储数≥20亿条； 审计日志检索能力≥1500万条/秒；CPU≥4核8线程；内存≥8GB\*2；硬盘≥2TB\*2；内置≥300W交流双电源；≥4个千兆电口；≥4个千兆光口。 |
| 功能项 | 部署方式 | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计。 |
| 可在云环境操作系统中安装软件代理。 |
| 在目标数据库安装Agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计。 |
| 支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询、一键批量升级所有节点。 |
| 协议支持 | 支持Oracle（包括21C及其他版本）、PostgreSQL（14及其他版本）、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ、Vertica、TiDB、PolarDB、PolarDB-X、HANA等主流数据库的审计。 |
| 支持MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Cassandra、greenplum、LibrA、graphbase、cache、Redis、ArangoDB、Neo4j、OrientDB等数据库的审计。 |
| 审计功能 | 支持数据库操作表、视图、索引、存储过程等各种对象的所有SQL操作审计。 |
| 审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集,提供功能截图。 |
| **支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容，支持通过返回行数控制返回结果集大小。（提供截图证明）** |
| 支持超长SQL语句（最长4M）审计。 |
| 智能发现 | 支持自动发现流量中的数据库信息，简化配置。 |
| 安全审计 | 支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义。 |
| 产品具有内置规则，规则类型有SQL注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警。 |
| 支持信任规则，信任规则至少支持18个匹配条件。 |
| 统计报表 | 系统内置多种报表模板库，报表不少于20种。 |
| 报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告。 |
| 支持HTML、PDF、PNG、Word、csv、xls等格式的报表导出。 |
| 模型分析 | 可依据客户端工具名、数据库用户名、客户端IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器IP等配置行为模型，并可查看相应告警日志。 |
| Agent管理 | 支持在审计管理端批量安装、卸载、重新安装审计代理。 |
| 支持在审计页面直接升级或回退已安装在数据库服务器上的Agent，且升级或回退不需要输入数据库服务器的账号、密码。 |
| 可监控Agent的转发速率，以及Agent所在数据库服务器的CPU、内存利用率，并可设置CPU、内存利用率的上线阈值，超阈值时Agent将自动停止转发数据。 |
| 三层关联 | 可提供客户端访问Web服务器的URL和应用服务器访问数据库的SQL语句关联功能。 |

**11．威胁情报分析服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具基本要求 | ≥4\*GE管理电口；3\*USB3.0接口；1\*DB9 Console接口；冗余电源；内存≥128G；≥960G SSD + ≥8\*4TB SATA 存储硬盘。 |
| 日志存储 | 须满足网络安全法要求，满足用户方的6个月日志存储,需具备高性能的Syslog日志处理和存储方法的技术。 |
| 威胁感知 | 支持与云端安全运营中心联动。设备能连接互联网时，安全专家在云端分析并撰写威胁分析报告下发到设备上共用户查阅；设备离线时，可将关键数据离线导出上传到云端安全运营中心，安全专家进行分析撰写威胁分析报告。 |
| 支持大屏展示网络攻击态势，包括整体网络风险指数、告警总数、攻击次数、攻击IP数、攻击源国家/地区TOP5、攻击态势，并支持自动翻转的攻击全景地图展示。 |
| 支持大屏展示整体威胁事件态势，包括威胁类型分布、威胁类型TOP5、受害主机TOP5、威胁事件趋势、最新告警事件、威胁星云图。 |
| 支持大屏展示资产包括外部访问、横向访问、内网外联态势。 |
| 支持大屏展示整体资产风险态势，包含资产树结构、资产分类、开放服务统计、网段管理、资产风险趋势、资产风险状态。 |
| 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。 |
| 支持以受害资产维度进行分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组。 |
| 以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。 |
| 支持与云端威胁情报中心联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等。 |
| 威胁分析 | 支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析。 |
| 威胁情报维度分析包括：情报详情、影响资产列表、资产的行为（行为包含：DNS解析、TCP流量、UDP流量、WEB访问、文件传输）。 |
| 应用安全的细分维度包括：WEB安全、数据库安全、中间件安全；  系统安全的细分维度包括：暴力破解、弱口令、未授权访问、挖矿行为  设备安全。 |
| 白名单 | 支持对告警进行加白，加白参数包括受害IP、攻击IP、威胁情报、规则、XFF、URL、威胁名称。 |
| 行为分析 | 支持可疑DNS解析：能够检测发现DGA域名与DNS隧道域名，支持根据时间范围、请求次数、DNS域名总长度自定义DNS隧道检测规则。 |
| 支持疑似DNS服务器发现：能够根据响应DNS请求与发起DNS请求进行行为分类。 |
| 支持链路劫持分析：能够展示被劫持对象、CDN服务器、被劫持资源、文件MD5、访问时间等详细信息。 |
| 支持可疑代理分析：能够发现socks、http、reDuh、Regeory Tunnel、Tunna等代理类型。 |
| 支持邮件敏感词与敏感后缀发现，自定义敏感词与敏感后缀，并能进行邮箱白名单配置。 |
| 支持暴力破解行为检测，检测内容包含：源ip、目的ip、使用协议、爆破次数、爆破成功与否等。 |
| 支持外部访问分析，能展示源ip、资产ip、端口、协议、时间等详细信息，且能自定义源ip白名单。 |
| 支持异地账号登录行为检测，检测内容包含：登录IP归属、账号、登录资产IP、使用协议、登录次数、登录成功率。 |
| 威胁狩猎分析 | 支持对任意线索的自定义拓线及溯源取证分析，支持以可视化分析画布形式展示拓线过程并支持结果快照导出；支持对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。 |
| 响应处置 | 支持工作流程自定义编排。 |
| 支持联动服务管理，支持python语言与javascript语言在web页面编辑联动服务。 |
| 支持任务脚本自定义编辑，支持python语言与javascript语言在web页面进行编辑。 |
| 支持策略定义，可根据工作流进行处置动作定义，且能根据告警类型、攻击结果、威胁类别进行联动策略定义。 |
| 支持编排处置日志记录，记录处置时间、受害ip、攻击ip、告警类型、威胁名称、域名、处置策略、告警来源等信息。 |
| 威胁溯源 | 支持检索异常报文、域名解析、文件传输、FTP控制通道、LDAP行为、登录动作、邮件行为、MQ流量、网络阻断、数据库操作、SSL加密协商、TCP流量、Telnet行为、UDP流量、WEB访问等网络流量日志，并可基于时间、IP、端口、协议、上下行负载等多重字段组合进行日志检索。 |
| 可视化展示 | 支持大屏展示网络攻击态势，包括整体网络风险指数、告警总数、攻击次数、攻击IP数、攻击源国家/地区TOP5、攻击态势，并支持自动翻转的攻击全景地图展示。 |
| 支持大屏展示整体威胁事件态势，包括威胁类型分布、威胁类型TOP5、受害主机TOP5、威胁事件趋势、最新告警事件、威胁星云图。 |
| 支持大屏展示整体资产风险态势，包含资产树结构、资产分类、开放服务统计、网段管理、资产风险趋势、资产风险状态。 |
| 支持大屏展示资产包括外部访问、横向访问、内网外联态势。 |
| 系统管理 | 支持横向扩展至多台设备集群。 |
| 本系统需与省高院现有的威胁情报分析平台对接。 |
| 提供告警展示场景，支持展示场景的切换。每个告警展示场景中支持自定义页面数据展示的范围，方便管理人员的日常运维工作。 |

**12．威胁情报收集服务**

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基本要求 | | 千兆电口≥4个，流量吞吐≥1Gbps，并发会话≥150W，新建会话≥1W，内存≥32GB，硬盘容量≥1T。 |
| 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等）、压缩格式文件（RAR、ZIP、GZ、7Z等）、文档类型文件（word、excel、pdf、rtf、ppt等）。 |
| 数据库协议 | 支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、MySQL、PostgreSQL等协议。 |
| 会话流量 | 支持TCP/UDP会话记录、异常流量会话记录、web访问记录、域名解析、SQL访问记录、邮件行为、登录情况、文件传输、FTP控制通道、SSL加密协商、telnet行为、IM通信等行为描述。 |
| 自定义协议 | 支持自定义协议和端口，满足特殊场景下的流量抓取。 |
| 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200+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。 |
| 支持跨站请求伪造CSRF攻击检测。 |
| 支持其他类型的WEB攻击，如目录遍历、弱口令、权限绕过、信息泄露、文件包含、文件写入攻击等检测。 |
| 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。 |
| 支持基于webshell函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg\_replace代码执行等。 |
| 支持基于代理程序的攻击检测，如TCP代理程序、HTTP代理程序等。 |
| 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：协议异常、网络欺骗、黑市攻击、代码执行等。 |
| 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。 |
| 语义分析 | 支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力。 |
| 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。 |
| 支持基于URL的旁路阻断，并能将URL请求进行重定向。 |
| 自定义弱口令 | 支持自定义弱口令字典，支持HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP等协议的自定义弱口令检测。 |
| HTTPS威胁检测 | 支持旁路HTTPS解密、威胁检测。 |
| 高级参数 | web端提供针对恶意扫描、Flood攻击、IP碎片攻击、ARPSpoof、PingSweep等检测策略配置功能。 |
| 管理功能 | 部署模式 | 支持旁路部署，可同时接入多个镜像口，每个镜像口相互独立不影响。 |
| 系统配置 | 支持AES256、SM4数据传输加密，确保数据传输的安全性。 |
| 支持威胁告警信息发送给syslog服务器，支持将威胁告警、威胁等级、网络日志、攻击结果、威胁类型等日志传输给KAFKA、威胁分析平台。 |
| 支持与集中管理平台进行联动，统一进行情报、规则的升级。 |

**13．安全准入服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具要求 | 1、配置6个及以上1000MBASE-T接口；每秒事务数（TPS)：≥1700（次/秒），最大吞吐量：≥1Gbps，最大并发连接数：1600（条）；至少支持1000个认证终端。  2、支持在IPv4和IPv6双栈环境下的终端准入控制、重定向、认证、安检、修复等。  3、准入设备须支持802.1x协议准入方式，无需第三方RADIUS服务器支持。准入设备支持基于策略路由技术的准入控制模式，可以为来宾开通安全域,根据策略对来宾开放有限的网络资源，来宾访问无法获取内部网络的访问。  4、单台准入设备可支持至少4路策略路由准入控制。单台准入设备可支持至少4 个镜像口进行准入控制。  5、注册认证通过MAC地址、硬件信息得出唯一识别号绑定，终端入网IE浏览器重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。  6、检查终端是否安装杀毒软件,确保接入终端的防病毒能力,支持现有常用杀毒软件的检测,提供系统补丁安装情况的检查,为终端安全加固提供双重保障，对接入终端的软件安装进行规范管理,通过设置黑白名单禁止可疑、非法进程运行,监控业务进程使用。  7、具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，帮助清查通过网中网隐藏的真实网络终端。  8、能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP表等信息。支持在界面上提供对该网络设备进行TELNET、SSH等管理。能够在网络拓扑图上由用户自定义显示的节点类型，方便用户通过不同方式查看拓扑连接。  9、为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要包括：报警、安全风险等级、全网终端数、清理终端数、安检合规率、安检项状态分布。  10、准入设备后台提供每日入网报告、每周入网报告、每月入网报告。  11、基于双向认证的于双向认的网络准入控制,由终端代理认证机制和防火墙控制机制实现的,终端双方要实现可信通信必须进行终端代理双向认证,并且由认证防火墙阻断其非法的通信请求。 |

**14．安全培训服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每季度至少1次 |
| 服务内容 | 派遣资深信息安全培训专家提供现场信息安全培训课程。  1、安全意识培训  通过网络安全意识培训，对日益猖獗的病毒、木马等威胁进行必要的描述，使用户全体人员对网络安全的有初步的认识和逐步提高安全意识，并阐明具体的防范措施让安全事故可以得到有效的避免。  2、安全技术培训  介绍黑客攻击途径，着重描述当前流行的攻击技术和防御手段，对安全领域和知识进行清晰划分和描述，通过大量的现场模拟和环境加固实践提供用户专业技术人员的技术水平。  3、管理人员培训  对管理人员的培训，目的是使用户管理人员了解国家相关部门对系统网络安全管理和建设的相关标准，同时建立起一套具有针对性和适用性的安全管理办法。 |
| 交付物 | 《网络安全宣传教育培训签到表》、《网络安全宣传教育培训会议纪要》、网络安全宣传教育培训活动现场照片 |

**15．应急演练服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每年度至少1次 |
| 服务内容 | 每年进行至少1次应急演练服务，演练的系统范围包括全部定级业务系统，依据网络与信息安全应急预案，演练的系统范围包括定级业务系统或圈定的业务系统，依据网络与信息安全应急预案，模拟应对突发事件的活动。通过应急演练，进一步加强对应急处理预案的理解，通过演练检验预案中网络安全事件等级划分、响应流程等的合理性。 |
| 交付物 | 《应急预案》、《应急演练方案》、《攻防演练技战法报告》、《攻防演练总结报告》 |

**16．网络安全专项检查服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每年度至少1次 |
| 服务内容 | 安全检查的服务范围为信息系统及支撑信息系统的网络设备、安全设备、中间件、数据库等信息化资产  1、安全扫描：对网络设备、主机、数据库、操作系统、中间件、业务系统等应用等进行安全漏洞扫描。  2、数据分析：由安服专家对扫描的漏洞和采集的流量数据及安全日志进行分析工作，由安全专家根据现场实际情况与经验判断是否是关键风险，从而辅以主动发现。  3、安全加固：根据资产梳理、安全扫描、数据分析的输出结果进行总结之后，输出针对现有系统风险的安全加固建议报告，安全加固建议报告中为用户提供符合业务需求的安全整改建议，从多角度多维度整改存在的安全问题，将用户的安全水平提升至更高的层次，尽量避免风险的重复性出现，保障业务系统安全可靠运行。  4、开展本单位网络安全运维，包括安全加固、监测预警、响应处理工作。 |
| 交付物 | 《安全专项检查报告》 |

**17．漏洞扫描服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院 |
| 服务频率及期限 | 每季度至少1次 |
| 服务内容 | 漏洞扫描会对网络设备、主机、操作系统、中间件、业务系统等应用等进行安全漏洞识别，在政务部门的授权与监督下，采用漏洞扫描工具进行漏洞识别与分析，并给出漏洞修复建议。 |
| 交付物 | 《渗透测试报告》 |

**18．基线核查服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院 |
| 服务频率及期限 | 每季度至少1次 |
| 服务内容 | 根据定义的安全配置基线，对全市法院服务器安全配置情况进行检查，以发现可能会被攻击者利用的安全配置不当与建设不足，达到合规要求，提升安全防护有效性。 |
| 交付物 | 《渗透测试报告》 |

**19．渗透测试服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每年度至少1次 |
| 服务内容 | 通过真实模拟黑客使用的工具、分析方法对采购人指定系统进行模拟攻击，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误等以及其他专项内容测试与分析，重点发现应用层业务流程和逻辑上的安全漏洞和敏感信息泄露的风险。 |
| 交付物 | 《渗透测试报告》 |

**20．应用上线检查服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 根据采购人实际需求确定 |
| 服务内容 | 采用专业工具和安全专家人工检测相结合的方式，对采购人新上线系统进行安全检查服务，及时发现可能存在的安全漏洞，提出安全建设整改建议，作为漏洞修复和加固整改的参考依据，确认修复整改后方可上线。 |
| 交付物 | 《系统上线检查报告》 |

**21．安全运维服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 按需 |
| 服务频率及期限 | 按需提供/年 |
| 服务内容 | 1、按照等级保护要求，结合单位特点，协助搭建网络与信息安全工作架构，明确安全工作内容和职责，提供等级保护要求的各类文件、制度、机制参考模板。（中院）  2、明确年度网络安全工作主要目标、基本要求和工作任务（中院）  3、全市法院系统运维接入堡垒机。（中院、基层院）  4、全市法院防火墙配置细化到具体IP。（中院、基层院）  5、全市法院数据中心服务器部署安装安全防护软件、中院终端部署安装安全防护软件。（中院、基层院）  6、对全市法院服务器、操作系统、数据库、应用系统、中间件操作日志进行审计。（中院、基层院）  7、对全市法院数据库进行审计。（中院、基层院）  8、全市法院安全基础设施巡检（中院）  9、选派具有相关网络与信息安全技能和经验的技术人员现场服务，协助做好网络安全考核资料收集整理（中院、基层院） |
| 交付物 | 按需提供相应服务报告 |

1. **资产梳理服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每年度至少1次 |
| 服务内容 | 使用工具（RAP、TSS等）对包括：业务系统、服务器、安全设备、网络设备等进行自动化扫描发现、识别、评估。  建立信息系统数据资产清单，对资产进行分级分类和标识，对软件、硬件、电子及实体资产生成使用规范，网络拓扑图。 |
| 交付物 | 《IT资产表》、《网络拓扑图》、《业务关系统图》 |

1. **数据备份服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院 |
| 服务频率及期限 | 每月至少一次 |
| 服务内容 | 数据备份：实现重要数据进行异地定期增量备份，并定期验证备份文件。  配置归档：网络设备和安全设备配置定期备份保存。 |
| 交付物 | 《配置文档》、《备份记录》 |

**24.** **网络入侵攻击监测分析服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每月至少一次 |
| 服务内容 | 通过人工服务结合入侵检测相关大数据安全分析平台对骨干网络出口和重要网络节点进行严密监控，及时预警。 |
| 交付物 | 《每月日常威胁运维记录》 |

**25.** **异常流量态势监测服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每月至少一次 |
| 服务内容 | 通过人工服务结合异常流量监测相关探针，网流量进行深度检测。 |
| 交付物 | 《每月日常威胁运维记录》 |

**26.** **安全隐患处置服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院、基层院 |
| 服务频率及期限 | 每月至少一次 |
| 服务内容 | 通过网络安全监测平台监测本地区的高危隐患和安全事件，对本地区的高危隐患和安全事件进行主动发现，形成高危隐患和安全事件的整改处置报告。 |
| 交付物 | 《事件响应报告》 |

**27.重大事件应急响应服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院 |
| 服务频率及期限 | 按需提供 |
| 服务内容 | 发生安全事件时，提供远程或现场的7\*24小时应急响应服务。 |
| 交付物 | 《应急响应报告》 |

**28.特殊时期的安全巡检和保障服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 中院 |
| 服务频率及期限 | 按需提供 |
| 服务内容 | 在重要时间节点提供重保服务，在攻防演练时间段，对管辖范围内的重要系统进行安全监测。 |
| 交付物 | 《重保值守报告》 |

**三、其他要求**

1、项目服务期限：合同签订之日起1年。

**▲2、中标（成交）后5个工作日内，投标人提供样机进行功能要求的测试验证，测试中发现虚假应标的行为将予以废标处理并保留采购方对投标人追究相关责任的权利。合同签订后14天内完成设备安装调试。**

3、投标人在接到采购方故障申告电话后应在10分钟内给予响应，如故障未能在30分钟内通过远程支持得到解决，投标人应启动现场应急服务，在自采购方电话申告起4小时内赶到采购方现场；故障应在投标人工程师到达现场后不超过24小时内给予恢复运行；如不能恢复的应提供备用设备，保障采购方的正常工作，在最迟不超过5个工作日内，将损坏的硬件部件进行维修。如果确认设备或者部件损坏无法修复致使该设备无法继续使用，投标人应将损坏设备进行整体更换，更换的设备配置不得低于当前配置。

4、投标人应为本次工作的全部人员和第三方责任人员设备、设施等办理保险并承担全部风险责任，所需的费用包含在投标报价中。

5、付款方式：按中标方中标价总额签订合同，设备安装调试完成后（在财政资金下达前提下）的7个工作日内采购方支付合同总额的40%，其余60%待合同到期验收合格后支付。

6、如果运维不当，采购方发生网络安全事件被市本级相关单位通报，每次扣除合同金额的5%，累计三次扣除合同金额的60%并终止合同；被省级及以上单位通报一次，扣除合同金额的20%，通报两次，扣除合同金额的60%并终止合同。

7、采购文件中未提及但要实现本采购文件的功能而必配的其他设备(含配件及授权数量)由供应商自行考察并且计入本次投标总价中。

**▲8、要求提供一名具备安全服务工作经验的技术人员，进行驻场安全运维服务（中院及各县市区法院现场服务），并提供该名人员社保证明。**

9、驻场运维人员如在业主方食堂就餐需按照每人每年4200元标准缴纳搭伙费，投标人投标时需考虑相关费用。

**四、本项目中标（成交）供应商应在浙江省政府采购网（http://zfcg.czt.zj.gov.cn）上注册成为“政府采购供应商”，如不按要求注册的，采购方有权延期发布中标（成交）通知书和中标（成交）公告，后果由供应商自行承担。**

**第五章 政府采购合同主要条款**

（此稿为合同样本，最终定稿待双方协商后定，但不得背离实质性内容）

合同将由台州市中级人民法院（以下简称甲方）与经评审最终确定的中标人（以下简称乙方）结合本项目具体情况协商后签订。以下为采购人提出涉及乙方的主要条款，投标人在磋商响应文件中应对其进行确认或拒绝。如投标人在其磋商响应文件中未做拒绝或提出调整完善要求的，采购人将视作认同。具体如下：

项目编号：

**甲方：**（采购方）台州市中级人民法院

**乙方：**（供应商）

甲、乙双方根据台州市中级人民法院信息安全运维服务项目竞争性磋商的结果，签署本合同。

**第一条：服务内容**

详见本项目采购文件第四部分《项目需求》。

**第二条：合同金额**

本合同金额为(大写): 元 (￥: 元) 人民币。

**第三条：技术资料**

1、乙方应按采购文件规定的时间向甲方提供有关技术资料。

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。

**第四条：知识产权**

1、乙方应保证提供服务过程中不会侵犯任何第三方的知识产权和其他权利。

2、本项目所有成果以及采集的数据的知识产权和其他权利属甲方所有，乙方不得以任何形式向第三方提供，否则，按国家法律和有关规定追究乙方的一切责任，并要求乙方承担甲方因此造成的损失。

3、本项目作业过程中提供的或涉及的所有数据属甲方拥有，乙方无权在技术要求规定之外自行处置数据，不得自行删除、复制、调整完善、转移数据，不得以任何形式擅自使用或向第三方提供。

4、若侵犯,除承担本协议中的违约责任外，还应由乙方赔偿甲方因此遭受的损失（包括但不限于应对及追偿过程中所支付的律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）。

**第五条：转包或分包**

1、本合同范围的服务，应由乙方直接供应，不得转让他人供应；

2、乙方不得将本合同范围的服务全部或部分分包给他人供应；

3、如有转让和分包行为，甲方有权解除合同，并追究乙方的违约责任。

**第六条：付款方式**

1、按合同金额签订合同，设备安装调试完成后（在财政资金下达前提下）的7个工作日内甲方支付合同总额的40%，其余60%待合同到期验收合格后支付。

2、如果运维不当，甲方发生网络安全事件被市本级相关单位通报，每次扣除合同金额的5%，累计三次扣除合同金额的60%并终止合同；被省级及以上单位通报一次，扣除合同金额的20%，通报两次，扣除合同金额的60%并终止合同。

3、驻场运维人员如在甲方食堂就餐需按照每人每年4200元标准缴纳搭伙费。

**第七条：项目要求**

1、时间要求：合同签订之日起1年。

2、中标（成交）后5个工作日内，乙方提供样机进行功能要求的测试验证，测试中发现虚假应标的行为将予以废标处理并保留甲方对乙方追究相关责任的权利。合同签订后14天内完成设备安装调试。

3、乙方在接到甲方故障申告电话后应在10分钟内给予响应，如故障未能在30分钟内通过远程支持得到解决，乙方应启动现场应急服务，在自甲方电话申告起4小时内赶到甲方现场；故障应在乙方工程师到达现场后不超过24小时内给予恢复运行；如不能恢复的应提供备用设备，保障甲方的正常工作，在最迟不超过5个工作日内，将损坏的硬件部件进行维修。如果确认设备或者部件损坏无法修复致使该设备无法继续使用，乙方应将损坏设备进行整体更换，更换的设备配置不得低于当前配置。

4、要求提供一名具备安全服务工作经验的技术人员，进行驻场安全运维服务（中院及各县市区法院现场服务），并提供该名人员社保证明。

**第八条：违约责任**

1、甲方无正当理由拒收接受服务的，甲方向乙方支付合同款项百分之五作为违约金。

2、 甲方无故逾期验收和办理款项支付手续的，甲方应按逾期付款总额向乙方支付每日万分之五违约金。

3、乙方逾期提供服务的，乙方应按逾期天数向甲方支付每日万分之五违约金。逾期超过约定日期10个工作日提供服务的，甲方可解除本合同。乙方因逾期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同款项百分之五的违约金，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、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）。

**第九条：不可抗力事件处理**

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120天以上，双方应通过友好协商，确定是否继续履行合同。

4、如合同履行时间内，因不可抗力原因需要延迟相关活动或解除合同的，由双方进行协商；合同解除后，双方根据乙方的实际履行支付情况及凭证（发票）进行结算。

**第十条：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，可向甲方所在地法院起诉。

**第十一条：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、合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

3、本合同未尽事宜，遵照《民法典》有关条文执行。

4、本合同壹式陆份，甲、乙双方、采购代理机构各执贰份。本项目未尽事宜以采购文件、磋商响应文件及澄清文件等为准。

5、与本合同有关标书及记录同本合同具有同等法律效果。

（以下无正文）

（签章页）

甲方（公章）： 乙方（公章）：

法定代表人或授权委托代理人签字： 法定代表人或授权委托代理人签字：

联系电话： 联系电话：

开户银行： 开户银行：

账 号： 账 号：

合同见证方：

签订日期： 年 月 日

**第六章 响应文件格式附件**

**附件1**  　　　本

项目名称

项目编号：

**磋**

**商**

**响**

**应**

**文**

**件**

**（资格证明文件）**

供应商全称（公章）：

地 址：

时 间：

**资格证明文件目录**

1、磋商声明书（附件2）

2、授权委托书（附件3）

3、法人或者其他组织的营业执照等证明文件，法定代表人和授权代表的身份证明

4、供应商认为需要说明的其他材料

**附件2**

**磋商声明书**

台州市中级人民法院、台州永安工程咨询有限公司：

（ 供应商名称 ）系中华人民共和国合法企业，经营地址 。

我（ 姓名 ）系（ 供应商名称 ）的法定代表人，我公司自愿参加贵方组织的信息安全运维服务项目（编号为tzya2025-tz37）的磋商，为此，我公司就本次磋商有关事项郑重声明如下：

一、我公司声明截止投标时间前三年内：在经营活动中没有重大违法记录（重大违法记录是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚）。

二、我公司在参与磋商前已详细审查了磋商采购文件和所有相关资料，我方完全明白并认为此磋商采购文件没有倾向性，也没有存在排斥潜在供应商的内容，我方同意磋商采购文件的相关条款，放弃对磋商采购文件提出误解和质疑的一切权利。

三、我公司不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。

四、我公司保证，采购人在中华人民共和国境内使用我公司磋商响应的货物、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，该责任由我方承担。我方的总报价已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。

五、我公司严格履行采购合同，不降低合同约定的产品质量和服务，不擅自变更、中止、终止合同，或拒绝履行合同义务；

六、我公司承诺（若代理服务费由中标单位支付）：如在本项目中标，我公司在成交公告发布之日起5个工作日内按采购文件约定支付代理服务费。

七、以上事项如有虚假或隐瞒，我公司愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

供应商名称(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

**附件3**

**授权委托书**

台州市中级人民法院、台州永安工程咨询有限公司：

（供应商全称） 法定代表人（或营业执照中单位负责人） （法定代表人或营业执照中单位负责人姓名） 授权 （授权代表姓名） 为授权委托代理人，参加贵单位组织的信息安全运维服务项目（编号为tzya2025-tz37）的采购活动，并代表我方全权办理针对上述项目的磋商、签约等具体事务和签署相关文件。我方对授权委托代理人的签字事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。授权委托代理人在授权委托书有效期内签署的所有文件不因授权的撤销而失效。

授权委托代理人无转委托权，特此委托。

法定代表人签字或盖章：

供应商全称（公章）：

日期：

**附：**

|  |
| --- |
| **法定代表身份证正、反面复印件粘贴处** |

法定代表人姓名：

传真：

电话：

详细通讯地址：

邮政编码：

|  |
| --- |
| **授权委托代理人身份证正、反面复印件粘贴处** |

授权委托代理人姓名：

职务：

传真：

电话：

详细通讯地址：

邮政编码：

**政府采购活动现场确认声明书**

台州永安工程咨询有限公司：

本人经由 （供应商全称） 负责人 （法定代表人姓名） 合法授权参加信息安全运维服务项目（编号：tzya2025-tz37）政府采购活动，经与本单位法定代表人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

一、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 。

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

四、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。

五、本单位若有违反诚信投标、采购法律法规等行为，愿意按照采购文件规定接受投标担保的处理。如已中标，自动放弃中标资格；给招标人造成损失的，依法承担赔偿责任。

（供应商代表签字或盖章）

年 月 日

**附件4**  　　　本

项目名称

项目编号：

**磋**

**商**

**响**

**应**

**文**

**件**

**（商务与技术文件）**

供应商全称（公章）：

地 址：

时 间：

**商务与技术文件目录**

**第一部分：评标索引**

评标索引：自评表（附件5）

**第二部分 ：商务与技术部分**

1、供应商基本情况表（附件6）

2、项目组织实施方案；

3、项目实施人员一览表（附件7）；

4、项目负责人资格情况表(附件8)；

5、商务及技术响应表（附件9）

6、企业证书一览表（附件10）；

7、类似项目实施情况一览表（附件11）

8、售后服务措施及承诺（可视情选用附件12）；

**附件5**

**评标索引：自评表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **评标因素** | | **评分标准** | **分值** | **对应页码** | **自评分** |
| 商务分（13分） | 企业综合实力 | 投标人具有ITSS信息技术服务运行维护资质、信息安全服务资质的，每个资质证书得1分，本项最高得2分。  **（须提供相应的证书扫描件（相关证书应在有效期内）加盖投标人公章编入投标文件中，未提供的不得分）** | 2 |  |  |
| 投标人具有国家认证认可监督管理委员会批准认可的认证机构颁发的，且在有效期内的信息安全管理体系认证、信息技术服务管理体系认证的，每个认证证书得1分，本项最高得2分。  **（须提供相关证书扫描件及[全国认证认可信息公共服务平台](https://www.so.com/link?m=bgeKa5pUJ7jqGvX1HhllAJLNiphU7TZFNQwb4+7ZUZpVLH3/mqlCJ7rNGXZ5/YNpLh7l1an07AVpzdd+DNfDz03MHubLsbYxQOzT8llEFb57FaGuLm6gSmMhBy2lLDBrTFSNNDZqVzwQMcexMhSdw5Kuw+3MXS7HQcV4Anm9Fs1KmUyptcyDigHMKmFQMXtO7xSEBzzl+542xjBTD4X4Ft///zWSTHNTKcszTMLGSmT541nhMntevTSaKintmdBbT4YHZJEfW00MedhN8WiQ3A1LHjOM=" \t "https://www.so.com/_blank)网站截图并加盖投标人公章编入投标文件中，未提供或提供不全的不得分）** | 2 |  |  |
| 项目组人员配置情况 | 拟投入本项目的项目负责人：具有信息系统项目管理师（软考）证书、信息安全工程师（软考）证书、CISP认证证书的，每提供1个得1分，本项最高得2分。  **（须提供相应的证书扫描件（相关证书应在有效期内）和投标人为其缴纳的近3个月社保证明加盖投标人公章编入投标文件中，未提供或提供不全的不得分）** | 2 |  |  |
| 根据驻场服务技术人员（1名）的专业资质和从业经验情况进行打分。  1、专业资质优秀的得1分，资质一般的得0.5分，未提及此项不得分。  2、从业经验丰富的得1分，经验一般的得0.5分，未提及此项不得分。  本项最高得2分。  **（须提供投标人为其缴纳的近3个月社保证明加盖投标人公章编入投标文件中，未提供的不得分）** | 2 |  |  |
| 根据本地化服务团队支撑技术人员的专业资质和从业经验等情况进行打分。团队整体专业资质优秀，从业经验丰富的得2分，资质和经验一般的得1分，资质和经验有待加强的得0.5分，未提及此项不得分。  **（须提供投标人为相关人员缴纳的近3个月社保证明加盖投标人公章编入投标文件中，未提供或提供不全的不得分）** | 2 |  |  |
| 承接经验 | 投标人自2022年7月1日（以合同签订时间为准）以来，承接过类似项目的，每提供一个项目合同得1分，最高得3分。  **（须提供合同扫描件并加盖投标人公章编入投标文件中，未提供的不得分）** | 3 |  |  |
| 技术分（57分）  （54分） | 现状分析 | 根据投标人对项目现状了解的情况进行打分。  现状分析深入，内容全面准确，见解到位的得5分；  现状分析基本到位，内容基本全面准确的得4分；  现状分析内容一般，有欠缺的得3分；  现状分析基本提及的得1分；  未提及此项不得分。 | 5 |  |  |
| 项目建设思路 | 根据投标人对本项目建设思路的理解、重难点的把握进行打分。  思路清晰，重难点把握准确，理解深入的得5分；  思路基本清晰，重难点把握基本准确，理解基本深入的得4分；  思路模糊，重难点把握及定位不够准确的得3分；  建设思路基本提及的得1分；  未提及此项不得分。 | 5 |  |  |
| 技术方案 | 根据投标人技术方案与本项目需求的吻合程度进行打分。  方案详细、完善、科学合理，适用本项目需求的得5分；  方案比较详细完善，基本满足本项目需求的得4分；  方案内容欠佳，不够详细的得3分；  技术方案简单提及的得1分；  未提及此项不得分。 | 5 |  |  |
| 技术参数响应 | 根据投标人所提供的设备技术指标与需求全部满足采购文件要求的得满分18分，负偏离或不满足的一项扣1分，扣完为止。 | 18 |  |  |
| 根据投标人所提供的服务全部满足采购文件要求的得满分10分，负偏离或不满足的一项扣1分，扣完为止。 | 10 |  |  |
| 实施方案 | 根据投标人提供的组织实施方案，包括产品供货、验货、安装调试、调优、验收等内容进行打分。  方案详实、内容完整、供货安排操作性强，进度详细有保障，验收标准符合行业标准且有针对性的得5分；  方案基本详实、内容基本完整、供货安排操作性比较强强，进度安排基本合理，验收标准基本符合行业标准的得4分；  方案粗糙、内容缺漏、供货安排操作性一般，保障性和合理性有待加强的得3分；  实施方案简单提及的得1分；  未提及此项不得分。 | 5 |  |  |
| 培训方案 | 根据投标人针对本项目制定的培训方案的合理性、科学性、可行性等情况进行打分。  培训方案内容齐全，可操作性强的得4分；  培训方案内容基本齐全，可操作性比较强的得3分；  培训方案内容一般，可操作性一般的得2分；  培训方案不够周全、可操作性有待加强的得1分；  未提及此项不得分。 | 4 |  |  |
| 应急处置方案 | 根据投标人结合本项目的特点，对网络信息安全中可能出现的突发情况分析以及应急处置方案的完整性、合理性、针对性等因素进行打分。  方案说明详细、考虑齐全、科学合理，与本项目吻合的得5分；  方案说明内容一般，基本科学合理，基本满足需求的得4分；  方案说明内容欠佳，不够详细的得3分；  应急方案简单提及的得1分；  未提及此项不得分。 | 5 |  |  |

**附件6**

**供应商基本情况表**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 企业名称 |  | | | | | | 法定代表人代表 | | |  | |
| 地址 |  | | | | | | 企业性质 | | |  | |
| 股东姓名 |  | 股权结构（%） | |  | | | 股东关系 | | |  | |
| 联系人姓名 |  | 固定电话 | |  | | | 传真 | | |  | |
| 手机 | |  | | |
| 一、  企  业  概  况 | 职工人数 |  | | 具备大专以上学历人数 |  | | 国家授予技术职称人数 | | |  | |
| 占地面积 |  | | 建筑面积 | 平方米  □自有□租賃 | | 生产经营场所及场所的设施与设备 | | |  | |
| 注册资金 |  | | 注册发证机关 |  | | | | | 公司成立时间 |  |
| 核准经营范围 |  | | | | | | | | | |
| 发展历程及主要荣誉： | | | | | | | | | | |
| 二、  企业有关资质获证情况 | 产品生产许可证情况（对需获得生产许可证的产品要填写此栏） | | 产品名称 | | | 发证机关 | | 编号 | 发证时间 | | 期限 |
|  | | |  | |  |  | | |
| 企业通过质量体系、环保体系、计量等认证情况 | |  | | | | | | | | |
| 企业获得专利情况 | |  | | | | | | | | |

**要求：**

1、姓名栏必须将所有股东都统计在内，若非股份公司此行（第三行）无需填写；

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件7**

**项目实施人员一览表**

（主要从业人员及其技术资格）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **姓名** | **职务** | **职责** | **专业技术资格** | **证书编号** | **参加本单位工作时间** | **劳动合同编号** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**要求：**

1、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。

2、附人员证书复印件；

3、出具上述人员在本单位服务的外部证明，如：投标截止日之前的代缴个税税单、参加社会保险的《投保单》或《社会保险参保人员证明》等。

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件8**

**项目负责人资格情况表**

采购项目： 采购编号：

|  |  |  |
| --- | --- | --- |
| **姓名** |  | **近年来主要工作业绩** |
| **性别** |  | 注：业绩证明应提供佐证材料  （服务合同或中标通知书）。 |
| **年龄** |  |
| **职称** |  |
| **毕业时间** |  |
| **学校专业** |  |
| **联系电话** |  |
| **最近一年工作状况** |  |
| **拟在本项目中担任主要工作** |  | |

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件9**

**商务及技术响应表**

**项目名称及编号：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **类别** | **内容** | **磋商文件技术要求** | **磋商响应文件技术响应** | **偏离情况** |
| 商务响应情况 | 服务期 |  |  |  |
| 付款方式 |  |  |  |
| …… |  |  |  |
|  |  |  |  |
| **类别** | **名称** | **磋商文件技术要求** | **磋商响应技术响应** | **偏离情况** |
| 技术响应情况 |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件10**

**企业证书一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **证书名称** | **发证单位** | **证书等级** | **证书有效期** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**要求：**

1、填写磋商供应商获得资质、认证或企业信誉证书。

2、附所列证书复印件或其他证明材料。

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件11**

**类似项目实施情况一览表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **项目地址** | **合同总价** | **实施时间** | **项目质量** | **项目单位名称及其联系人电话** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**要求：**

1、业绩证明应提供证明材料（合同复印件可只提供首页、含金额页、盖章页并加盖磋商供应商公章）；

2、磋商供应商可按此表格式复制。

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件12**

**售后服务情况表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **磋商供应商承诺** | **备注** |
| 1 | 服务期内售后服务情况(服务方式、服务网点、售后服务的内容和措施等等，可用附页和宣传材料) | 磋商供应商售后服务情况： |  |
| 2 | 服务期后售后服务 |  |  |
| 3 | 培训方案（可用附页） |  |  |
| …… | …… |  |  |

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件13**  　　　本

项目名称

项目编号：

**磋**

**商**

**响**

**应**

**文**

**件**

**（报价文件）**

供应商全称（公章）：

地 址：

时 间：

**报价文件目录**

1、开标一览表（附件14）；

2、报价明细表（附件15）

3、中小企业声明函（附件16）；（如有需提供）

4；针对报价投标人认为其他需要说明的；

**附件14**

**开标一览表**

**项目编号：**

**项目名称：**  [货币单位：人民币元]

|  |  |  |
| --- | --- | --- |
| 投标总报价(元) | 大写 |  |
| 小写 |  |

**填报要求：**

1、投标总报价为完成本项目的所有费用，包括所有人员的人工费、交通费、住宿费、伙食费、办公设施费、管理费、利润、税金、合同包含的所有风险责任等各项费用及不可预见费等所需的全部费用，全部费用已包含在投标报价中。

▲2、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代理人签字或盖章，否则作无效标处理。

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件15**

**报价明细表**

**项目编号：**

**项目名称：** [货币单位：人民币元]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **服务内容清单** | **数量** | **单位** | **单价** | **小计** | **备注** |
| **互联网安全服务** | | | |  |  |  |
| 1 | 互联网出口安全防护服务 | 1 | 套 |  |  |  |
| 2 | 终端入网控制服务 | 1 | 套 |  |  |  |
| 3 | 上网行为管理服务 | 1 | 套 |  |  |  |
| 4 | 互联网大数据安全分析服务 | 1 | 套 |  |  |  |
| 5 | 互联网主机安全及管理服务 | 1 | 套 |  |  |  |
| **法院专网安全服务** | | | |  |  |  |
| 6 | 专网运维审计系统服务 | 1 | 套 |  |  |  |
| 7 | 专网综合日志审计系统服务 | 1 | 套 |  |  |  |
| 8 | 专网APT预警平台服务 | 1 | 套 |  |  |  |
| 9 | 专网大数据安全管理平台服务 | 1 | 套 |  |  |  |
| 10 | 专网数据库审计服务 | 1 | 套 |  |  |  |
| 11 | 威胁情报分析服务 | 1 | 套 |  |  |  |
| 12 | 威胁情报收集服务 | 1 | 套 |  |  |  |
| 13 | 安全准入服务 | 1 | 套 |  |  |  |
| **其他安全服务** | | | |  |  |  |
| 14 | 安全培训服务 | 1 | 年 |  |  |  |
| 15 | 应急演练服务 | 1 | 年 |  |  |  |
| 16 | 网络安全专项检查服务 | 1 | 年 |  |  |  |
| 17 | 漏洞扫描服务 | 1 | 年 |  |  |  |
| 18 | 基线核查服务 | 1 | 年 |  |  |  |
| 19 | 渗透测试服务 | 1 | 年 |  |  |  |
| 20 | 应用上线检查服务 | 1 | 年 |  |  |  |
| 21 | 安全运维服务 | 1 | 年 |  |  |  |
| 22 | 资产梳理服务 | 1 | 年 |  |  |  |
| 23 | 数据备份服务 | 1 | 年 |  |  |  |
| 24 | 网络入侵攻击监测分析服务 | 1 | 年 |  |  |  |
| 25 | 异常流量态势监测服务 | 1 | 年 |  |  |  |
| 26 | 安全隐患处置服务 | 1 | 年 |  |  |  |
| 27 | 重大事件应急响应服务 | 1 | 年 |  |  |  |
| 28 | 特殊时期的安全巡检和保障服务 | 1 | 年 |  |  |  |
| 投标人认为需说明的其他 | | | | |  |  |
| **合计 大写**  **小写** | | | | | | |

**要求：**

1、本表为《开标一览表》的报价明细表，如有缺项、漏项，视为投标报价中已包含相关费用，采购人无需另外支付任何费用。

2、“报价明细表”中的报价合计应与“开标一览表”中的投标总报价相一致，不一致时，以开标一览表为准。

▲3、投标报价明细表所填内容按采购文件采购内容要求为准。如有漏报的，视同已包含在投标总价内或已作优惠处理。有重大缺项的将作无效标处理。

磋商供应商名称（盖章）：

法定代表人或授权委托代理人签字或盖章：

职 务：

日 期：

**附件16**

**中小企业声明函**

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，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

注：1、从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2、投标人按各自参加投标的对应标包分别编制、分别成册、分别提交。

**残疾人福利性单位声明函**

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

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

磋商供应商名称（盖章）：

法定代表人（签字或盖章）：

日期：