深 圳 市 中 正 招 标 有 限 公 司

SHENZHEN ZHONGZHENG TENDERING CO.,LTD.

深圳市公安局福田分局网络安全加固建设项目

货物类招标文件

项目编号：FTDL2023000163

二〇二三年十一月

特别警示条款

一、《深圳经济特区政府采购条例》

第五十七条 供应商在政府采购中，有下列行为之一的，一至三年内禁止其参与本市政府采购，并由主管部门记入供应商诚信档案，处以采购金额千分之十以上千分之二十以下的罚款；情节严重的，取消其参与本市政府采购资格，处以采购金额千分之二十以上千分之三十以下的罚款，并由市场监管部门依法吊销其营业执照；给他人造成损失的，依法承担赔偿责任；构成犯罪的，依法追究刑事责任：

（一）在采购活动中应当回避而未回避的；

（二）未按本条例规定签订、履行采购合同，造成严重后果的；

（三）隐瞒真实情况，提供虚假资料的；

（四）以非法手段排斥其他供应商参与竞争的；

（五）与其他采购参加人串通投标的；

（六）恶意投诉的；

（七）向采购项目相关人行贿或者提供其他不当利益的；

（八）阻碍、抗拒主管部门监督检查的；

（九）其他违反本条例规定的行为。

二、《深圳经济特区政府采购条例实施细则》

第七十九条 供应商有下列情形的，属于采购条例所称的串通投标行为，按照采购条例第五十七条有关规定处理：

（一）投标供应商之间相互约定给予未中标的供应商利益补偿；

（二）不同投标供应商的法定代表人、主要经营负责人、项目投标授权代表人、项目负责人、主要技术人员为同一人、属同一单位或者在同一单位缴纳社会保险；

（三）不同投标供应商的投标文件由同一单位或者同一人编制，或者由同一人分阶段参与编制的；

（四）不同投标供应商的投标文件或部分投标文件相互混装；

（五）不同投标供应商的投标文件内容存在非正常一致；

（六）由同一单位工作人员为两家以上（含两家）供应商进行同一项投标活动的；

（七）主管部门依照法律、法规认定的其他情形。

第八十一条 供应商有下列情形之一的，属于隐瞒真实情况，提供虚假资料，按照采购条例第五

十七的有关规定处理：

（一）通过转让或者租借等方式从其他单位获取资格或者资质证书投标的；

（二）由其他单位或者其他单位负责人在投标供应商编制的投标文件上加盖印章或者签字的；

（三）项目负责人或者主要技术人员不是本单位人员的；

（四）投标保证金不是从投标供应商基本账户转出的；

（五）其他隐瞒真实情况、提供虚假资料的行为。

投标供应商不能提供项目负责人或者主要技术人员的劳动合同、社会保险等劳动关系证明材料的，视为存在前款第（三）项规定的情形。

三、根据《中华人民共和国政府采购法实施条例》第十八条规定：“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。”

投标供应商涉嫌存在串通投标等违法行为的，将书面报告财政主管部门依法处理。

深圳市公安局福田分局网络安全加固建设项目

招标文件信息

项目编号： FTDL2023000163

项目名称： 深圳市公安局福田分局网络安全加固建设项目

包 号： A

项目类型： 货物类

采购方式： 公开招标

货币类型： 人民币

评标方法： 综合评分法（新价格分算法）

资格性审查表

序号	内容
1	投标人具备招标文件所列的资格要求，且提交相应的资格证明资料（详见招标公告申请人的资格要求）

符合性审查表

序号	内容
1	未将一个包或一个标段的内容拆开投标
2	对同一项目投标时，未提供两套及以上的投标方案（招标文件另有规定的除外）
3	分项报价或投标总价未超过预算金额（最高投标限价）

4	如评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人应证明其报价合理性（评审委员会成员对投标人提供的说明材料判断不一致的，按照“少数服从多数”的原则确定评审委员会的意见）
5	投标报价满足招标文件报价要求且无严重缺漏项目
6	所投产品、工程、服务在商务、技术等方面实质性满足招标文件要求（是否实质性满足招标文件要求，由评标委员会根据《实质性条款响应情况表》做出评判）
7	按招标文件所提供的样式填写《投标函》；按招标文件所提供的《政府采购投标及履约承诺函》进行承诺；并按招标文件对投标文件组成的要求提供投标文件（投标文件组成完整）
8	投标文件不存在列放位置错误，导致属于信息公开内容没有被公开的情形
9	投标文件不存在电子文档带病毒或使用其他投标人的电子密钥进行加密的情形
10	法律、法规、规章、规范性文件规定的其他情形

特别说明：

1、投标人须在开标当日的开标时间至解密截止时间内完成投标文件在线解密，逾期未解密的作无效处理。

2、投标人不符合《资格性审查表》或《符合性审查表》中任一情形的，初审不通过，投标无效。

3、评标系统执行标书雷同性分析，包括分析文件制作机器码、文件创建标识码、IP 地址是否一致，以及文本内容相似度分析，供评标委员会参考。

评标信息

评标方法：综合评分法（新价格分算法）

综合评分法，是指在最大限度地满足招标文件实质性要求的前提下，按照招标文件中规定的各项因素进行综合评审，评标总得分排名前列的投标人，作为推荐的候选中标供应商。

价格分计算方法：

采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：

投标报价得分=(评标基准价 / 投标报价)×100

评标总得分＝F1×A1＋F2×A2＋……＋Fn×An

F1、F2……Fn 分别为各项评审因素的得分；

A1、A2、……An 分别为各项评审因素所占的权重(A1＋A2＋……＋An＝1)。

评标过程中，不得去掉报价中的最高报价和最低报价。

此方法适用于货物类、服务类、工程类项目。

序号	评分项	权重(%)

<table>
<tr><td>1</td><td colspan="3">价格</td><td>30</td></tr>
<tr><td rowspan="4">2</td><td colspan="3">技术</td><td>52</td></tr>
<tr><td>序号</td><td>评分因素</td><td>权重(%)</td><td>评分准则</td></tr>
<tr><td>1</td><td>重要技术参数偏离情况</td><td>22</td><td>（一）评分内容：
以投标文件《技术规格偏离表》为评审依据，标注“▲”的技术参数指标及要求全部满足的得 100 分，每负偏离一项扣 5 分，最低 0 分。
（二）评分依据：
以投标文件《技术规格偏离表》为评分依据，投标人按招标文件要求提供相应的证明材料复印件或扫描件加盖投标人公章（原件备查），并注明证明材料在投标文件中的具体位置。未提供有效证明材料或未注明证明材料在投标文件中的具体位置或提供的证明资料显示不符合招标文件要求、模糊不清无法判断或未显示是否满足招标文件参数的，该项技术指标按负偏离处理。</td></tr>
<tr><td>2</td><td>一般技术参数偏离情况</td><td>5</td><td>（一）评分内容：
以投标文件《技术规格偏离表》为评审依据，未标注▲的普通技术参数指标及要求全部满足的得 100 分，每负偏离一项扣 3 分，最低 0 分。
（二）评分依据：
以投标文件《技术规格偏离表》为评分依据，投标人按招标文件要求提供相应的证明材料复印件或扫描件加盖投标人公章（原件备查），并注明证明材料在投标文件中的具体位置。未提供有效证明材料或未注明证明材料在投标文件中的具体位置或提供的证明资料显示不符合招标文件要求、模糊不清无法判断或未显示是否满足招标文件参数的，该项技术指标按负偏离处理。</td></tr>
<tr><td>3</td><td>产品演示</td><td>10</td><td>（一）评分内容：</td></tr>
</table>

				演示内容： 要求投标人对招标文件“第二章 招标项目需求”中的“ 六、演示要求”进行现场演示，演示内容包括： 1、网络安全网关三项功能演示； 2、服务器安全管理系统三项功能演示； 3、分析平台两项功能演示； 4、流量采集器两项功能演示。 演示时长：20 分钟内 （二）评分依据： 1、十项功能演示完整且符合招标演示要求，得 100 分； 2、九项功能演示完整且符合招标演示要求，得 50 分； 3、八项功能演示完整且符合招标演示要求，得 20 分； 4、其他不得分。
	4	技术保障措施	5	（一）评分内容： 投标人在投标文件中详细说明技术保障措施，包括但不限于： 1、技术方案； 2、项目管理方案； 3、售后服务方案； 4、培训方案。 （二）评分标准： 满足以上四项内容得 40 分，满足以上三项内容得 30 分，满足以上两项内容得 20 分，满足以上一项内容得 10 分，其他情况不得分。 在此基础上，专家根据方案响应情况进一步评审： 1、方案符合实际、完整、规范、思路清晰，内容合理性强，加 60 分； 2、方案较符合实际、较完整规范、思路较清晰，内容合理性较强，加 40 分；

				3、方案较普通、完整性规范性一般，思路不够清晰，内容合理性一般，加 20 分； 4、方案不全、不规范，思路不清晰，内容合理性差，不加分。
	5	项目经理(仅限一人）情况	5	（一）评分内容： 拟安排的项目经理（仅限一人）须为投标人自有员工，否则本项不得分。在此基础上，按以下标准评分： 1）具有注册信息安全专业人员(CISP)证书； 2）具有信息安全保障人员（CISAW）认证证书； 3）具有由人力资源和社会保障局颁发的信息通信技术服务相关专业副高或以上职称证书； 4）具有网络与信息安全管理师证书； 全部满足以上 4 个证书得 100 分，不满足不得分。 注：技术负责人与项目经理不为同一人。 （二）评分依据： 1、提供项目经理通过投标单位缴纳的载有社保部门或税务部门公章的开标前近三个月个人社保证明（由于社保部门或税务部门原因无法提供最近一个月社保证明的，可往前顺延一个月，投标人需同时提供社保部门或税务部门相关说明或证明材料）；如供应商为新成立单位且成立时间不足三个月的，可提供加盖公章的情况说明或者证明材料亦视为符合； 2、提供上述证书； 3、提供以上证明文件扫描件，如涉及网站截图或照片等证明材料,需提供清晰图片,原件备查。未按要求提供有效证明材料或提供不清晰导致评委无法识别的不计得分。
	6	项目团队（项目经理除外）情况	5	（一）评分内容： 拟安排的项目团队成员（项目经理除外）须为投标人自有员工，否则本项不得分。在此基础上，按以下标准评分：

				1.技术负责人（仅限1名）： 技术负责人具有硕士研究生或以上学历，且同时具有副高或以上工程师职称证书、注册信息安全专业人员(CISP)证书以及信息安全保障人员（CISAW）认证证书，得30分，本小项最高得30分。 注：技术负责人与项目经理不为同一人。 **2.技术团队成员（项目经理和技术负责人除外）：** 1）具有本科或以上学历，且同时具有通信相关的质量员证书、注册信息安全专业人员(CISP)证书以及计算机技术与软件专业技术资格证书（专业：网络工程师），每提供1人得10分，最高得10分。 2）具有本科或以上学历，且同时具有注册信息安全专业人员(CISP)证书以及计算机技术与软件专业技术资格证书（专业：信息系统项目管理师），每提供1人得10分，最高得10分。 3）具有本科或以上学历，且同时具有信息通信建设工程管理人员能力相关证书以及注册信息安全专业人员(CISP)证书，每提供1人得10分，最高得10分。 4）具有本科或以上学历，且同时具有注册信息安全专业人员(CISP)证书以及计算机技术与软件专业技术资格证书（专业：信息安全工程师），每提供1人得10分，最高得10分。 5）具有本科或以上学历，且同时具有计算机技术与软件专业技术资格证书（专业：数据库系统工程师）以及注册信息安全专业人员(CISP)证书，每提供1人得10分，最高得10分。 6）具有本科或以上学历，且同时具有注册信息安全专业人员(CISP)证书以及信息安全保障人员（CISAW）认证证书，每提供1人得10分，最高得10分。

<table>
<tr><td></td><td></td><td></td><td></td><td>7）具有本科或以上学历，且具有售后服务高级管理师相关证书的，每提供 1 人得 5 分，最高得 10 分。
注：同一人员不可累计得分，如同一人员具有上述多个证书的，按得分最优情况计分。
（二）评分依据：
1、提供项目团队成员通过投标单位缴纳的载有社保部门或税务部门公章的开标前近三个月个人社保证明（由于社保部门或税务部门原因无法提供最近一个月社保证明的，可往前顺延一个月，投标人需同时提供社保部门或税务部门相关说明或证明材料）；如供应商为新成立单位且成立时间不足三个月的，可提供加盖公章的情况说明或者证明材料亦视为符合；
2、提供上述资格证书、毕业证书（或学位证书）以及学信网查询记录，对于学信网无法查询的，还需提供毕业院校或人社部门或教育部门等颁发机构或监管机构出具的证明，否则无效；
3、提供以上证明文件扫描件，如涉及网站截图或照片等证明材料，需提供清晰图片，原件备查。未按要求提供有效证明材料或提供不清晰导致评委无法识别的不计得分。</td></tr>
<tr><td>3</td><td colspan="2">商务</td><td>13</td><td></td></tr>
<tr><td></td><td>序号</td><td>评分因素</td><td>权重(%)</td><td>评分准则</td></tr>
<tr><td></td><td>1</td><td>同类项目业绩情况</td><td>5</td><td>（一）评分内容：
2019年1月1日至本项目投标截止日（以合同签订日期或合同中载明的履约起始日期为准），投标人承接过同类项目业绩（同类项目业绩指的是政府机关或事业单位委托的信息网络安全项目，项目内容至少包括堡垒机、日志审计系统、漏洞扫描系统、数据库审计系统、下一代防火墙、内网安全检测（或检查）系统、网络违规行为监测（或检测）</td></tr>
</table>

				系统、风险评估服务、威胁分析与处置服务、应急演练与响应服务以及渗透测试服务的，每提供1个有效项目业绩得100分，最高得100分。 （二）评分依据： 1.提供项目合同关键页（合同关键页必须包含：首页、双方信息页、签字盖章页，体现信息化建设内容页）； 2. 以上证明文件均提供扫描件，原件备查。未按要求提供有效证明材料或提供不清晰导致评委无法识别的不计得分。
	2	企业认证情况	2	（一）评分内容： 1）具有质量管理体系认证证书的得 20 分； 2）具有职业健康安全管理体系认证证书得得 20 分； 3）具有业务连续性管理体系认证证书的得 20 分； 4）具有信息技术服务管理体系认证证书的得 20 分； 5）具有信息安全管理体系认证证书的得 20 分； 以上 5 项可累计计分，最高可得 100 分。 （二）评分依据： 1.提供有效认证证书（如认证证书注明年审要求的，必须按规定年审且证书在有效期内的方为有效；如未注明年审要求的，证书必须在有效期内的方为有效）； 2.提供证书官网或权威机构【如：全国认证认可信息公共服务平台（cx.cnca.cn）】认证信息查询截图（截图需显示证书状态为有效）。相关证书在公开渠道无法查询的，投标人需提供颁发部门或者监管机构的证明材料，证明证书真实有效且为合法机构颁发； 3.提供以上证明文件扫描件，如涉及网站截图或照片等证明材料，需提供清晰图片，原件备查。对于未提供证明文件，未提供查询记录且无其他证明材料的，或者提供不清晰导致评委无法判断的，均作不得分处理。

	3	企业获奖情况	3	（一）评分内容： 2019 年 1 月 1 日至本项目投标截止日（以证书颁发日期为准），投标人在信息化领域（含通信或网络或数据库技术）获得以下荣誉或奖项： 1）国家级奖项每一个得 50 分，本小项最高得 50 分； 2）省级或以上奖项每一个得 10 分；本小项最高得 50 分； 以上两项合计最高得 100 分。 国家级奖项要求奖项颁发单位为国务院、国家部委或相关的全国性行业协会（学会）；省级奖项要求奖项颁发单位为省（自治区、直辖市）人民政府（或行业主管行政机关）或相应区域的行业协会（学会），不含副省级；由行业协会颁发的，需提供该行业协会在“中国社会组织政务服务平台”（网址：https://chinanpo.mca.gov.cn/）查询的已合法登记且状态正常截图，否则不予认可，视为无效证书。 （二）评分依据： 1. 要求提供奖项照片或获奖（荣誉）证书作为得分依据； 2. 提供以上证明文件扫描件，如涉及网站截图或照片等证明材料,需提供清晰图片,均要求加盖投标人公章,原件备查。未按要求提供有效证明材料或提供不清晰导致评委无法识别的不计得分。
	4	企业资质情况	1	（一）评分内容： 投标人具有 ITSS 信息技术服务运行维护标准符合性证书二级或以上，得 100 分。 （二）评分依据： 提供证书扫描件，如涉及网站截图或照片等证明材料，需提供清晰图片，原件备查。对于未提供证明文件，未提供查询记录且无其他证明材料的，或者提供不清晰导致评委无法判断的，均作不得分处理。

	5	计算机软件著作权登记证书	2	（一）评分内容： 投标人提供网络安全类计算机软件著作权登记证书，每提供 1 个证书得 10 分，最高得 100 分。 （二）评分依据： 1.提供有效计算机软件著作权登记证书作为得分依据； 2.提供以上证明文件扫描件，如涉及网站截图或照片等证明材料，需提供清晰图片，原件备查。未按要求提供有效证明材料或提供不清晰导致评委无法识别的不计得分。
4	其他			5
	序号	评分因素	权重(%)	评分准则
	1	诚信评审	5	根据《深圳市财政局关于印发<深圳市财政局政府采购供应商信用信息管理办法>的通知》（深财规〔2023〕3 号）相关规定，如供应商在全国范围内存在因政府采购违法、违规行为受到财政部门罚款等一般行政处罚信息，或者存在该办法第十一条所称在本市集中采购活动中的一般违法失信行为记录信息，且在公示期内的，本项不得分，否则得 100 分。 （采购代理机构通过“信用中国”、“中国政府采购网”、“深圳市政府采购监管网”以及市、区财政部门认定的其他渠道查询供应商信用信息，投标人无需提供证明材料。）

其它关键信息

一、评标定标信息

是否评标定标分离	非评定分离
定标方法	/
评标方法	综合评分法
中标供应商家数	1
候选中标供应商家数	1

二、报价明显偏低的合理性说明

根据《中华人民共和国财政部令第 87 号-政府采购货物和服务招标投标管理办法》第六十条规定：评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

三、关于享受政府采购扶持政策的主体及价格扣除比例

（一）本项目所属行业为 工业 ，投标人应根据《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）规定的中小企业划型标准填写《中小企业声明函》。

（二）价格评审优惠

□预留份额专门面向中小企业采购的采购项目或采购包：不执行价格评审优惠的扶持政策。

☑未预留份额专门面向中小企业采购的采购项目或采购包：

（1）本项目货物全部由小型、微型企业制造的，可给予投标人 10 %**（请在 10%-20%范围内选择）**的价格扣除，用扣除后的价格参与评审。如所投产品制造商全部为监狱企业或残疾人福利性单位视同小微企业享受以上价格扣除；对于同时属于小微企业、监狱企业或残疾人福利性单位的，不重复进行价格扣除。

（2）小型、微型企业承担的合同份额占到合同总金额 30%以上的，可给予投标人 / %**（请在 4%-6%范围内选择）**的价格扣除，用扣除后的价格参与评审。

（3）优惠主体资格的认定资料为《中小企业声明函》、《残疾人福利性单位声明函》以及《监

狱企业声明函》等承诺性质的资料（格式详见招标文件第三章）；监狱企业或者代理提供监狱企业货物的供应商如需享受优惠政策，除上述资料外，还须提供省级以上监狱管理局、戒毒管理局出具的监狱企业证明文件。

四、其他说明

拟采购的产品属于《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）、《关于印发环境标志产品政府采购品目清单的通知》（财库〔2019〕18 号）和《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19 号）品目清单范围内的，应依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。对于已列入品目清单的产品类别，采购人可在采购需求中提出更高的节约资源和保护环境要求，对符合条件的获证产品给予适当评审加分。对于未列入品目清单的产品类别，鼓励采购人综合考虑节能、节水、环保、循环、低碳、再生、有机等因素，参考相关国家标准、行业标准或团体标准，在采购需求中提出相关绿色采购要求，促进绿色产品推广应用。

为缓解中小企业融资难题，深圳市推出政府采购订单融资改革举措。订单融资具体流程及试点金融机构订单融资服务承诺可参阅深圳市政府采购监管网（zfcg.sz.gov.cn）政府采购订单融资栏目。

目　录

备注：

1.本招标文件分为第一册“专用条款”和第二册“通用条款”。

2.“专用条款”是对本次采购项目的具体要求，包含招标公告、招标项目需求、投标文件格式、合同及履约情况反馈格式等内容。

3.“通用条款”是适用于政府采购项目的基础性条款，具有普遍性和通用性。

4.当出现“专用条款”和“通用条款”表述不一致或有冲突时，以“专用条款”为准。

第一册　专用条款

第一章　招标公告

项目概况:

深圳市公安局福田分局网络安全加固建设项目招标项目的潜在投标人应在（本公告附件中）获取招标文件，并于 2023 年 12 月 04 日 09:00（北京时间） 前递交投标文件。

一、项目基本情况

1、项目编号：FTDL2023000163

2、项目名称：深圳市公安局福田分局网络安全加固建设项目

3、预算金额：人民币 16,849,000.00 元

4、最高限价：人民币 16,849,000.00 元

5、采购需求：

标的名称	数量	单位	简要技术需求或服务要求	备注
详见《货物清单明细》	1	批	详见招标文件	无

6、合同履行期限：详见招标文件

7、本项目（是/否）接受联合体投标：详见“申请人的资格要求”

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（须提供具有独立承担民事责任能力的法人或其他组织的营业执照或法人证书等证明材料扫描件以及《政府采购投标及履约承诺函》）。如果是分支机构参与投标，还须同时提供其具有独立法人资格的上级主体出具的有效授权书及上级主体的营业执照或法人证书等证明材料扫描件；本项目不接受总公司与分支机构同时参与投标，也不接受同一总公司有两个或以上分支机构参与投标，如出现以上情形，该两家或以上投标人均按无效投标处理。

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：

（1）参与本项目采购活动前三年内，在经营活动中没有重大违法记录（由供应商在《政府采购投标及履约承诺函》中作出声明）；

（2）参与本项目政府采购活动时不存在被有关部门禁止参与政府采购活动且在有效期内的情况（由供应商在《政府采购投标及履约承诺函》中作出声明）；

（3）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动（由供应商在《政府采购投标及履约承诺函》中作出声明）；

（4）除单一来源采购项目外，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（由供应商在《政府采购

投标及履约承诺函》中作出声明）；

（5）参与本项目政府采购活动不存在与其他采购参加人串通投标，隐瞒真实情况，提供虚假资料等违法违规情形（由供应商在《政府采购投标及履约承诺函》中作出声明）；

（6）未被列入失信被执行人、重大税收违法案件当事人名单及政府采购严重违法失信行为记录名单（信用中国网“信用服务”栏的“重大税收违法失信主体”、“失信被执行人”，中国政府采购网“政府采购严重违法失信行为记录名单”，深圳信用网以及深圳市政府采购监管网为供应商信用信息查询渠道，相关信息以开标当日的查询结果为准。由采购代理机构查询，供应商无需提供证明材料）；

（7）本项目不接受联合体投标，不允许非法分包或转包；

（8）本项目不接受进口产品投标（进口产品是指通过中国海关报关验放进入中国境内且产自关境外的产品，相关内容以“财库【2007】119 号文”和“财办库【2008】248 号文”的相关规定为准）。

注：供应商投标（上传投标文件）必须先行办理注册手续，具体请按照本公告“三、获取招标文件”相关内容指引办理。

三、获取招标文件

1、时间：**2023 年 11 月 18 日至 2023 年 12 月 04 日 09:00，每天上午 0:00 至 12:00，下午 12:00 至 24:00（北京时间，法定节假日除外）**。

2、地点：登录深圳政府采购智慧平台（http://zfcg.szggzy.com:8081/）下载本项目的招标文件。

3、方式：在线下载。

4、售价：免费。

凡已注册的深圳市网上政府采购供应商，按照授予的操作权限，可于**获取招标文件时间内**登录深圳政府采购智慧平台（http://zfcg.szggzy.com:8081/）下载本项目的采购文件。投标人如确定参加投标，首先要在深圳政府采购智慧平台网上办事子系统（http://zfcg.szggzy.com:8081/TPBidder/memberLogin）网上报名投标，方法为登陆网上办事子系统后点击“【招标公告】→【我要报名】”；如果网上报名后上传了投标文件，又不参加投标，应再到【我的项目】→【项目流程】→【递交投标(应答)文件】功能点中进行“【撤回本次投标】”操作；如果是未注册为深圳政府采购智慧平台（http://zfcg.szggzy.com:8081/）的供应商，请先办理密钥（请点击），并前往深圳公共资源交易中心绑定深圳政府采购智慧平台用户（电子密钥办理咨询电话：0755-83948165、0755-83938966、020-89524338），再进行投标报名。在网上报名后，点击“【我的项目】→【项目流程】→【采购文件下载】”进行招标文件的下载。

四、提交投标文件截止时间、开标时间和地点

1、投标截止时间：所有投标文件应于 **2023 年 12 月 04 日 09:00（北京时间）**之前上传到深圳政府采购智慧平台（http://zfcg.szggzy.com:8081/）。具体操作为登录“深圳政府采购智慧平台用户网上办事子系统

（http://zfcg.szggzy.com:8081/TPBidder/memberLogin）”，用“【我的项目】→【项目流程】→【递交投标(应答)文件】”功能点上传投标文件。本项目电子投标文件最大容量为200MB，单个节点文件不能超过50MB，超过此容量的文件将被拒绝。

2、开标时间和地点：定于2023年12月04日09:00（北京时间），在深圳市中正招标有限公司公开开标。供应商可以登录“深圳政府采购智慧平台用户网上办事子系统（http://zfcg.szggzy.com:8081/TPBidder/memberLogin）”，在“【我的项目】→【项目流程】→【开标及解密】”进行在线解密、查询开标情况。

3、在线解密：投标人须在2023年12月04日09:00-10:00（北京时间）期间进行解密，逾期未解密的作无效处理。解密方法：登录“深圳政府采购智慧平台用户网上办事子系统（http://zfcg.szggzy.com:8081/TPBidder/memberLogin）”，使用本单位制作电子投标文件同一个电子密钥，在“【我的项目】→【项目流程】→【开标及解密】”进行在线解密、查询开标情况。

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、本项目实行网上投标，采用电子投标文件。

2、采购文件澄清/修改事项：2023年11月29日00:00（北京时间）前，供应商如果认为采购文件存在不明确、不清晰和前后不一致等问题，可登录“深圳政府采购智慧平台用户网上办事子系统（http://zfcg.szggzy.com:8081/TPBidder/memberLogin）”，在“【我的项目】→【项目流程】→【提问】”功能点中填写需澄清内容。2023年12月01日00:00（北京时间）前将采购文件澄清/修改情况在“【我的项目】→【项目流程】→【答疑澄清文件下载】”中公布，望投标人予以关注。

（重要提示：“提出采购文件澄清要求”不等同于“对采购文件质疑”，供应商提出的澄清要求内容如出现“质疑”字眼，将予以退回。供应商如认为采购文件存在限制性、倾向性、其权益受到损害，应在采购文件公布之日起七个工作日内以书面形式提出质疑。请质疑供应商根据深圳公共资源交易网（ https://www.szggzy.com/fwdh/fwdhzfcg/bszn1/content_203163.html ）所发布的质疑指引、质疑函模板填写质疑函并提交质疑材料。质疑材料可以采用现场或邮寄方式提交，采用邮寄方式提交的，交邮时间应在本公告发布之日起七个工作日内。质疑材料现场提交、邮寄地址：深圳市福田区民田路171号新华保险大厦903深圳市中正招标有限公司。质疑咨询电话：0755-83026699。根据《深圳经济特区政府采购条例》第四十二条“供应商投诉的事项应当是经过质疑的事项”的规定，未经正式质疑的，将影响供应商行使向财政部门提起投诉的权利。）

3、深圳市中正招标有限公司有权对投标人就本项目要求提供的相关证明资料（原件）进行审查。供应商提供虚假资料被查实的，则可能面临被取消本项目中标资格、列入不良行为记录名单和三年内禁止参与深圳市政府采购活动的风险。

4、本招标公告及本项目招标文件所涉及的时间一律为北京时间。投标人有义务在招标活动期间浏览深圳公共资源交易网（https://www.szggzy.com），在深圳公共资源交易网上公布的与本次招标项目有关的信息视为已送达各投标人。

5、本项目不需要投标保证金。

七、对本次招标提出询问，请按以下方式联系。

1、采购人信息

名称：深圳市公安局福田分局

地址：福田区福民路 123 号

2、采购代理机构信息

名称：深圳市中正招标有限公司

地址：深圳市福田区民田路 171 号新华保险大厦 903

联系方式：0755-83026699

3、项目联系方式

项目联系人：杨小姐

电话：0755-83026699

深圳市中正招标有限公司

2023 年 11 月 18 日

第二章　招标项目需求

一、对通用条款的补充内容

序号	内　　容	规　　定
1	联合体投标	见《招标公告》中“项目基本情况”部分的相关内容
2	投标有效期	90 日历天（从投标截止之日算起）
3	投标人的替代方案	不允许
4	投标文件的投递	本项目实行网上投标，投标人必须在招标文件规定的投标截止时间前登录“深圳政府采购智慧平台用户网上办事子系统”，使用“【我的项目】→【项目流程】→【递交投标(应答)文件】”功能点，将编制好的电子投标文件上传，投标文件大小不得超过 200MB，单个节点文件不能超过 50MB。
5	中标服务费	1、中标人须向采购代理机构缴纳中标服务费，收费标准详见通用条款 41.4，最低收取人民币 7000 元。 2、中标服务费缴纳至： 开户名称：深圳市中正招标有限公司 银行帐号：03003729353 开户银行：上海银行深圳天安支行
6	履约保证金	本项目不收取履约保证金。

备注：本表为通用条款相关内容的补充和明确，如与通用条款相冲突的以本表为准。

二、货物清单

（一）货物总清单

序号	项目名称	数量	单位	备注	**采购预算金额（人民币元）**
1	深圳市公安局福田分局网络安全加固建设项目	1	批	拒绝进口	16,849,000.00

（二）货物清单明细

序号	**货物名称**	**行业属性**	**数量**	**单位**	**备注**	**单项财政预算限额（元）**	**财政预算限额（元）**
一	公安信息网安全加固建设						
1	安全区域边界						

1.1	网络安全网关	工业	4	台	拒绝进口	4,233,000.00	16,849,000.00
1.2	数据安全交换系统						
1.2.1	边界安全控制网关	工业	1	台	拒绝进口		
1.2.2	下一代防火墙	工业	1	台			
1.2.3	入侵防御系统	工业	1	台			
1.2.4	万兆交换机	工业	1	台			
1.2.5	集中监控与审计系统探针子系统	工业	1	台			
1.2.6	视频安全接入系统	工业	1	套			
1.3	数据采集分流设备	工业	2	台			
1.4	专线	工业	20	条			
2	安全计算环境						
2.1	WEB 应用防火墙	工业	2	台	拒绝进口		
2.2	数据库防护与审计系统	工业	1	台			
3	安全管理中心						
3.1	堡垒机	工业	1	台	拒绝进口		
3.2	漏洞扫描系统	工业	1	台			
4	安全运营平台及工具						
4.1	移动工作站	工业	3	台	拒绝进口		
4.2	服务器(配套设备)	工	3	台			

		业				
二	视频专网安全加固建设					
1	安全区域边界					
1.1	网络安全网关	工业	6	台	拒绝进口	
1.2	视频专网安全雷达系统					
1.2.1	采集模块	工业	3	台	拒绝进口	
1.2.2	分析模块	工业	1	台		
1.3	视频专网精准防护系统					
1.3.1	管理中心	工业	1	套	拒绝进口	
1.3.2	采集分析引擎	工业	2	台		
1.3.3	大数据中心	工业	1	套		7,585,000.00
2	安全计算环境					
2.1	终端管理系统	工业	400	点	拒绝进口	
2.2	WEB 应用防火墙	工业	2	台		
2.3	数据库防护与审计系统	工业	1	台		
2.4	服务器安全管理系统	工业	100	点		
3	安全管理中心					
3.1	堡垒机	工业	2	台	拒绝进口	
3.2	漏洞扫描系统	工业	1	台		

4	安全运营平台及工具					
4.1	移动客户端	工业	3	台	拒绝进口	
4.2	工作站	工业	2	台		
4.3	安全运营管理平台（二级平台）					
4.3.1	流量采集器	工业	3	台	拒绝进口	
4.3.2	日志采集器	工业	1	台		
4.3.3	分析平台	工业	1	台		
三	互联网安全加固建设					
1	安全区域边界					1,690,000.00
1.1	网络安全网关	工业	4	台	拒绝进口	
2	安全计算环境					
2.1	WEB 应用防火墙	工业	2	台	拒绝进口	
2.2	数据库防护与审计系统	工业	1	台		
3	安全管理中心					
3.1	堡垒机	工业	1	台	拒绝进口	
3.2	日志审计系统	工业	1	台		
3.3	漏洞扫描系统	工业	1	台		
4	安全运营平台及工具					
4.1	流量采集器	工业	1	台	拒绝进口	
四	内网安全检测系统建设					

1	安全运营管理平台（一级平台）					
1.1	流量采集器	工业	1	台	拒绝进口	1,098,000.00
1.2	日志采集器	工业	1	台		
1.3	分析平台	工业	1	台		
五	公安网违规行为和安全监测建设					
1	网络违规行为监测系统（平台和探针）					
1.1	采集模块	工业	1	台	拒绝进口	759,000.00
1.2	分析模块	工业	1	台		
六	公安网终端准入建设					
1	准入控制（公安网核心）					
1.1	终端准入 Licencce 授权	工业	6000	点	拒绝进口	1,004,000.00
1.2	终端准入控制设备	工业	2	台		
2	准入控制（业务接入网）	工业	1	套		
七	信息安全服务体系建设					
1	威胁分析与处置服务（含人工）	工业	1	项/1年	拒绝进口	480,000.00
2	风险评估服务	工业	1	项/1年		
3	渗透测试服务	工业	1	项/1年		
4	应急演练服务	工业	1	项/1年		

5	应急响应服务	工业	1	项/1年			

备注：

1、**本项目核心产品为：下一代防火墙**。如同时有两家或两家以上（均为制造商的合法代理商）通过资格审查及符合性审查的合格投标人**所投核心产品为相同品牌的，按一家投标人计算**。在此种情况下，评审后得分最高的投标人获得中标人推荐资格；评审得分相同的由报价相对最低的获得中标人推荐资格；评审得分及报价均相同的由技术评分相对最高的获得中标人推荐资格；以上均相同的由评标委员会采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。**货物清单中任意一项产品的投标报价超过其预算金额或最高限价的，将导致投标无效。**

2、备注栏注明“拒绝进口”的产品不接受投标人选用进口产品参与投标；注明“接受进口”的产品允许投标人选用进口产品参与投标，但不排斥国内产品。

3、进口产品是指通过海关验放进入中国境内且产自关境外的产品。即所谓进口产品是指制造过程均在国外，如果产品在国内组装，其中的零部件（包括核心部件）是进口产品，则应当视为非进口产品。采用“接受进口”的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，相关内容以财库〔2007〕119 号文和财办库〔2008〕248 号文的相关规定为准。

4、根据《中华人民共和国财政部令第 87 号-政府采购货物和服务招标投标管理办法》第六十条规定：评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。若评标委员会成员对是否须由投标人作出报价合理性说明，以及书面说明是否采纳等判断不一致的，按照“少数服从多数”的原则确定评标委员会的意见。

5、本项目需求中出现的工艺、材料、设备或参照的品牌等仅为方便描述而没有限制性，投标人可以在其提供的文件资料中选用替代标准，但这些替代标准要优于或相当于项目需求中要求的标准。

6、如要求提供证明材料，投标文件需提供相应证明材料扫描件（或截图等）并注明证明材料在投标文件中的具体位置，未按要求提供证明材料或未注明证明材料的具体位置或提供的证明资料显示不符合招标文件要求、模糊不清无法判断或未显示是否满足招标文件要求的，均视为负偏离；未要求提供相应证明材料的，投标人可以不提供。

7、投标人提供证书或检测报告等证明材料的，颁发证书、出具报告的机构须是合法设立的机构，且具有颁发相应证书或者出具相应报告的资质。

8、技术参数设置为区间要求的（例如：潮气量：0-2000ML），投标产品参数区间与招标要求不完全一致的均视为负偏离。

9、对于定制类产品，投标人需在投标文件“分项报价表”中明确注明“定制”，否则该产品技术参数按负偏离处理。

10、加注▲的条款为重要条款要求，如不满足将按评标信息进行扣分。

11、加注★的条款为不可负偏离条款，任一项未响应或不满足要求的，将导致投标无效。

三、实质性条款

序号	具体内容
1	交货时间：合同签订后 30 个日历日内

注：上表所列内容为不可负偏离条款。

四、具体技术要求

序号	货物名称	技术要求
一	公安信息网安全加固建设	
1	安全区域边界	
1.1	网络安全网关	网络处理能力≥10G，并发连接≥260 万，每秒新建连接≥18 万/秒， 标准 2U 机箱，冗余电源，标准配置 1 个 Console 口，6 个 10/100/1000M 自适应电口，4 个千兆光口，4 个万兆光口，含 4 个万兆多模光模块，4 个千兆多模光模块；含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能；含三年硬件维保服务，含三年全功能模块升级服务。
1.2	数据安全交换系统	
1.2.1	边界安全控制网关	1、采用标准 2U 设备设计，采用边界 2.0 标准系统架构，配置内存≥16G 内存，接口默认提供≥6 个万兆光口和≥2 个千兆电口。
		2、含三年硬件维保服务，含三年软件维保升级服务。
		3、设备支持基于硬件数字证书的身份认证。
		4、设备支持基于终端特征的设备认证。
		5、设备支持终端进程控制。
		6、设备支持多服务器的集中授权管理。
		7、基于资源的访问控制。
		8、基于 URL 的细粒度授权管理。
		9、具有黑名单动态下载功能。
		10、具有自动登录、免应用开发功能。

		11、基于链路服务的策略管理和下发。
		12、基于个人证书及证书 DN 项的访问控制。
		13、实现单点登录功能。
		14、支持双机热备。
		15、实现系统配置备份和恢复、日志审计系统管理功能。
		16、设备稳定性运行时间>50000 小时。
		17、设备最大支持的吞吐量≥4Gbps。
		18、提供的访问限制能力需包括访问用户限制、访问内容限制功能。
		19、全面完善支持公安当前 PKI 体系，基于硬件数字证书的身份认证。支持对接入的终端进行认证，支持多条证书链同时存在、同时生效。提供全面的权限策略控制功能，基于个人证书及证书 DN 项的访问控制，基于资源的访问控制，基于 URL 的细粒度授权管理，支持对资源的多种模式管理。实现单点登录功能，实现客户端自动安装，策略支持黑名单和白名单方式，实现系统配置备份和恢复、日志审计系统管理功能。
		20、支持公安 PKI/PMI 系统，结合终端用户身份认证，实现接入终端设备认证、接入用户权限管理、传输加密保护。
1.2.2	下一代防火墙	1、配置≥6 个 10/100/1000BASE-T 接口和≥2 个 SFP 插槽，≥2 个可插拔的扩展槽， 标配模块化双冗余电源 。
		2、性能：防火墙吞吐率：≥12Gbps，并发连接数：≥300 万；应用层吞吐量：≥10bps；HTTP 新建连接速率：≥10 万；FW+IPS 吞吐量：≥2Gbps。
		3、含三年硬件维保服务，含三年应用特征库升级许可。
		4、防火墙采用端口映射、包过滤技术实现正常访问；同时，启动防火墙抗攻击功能，如抗 DOS 攻击来抵御常见的攻击。
1.2.3	入侵防御系统	1、2U 机架式结构，配置≥10 个接口，默认包括≥2 个扩展槽位；≥1 个管理口，≥5 个 10/100/1000BASE-T 接口(支持 1 组 Bypass)，≥4 个 SFP 插槽； ≥1 个 CONSOLE，≥2 个 USB，≥1TB 硬盘； 标配冗余电源； 默认含：3 年 IPS 攻击规则库升级许可；3 年 URL 过滤规则库升级许可。
		2、含三年硬件维保服务，含三年软件维保升级服务。
		3、性能：整机吞吐率：≥8Gbps，最大并发连接数：≥150 万，IPS 吞吐率：≥3Gbps。
1.2.4	万兆交换机	以太网交换机配置≥24 口万兆光口，≥4 个 40GE 光口；≥8 个万兆多模模块；双电源；含三年硬件维保服务。
1.2.	集中监	1、每秒可接收日志条数≥200 条。

5	控与审计系统探针子系统	2、支持链路数：≥1 条。
		3、最大可支持业务数≥20 个。
		4、最大可支持设备数≥20 个。
		5、对所有授权访问类用户或设备的行为进行审计，保障用户已发生行为的可追溯性。
		6、支持多种设备状态信息的采集（设备需支持 SNMP 协议）。
		7、支持应用流量信息的探测。
		8、支持基于 SysLog、SNMP2.0/3.0 协议的事件收集和处理。
		9、需支持对边界安全传输设备的运行状态监测功能。
		10、需支持对边界安全传输设备运行的日志报警信息收集功能。
		11、需支持对收集的日志进行统一日志格式功能。
1.2.6	视频安全接入系统	1、由视频接入认证设备、视频用户认证设备和视频安全隔离设备组成。
		2、视频接入认证设备和视频用户认证设备，每台设备配置： 2U 机箱。网口配置：≥2 个千兆电口，≥2 个万兆光口；工作电源：550W 单电源或 500W 单电源；操作系统：≥CentOS 6.5 64bit。
		3、视频安全隔离设备，由内端机和外端机两部分组成。每端配置： 2U 机箱；网口配置：≥2 个千兆电口，≥2 个万兆光口；工作电源：400W 单电源或 460W 单电源。
		3、进行视频信令流与视频数据流的全剥离，支持信令双向传输，视频数据单向传输，对内外网数据均有安全检查机制。
		4、基于 0 反馈单向传输硬件实现视频数据单向传输，完全阻断反向数据的传输，保障安全。
		5、提供数据安全检查功能，具有高度安全性。数据安全检查包括数据源检查，数据格式检查，控制协议检查，病毒木马扫描，关键字扫描等措施。
		6、提供证书认证功能，采用通用的 PKI/PMI 系统架构，建立快速安全的通道，并对通信数据集进行加密，保障传输安全。
		7、对用户和视频主机进行注册和管理，只允许合法用户访问注册的视频资源，从用户和资源两方面保证安全性。
		8、支持多种协议格式检查，包括视频信令协议格式、视频传输协议、视频压缩编码格式、主流视频监控公司的私有协议视频信令协议格式。
		9、视频数据和信令数据经不同的传输方式传输，信令采取双向隔离模块传输，具有物理隔离特性，视频流采用单向隔离模块传输。
		10、内嵌防病毒和入侵检测模块，并能及时记录并告警。

		11、支持流量审计、设备访问审计、告警审计多种日志审计与告警功能，并与监管联动。
		12、视频控制信令格式检查，支持对 SIP 信令的识别，支持对不符合格式的信令进行拦截丢弃，并进行日志报警。如：RTSP、SIP、DB33、GB 35114 等视频控制信令格式进行白名单方式检查，并进行及时阻断和告警。
		13、支持一个下级应用平台的视频资源分享给多少上级应用平台的级联；支持多个下级应用平台的视频资源汇聚到一个上级应用平台的级联。
		14、支持对视频业务流量进行实时监控，根据规则定义判定业务每秒最大吞吐实施控制，超出范围即阻断。
1.3	数据采集分流设备	1U 机架式，≥48*10GE SFP+，支持掩码/精确五元组、固定特征码规则，业务复制与负载均衡，1+1 冗余 220V(AC)/260V(DC)电源。含≥16 个万兆光模块，SFP+ Transceiver，10GE，10.3125Gb/s，850nm(Rx/Tx)，300m，MM，LC。
1.4	专线	专线，街道办、社区工作站、办事大厅等点对点专线 20 条；要求 12 芯、裸光纤。
2	安全计算环境	
2.1	WEB 应用防火墙	1、机箱高度：2U，标配网口：≥2 千兆电口管理口，≥千兆业务电口*4（含 2 组硬件 BYPASS 模块），≥千兆业务光口*4（标配 GE 多模 SFP 模块*2，不含硬件 BYPASS 模块），≥2 万兆光口，硬盘容量：≥1T，内存：≥16G，USB 口：≥USB2.0 口*2，串口：≥RJ45 口*1，电源：1+1 热插拔冗余电源。
		2、硬件性能：网络吞吐量≥8Gbps，HTTP 应用吞吐量≥6Gbps，HTTP 最大并发数≥35 万，HTTP 最大新建数≥3.2 万，HTTPS 应用吞吐量≥1.5Gbps，HTTPS 最大并发数≥6.5 万，HTTPS 最大新建数≥6500，保护站点：无限制。
		3、含三年软件维保服务，三年硬件维修服务。
		4、帮助网站应对 Web 攻击、防入侵、防挂马、防通报、防爬虫、防 CC 攻击、防 WebShell 攻击，事前阻止黑客篡改、事后自动恢复被篡改网页。杜绝一切漏洞攻击，满足网络安全等级保护 2.0 要求。
2.2	数据库防护与审计系统	1、硬件尺寸：标准 2U，CPU 规格：8 核*2，内存容量：≥64G，硬盘容量：≥4TB*4（Raid 5），硬盘接口：企业级 SATA，网口：≥6 审计口，网口类型：≥4 千兆电口+2 万兆光口（配 2 万兆多模光模块），电源配置：双电源。

		2、总网络吞吐量：≥7000Mbps，双向审计最大数据库流量：≥700Mbps，峰值事务处理能力 TPS：≥70000 条/秒，日志数量存储：≥80 亿条，数据库实例授权许可数量：无限数据库授权。
		3、含三年软件维保服务，三年硬件维修服务。
		4、通过数据库协议分析与识别，操作行为识别方式对数据库高危风险以及违规操作行为进行检测并实现阻断；通过攻击特征库对针对数据库的攻击进行检测，并通过虚拟补丁相关策略功能进行针对性的安全策略建立，实现数据库安全防护。针对不同用户及管理员数据库表的增删改查操作行为进行记录，避免违规操作，确保事后可以进行追踪溯源。
3	安全管理中心	
3.1	堡垒机	1、采用专用千兆多核硬件平台和安全操作系统；外观：标准机架式；支持≥6 个千兆电口，≥4 个千兆光口；内置≥4TB 硬盘；冗余电源；最大支持≥500 路图形会话或≥1000 路字符会话并发；配置≥1000 授权许可。含三年软件维保服务，三年硬件维修服务。
		2、支持对网络设备、数据库、安全设备、主机系统资源的运维与审计，通过集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计功能。实时完整地记录用户的操作；提供方便灵活的操作回放和查询检索的手段，具备对运维人员的操作过程做到事前防范、事中控制及事后审计的能力。
3.2	漏洞扫描系统	1、Web 扫描域名无限制，Web 扫描任务并发数为≥10 个域名。系统扫描 IP 地址最大支持≥1024 个，支持扫描 A 类、B 类、C 类地址，系统扫描支持≥100 个 IP 地址并行扫描。标准 1U 机架式，≥1T 硬盘，标准配置≥6 个 10/100/1000M 自适应电口，≥2 个扩展插槽,2 个 USB 口，1 个 Console 口，单电源。
		2、含三年漏洞特征库升级，三年硬件维修服务。
4	安全运营平台及工具	
4.1	移动工作站	1、不低于 i7-13700 处理器。
		2、Windows 11 或以上。
		3、集成显卡。
		4、内存≥16GB 。
		5、固态硬盘≥1TB。
4.2	服务器(配套设	1、cpu: 主频≥2.5G 核数≥10C。
		2、内存:≥8*64G。

	备）	3、硬盘:≥8*2.4T 10K。
		4、含阵列卡。
		5、网口：≥2*1Gb+2*10Gb。
		6、电源：1100W*2。
二	视频专网安全加固建设	
1	安全区域边界	
1.1	网络安全网关	1、网络层吞吐量≥50G，并发连接≥800 万，每秒新建连接数≥50 万，标准 2U 机箱，冗余电源， 标准配置≥16 个千兆电口，≥8 个万兆光口，≥4 个千兆光口，含≥8 个万兆多模光模块，≥4 个千兆多模光模块，含应用控制、URL 过滤、入侵防御、威胁情报检测功能。
		2、含三年硬件维保服务，含三年全功能模块升级服务。
		3、其中两台提供主机房的业务服务器区的访问控制功能，明确访问的来源、访问的对象及访问的类型，确保合法访问的正常进行，杜绝非法及越权访问。同时有效预防、发现、处理异常的网络访问，确保该区域信息网络正常访问活动。
		4、其中两台提供莲花机房的业务服务区的访问控制功能，明确访问的来源、访问的对象及访问的类型，确保合法访问的正常进行，杜绝非法及越权访问。同时有效预防、发现、处理异常的网络访问，确保该区域信息网络正常访问活动。
		5、其中两台提供反恐机房的业务服务区的访问控制功能，明确访问的来源、访问的对象及访问的类型，确保合法访问的正常进行，杜绝非法及越权访问。同时有效预防、发现、处理异常的网络访问，确保该区域信息网络正常访问活动。
		▲6、具备账号安全防护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲7、支持防病毒，支持 16 层压缩文件进行检测和拦截**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		8、具备入侵防护 IPS 功能模块，支持用户自定义 IPS 规则，包括：WEB 应用防护规则、漏洞攻击规则、僵尸网络规则等。内置漏洞攻击规则库不

		少于 16600 条。僵尸网络与病毒防护规则库不少于 160 万条，应用特征识别规则库不少于 9300 条**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		9、支持联动云端蜜罐（非本地蜜罐）获取黑客指纹信息，自动封锁高危 IP。可选择诱捕外网攻击和内网扩散策略，通过云端高仿真的蜜罐，分析攻击者画像，溯源社交账号**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲10、具备策略全生命周期管理功能。支持记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲11、支持自定义流量监控组件，可基于设备、应用、源目的 IP、接口设置不同的流量和会话数排行动态展示，展示效果支持面积图、折线图、柱状图等至少三种形式**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲12、支持工控协议审计，支持对 OPC-DA、S7-Plus、S7、profinetIO、IEC104、MODBUS、OPCUA、DNP3、Fins、MMS、CIP、Scnet、SMTP、Sonet、SV、BACnet、ENIP-IO 等多种工控协议的审计。审计信息包括：时间、源/目的 IP、源/目的端口、协议类型、协议详情等**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲13、支持 IoT 协议准入，可识别 ONVIF、MQTT、Modbus、S7 等 IoT 协议基于协议进行应用层准入，仅允许指定协议入网通信，可设置生效时间、新增单次时间计划和循环时间计划等。支持视频信令准入，可识别 SIP、RTP、RTCP、RTSP 等视频信令进行准入控制。支持标准合规准入，可识别 GA/T 1400、GB/T 28181、GB 35114 等相关国家标准，基于国家标准进行应用层准入，仅允许符合国家标准的设备入网通信**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
1.2	视频专	视频专网安全雷达系统—注重监测、考核。

	网安全雷达系统	
1.2.1	采集模块	1、2U 独立机架，电源 800W 1+1 冗余，双路 CPU（单路 8 核），内存≥64GB，配备千兆流量采集口≥4 个和万兆流量采集口≥2 个，存储容量≥2*250GB SSD+4*4TB SAS（Raid 5），具备并发会话处理能力≥120 万。
		2、支持构建资产指纹库，资产遥感授权≥3 万个 IP。
		3、支持各种常见的网络链路环境（包括 QinQ 等），采用多种数据采集方式： （1）分光或分流、交换机端口镜像等旁路方式采集网络流量； （2）无代理远程主动探测方式； （3）基于浏览器插件方式，无需在终端机器安装软件，设备实体终端浏览器在进行业务访问行为时，嵌入监控缓存（支持动态及静态），实现监测终端信息； （4）支持 VLAN 及 LAN 内静默运行网络末梢探针方式采集局域网内安全风险行为。
		4、支持数据过滤能力： （1）提供对指定范围内的 IP 段或者 IP 进行数据过滤，不再分析已过滤数据； （2）提供只对指定范围内的 IP 段或 IP 进行数据分析，其他 IP 数据不进行分析。
		5、支持数据汇聚能力： （1）支持对多链路流量独立分析； （2）支持对多链路流量汇聚后统一分析。
		6、支持原始数据包存储能力： （1）提供对原始数据包压缩存储； （2）提供网络原始数据包的检索、自动关联提取、图形化定义检索条件、支持 BPF 表达式。
		7、基于实体行为分析，并针对视频传输网的特征，实现对专网安全的监控和管理。系统通过发现和识别专网内各类在线设备，特别是视频类设备，监控设备实体的网络行为，分析、预测及获知实体使用者的目的，从而识别专网内存在的各类安全问题，包括资产安全、信令安全、边界安全、违规行为、异常行为及潜在的安全隐患，对发现的安全问题实现安全阻断，

		并同时提供完整的数据取证。
		8、视频专网安全雷达系统具备回溯响应以及预防通报能力，偏重于广东省厅的通报项的检查。提前发现深圳市福田视频专网可能存在的一些违规现象。
		9.具备网络巡航管控系统采集能力，监测目标授权：不少于 999 个 IP，支持以 ID 智能值守模式和以 IP 智能值守模式，支持状态查询、数据查询、访控调度等 API 接口。
1.2.2	分析模块	1、2U 独立机架，电源 800W 1+1 冗余，双路 CPU（单路 8 核），内存≥128GB，存储容量≥2*250GB SSD+32TB SAS（Raid 5），数据存储周期≥180 天；含三年软硬件维保服务。
		2、支持网络空间测绘，实现网络空间拓扑，标注全网节点路由节点，梳理合规性路由，发现异常节点、异常路由。
		3、支持资产安全识别，识别网络测绘节点的资产类型、系统版本、应用/服务、开放端口信息，支持统计、检索功能。
		4、支持边界完整性监测，发现外联节点、不受控边界通道、非授权入网、边界穿透服务以及网中网。
		5、支持信令安全审计，还原信令类型、格式和内容，对控制信令进行格式检查和内容过滤审计，对高危、异常控制信令进行告警。
		6、支持违规服务监测，基于行为特征和风险扫描分析违规入网设备、违规游戏、违规站点搭建、违规通讯以及违规传输服务。
		7、支持安全隐患监测，主动监测网内存在的高危端口及服务、不受控站点、资产脆弱性问题安全风险隐患。
		8、专网空间测绘，以全网在网资产的网络路径为线，形成网络空间测绘拓扑图，标注全网关键路由节点，提供依据不同角度、不同层面的统计分析数据。能通过网络空间测绘拓扑图进行全网节点、路由合规性梳理，发现异常节点、异常路由问题，包括：高危互联网路由、其他专网路由、私网路由、过长路由、环线路由。
		9、支持对安全事件自动化取证，定位涉事资产和对威胁行为进行行为画像，提取网络原始流量、明细会话记录以及行为数据证据。
1.3	视频专网精准	视频专网精准防护系统—注重防护、预警，视频专网精准防护系统具备防御以及检测能力，构建福田视频专网重要资产的防护模型，检测违规、非

	防护系统	法访问行为后，执行阻断防御策略，保障关键资产和业务系统的正常运行。
1.3.1	管理中心	部署在深圳市公安局福田分局核心区域，对多采集分析引擎的数据进行统一整合以及多引擎策略进行统一管理，根据采集分析引擎和大数据中心的智能学习结果，自动生成监测模型，对重要资产或重要类型的资产开启精准防护，对异常设备和行为进行告警和阻断。以可视化的方式实时呈现全网面临的威胁及各类违规信息。通过分布图、趋势图、GIS 图方式帮助用户清晰的了解整体安全状况，及时感知威胁，统一防护和处置策略。
1.3.2	采集分析引擎	1、硬件参数：2U 标准机架式设备，系统底层采用 Linux 专用嵌入式安全操作系统，标配≥2 个 USB2.0 接口、≥2 个千兆电口，≥2 个万兆光纤模块，可扩展到≥6 个万兆光纤模块。
		2、性能指标：会话处理能力＞50 万条/秒；白名单并发处理能力＞100 万条。
		3、功能指标： （1）视频专网业务系统全识别：精准识别视频专网的视频联网平台，视频运行平台等常见业务应用系统，自学习各应用系统的业务流量特征，监测告警业务系统相关的异常访问、异常活动、数据泄露、异常账户行为等问题。 （2）精准防护：采集引擎把数据汇总到大数据中心，大数据中心智能学习设备的上下行流量、上下行数据包，连出 IP，连入 IP，总连接 IP，连接协议、信令、连出目的端口数、和谁连接以及被谁连接等信息学习到同类型设备有特征的指标项，通过特征指标项对接入终端的访问权限，协议、信令、流量区间等进行控制，只允许正常的业务类协议、信令访问、流量大小等通行。其他特征拒绝，最大限度的控制视频专网核心设备的访问权限及保障核心业务的安全。 （3）设备画像掌握设备活动规律：从访问时间、访问动作、访问对象、流量大小、数据包、端口等多个维度提取设备的动态属性和行为习惯，在此基础上结合连接访问关系完美呈现设备画像。对设备进行分类，针对同类型设备建立精准防护策略。系统可自动完成摄像头、NVR、视频存储平台、视频运维平台、大屏、运维 PC 等各类设备的画像工作，掌握每类设备活动规律。 （4）异常行为监管：对越权访问、非法数据下载、违规运维、非法扫描等一切非正常网络行为及时预警并可进行定向阻断。 （5）联动控制：支持与前端准入控制系统，防火墙联动，发现异常设备

		或行为通知准入控制系统或防火墙，就近阻断。
1.3.3	大数据中心	1、大数据中心部署在深圳市公安局福田分局核心区域，采集分析引擎的数据汇总到大数据中心，通过机器智能学习建立各类监测指标和基线，生成网络互访关系生态图，利用算法剔除毛刺数据，同时能够根据监测情况和处置意见进行动态调整和生长，监测指标自动转化为智能分析模型。利用以上措施，彻底改变原有基于黑名单匹配的安全监测和防护做法，真正实现对未知攻击的预警。
		2、资产监测：支持重要资产监测添加、修改、删除操作；支持智能学习后展示设备访问关系图、监测模型、数据表、点阵图、流量统计等；支持终端画像显示设备访问关系图和流量分析数据**【投标供应商需提供操作界面关于上述功能的截图和第三方检测机构出具的检测报告扫描件，报告须体现出满足上述功能要求】。**
2	安全计算环境	
2.1	终端管理系统	1、针对常见操作系统实现恶意代码检测、恶意代码处置安全防护能力。
		2、针对办公电脑实现进程、软件使用情况、外设使用情况、文件操作以及打印终端行为日志的记录。
		3、包含对终端的流量监控、非法外联、应用程序安全、网络安全、外设、桌面安全加固。
		4、采用 B/S 架构管理端，具备终端分组管理、策略制定下发、统一杀毒、统一漏洞修复、统一管控、资产管理以及各种报表和查询功能。
		5、产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；要求客户端程序具备自保功能，避免被恶意篡改。
		6、提供多引擎检测能力，包括但不限于云查引擎、人工智能 AI 引擎、启发式引擎，且查杀引擎可配置。对恶意代码进行有效检测和识别，对已知、未知病毒、病毒变种提供全面检测、拦截和清除能力。
		7、扫描到感染型病毒时，自动进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件。
		8、支持 USB、蓝牙或红外终端外设接口接入外设的使用情况审计；支持本机账户或域账户登录日志统计。
		9、具备自有漏洞补丁管理服务器，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理。

		10、支持补丁下载安装顺序设置，可以有效节省漏洞修复时间与减少 CPU 占用。
		11、支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃。
		12、**提供公安部颁发的《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（一级品）内网主机监测（一级）资质证书扫描件。**
		13、部署在福田分局机房（部署环境：CPU 至少 4 核或以上；内存不低于 4GB；硬盘不低于 500GB，Windows server 2008R2 或以上系统，IP 全网可达），客户端安装在全福田分局视频网终端计算机，为全福田分局终端计算机提供恶意代码防护、补丁管理、终端审计安全能力，实现终端安全全面防护，满足等保 2.0 安全计算环境终端安全防护的技术要求；同时系统支持对接深圳市公安局终端安全管理平台。
2.2	WEB 应用防火墙	1、机箱高度：2U，标配网口：≥2 千兆电口管理口，≥千兆业务电口*4（含 2 组硬件 BYPASS 模块），≥千兆业务光口*4（标配 GE 多模 SFP 模块*2，不含硬件 BYPASS 模块），≥2 万兆光口，硬盘容量：≥1T，内存：≥16G，USB 口：≥USB2.0 口*2，串口：≥RJ45 口*1，电源：1+1 热插拔冗余电源。硬件性能：网络吞吐量≥8Gbps，HTTP 应用吞吐量≥6Gbps，HTTP 最大并发数≥35 万，HTTP 最大新建数≥3.2 万，HTTPS 应用吞吐量≥1.5Gbps，HTTPS 最大并发数≥6.5 万，HTTPS 最大新建数≥6500。
		2、含三年硬件维保服务，含三年软件维保升级服务。
		3、支持根据细粒度条件对 CC 攻击进行检测和防护；匹配条件由 URL 参数、请求头部字段、目的 IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成；客户端检测对象由 IP、IP+URL、IP+User_Agent 参数组成；支持从请求头字段获取真实源 IP 地址。
		4、支持客户端安全防护，插入特殊的 HTTP 报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受 Clickjacking 攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）、X-XSS-Protect（用于当检测到 XSS 攻击时，指示浏览器停止加载页面）、Content-Security-Policy（用于降低浏览器上的 XSS 风险和数据注入攻击）。
		5、帮助反恐机房以及莲花机房的业务服务器应对 Web 攻击、防入侵、防挂马、防通报、防爬虫、防 CC 攻击、防 WebShell 攻击，事前阻止黑客篡改、事后自动恢复被篡改网页。杜绝一切漏洞攻击，满足网络安全等级保

		护 2.0 要求。
2.3	数据库防护与审计系统	1、硬件尺寸：标准 2U，CPU 规格：8 核*2，内存容量：≥64G，硬盘容量：≥4TB*4（Raid 5），硬盘接口：企业级 SATA，网口：≥6 审计口，网口类型：≥4 千兆电口+2 万兆光口（配≥2 万兆多模光模块），电源配置：双电源。
		2、总网络吞吐量：≥7000Mbps，双向审计最大数据库流量：≥700Mbps，峰值事务处理能力 TPS：≥70000 条/秒，日志数量存储：≥80 亿条，数据库实例授权许可数量：无限数据库授权。
		3、含三年软件维保服务，三年硬件维修服务。
		4、通过数据库协议分析与识别，操作行为识别方式对数据库高危风险以及违规操作行为进行检测并实现阻断；通过攻击特征库对针对数据库的攻击进行检测，并通过虚拟补丁相关策略功能进行针对性的安全策略建立，实现数据库安全防护。针对不同用户及管理员数据库表的增删改查操作行为进行记录，避免违规操作，确保事后可以进行追踪溯源。
2.4	服务器安全管理系统	1、服务器安全管理系统，统一运维管理、安全策略维护及全网安全日志分析、威胁溯源；采用轻代理 Agent，支持 Windows 和 Linux 系统，提供完整的系统加固和防护能力，包括资产梳理、风险发现、病毒扫描、安全基线、入侵检测功能；含三年使用升级服务。
		2、客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制。
		3、支持展示当前服务器、进程、账户、软件应用、Web 资产、Web 服务、Web 框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块分类资产数量统计，可对分类资产全局进行快速搜索，保留历史搜索记录并保存搜索条件以进行快捷搜索，同时提供服务器名、IP 地址、操作系统、资产类型的筛选搜索；针对搜索结果，支持按资产类型导出。
		4、支持对局域网内的服务器进行扫描，并自动获取服务器相关信息，包括服务器名、在线状态、别名、主机 IP、AgentID、操作系统、IPv4、IPv6 信息，可通过自动、手动的进行资产发现的任务设置。
		5、支持服务器操作系统、数据库、中间件、应用级的弱口令、口令复用扫描，并可对扫描的结果进行修复验证，还可对口令风险的扫描任务进行设置，包括任务名称、目标服务器、扫描类型、扫描所用字典、执行周期方式。

		6、可对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置，并以报告的形式展示软件漏洞扫描结果，包括：问题机器 TOP5、影响最多漏洞 TOP5、漏洞发现趋势。
		7、采用主动的方式进行自动化病毒查杀，可支持多引擎技术识别并查杀最新病毒；可支持病毒文件自动隔离、自动删除、不处理三种方式，并可将病毒查杀的结果导出报告。
		8、对暴力登录系统的账号和 IP 进行自动发现并上报暴力破解入侵事件，支持对 RDP、SSH、FTP 服务的暴力破解行为进行检测拦截，支持设定暴力破解行为的请求范围、失败次数，针对暴力破解的 IP 支持设定锁定时长。
		9、自动识别 web 服务目录，并实时进行 webshell 后门的扫描，包括：危险级别、文件路径、文件代销、文件 MD5、文件修改时间、webshell 发现时间、感染服务器信息。
		10、部署在福田分局机房（需要一台物理或虚拟机，支持 windows 或 linux 主流操作系统，支持中标麒麟、红旗等国产化操作系统），服务器或虚拟机部署轻代理；事前，通过自动识别应用系统资产、应用系统漏洞及网络资产的风险点，进行扫盲清障；事中，通过内网流量边界管理、动态防御模块、组成强有力的防护盾牌，进行自动防御；事后，通过实时监控的攻击朔源日志及事件来发现入侵痕迹、掌握威胁点，构建闭环的立体防御体系，实现混合数据中心架构下的服务器安全。
		11、支持 windows RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		12、支持 Linux 服务器 SSH 远程登录保护，可开启 SSH 远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		13、支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲14、支持以可视化形式展现攻击故事，提供可视化的进程树溯源，可直

		观看出攻击入口、相关操作行为、高危实体文件等信息，协助客户进行事件攻击溯源和研判分析**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲15、支持基于终端侧采集记录的行为数据，对文件变更、进程变更、网络连接、DNS 查询等多种行为，在全网中搜索命中指定条件的端点和行为，进行高级威胁的狩猎对全网终端发起威胁狩猎，挖掘潜伏攻击**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲16、支持对攻击事件深度分析，展示每步关键进程相关的文件行为、域名访问行为、进程操作行为、命令行参数等攻击相关的关键行为，帮助用户快速了解攻击者操作，洞悉目的和危害面**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲17、支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲18、**提供公安部颁发的《计算机信息系统安全专用产品销售许可证》主机型入侵检测产品（增强级）资质证书扫描件或信息产业信息安全测评中心出具的主机型入侵检测（增强级）产品合格检测报告扫描件。**
		▲19、联动本项目分析平台可以实现一键遏制（自动回溯事件行为链，定位恶意进程，阻断相关文件、进程外连通信、横向扩散行为）；一键根除（根据回溯出的风险项全部清除干净。清除后进程无法被创建、运行）；一键回滚（用户可以一键恢复被删除的文件、进程和注册表等，防止误操）；自动化响应（根据设置的剧本自动化遏制、根除）和精细化设置策略（根据业务情况，可设置对某些进程的某几个外连 ip 阻断，其余进程外连这些 ip 均不受影响）**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
3	安全管理中心	
3.1	堡垒机	1、采用专用千兆多核硬件平台和安全操作系统；外观：标准机架式；持≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆光口；内置≥4TB 硬盘；冗

		余电源；配置≥1000 授权许可。含三年标准售后服务。
		2、含三年软件维保服务，三年硬件维修服务。
		3、支持对网络设备、数据库、安全设备、主机系统资源的运维与审计，通过集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计功能。实时完整地记录用户的操作；提供方便灵活的操作回放和查询检索的手段，具备对运维人员的操作过程做到事前防范、事中控制及事后审计的能力。
3.2	漏洞扫描系统	1、Web 扫描域名无限制，Web 扫描任务并发数为≥10 个域名。系统扫描 IP 地址最大支持≥1024 个，支持扫描 A 类、B 类、C 类地址，系统扫描支持≥100 个 IP 地址并行扫描。标准 1U 机架式，≥1T 硬盘，标准配置≥6 个 10/100/1000M 自适应电口，≥2 个扩展插槽,≥2 个 USB 口，≥1 个 Console 口，单电源，含三年漏洞特征库升级，三年硬件维修服务。
		2、含三年漏洞特征库升级，三年硬件维修服务。
		3、支持接入平台自身采集分析的漏洞信息，也支持导入第三方漏洞报告。支持对漏洞信息进行统一管理，包括归并、修改、排序相关操作。
4	安全运营平台及工具	
4.1	移动客户端	CPU 型号：不低于 i7-13700； 操作系统：Windows 11 专业版或以上； 屏幕尺寸：14.0 英寸及以上； 物理分辨率：不低于 3840x2400； 内存容量：不低于 32GB； 硬盘容量：不低于 2TB SSD 固态硬盘； 显卡类型：集成显卡； 无线网卡：Wi-Fi 6 ； 保修要求：不少于 3 年部件和不少于 3 年人工全国联保。
4.2	工作站	CPU：不低于 i9-10900KF/i9-10900K； 操作系统：Windows 11 及以上； 内存容量：不低于 64GB； 硬盘容量：不低于 2TB HDD+1TB SSD； 显示芯片：不低于 RTX 3090； 显存容量：不低于 24GB； 无线网卡：WiFi6； 电源功率：850W 电源；

		保修要求：不少于三年有限保修及上门。
4.3	安全运营管理平台（二级平台）	
4.3.1	流量采集器	1、硬件外形：软硬一体化 2U 标准机架式设备；电源：1+1 冗余电源，内存：≥48G，硬盘容量：硬盘容量：≥4T，可用磁盘空间≥4T；接口数量：标配≥10 个；≥千兆 RJ45 网口*4、≥千兆业务 SFP 光口*4，≥万兆 SFP 光口*8，MTBF 大于 65000 小时，吞吐率：≥9Gbps。
		2、含三年软件维保服务，三年硬件维修服务。
		3、对网络流量进行进行采集，并根据采集到的网络流量进行初步检测与筛选，将加工后的数据通过接入接口传输到对应的分析模块进行深度分析。
		4、功能指标： （1）具备流量威胁深度检测能力，联动分析平台支持异常会话检测、WEB 攻击检测、挖矿行为检测、僵木蠕检测、Webshell 文件检测、异常文件检测、漏洞利用检测、DoS 攻击检测、扫描行为检测、配置风险检测、异常登录检测、横向移动检测、违规访问检测等 13 大类、超过 4 万条威胁检测规则； （2）具备流量协议内容深度还原，包括 http、dns、smb、ftp、smtp、pop3、imap、tls、tftp、ikev2、krb5、ssh 等协议； （3）具备网络入侵攻击报文检测引擎，触发告警，记录入侵攻击事件，记录：事件名称、来源 IP、来源端口、目的 IP、目的端口、原始流 ID、攻击报文、传输协议、应用协议、原始内容等。
		（4）流量采集系统负责对内外网的流量文件进行旁路镜像采集、审计和还原，还原后的流量日志会加密传输至分析系统。采集系统进行全协议审计，包含网络第 2 层至第 7 层数据流量，并支持特定的协议或 IP 进行自定义检测以及支持自定义 IP 地址、URL、域名与文件的访问监控，内置包括行为审计、探测扫描、漏洞利用、可疑通信、DDOS、恶意程序、配置风险、账号异常、主机异常、Web 攻击、横向移动等在内的 11 大类、70 小类共计近 4 万种的威胁检测规则，系统进行流量解析的同时，同时对数据包进行基于规则的威胁检测分析，并保存风险 pcap 数据包进行取证分析，并通过审计分析流量数据，详细记录所有的审计数据包，可展现审计数据包的时间、客户端 IP、服务端 IP、应用层协议、报文、返回码、详细信息等，这些信息通过加密通道传送至分析系统统一处理。
		▲6、支持不少于 5 种类型日志传输模式，包含但不限于标准模式、精简

		模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲7、审计白名单支持源目 IP、源目端口和日志类型、日志来源**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲8、具备违规访问检测能力。通过设置白名单和黑名单，建立针对性的业务和应用访问逻辑规则。策略从上到下进行匹配，可以通过右侧置顶功能对策略优先级进行调节。支持定义 IP 组、服务、端口、访问时间等访问策略**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		9、具备确定网络系统的脆弱点的技术能力。
		10、具备应急排查网络攻击的技术能力。
		11、具备检测日志流异常的技术能力。
4.3.2	日志采集器	1、机箱 2U 硬件，含 500 个接入设备许可，包含日志分析系统全功能模块（日志的采集、过滤、归并、关联分析、展现、告警监控、实施事件监控、报表）。内存：≥32GB，磁盘：≥12T*2 raid1，EPS：10000/秒，双冗余电源。含三年软件维保服务，三年硬件维修服务。
		2、可以以标准方式处理各种安全事件日志(攻击、入侵、异常)、各种行为事件日志(内控、违规)、各种弱点扫描日志(弱点、漏洞)、各种状态监控日志(可用性、性能、状态)、安全视角的事件描述：事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击分类、检测设备归类；日志审计系统采用了安全策略与基础系统分离的设计架构，将事件格式分析规则、关联分析规则、报警规则、综合报表规则等策略内容独立出来，变成可以独立演进、独立配置、独立升级的内容。
		3、支持接入 TLS 加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		4、支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**

		5、支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		6、支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
4.3.3	分析平台	1、机箱 2U 硬件/2*物理 CPU*24 核/内存≥256GB/硬盘≥4TB*12/支持 raid0、1、5、10、50/冗余 1+1 电源模块/1G RJ45*4/滑轨。
		2、含三年软件维保服务，三年硬件维修服务。
		3、模块具备云端威胁情报订阅模块：内置威胁情报离线库并支持更新。
		4、设备支持采用情报数据进行实时检测防御。
		5、设备支持在线查询与溯源：云端提供对 IoC 威胁类型、多源情报进行多维度的溯源分析。
		6、云端服务：支持订阅高级威胁分析情报，云端提供最新 APT 入侵、0day 漏洞预警、病毒变种情况分析报告订阅。
		7、分析系统主要实现以下效果：用户异常行为分析，智能深度感知，安全事件智能研判，安全自动响应编排，通过智能分析研判识别出真正有效的攻击和事件，结合用户实际场景进行全面溯源与取证、自动化响应处置，实现安全运营和管理的闭环。
		8、安全分析系统是一款融合了大数据技术和智能算法的安全运营系统，并依托于云端的海量数据及时共享最新的安全威胁情报，提供更为精准的威胁分析能力，通过深度解析流量中的 7 层协议，从而实现基于安全告警和攻击者的追踪溯源功能，并结合先进的大数据关联技术实现对安全告警时间和攻击者的追踪与取证，感知内网的安全状态，提供全天候全访问安全态势感知的能力。
		9、分析系统部署在用户的业务网络环境中，通过威胁发现、智能研判和自动化响应处置，实现安全运营的闭环管理，提高安全运维工作效率，构建智能安全运营体系。
		10、支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH 漏洞、OpenLDAP 等操作系统、数据库、Web 等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支

		持导出脆弱性感知报告**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		11、密码检测技术基于 UEBA 学习技术提取登陆成功的"举证信息"，通过 UEBA 技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容 Json、响应体关键字 Keyword、响应体 MD5 值、响应体长度 Length**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲12、支持挖矿专项检测页面。支持基于规则的“本地挖矿检测”和基于主动探测技术的“云端挖矿检测”，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲13、平台内置挖矿安全知识库，对常见的挖矿如：Bluehero 挖矿蠕虫变种、虚拟货币挖矿、EnMiner 挖矿病毒、PowerGhost 挖矿病毒、DDG 挖矿病毒、Docker 挖矿、DDG 挖矿变种、GroksterMiner 挖矿病毒、Linux 挖矿木马、ZombieBoy 挖矿木马等提供详细的背景介绍、感染现象、详细分析、相关 IOC（MD5、C2、URL）、解决方案**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲14、支持云端挖矿检测增强级赋能，通过主动探测技术，100%有效识别矿池服务，覆盖挖矿主流协议，支持加密“挖矿”检测，覆盖至少 100 种币种，支持网页挖矿、无文件挖矿、病毒挖矿、代理挖矿等各类挖矿手法检测**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲15、通过全流量分析，能够检测加密挖矿、DDG 挖矿病毒、DDG 挖矿变种、GroksterMiner 挖矿病毒、ZombieBoy 挖矿木马等挖矿病毒**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲16、通过对全流量深度分析，对 SSL/TLS 加密后的流量进行建模检测，有效检出包括但不限于加密挖矿、加密黑客工具、加密反弹 shell、加密 webshell 等加密流量通信**【投标供应商需提供具备 CMA 和 CNAS 标识的检**

		测报告扫描件，报告须体现出满足上述功能要求】。
		▲17、能够识别对相关单位应用站点的“混淆载荷攻击”和“协议错误攻击”，能够监测网络中的“无回显成功攻击”和“无文件落地的恶意脚本”。通过全流量深度分析技术，从而实现监测效果**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲18、具备威胁定性引擎，通过分析告警的上下文关联、时序关系、历史告警发生的频率等特征，从而确认安全告警的性质，包括：人工渗透、扫描器攻击、病毒、业务不规范、脆弱性风险等多个维度。告警信息包括：最近发生时间、威胁描述、标签、威胁定性、威胁类型、攻击阶段、威胁等级、受害者 IP、攻击者 IP、代理服务器 IP、结果、状态码、攻击次数、URL、威胁情报、数据来源、处置状态等 17 类关键信息，帮助安全人员快速处置重点关注的告警**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		19、需具备网络资产持续安全监控的技术能力。
三	互联网安全加固建设	
1	安全区域边界	
1.1	网络安全网关	1、网络处理能力≥15Gbps，并发连接≥200 万，每秒新建连接≥10 万/秒，2U 机箱，冗余电源，标准配置板载≥8 个 10/100/1000M 自适应电、≥2 个千兆光口和≥2 个万兆光口,≥1 个 Console 口，包含访问控制、地址转换、静态路由、动态路由、策略路由、流量控制、应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测功能。
		2、提供公安网络与互联网之间的边界访问控制，严格控制进出该安全区域的访问，明确访问的来源、访问的对象及访问的类型，确保合法访问的正常进行，杜绝非法及越权访问。同时有效预防、发现、处理异常的网络访问，确保该区域信息网络正常访问活动。
		3、含三年硬件维保服务，含三年全功能模块升级服务。
		4、配置不少于 1 台交换机，带路由功能，汇聚互联网专线，配置不少于 8 千兆光口。
2	安全计算环境	
2.1	WEB 应用防火墙	1、机箱高度：2U，标配网口：≥2 千兆电口管理口，≥千兆业务电口*4（含 2 组硬件 BYPASS 模块），≥千兆业务光口*4（标配 GE 多模 SFP 模块*2，不含硬件 BYPASS 模块）。

		2、硬盘容量：≥1T，内存：≥16G，USB 口：≥USB2.0 口*2，串口：≥RJ45 口*1，电源：1+1 热插拔冗余电源。
		3、含三年硬件维保服务，含三年全功能模块升级服务。
		4、保护站点：无限制，硬件性能：网络吞吐量≥6Gbps（需要内置 12 个千兆口才能达到 6G），HTTP 应用吞吐量≥4Gbps， HTTP 最大并发数≥30 万，HTTP 最大新建数≥3 万，HTTPS 应用吞吐量≥1Gbps，HTTPS 最大并发数≥6 万，HTTPS 最大新建数≥6000。
		5、帮助网站应对 Web 攻击、、防入侵、防挂马、防通报、防爬虫、防 CC 攻击、防 WebShell 攻击，事前阻止黑客篡改、事后自动恢复被篡改网页。杜绝一切漏洞攻击，满足网络安全等级保护 2.0 要求。
2.2	数据库防护与审计系统	1、硬件类型：工控机，硬件尺寸：标准 2U，CPU 规格：4 核，内存容量：≥8GB*2，硬盘容量：≥2TB*2（Raid 1），硬盘接口：企业级 SATA，网口：≥1 管理口+1HA 口+8 审计口（4 个千兆电+4 个千兆光），网口类型：≥1000M 电口*6，≥1000M 光口*4（多模，标配 2 个 SFP 模块、3 米 LC-LC 跳线 2 根），电源配置；双电源，空余拓展板卡位：2 个。
		2、总网络吞吐量：≥2000Mbps，双向审计最大数据库流量：≥200Mbps，峰值事务处理能力 TPS：≥20000 条/秒，日志数量存储：≥20 亿条，数据库实例授权许可数量：≥12。
		3、含三年软件维保服务，三年硬件维修服务。
		4、通过数据库协议分析与识别，操作行为识别方式对数据库高危风险以及违规操作行为进行检测并实现阻断；通过攻击特征库对针对数据库的攻击进行检测，并通过虚拟补丁相关策略功能进行针对性的安全策略建立，实现数据库安全防护。针对不同用户及管理员数据库表的增删改查操作行为进行记录，避免违规操作，确保事后可以进行追踪溯源。
3	安全管理中心	
3.1	堡垒机	1、采用专用千兆多核硬件平台和安全操作系统；外观：标准机架式；≥6 个千兆电口；支持≥2 个接口扩展槽位；内置≥4TB 硬盘；双电源；最大支持≥150 路图形会话或≥400 路字符会话并发；配≥100 授权许可。含三年标准售后服务。
		2、含三年软件维保服务，三年硬件维修服务。
		3、支持对网络设备、数据库、安全设备、主机系统资源的运维与审计，通过集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计功能。实时完整地记录用户的操作；提供方便灵活的操作回

		放和查询检索的手段，具备对运维人员的操作过程做到事前防范、事中控制及事后审计的能力。
3.2	日志审计系统	1、标准 1U 硬件，≥1 个 console 口，网口：≥6 个千兆工作管理口，≥1 个 console 口，内存：≥8GB，磁盘：≥1T*1，日志处理能力 EPS：≥4000/秒，双电源，可扩展项：磁盘：单个磁盘可扩展至 4T，含≥100 个接入设备许可。
		2、含三年软件维保服务，三年硬件维修服务。
		3、支持对主流安全设备、速通设备以及部分主机系统的日志进行收集与管理。
3.3	漏洞扫描系统	1、Web 扫描域名无限制，Web 扫描任务并发数≥5 个域名。系统扫描 IP 地址最大支持≥1024 个，支持扫描 A 类、B 类、C 类地址，系统扫描支持≥50 个 IP 地址并行扫描。标准 1U 机架式，≥1T 硬盘，标准配置≥6 个 10/100/1000M 自适应电口,≥2 个扩展插槽,≥2 个 USB 口,≥1 个 Console 口，单电源。含三年漏洞特征库升级，三年硬件维修服务。
		2、支持接入平台自身采集分析的漏洞信息，也支持导入第三方漏洞报告。支持对漏洞信息进行统一管理，包括归并、修改、排序相关操作。
		3、支持新建扫描任务包含系统扫描、Web 扫描、口令猜解、仅存活探测等任务类型，扫描方式为手动输入、使用资产、批量导入，可自定义扫描目标与任务名称，可选择执行方式、系统漏洞模板、口令猜解服务以及检测模式，支持开启调试模式；支持 Web 扫描检测包含暗链检测、网站木马检测、检测深度、爬虫策略、HTTP 请求头、表单填充内容、最大页面数、页面最大 KB 数、例外 URL、例外文件类型以及例外特定参数等选项，支持口令猜解字典选择包含 TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP 等服务类型以及 Oracle、REDIS、MySQL、Postgres、MsSQL 等数据库类型，对系统扫描、WEB 扫描、弱口猜解进行综合检查和分析，可输出同时包含系统扫描、WEB 扫描、弱口猜解结果的漏洞扫描安全评估报告。
4	安全运营平台及工具	
4.1	流量采集器	1、硬件外形：软硬一体化 2U 标准机架式设备；电源：1+1 冗余电源，内存：≥32G，硬盘容量：128G SSD+2T SATA，可用磁盘空间≥2T；接口数量：标配≥10 个；接口类型：≥千兆 RJ45 网口*4(管理口*1)、≥千兆业务 SFP 光口*4、≥万兆光口*8，吞吐率：5Gbps，含三年软件维保服务，三年硬件维修服务。
		2、对网络流量进行进行采集，并根据采集到的网络流量进行初步检测与

		筛选，将加工后的数据通过接入接口传输到对应的分析模块进行深度分析。
		3、功能指标： （1）具备流量威胁深度检测能力，支持异常会话检测、WEB 攻击检测、挖矿行为检测、僵木蠕检测、Webshell 文件检测、异常文件检测、漏洞利用检测、DoS 攻击检测、扫描行为检测、配置风险检测、异常登录检测、横向移动检测、违规访问检测等 13 大类、超过 4 万条威胁检测规则； （2）具备流量协议内容深度还原，包括 http、dns、smb、ftp、smtp、pop3、imap、tls、tftp、ikev2、krb5、ssh 等协议； （3）具备网络入侵攻击报文检测引擎，触发告警，联动分析平台可以记录入侵攻击事件，记录：事件名称、来源 IP、来源端口、目的 IP、目的端口、原始流 ID、攻击报文、传输协议、应用协议、原始内容等。
		4、流量采集系统负责对内外网的流量文件进行旁路镜像采集、审计和还原，还原后的流量日志会加密传输至分析系统。采集系统进行全协议审计，包含网络第 2 层至第 7 层数据流量，并支持特定的协议或 IP 进行自定义检测以及支持自定义 IP 地址、URL、域名与文件的访问监控，联动分析平台可以支持行为审计、探测扫描、漏洞利用、可疑通信、DDOS、恶意程序、配置风险、账号异常、主机异常、Web 攻击等多种威胁检测规则，系统进行流量解析的同时，同时对数据包进行基于规则的威胁检测分析，并保存风险 pcap 数据包进行取证分析，并通过审计分析流量数据，详细记录所有的审计数据包，可展现审计数据包的时间、客户端 IP、服务端 IP、应用层协议、报文、返回码、详细信息，这些信息通过加密通道传送至分析系统统一处理。
		▲5、具备账号安全防护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲6、支持防病毒，支持 6 种协议和 16 层压缩文件进行检测和拦截，**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		7、具备入侵防护 IPS 功能模块，支持用户自定义 IPS 规则，包括：WEB 应用防护规则、漏洞攻击规则、僵尸网络规则等。内置漏洞攻击规则库不少于 16600 条。僵尸网络与病毒防护规则库不少于 160 万条，应用特征识

		别规则库不少于 9300 条**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲8、支持联动云端蜜罐（非本地蜜罐）获取黑客指纹信息，自动封锁高危 IP。可选择诱捕外网攻击和内网扩散策略，通过云端高仿真的蜜罐，分析攻击者画像，溯源社交账号**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲9、具备策略路由的自动选路和全生命周期管理功能。支持网络对象、ISP 地址、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等。支持记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲10、支持自定义流量监控组件，可基于设备、应用、源目的 IP、接口设置不同的流量和会话数排行动态展示，展示效果支持面积图、折线图、柱状图等至少三种形式**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
四	内网安全检测系统建设	
1	安全运营管理平台（一级平台）	1、安全运营平台—注重态势感知、联动响应、溯源分析。
		2、通过合理的流程和机制，将运营平台平台和安全服务（人）有机地结合在一起。安全运营最核心的目的是要高效的解决问题，实质上在运营平台上人通过平台联动的工具来运营数据，能够在分析响应管理上形成闭环，形成固化。
		3、汇总福田分局三张网的安全数据，以可视化的方式实时呈现设备的数量、分布情况、面临的威胁及各类违规信息。通过分布图、趋势图、GIS 图方式帮助用户清晰的了解整体安全状况，及时感知威胁，统一防护和处置策略。
1.1	流量采集器	1、硬件外形：软硬一体化 2U 标准机架式设备；电源：1+1 冗余电源，内存：≥48G，硬盘容量：硬盘容量：≥4T，可用磁盘空间≥2T；接口数量：标配≥10 个；接口类型：≥千兆 RJ45 网口*4（管理口*1）、≥千兆业务 SFP 光口*4、≥万兆 SFP 光口*2。接口扩展：≥（千兆 RJ45 网口*4+千兆

		SFP 光口*4)或万兆 SFP 光口*2,MTBF 大于 65000 小时,吞吐率:≥10Gbps。
		2、含三年软件维保服务，三年硬件维修服务。
		3、对网络流量进行进行采集，并根据采集到的网络流量进行初步检测与筛选，将加工后的数据通过接入接口传输到对应的分析模块进行深度分析。
		4、功能指标：具备流量威胁深度检测能力，联动分析平台可以支持异常会话检测、WEB 攻击检测、挖矿行为检测、僵木蠕检测、Webshell 文件检测、异常文件检测、漏洞利用检测、DoS 攻击检测、扫描行为检测、配置风险检测、异常登录检测等。
		5、具备流量协议内容深度还原，包括 http、dns、smb、ftp、smtp、pop3、imap、tls、tftp、ikev2、krb5、ssh 协议。
		6、具备网络入侵攻击报文检测引擎，触发告警，联动分析平台可以记录入侵攻击事件，记录：事件名称、来源 IP、来源端口、目的 IP、目的端口、攻击报文、传输协议、应用协议。
		7、流量采集系统负责对内外网的流量文件进行旁路镜像采集、审计和还原,还原后的流量日志会加密传输至分析系统。采集系统进行全协议审计，包含网络第 2 层至第 7 层数据流量，并支持特定的协议或 IP 进行自定义检测以及支持自定义 IP 地址、URL、域名与文件的访问监控，联动分析平台可以支持行为审计、探测扫描、漏洞利用、可疑通信、DDOS、恶意程序、配置风险、账号异常、主机异常、Web 攻击等多种威胁检测规则，系统进行流量解析的同时，同时对数据包进行基于规则的威胁检测分析，并保存风险 pcap 数据包进行取证分析，并通过审计分析流量数据，详细记录所有的审计数据包，可展现审计数据包的时间、客户端 IP、服务端 IP、应用层协议、报文、返回码、详细信息，这些信息通过加密通道传送至分析系统统一处理。
		▲8、支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲9、审计白名单支持源目 IP、源目端口和日志类型、日志来源**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲10、具备违规访问检测能力。通过设置白名单和黑名单，建立针对性的

		业务和应用访问逻辑规则。策略从上到下进行匹配，可以通过右侧置顶功能对策略优先级进行调节。支持定义 IP 组、服务、端口、访问时间等访问策略**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		11、需具备确定网络系统的脆弱点的技术能力。
		12、需具备应急排查网络攻击的技术能力。
		13、需具备检测日志流异常的技术能力。
1.2	日志采集器	1、机箱 2U 硬件，≥500 个接入设备许可，包含日志分析系统全功能模块（日志的采集、过滤、归并、关联分析、展现、告警监控、实施事件监控、报表）。内存：≥32GB，磁盘：≥12T*2 raid1，EPS：10000/秒，双冗余电源。
		2、含三年软件维保服务，三年硬件维修服务。
		3、支持与主流日志审计设备、数通厂商设备或者 soc 日志直接对接。
		4、在联动本项目分析平台的情况下，可以以标准方式处理各种安全事件日志(攻击、入侵、异常)、各种行为事件日志(内控、违规)、各种弱点扫描日志(弱点、漏洞)、各种状态监控日志(可用性、性能、状态)、安全视角的事件描述包括：事件目标对象、事件行为、事件特征、事件命中结果、攻击事件描述、检测结果；日志审计系统采用了安全策略与基础系统分离的设计架构，将事件格式分析规则、关联分析规则、报警规则、综合报表规则策略内容独立出来，变成可以独立演进、独立配置、独立升级的内容。
		5、支持接入 TLS 加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		6、支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲7、支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		▲8、支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网

		络带宽和数据库存储空间的占用**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
1.3	分析平台	1、机箱 2U 硬件/2*物理 CPU*24 核/内存≥256GB/硬盘≥4TB*12/支持 raid0、1、5、10、50/冗余 1+1 电源模块/1G RJ45*4/滑轨。
		2、含三年软件维保服务，三年硬件维修服务。
		3、模块具备云端威胁情报订阅模块：内置威胁情报离线库并支持更新。
		4、设备支持采用情报数据进行实时检测防御。
		5、设备支持在线查询与溯源：云端提供对 IoC 威胁类型、多源情报进行多维度的溯源分析；
		6、云端服务：支持订阅高级威胁分析情报，云端提供最新 APT 入侵、0day 漏洞预警、病毒变种情况分析报告订阅。
		7、分析系统主要实现以下效果：用户异常行为分析，智能深度感知，安全事件智能研判，安全自动响应编排，通过智能分析研判识别出真正有效的攻击和事件，结合用户实际场景进行全面溯源与取证、自动化响应处置，实现安全运营和管理的闭环。
		8、安全分析系统是一款融合了大数据技术和智能算法的安全运营系统，并依托于云端的海量数据及时共享最新的安全威胁情报，提供更为精准的威胁分析能力，通过深度解析流量中的 7 层协议，从而实现基于安全告警和攻击者的追踪溯源功能，并结合先进的大数据关联技术实现对安全告警时间和攻击者的追踪与取证，感知内网的安全状态，提供全天候全访问安全态势感知的能力。
		9、分析系统部署在用户的业务网络环境中，通过威胁发现、智能研判和自动化响应处置，实现安全运营的闭环管理，提高安全运维工作效率，构建智能安全运营体系。
		10、支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH 漏洞、OpenLDAP 等操作系统、数据库、Web 等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		11、密码检测技术基于 UEBA 学习技术提取登陆成功的"举证信息"，通过 UEBA 技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容 Json、响应体关键字 Keyword、响应体 MD5 值、响应体长度 Length**【投标供应商需提供操作界面关于上述功能的截图和具备 CMA**

		和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。
		▲12、支持挖矿专项检测页面。支持基于规则的“本地挖矿检测”和基于主动探测技术的“云端挖矿检测”，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。
		▲13、平台内置挖矿安全知识库，对常见的挖矿如：Bluehero 挖矿蠕虫变种、虚拟货币挖矿、EnMiner 挖矿病毒、PowerGhost 挖矿病毒、DDG 挖矿病毒、Docker 挖矿、DDG 挖矿变种、GroksterMiner 挖矿病毒、Linux 挖矿木马、ZombieBoy 挖矿木马等提供详细的背景介绍、感染现象、详细分析、相关 IOC（MD5、C2、URL）、解决方案【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。
		▲14、支持云端挖矿检测增强级赋能，通过主动探测技术，100%有效识别矿池服务，覆盖挖矿主流协议，支持加密“挖矿”检测，覆盖至少 100 种币种，支持网页挖矿、无文件挖矿、病毒挖矿、代理挖矿等各类挖矿手法检测【投标供应商需提供操作界面关于上述功能的截图和具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。
		▲15、通过全流量分析，能够检测加密挖矿、DDG 挖矿病毒、DDG 挖矿变种、GroksterMiner 挖矿病毒、ZombieBoy 挖矿木马等挖矿病毒【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。
		▲16、通过对全流量深度分析，对 SSL/TLS 加密后的流量进行建模检测，有效检出包括但不限于加密挖矿、加密黑客工具、加密反弹 shell、加密 webshell 等加密流量通信【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。
		▲17、能够识别对相关单位应用站点的“混淆载荷攻击”和“协议错误攻击”，能够监测网络中的“无回显成功攻击”和“无文件落地的恶意脚本”。通过全流量深度分析技术，从而实现监测效果【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。

		▲18、具备威胁定性引擎，通过分析告警的上下文关联、时序关系、历史告警发生的频率等特征，从而确认安全告警的性质，包括：人工渗透、扫描器攻击、病毒、业务不规范、脆弱性风险等多个维度。告警信息包括：最近发生时间、威胁描述、标签、威胁定性、威胁类型、攻击阶段、威胁等级、受害者 IP、攻击者 IP、代理服务器 IP、结果、状态码、攻击次数、URL、威胁情报、数据来源、处置状态等 17 类关键信息，帮助安全人员快速处置重点关注的告警**【投标供应商需提供具备 CMA 和 CNAS 标识的检测报告扫描件，报告须体现出满足上述功能要求】。**
		19、需具备网络资产持续安全监控的技术能力。
五	公安网违规行为和安全监测建设	
1	网络违规行为监测系统（平台和探针）	
1.1	采集模块	1、2U 独立机架，电源 800W 1+1 冗余，双路 CPU（单路 8 核），内存≥64GB，配备千兆流量采集口≥2 个或万兆流量采集口≥1 个，存储容量≥2*250GB SSD+4*4TB SAS（Raid 5），具备并发会话处理能力≥120 万；含三年软硬件维保服务。
		2、支持各种常见的网络链路环境（包括 QinQ），采用多种数据采集方式。
		3、分光/分流、交换机端口镜像旁路方式采集网络流量。
		4、无代理远程主动探测方式。
		5、基于浏览器插件方式，无需在终端机器安装软件，设备实体终端浏览器在进行业务访问行为时，嵌入监控缓存，实现监测终端信息。
		6、支持 VLAN/LAN 内静默运行网络末梢探针方式采集局域网内安全风险行为。
		7、支持数据过滤能力。
		8、提供对指定范围内的 IP 段或者 IP 进行数据过滤，不再分析已过滤数据。
		9、提供只对指定范围内的 IP 段或 IP 进行数据分析，其他 IP 数据不进行分析。
		10、支持数据汇聚能力。
		11、支持对多链路流量独立分析。
		12、支持对多链路流量汇聚后统一分析。
		13、支持原始数据包存储能力。
		14、提供对原始数据包压缩存储。
		15、提供网络原始数据包的检索、自动关联提取，图形化定义检索条件、

		支持 BPF 表达式。
		16、网络末梢传感器应用模式: （1）支持软件分发平台分发； （2）支持终端独立部署； （3）支持静默安装部署。
		17、具备网络巡航管控系统采集能力，支持监测目标授权：999 个 IP，支持以 ID 智能值守模式和以 IP 智能值守模式，支持状态查询、数据查询、访控调度等 API 接口。
1.2	分析模块	1、2U 独立机架，电源 800W 1+1 冗余，双路 CPU（单路 8 核），内存≥96GB，存储容量≥2*250GB SSD+8*4TB SAS（Raid 5），数据存储周期≥180 天。
		2、支持违规和非授权网络边界监测，发现外联节点、不受控边界通道、非授权入网、边界穿透服务以及网中网。
		3、支持网络攻击监测，分析攻击特征和传播行为，包括病毒传播、高频失败连接、定向探测、敏感端口/控制端口/数据库端口恶意扫描。
		4、支持异常访问监测，识别敏感业务、应用、数据的异常连接访问行为，包括异常访问设备/应用、数据异常访问、跨域异常访问行为；
		5、支持违规行为监测，基于行为特征和风险扫描分析违规入网设备、违规游戏、违规站点搭建、违规通讯服务以及违规传输行为；
		6、支持安全隐患分析，主动分析设备的端口、服务开放详情，及时发现网内开放敏感端口、全端口、可登录匿名 FTP 服务器自身存在脆弱性的资产设备。
		7、支持对安全事件自动化取证，定位涉事资产和对威胁行为进行行为画像，提取网络原始流量、明细会话记录以及行为数据数据证据。
六	公安网终端准入建设	
1	准入控制（公安网核心）	1、实时监测并发现接入内网的 PC、平板电脑、智能手机、哑终端（视频类）设备，能够在第一时间隔离阻断并通知管理员。支持多种准入控制技术，支持 DHCP 准入控制技术、ARP 准入控制技术、SNMP 准入控制技术、SPAN 准入控制技术、MVG 准入控制技术、SPS 准入控制技术，并且支持多种准入技术的混合部署方案。
		2、支持静态密码+人脸识别”的双因素认证技术。
		3、人脸识别”支持“扫一扫二维码”的方式实现，应要求网络准入控制系统无须与互联网通信 。
		4、“人脸识别”技术无须预先后台录入人脸数据，具备自动对比公安人

		脸数据库的能力。
1.1	终端准入 Licencce 授权	1、针对内网的 PC、平板电脑、智能手机、哑终端（视频类）设备进行身份识别及接入管控，实现终端合规接入，避免黑客仿冒及非法接入。
1.2	终端准入控制设备	1、规格：2U 机架式，≥4 个 10/100/1000M 电口，硬盘≥2*2T,冗余电源；出货标配入网总许可数≥4000 点，设备采用双机热备，不可分开使用。功能描述：具有独立自主知识产权，支持旁路部署；设备宕机或断网不影响正常入网;支持多种准入控制技术,内置强大的视频网专用指纹识别库，精准识别海康、大华、华为、宇视品牌摄像机、NVR\DVR、的设备型号、设备功能和硬件特征码；支持无客户端的违规外联检测：支持无客户端的违规外联检测和邮箱告警，支持无客户端的违规外联自动阻断，无客户端的违规外联告警，包括：内网 IP 地址、内网 MAC 地址、内网连接位置（交换机端口）、外网 IP 地址、违规时长，支持自动扫描全网设备是否存在内外网同时连接的违规外联；支持图形化定位 HUB、小交换机、虚拟集群的位置和下联检索，支持堆叠交换机的图形化分层展示和上下左右切换；支持提供每日入网报告、每周入网报告、每月入网报告，并提供导出和打印功能。
		2、含三年软件维保服务，三年硬件维修服务。
		3、支持违规外联告警邮件，包括：内网 IP 地址、设备 MAC 地址、内网连接位置（交换机端口）、外网 IP 地址、违规时间。
2	准入控制（业务接入网）	1、规格：1U 机架式，≥6 个 10/100/1000M 电口，硬盘≥1T，单电源。
		2、出货标配入网许可数≥100 点。
		3、含三年软件维保服务，三年硬件维修服务。
		4、功能描述：具有独立自主知识产权，标准机架式硬件产品，可与公安网安全准入进行对接使用，除自身硬件设备外，产品功能的实现无需额外增加服务器设备。支持多种准入控制技术，支持 DHCP 准入控制技术、ARP 准入控制技术、SNMP 准入控制技术、SPAN 准入控制技术、MVG 准入控制技术、SPS 准入控制技术，并且支持多种准入技术的混合部署方案。支持图形化定位 HUB、小交换机、虚拟集群的位置和下联检索，支持堆叠交换机的图形化分层展示和上下左右切换,提供每日入网报告、每周入网报告、每月入网报告，并提供导出和打印功能。
		5、支持通过准入系统勾选 VLAN，并自动下发 VLAN 表库至交换机，无需

		人工登录交换机后台配置。
		6、对接入公安网的办事大厅办公终端、自助办证一体机以及自助机旁部署的监控摄像头进行准入控制。支持多种准入控制技术，支持 DHCP 准入控制技术、ARP 准入控制技术、5、SNMP 准入控制技术、SPAN 准入控制技术、MVG 准入控制技术、SPS 准入控制技术，并且支持多种准入技术的混合部署方案。支持图形化定位 HUB、小交换机、虚拟集群的位置和下联检索，支持堆叠交换机的图形化分层展示和上下左右切换，提供每日入网报告、每周入网报告、每月入网报告，并提供导出和打印功能。
七	信息安全服务体系建设	
1	威胁分析与处置服务（含人工）	1、安全威胁分析：结合安全感知日志和威胁情报进行深度分析，研判网络中存在的威胁和攻击行为，明确对业务的影响和危害。
		2、安全事件处置：对安全事件进行处置，清除恶意文件、快速恢复业务。
		3、事件溯源分析：深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径。
		4、安全加固建议：根据事件发生的根因、影响范围，针对性给出安全加固方案；按季度输出安全加固方案及安全运营效果汇报。
		5、拟投入 1 个人员提供驻场服务（驻场人员需满足 CDSP 认证或系统集成项目管理工程师认证）
2	风险评估服务	资产梳理：安全访谈和调研，梳理信息资产和业务环境状况，针对重要业务系统制定评估详细方案。脆弱性评估：通过 web 扫描，漏洞扫描、基线检查、漏洞验证手段，识别业务系统安全脆弱性风险。防御能力评估：通过模拟黑客进行信息收集、应用及系统入侵，验证防御体系的安全防御能力。失陷检查：通过人工或工具产品检测主机系统上的恶意文件和网络行为判断是主机失陷状态。安全整改建议：基于安全评估结果分析系统安全风险和威胁，给出针对性的风险处理方案。
3	渗透测试服务	对应用系统模拟黑客攻击进行安全性测试，发现系统存在的安全问题，对过程中发现的问题及风险提出安全加固建议。通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用，从而发现最严重的安全漏洞，同时通过对系统进行准确、全面的测试，发现系统最脆弱的环节，以便对危害性严重的漏洞及时修补，防止漏洞被利用。
4	应急演练服务	协助采购单位制定应急响应机制，完善应急响应预案，并根据用户实际情况，提供应急事件演练方案。
5	应急响	1、包括但不限于：应急响应服务，风险评估服务、渗透测试服务、应急

	应服务	演练服务。 2、投标供应商需协调本项目中“安全运营管理平台”产品生产厂家提供驻场服务，拟投入 1 个人员（驻场人员需满足 CDSP 认证或系统集成项目管理工程师认证）。

五、商务要求

1、交货地点：深圳市公安局福田分局

★2、交货时间：合同签订后 30 个日历日内。

3、验收方式：

（1）中标人已按照合同规定提供了项目全部产品及完整的技术资料。

（2）项目符合招标文件技术规格书的要求，性能满足要求。

（3）货物具备产品合格证。

4、付款方式：

（1）预付款：合同签订生效后，采购人支付合同金额的 50%作为项目预付款；

（2）到货款：设备到货后，采购人支付合同金额的 20%作为项目到货款；

（3）验收款：

a.本项目通过初步验收，签署项目初步验收报告后，采购人支付合同金额 15%的项目初步验收款；

b.本项目通过最终验收，签署项目最终验收报告后，采购人支付合同金额 10%的项目竣工验收款；

（4）尾款：项目通过审计后，采购人支付合同金额 5%的尾款。

5、售后服务要求；

（1）货物免费保修期不少于 3 年，时间自最终验收合格并交付使用之日起计算。

（2）免费保修期内，所有服务及配件全部免费。

（3）在保修期内，一旦发生质量问题，投标人保证在接到通知 4 小时内响应并赶到现场，24 小时内解决故障确保正常使用。

（4）以上响应 7x24 小时，不分节假日。

6、如后续年度经人大审议通过的部门预算中，该采购项目预算金额较提前采购金额发生变化的，双方可根据相关规定签订补充协议或终止协议执行。

六、演示要求

（一）总体要求：

演示地点提供电源、投影仪及宽带上网环境（有 WIFI），由投标人代表自带手提电脑、无线路由器、便携式服务器、U 盘及其它能完成演示操作的设备（具体以投标人实际需要为准，但严禁携带手机等通讯工具）等进行演示。由于演示场地有限，建议勿携带过大设备进行演示。

每个投标人的现场演示时间不超过 20 分钟（演示期间评委将进行提问，并有权酌情延长时间），现场演示人员不得超过 2 人。

（二）签到要求：

参加现场演示的投标人须在投标截止时间前进行现场演示签到，携带法定代表人证明书（盖公章）、法人授权委托书（盖公章）、现场演示人员的身份证原件和复印件，到达深圳市中正招标有限公司开标室，按工作人员指引进行签到。

特别注意事项：（1）资料提供不齐全的，不予签到；（2）投标截止时间后不再受理签到；（3）未签到的人员，不能参与现场演示。

（三）演示内容：

序号	货物名称	功能演示内容
一	视频专网安全加固建设	
1	安全区域边界	
	网络安全网关	1、支持防病毒，支持 16 层压缩文件进行检测和拦截。
		2、支持工控协议审计，支持对 OPC-DA、S7-Plus、S7、profinetIO、IEC104、MODBUS、OPCUA、DNP3、Fins、MMS、CIP、Scnet、SMTP、Sonet、SV、BACnet、ENIP-IO 等多种工控协议的审计。审计信息包括：时间、源/目的 IP、源/目的端口、协议类型、协议详情等。
		3、支持 IoT 协议准入，可识别 ONVIF、MQTT、Modbus、S7 等 IoT 协议基于协议进行应用层准入，仅允许指定协议入网通信，可设置生效时间、新增单次时间计划和循环时间计划等。支持视频信令准入，可识别 SIP、RTP、RTCP、RTSP 等视频信令进行准入控制。支持标准合规准入，可识别 GA/T 1400、GB/T 28181、GB 35114 等相关国家标准，基于国家标准进行应用层准入，仅允许符合国家标准的设备入网通信。
2	安全计算环境	
	服务器安全管理系统	1、支持以可视化形式展现攻击故事，提供可视化的进程树溯源，可直观看出攻击入口、相关操作行为、高危实体文件等信息，协助客户进行事件攻击溯源和研判分析。

		2、支持基于终端侧采集记录的行为数据，对文件变更、进程变更、网络连接、DNS 查询等多种行为，在全网中搜索命中指定条件的端点和行为，进行高级威胁的狩猎对全网终端发起威胁狩猎，挖掘潜伏攻击。
		3、支持对攻击事件深度分析，展示每步关键进程相关的文件行为、域名访问行为、进程操作行为、命令行参数等攻击相关的关键行为，帮助用户快速了解攻击者操作，洞悉目的和危害面。
3	安全运营管理平台（二级平台）	
	分析平台	1、支持挖矿专项检测页面。支持基于规则的“本地挖矿检测”和基于主动探测技术的“云端挖矿检测”，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息。
		2、具备威胁定性引擎，通过分析告警的上下文关联、时序关系、历史告警发生的频率等特征，从而确认安全告警的性质，包括：人工渗透、扫描器攻击、病毒、业务不规范、脆弱性风险等多个维度。告警信息包括：最近发生时间、威胁描述、标签、威胁定性、威胁类型、攻击阶段、威胁等级、受害者 IP、攻击者 IP、代理服务器 IP、结果、状态码、攻击次数、URL、威胁情报、数据来源、处置状态等 17 类关键信息，帮助安全人员快速处置重点关注的告警。
二	互联网安全加固建设	
1	安全运营平台及工具	
	流量采集器	1、支持联动云端蜜罐（非本地蜜罐）获取黑客指纹信息，自动封锁高危 IP。可选择诱捕外网攻击和内网扩散策略，通过云端高仿真的蜜罐，分析攻击者画像，溯源社交账号。
		2、具备策略路由的自动选路和全生命周期管理功能。支持网络对象、ISP 地址、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等。支持记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。

七、其他要求

为保障项目完成质量，投标人应具备履约相关的资质、能力等，包括但不限于：

1、质量管理体系、职业健康安全管理体系、业务连续性管理体系、信息技术服务管理体系、信息安全管理体系等认证证书；

2、同类项目业绩；

3、获奖（荣誉）、网络安全类计算机软件著作权登记证书；

4、拟投入不少于 10 人的项目团队，其中包含项目经理 1 人，技术负责人 1 人，不少于 8 人的技术团队成员；

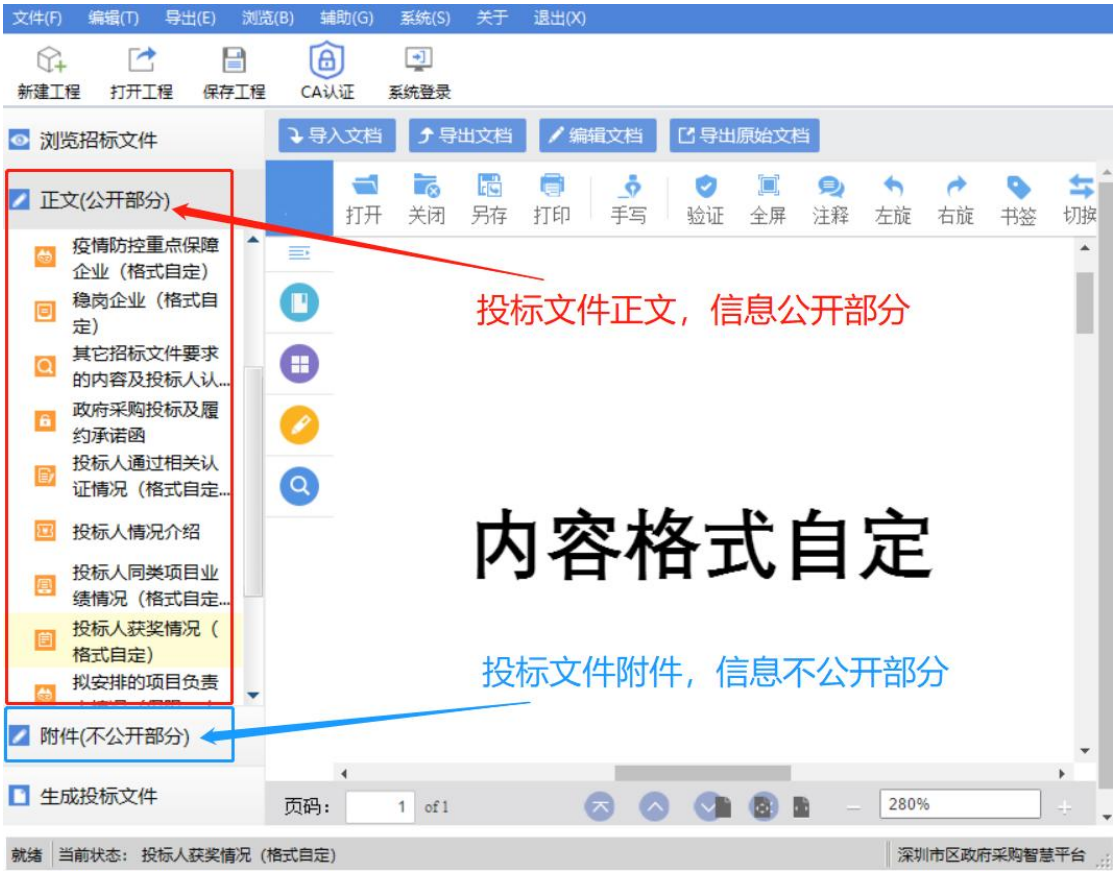
5、技术方案、项目管理方案、售后服务方案、培训方案等。

第三章　投标文件格式、附件

特别提醒：

投标文件正文将对外公开，投标文件附件不公开。投标人在编辑投标文件时，在投标文件目录中属于本节点内容的必须在本节点中填写，填写到其他节点或附件的将可能导致投标无效，一切后果由供应商自行承担。

投标人应按招标文件规定的“投标文件组成”编制投标文件正文（信息公开部分）和投标文件附件（信息不公开部分），举例如下图：



采购代理机构公布投标文件正文（信息公开部分）时为计算机截取信息自动公布，**如投标人误将涉及个人隐私或其他重要信息放入投标文件正文，相关后果由投标人自负；如投标人将必须放于投标文件正文（信息公开部分）的内容放入投标文件附件（信息不公开部分），将作投标无效处理。**

投标文件组成：

1. **投标文件正文（信息公开部分）**，主要包括以下内容：

（1）投标函

（2）资格响应文件

（3）投标人情况介绍

（4）中小企业声明函等符合政府采购扶持政策的证明材料

2. **投标文件附件（信息不公开部分）**，主要包括以下内容：

（5）政府采购违法行为风险知悉确认书

（6）法定代表人（负责人）资格证明书
（7）投标文件签署授权委托书
（8）实质性条款响应情况表
（9）分项报价表
（10）技术规格偏离表
（11）商务条款偏离表
（12）产品演示
（13）技术保障措施
（14）项目经理（仅限一人）情况
（15）项目团队（项目经理除外）情况
（16）同类项目业绩情况
（17）企业认证情况
（18）企业获奖情况
（19）企业资质情况
（20）计算机软件著作权登记证书
（21）招标文件要求的其它内容或投标人认为需要补充的资料

备注：

1.本项目为网上电子投标项目，投标文件不需法人或授权委托人另行签字，无需加盖单位公章，招标文件专用条款另有规定的除外。

2.关于填写“开标一览表”的说明：“开标一览表”中除“投标报价”外，其他信息不作为评审依据。

投标文件正文（信息公开部分）：

一、投标函

深圳市中正招标有限公司：

1.根据已收到贵方的（项目编号为_____）的（_____项目）的招标文件，遵照《深圳经济特区政府采购条例》和《深圳网上政府采购管理暂行办法》等有关规定，我方经研究上述招标文件的专用条款及通用条款后，愿以投标书编制软件中《开标一览表》中填写的投标报价并按招标文件要求承包上述项目并修补其任何缺陷。

2.我方已认真核实了投标文件的全部资料，所有资料均为真实资料。我方对投标文件中全部投标资料的真实性负责，如被证实我方的投标文件中存在虚假资料的，则视为我方隐瞒真实情况、提供虚假资料，我方愿意接受主管部门作出的行政处罚。

3. 我方同意所递交的投标文件在“对通用条款的补充内容”中的投标有效期内有效，在此期间内我方的投标有可能中标，我方将受此约束。

4. 除非另外达成协议并生效，贵方的中标通知书和本投标文件将构成约束我们双方的合同。

5. 我方理解贵方将不受必须接受你们所收到的最低标价或其它任何投标文件的约束。

投标人：_____ 单位地址：_____
法定代表人或其委托代理人：_____
邮政编码：_____ 电话：_____ 传真：_____
开户银行名称：_____ 开户银行帐号：_____
开户银行地址：_____ 开户银行电话：_____
日期：_____年_____月____日

二、资格响应文件

1、营业执照或法人证书等证明材料（扫描件）

2、政府采购投标及履约承诺函

3、其它资格证明材料（如有，按招标公告“申请人的资格要求”提供）

政府采购投标及履约承诺函

深圳市中正招标有限公司：

我单位承诺：

1. 我单位满足《中华人民共和国政府采购法》第二十二条规定的下列条件：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（六）法律、行政法规规定的其他条件。

2.我单位参与本项目采购活动前三年内，在经营活动中没有重大违法记录，包括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。

3.我单位参与本项目政府采购活动时不存在被有关部门禁止参与政府采购活动且在有效期内的情况；与其他投标供应商不存在“单位负责人为同一人或者存在直接控股、管理关系”的情况；除单一来源采购项目外，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.我单位承诺不非法转包或分包。

5.我单位本招标项目所提供的货物或服务未侵犯知识产权。

6.我单位参与该项目投标，严格遵循公平竞争的原则，不妨碍其他投标人的竞争行为，不损害采购人或者其他投标人的合法权益，与其他采购参加人不存在下列串通投标情形：

（1）投标供应商之间相互约定给予未中标的供应商利益补偿；

（2）不同投标供应商的法定代表人、主要经营负责人、项目投标授权代表人、项目负责人、主要技术人员为同一人、属同一单位或者在同一单位缴纳社会保险；

（3）不同投标供应商的投标文件由同一单位或者同一人编制，或者由同一人分阶段参与编制的；

（4）不同投标供应商的投标文件或部分投标文件相互混装；

（5）不同投标供应商的投标文件内容存在非正常一致；

（6）由同一单位工作人员为两家以上（含两家）供应商进行同一项投标活动的；

（7）主管部门依照法律、法规认定的其他情形。

7.我单位如果中标，做到守信，不偷工减料，依照本项目招标文件需求内容、签署的采购合同及本单位在投标中所作的一切承诺履约。

8.我单位承诺不恶意低价谋取中标；我单位对本项目的报价负责，中标后将严格按照本项目招标文件需求、签署的采购合同及我单位在投标中所作的全部承诺履行。我单位清楚，若我单位以“报价太低而无法履约”为理由放弃本项目中标资格，愿意接受主管部门的处理处罚。若我单位中标本项目，我单位的报价明显低于其他投标人的报价时，我单位清楚，本项目将成为重点监管、重点验收项目，我单位将按时保质保量完成，并全力配合有关监管、验收工作；若我单位未按上述要求履约，我单位愿意接受主管部门的处理处罚。

9.我单位已认真核实了投标文件的全部内容，所有资料均为真实资料。我单位对投标文件中全部投标资料的真实性负责，如被证实我单位的投标文件中存在虚假资料的，则视为我单位隐瞒真实情况、提供虚假资料，我单位愿意接受主管部门作出的行政处罚。

10.我单位获得中标、成交资格后无正当理由放弃中标、成交资格的，自愿接受政府采购主管部门将我单位放弃中标、成交资格的信息公示在深圳市政府采购监管网，公示期一年，一切不利后果我单位均自愿承担。

以上承诺，如有违反，愿依照国家相关法律处理，并承担由此给采购人带来的损失。

投标人：

日期：____年___月___日

三、投标人情况介绍

序号	项　目	内容及说明	备注
一	**营业执照**		
1	注册年度及注册编号		
2	注册资金（万元）		
3	法定代表人		
4	住所地		

5	经营范围		
6	开户银行及账号		
7	联系方式		
二	**其他材料**		

注：供应商应填写上述表格内容，并可根据自身情况自行对表格内容进行补充和完善。

四、中小企业声明函等符合政府采购扶持政策的证明材料

填写指引：

1、该部分内容由投标人根据自身实际情况填写，投标人提供的声明函不属实的，属于提供虚假资料谋取中标，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。

2、该部分内容填写需要参考的相关文件包括但不限于（具体内容详见附件）：

(1) 财政部 工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知（财库〔2020〕46 号）

(2)《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）

(3) 国家统计局关于印发《统计上大中小微型企业划分办法 （2017）》的通知（国统字〔2017〕213 号）

(4) 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）

(5) 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）

3、请依照招标文件提供的格式和内容填写声明函，不要随意变更格式；声明函不需要盖章或签字；满足多项优惠政策的投标人，不重复享受多项价格扣除政策。

4、《中小企业声明函》填写要求：

（1）在“单位名称”下划线处如实填写**采购人名称（详见采购人信息，非采购代理机构）**；

（2）在“项目名称”下划线处如实填写**采购项目名称**；

（3）在“标的名称”下划线处填写所**采购标的（货物或服务或工程）的具体名称（具体详见第二章招标项目需求，如涉及多项标的，投标人需逐项进行响应）**；

（4）在“采购文件中明确的所属行业”下划线处填写**采购文件规定的本项目所属行业（详见其它关键信息）**；

（5）在“从业人员”、“营业收入”、“资产总额”下划线处如实填写**制造商（货物类）或承接企业（服务或工程类）**上一年度从业人员、营业收入、资产总额，无上一年度数据的新成立企业可以不填报；

（6）在“中型企业、小型企业、微型企业”下划线处如实依照工信部联企业〔2011〕300 号文填写相应的企业类型。

1、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，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

2. （标的名称），属于（采购文件中明确的所属行业）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。

本企业已知悉《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）、《中小企业划型标准规定》（工信部联企〔2011〕300 号）、《统计上大中小微型企业划分办法（2017）》等规定，承诺提供的声明函内容是真实的，并知悉根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）第二十条规定，供应商按照本办法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《政府采购法》等政府采购有关法律法规规定追究相应责任。

企业名称：

日期：____年___月___日

备注：

1、填写前请认真阅读《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)和《财政部 工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知》(财库〔2020〕46 号)相关规定。

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、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，不享受中小企业扶持政策。

2、监狱企业声明函

本单位郑重声明，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，本单位为符合条件的监狱企业。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称：

日期：____年___月___日

附：省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的监狱企业证明文件。

备注：填写前请认真阅读《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）相关规定。如不符合前述相关规定所确定的监狱企业，则不需要在投标文件中提供本《监狱企业声明函》；若符合前述相关规定所确定的监狱企业，除了提供本《监狱企业声明函》，还需提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。否则视为在本项目中放弃政府采购政策扶持，不进行价格扣除。

3、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，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。

本单位知悉《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，承诺提供的声明函内容是真实的，如提供声明函内容不实，则依法追究相关法律责任。

单位名称：

日期：____年___月___日

备注：填写前请认真阅读《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)相关规定。如不符合前述相关规定所确定的残疾人福利性单位，则不需要在投标文件中提供本《残疾人福利性单位声明函》；若符合前述相关规定所确定的残疾人福利性单位，但在投标文件中没有提供本《残疾人福利性单位声明函》，视为在本项目中放弃政府采购政策扶持，不进行价格扣除。

投标文件附件（信息不公开部分）：

五、政府采购违法行为风险知悉确认书

本公司在投标前已充分知悉以下情形为参与政府采购活动时的重大风险事项，并承诺已对下述风险提示事项重点排查，做到严谨、诚信、依法依规参与政府采购活动。

一、本公司已充分知悉“隐瞒真实情况，提供虚假资料”的法定情形，相关情形包括但不限于：

（一）通过转让或者租借等方式从其他单位获取资格或者资质证书投标的。

（二）由其他单位或者其他单位负责人在投标供应商编制的投标文件上加盖印章或者签字的。

（三）项目负责人或者主要技术人员不是本单位人员的。

（四）投标保证金不是从投标供应商基本账户转出的。

（五）其他隐瞒真实情况、提供虚假资料的行为。

二、本公司已充分知悉“与其他采购参加人串通投标”的法定情形，相关情形包括但不限于：

（一）投标供应商之间相互约定给予未中标的供应商利益补偿。

（二）不同投标供应商的法定代表人、主要经营负责人、项目投标授权代表人、项目负责人、主要技术人员为同一人、属同一单位或者在同一单位缴纳社会保险。

（三）不同投标供应商的投标文件由同一单位或者同一人编制，或者由同一人分阶段参与编制的。

（四）不同投标供应商的投标文件或部分投标文件相互混装。

（五）不同投标供应商的投标文件内容存在非正常一致。

（六）由同一单位工作人员为两家以上（含两家）供应商进行同一项投标活动的。

（七）不同投标人的投标报价呈规律性差异。

（八）不同投标人的投标保证金从同一单位或者个人的账户转出。

（九）主管部门依照法律、法规认定的其他情形。

三、本公司已充分知悉下列情形所对应的法律风险，并在投标前已对相关风险事项进行排查。

（一）对于从其他主体获取的投标资料，供应商应审慎核查，确保投标资料的真实性。**如主管部门查实投标文件中存在虚假资料的，无论相关资料是否由第三方或本公司员工提供，均不影响主管部门对供应商存在“隐瞒真实情况，提供虚假资料”违法行为的认定。**

（二）对于涉及国家机关出具的公文、证件、证明材料等文件，一旦涉嫌虚假，经查实，主管部门将依法从严处理，并移送有关部门追究法律责任；涉嫌犯罪的，主管部门将一并移送司法机关追究法律责任。

（三）对于涉及安全生产、特种作业、抢险救灾、防疫等政府采购项目，供应商实施提供虚假资料、串通投标等违法行为的，主管部门将依法从严处理。

（四）供应商应严格规范项目授权代表、员工参与招标投标的行为，加强对投标文件的审核。项目授权代表、员工编制、上传投标文件等行为违反政府采购法律法规或招标文件要求的，投标供应商应当依法承担相应法律责任。

（五）供应商对投标电子密钥负有妥善保管、及时变更和续期等主体责任。供应商使用电子密钥在深圳政府采购网站进行的活动，均具有法律效力，须承担相应的法律后果。供应商擅自将投标密钥出借他人使用所造成的法律后果，由供应商自行承担。

（六）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。相关情形如查实，依法作投标无效处理；涉嫌串通投标等违法行为的，主管部门将依法调查处理。

四、本公司已充分知悉政府采购违法、违规行为的法律后果。经查实，若投标供应商存在政府采购违法、违规行为，主管部门将依据《深圳经济特区政府采购条例》第五十七条的规定，处以一至三年内禁止参与本市政府采购，并由主管部门记入供应商诚信档案，处采购金额千分之十以上千分之二十以下罚款；情节严重的，取消参与本市政府采购资格，处采购金额千分之二十以上千分之三十以下罚款，并由市场监管部门依法吊销营业执照。

以下文字请投标供应商抄写并确认：“本公司已仔细阅读《政府采购违法行为风险知悉确认书》，充分知悉违法行为的法律后果，并承诺将严谨、诚信、依法依规参与政府采购活动”。

_____

_____

_____

负责人/投标授权代表签名：

知悉人（公章）：

日期：

六、法定代表人（负责人）资格证明书

_____同志，现任我单位_____职务，为法定代表人**（负责人）**，特此证明。

说明：1、法定代表人为企业事业单位、国家机关、社会团体的主要负责人。

2、内容必须填写真实、清楚，涂改无效，不得转让、买卖。

附：要求必须提供法定代表人（负责人）身份证扫描件（正反两面）。

七、投标文件签署授权委托书

本授权委托书声明：我_____（姓名）系_____（投标供应商名称）的法定代表人**（负责人）**，现授权委托_____（姓名）为我公司签署本项目已递交的投标文件的法定代表人的授权委托代理人，代理人全权代表我所签署的本项目已递交的投标文件内容我均承认。

代理人无转委托权，特此委托。

代理人：_____

联系电话：_____ 手机：_____

身份证号码：_____职务：_____

授权委托日期：_____年_____月 _____日

附：要求必须提供代理人身份证扫描件（正反两面）。

八、实质性条款响应情况表

序号	采购人要求内容	投标人响应情况
1	交货时间：合同签订后 30 个日历日内	

注：1.“采购人要求内容”为**“第一册　专用条款/第二章　招标项目需求”**中的不可负偏离条款，即“实质性条款”。

2.“投标人响应情况”一栏应如实填写“响应”或“不响应”。

3.“实质性条款响应情况表”与投标文件其它内容冲突的，以“实质性条款响应情况表”为准。

4.“采购人要求内容”中涉及提供证明材料的，应附在本表后，未提供证明材料或证明材料与响应情况不相符的，按负偏离处理。

九、分项报价表

（一） 分项报价表

序号	货物名称	品牌	规格/型号	**原产地**	是否为进口产品	制造商名称	数量	单位	单价(元)	合价(元)	财政预算限额（元）

序号	货物名称	品牌	规格/型号	原产地	是否为进口产品	制造商名称	数量	单位	单价(元)	合价(元)	财政预算限额（元）
一、公安信息网安全加固建设											
1、安全区域边界											
1.1	网络安全网关						4	台			/
1.2、数据安全交换系统											
1.2.1	边界安全控制网关						1	台			/
1.2.2	下一代防火墙						1	台			/
1.2.3	入侵防御系统						1	台			/
1.2.4	万兆交换机						1	台			/
1.2.5	集中监控与审计系统探针子系统						1	台			/
1.2.6	视频安全接入系统						1	套			/
1.3	数据采集分流设备						2	台			/
1.4	专线						20	条			/
2、安全计算环境											
2.1	WEB 应用防火墙						2	台			/
2.2	数据库防护与审计系统						1	台			/
3、安全管理中心											
3.1	堡垒机						1	台			/
3.2	漏洞扫描系统						1	台			/
4、安全运营平台及工具											
4.1	移动工作站						3	台			/
4.2	服务器(配套设备)						3	台			/
小计：											4,233,000.00
二、视频专网安全加固建设											

序号	货物名称	品牌	规格/型号	**原产地**	是否为进口产品	制造商名称	数量	单位	单价(元)	合价(元)	财政预算限额（元）
1、安全区域边界											
1.1	网络安全网关						6	台			/
1.2、视频专网安全雷达系统											
1.2.1	采集模块						3	台			/
1.2.2	分析模块						1	台			/
1.3、视频专网精准防护系统											
1.3.1	管理中心						1	套			/
1.3.2	采集分析引擎						2	台			/
1.3.3	大数据中心						1	套			/
2、安全计算环境											
2.1	终端管理系统						400	点			/
2.2	WEB 应用防火墙						2	台			/
2.3	数据库防护与审计系统						1	台			/
2.4	服务器安全管理系统						100	点			/
3、安全管理中心											
3.1	堡垒机						2	台			/
3.2	漏洞扫描系统						1	台			/
4、安全运营平台及工具											
4.1	移动客户端						3	台			/
4.2	工作站						2	台			/
4.3、安全运营管理平台（二级平台）											
4.3.1	流量采集器						3	台			/
4.3.2	日志采集器						1	台			/
4.3.3	分析平台						1	台			/
小计：											7,585,000.00
三、互联网安全加固建设											
1、安全区域边界											

序号	货物名称	品牌	规格/型号	**原产地**	是否为进口产品	制造商名称	数量	单位	单价(元)	合价(元)	财政预算限额（元）
1.1	网络安全网关						4	台			/
2、安全计算环境											
2.1	WEB 应用防火墙						2	台			/
2.2	数据库防护与审计系统						1	台			/
3、安全管理中心											
3.1	堡垒机						1	台			/
3.2	日志审计系统						1	台			/
3.3	漏洞扫描系统						1	台			/
4、安全运营平台及工具											
4.1	流量采集器						1	台			/
小计：											1,690,000.00
四、内网安全检测系统建设											
1、安全运营管理平台（一级平台）											
1.1	流量采集器						1	台			/
1.2	日志采集器						1	台			/
1.3	分析平台						1	台			/
小计：											1,098,000.00
五、公安网违规行为和安全监测建设											
1、网络违规行为监测系统（平台和探针）											
1.1	采集模块						1	台			/
1.2	分析模块						1	台			/
小计：											759,000.00
六、公安网终端准入建设											
1、准入控制（公安网核心）											
1.1	终端准入 Licencce 授权						6000	点			/
1.2	终端准入控制设备						2	台			/
2	准入控						1	套			/

序号	货物名称	品牌	规格/型号	**原产地**	是否为进口产品	制造商名称	数量	单位	单价(元)	合价(元)	财政预算限额（元）
	制（业务接入网）										
小计：											1,004,000.00
七、信息安全服务体系建设											
1	威胁分析与处置服务（含人工）						1	项/1年			/
2	风险评估服务						1	项/1年			/
3	渗透测试服务						1	项/1年			/
4	应急演练服务						1	项/1年			/
5	应急响应服务						1	项/1年			/
小计：											480,000.00
合计（即：投标总价；币种：人民币；单位：元）：											

注：1. 请根据“第二章 招标项目需求” **“二、货物清单”中的“（二）货物清单明细”** 填写；本表格式不得修改。

2. 所有价格应按“招标文件”中规定的货币单位填写；投标总价应为以上各分项价格之和；投标总价和项目报价表中单个采购预算条目报价均不得超过对应的财政预算限额，否则将导致无效投标。

3. 单价、合价和投标总价为包干价，即三者均应包含设备的价款、包装、运输、装卸、安装、调试、技术指导、培训、咨询、服务、保险、税费、检测、验收合格交付使用之前以及技术和售后服务等其他各项有关费用。

4. 开标一览表的投标总价必须与项目报价表的投标总价一致。

5. “原产地”是指该产品的实际生产加工地，而非品牌总公司所在地。

6. 投标人必须对照进口产品的规定明确其投标产品是否为进口产品。进口产品是指通过海关验放进入中国境内且产自关境外的产品。即所谓进口产品是指制造过程均在国外，如果产品在国内组装，其中的零部件（包括核心部件）是进口产品，则应当视为非进口产品。采用“接受进口”的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，相关内容以财库〔2007〕119 号文和财办库〔2008〕248 号文的相

关规定为准。

7. 如所投产品属于定制类的非量产货物，投标供应商无需填写规格/型号等信息，但必须注明“定制”，否则该产品技术参数按负偏离处理。

8. 根据《中华人民共和国财政部令第 87 号-政府采购货物和服务招标投标管理办法》第六十条规定：评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

（二）可选配件报价清单（不包括在总报价内）

注：格式参照《（一）分项报价表》表格，但须提供相应的品牌、规格型号、原产地、单价等详细信息

（三）供应商认为需要涉及的其他内容报价清单

十、技术规格偏离表

序号	货物名称	招标技术要求	投标技术响应	偏离情况	说明
					如需附证明文件，应在“说明”栏填写证明文件对应名称和页码。

备注：

1、“招标技术要求”一栏应根据**招标文件第二章“四、具体技术要求”**的内容填写。

2、“投标技术响应”一栏详细填写投标产品的具体参数，并应对照招标技术要求一一对应响应。

3、“偏离情况”一栏应如实填写“正偏离”、“负偏离”或“无偏离”。

4. 对于实质性条款，投标文件响应为“负偏离”的，投标文件将按无效投标处理。

4、**投标产品的技术参数应按招标文件第二章“四、具体技术要求”中的要求提供相应的证明资料，以证明投标人响应的真实性。**证明资料包括制造商公布的产品说明书、产品彩页和我国政府机构出具的产品检验和核准证件等。投标人应在“说明”一栏中列出技术参数的证

明资料名称，并指明该证明资料在投标文件中的具体位置，未按要求提供证明材料或未注明证明材料的具体位置或提供的证明资料显示不符合招标文件要求、模糊不清无法判断或未显示是否满足招标文件要求的，均视为负偏离。未要求提供相应证明材料的，投标人可以不提供。

5、证明资料（均为扫描件）的提供要求：

（1）产品说明书或彩页应为制造商公布或出具的中文产品说明书或彩页；提供外文说明书或彩页的，需同时提供加盖制造商公章的对应中文翻译说明，评标依据以中文翻译内容为准，外文说明书或彩页仅供参考；产品说明书或彩页的尺寸和清晰度应该能够在电脑上被阅读、识别和判断；

（2）我国政府机构出具的产品检验和核准证件应为证件正面、背面和附件标注的全部具体内容；产品检验和核准证件的尺寸和清晰度应该能够在电脑上被阅读、识别和判断。

十一、商务条款偏离表

序号	招标商务条款	投标商务响应	偏离情况	说明
				如需附证明文件，应在“说明”栏填写证明文件对应名称和页码。

备注：

1. “招标商务条款”一栏逐项填写**招标文件第二章“五、商务要求”的内容**。
2. “投标商务响应”一栏详细填写投标商务响应的内容。
3. “偏离情况”栏中应如实填写“正偏离”、“负偏离”或“无偏离”。
4. 对于实质性条款，投标文件响应为“负偏离”的，投标文件将按无效投标处理。
5. 投标人应在“说明”一栏中列出商务条款的证明资料名称，并注明该证明资料在投标文件中的具体位置，未按要求提供证明材料或未注明证明材料的具体位置或提供的证明资料显示不符合招标文件要求、模糊不清无法判断或未显示是否满足招标文件要求的，均视为负偏离。未要求提供相应证明材料的，投标人可以不提供。

十二、产品演示（格式自定）

十三、技术保障措施（格式自定）

十四、项目经理（仅限一人）情况（格式自定）

十五、项目团队（项目经理除外）情况（格式自定）

十六、同类项目业绩情况（格式自定）

十七、企业认证情况（格式自定）

十八、企业获奖情况（格式自定）

十九、企业资质情况（格式自定）

二十、计算机软件著作权登记证书（格式自定）

二十一、招标文件要求的其它内容或投标人认为需要补充的资料（格式自定）

特别提醒：

《深圳经济特区政府采购条例实施细则》第七十九条规定：供应商有下列情形的，属于采购条例所称的串通投标行为。

（一）投标供应商之间相互约定给予未中标的供应商利益补偿；

（二）不同投标供应商的法定代表人、主要经营负责人、项目投标授权代表人、项目负责人、主要技术人员为同一人、属同一单位或者在同一单位缴纳社会保险；

（三）不同投标供应商的投标文件由同一单位或者同一人编制，或者由同一人分阶段参与编制的；

（四）不同投标供应商的投标文件或部分投标文件相互混装；

（五）不同投标供应商的投标文件内容存在非正常一致；

（六）由同一单位工作人员为两家以上（含两家）供应商进行同一项投标活动的；

（七）主管部门依照法律、法规认定的其他情形。

投标人提供以下资料（格式自拟）：

1、投标单位法定代表人、主要经营负责人、项目投标授权代表人、项目负责人及主要技术人员近一年社保缴纳查询记录（包含在投标单位及其他缴纳社保单位的记录）；社保缴纳不满一年的按实际缴纳情况提供（因社保部门原因暂时无法提供社保证明的，需提供加盖公章的情况说明或者证明材料。）

2、其他招标文件要求提供的资料或投标人认为需要补充的资料。

第四章　合同及履约情况反馈格式

一、合同条款及格式（仅供参考）

（拟签订的合同文本）

重要说明:采购人在签订合同前有权依据招标文件要求和项目实际情况对以下合同内容进行删改或补充。

甲方（采购人）：

乙方（中标人）：

根据_____招标项目（项目编号_____）的中标结果，由_____单位为中标人。根据《中华人民共和国政府采购法》、《深圳经济特区政府采购条例》、《中华人民共和国民法典》之规定，经_____（以下简称采购人）和_____（以下简称中标人）协商，就_____项目，达成以下合同条款：

第一条　合同标的

货物名称、规格型号、制造商、产地、单位、数量、单价、合同价，详见_____。

第二条　合同价款

本合同项下总价款为_____（大写）人民币，分项价款详见_____。本合同总价款已包括乙方为履行本合同义务所发生的一切费用，系固定不变价格，且不随通货膨胀的影响而波动。

第三条　交货时间、地点和交货状态

3.1 交货时间：

3.2 交货地点：

3.3 交货状态：

第四条　质量标准和要求

4.1 乙方所提供的货物质量标准按照国家标准或者行业标准或者企业标准明确。没有国家标准、行业标准或企业标准的，按照通常标准或者符合合同目的的特定标准确定。

4.2 乙方应保证货物是全新、未使用过的原装合格正品（包括零部件），并完全符合甲方要求的质量、规格和性能的要求。如货物安装或配置了软件的，乙方保证相关软件均为正

版软件。

4.3 乙方保证交货时一并提供货物的质量合格凭证或文件。

4.4 乙方所提供的全部货物均应按照标准保护措施进行包装，包装应适用于远距离运输、防潮、防震、防锈、防野蛮装卸等要求，以确保货物安全无损抵运指定交货地点。

第五条　权利保证

5.1 乙方保证甲方在使用本合同项下货物或货物的任何一部分时，不会产生因第三方提出的包括但不限于侵犯其专利权、商标权、工业设计权等知识产权和侵犯其所有权、抵押权等物权及其他权利而引发的纠纷。如有纠纷，乙方应承担全部责任。

5.2 乙方应保证其提供的货物不存在任何未曾向甲方透漏的担保物权，如抵押权、质押权、留置权等。

第六条　质量保障

6.1 乙方应保证其提供的货物是全新的，未使用过的，并且完全符合合同规定的质量、规格和性能要求。乙方应保证其提供的货物在正确安装、正常使用和保养条件下，在其使用寿命期限内应具有很满意的性能。在货物最终交付验收后的质量保证期限内，乙方应对由于设计、工艺或材料的缺陷而产生的故障承担责任。

6.2 在质量保证期限内，如果货物的质量或规格与合同不符，或者证实货物存在缺陷的，包括潜在的缺陷或者使用不符合要求的材料等，甲方可根据本合同追究乙方相应违约责任。

第七条　交货和验收

7.1 乙方应按照本合同或招投标文件规定的时间和方式向甲方交付货物，交货地点由甲方指定。因交货产生的费用由乙方自行承担。

7.2 乙方交付的货物应当完全符合招投标文件所规定的货物、数量、质量和规格要求。乙方提供的货物不符合招投标文件和合同规定的，甲方有权拒收货物，由此引起的风险，由乙方承担。

7.3 乙方应将所提供货物的使用说明书、原厂保修卡等附随资料和附随配件、工具等交付给甲方；乙方不能完整交付货物及本款规定的单证和工具的，视为未按合同约定交货，乙方负责补齐，因此导致逾期交付的，由乙方承担相关的违约责任。

7.4 甲方应当在到货后的_____个工作日内对货物进行验收；需要乙方对货物或系统进行安装调试的，甲方应在货物安装调试完毕后的_____个工作日内进行质量验收。

第八条　保修及其他服务

8.1 乙方应按照国家有关法律法规规章和“三包”规定和招标文件的要求及乙方在投标文件的相关承诺提供保修及其他服务。

8.2 保修期内，乙方负责对其提供的货物进行维修和系统维护，不再收取任何费用。所

有货物保修服务方式均为乙方上门保修，即由乙方派员到货物使用现场维修，由此产生的一切费用均由乙方承担。保修期后的货物维护另行协商。

第九条　履约保证金

9.1 乙方应在签订本合同之日，向甲方或甲方指定的机构提交履约保证金_____元。

9.2 如乙方未能履行合同规定的义务，甲方有权从履约保证金中取得补偿。

9.3 甲方在乙方履行完毕本合同项下全部义务后_____天内无息退还乙方。

第十条　货款支付

10.1 本合同以人民币付款。

10.2 付款条件：

10.3 付款方式和时间：

第十一条　违约责任

11.1 甲方无正当理由拒收货物、拒付货物款的，由甲方向乙方偿付合同总价的【】%违约金。

11.2 甲方未按合同规定的期限向乙方支付货款的，每逾期 1 天甲方向乙方偿付欠款总额的【】‰滞纳金，但累计滞纳金总额不超过欠款总额的【】%。

11.3 乙方逾期交付货物的，每逾期 1 天，乙方向甲方偿付逾期交货部分货款总额的【】‰的滞纳金。如乙方逾期交货达____天，甲方有权解除合同，履约保证金不予退回，同时乙方应向甲方支付合同总价【】%的违约金。

11.4 乙方所交付的货物品种、型号、规格不符合合同规定的，甲方有权拒收。甲方拒收的，乙方应向甲方支付货款总额【】%的违约金。

11.5 在乙方承诺的或国家规定的质量保证期内（取两者中最长的期限），如经乙方两次维修或更换，货物仍不能达到合同约定的质量标准，甲方有权退货，乙方应退回全部货款并赔偿甲方因此遭受的损失。

11.6 乙方未履行本合同项下的其他义务或违反其在投标文件中的相关承诺的，应按合同总价款的【】%向甲方承担违约责任。

11.7 乙方在承担上述一项或多项违约责任后，仍应继续履行合同规定的义务（甲方解除合同的除外）。甲方未能及时追究乙方的任何一项违约责任并不表明甲方放弃追究乙方该项或其他违约责任。

第十二条　合同的变更、解除或终止

12.1 在合同履行中，甲方需追加与合同标的项目的货物、工程或者服务的，应按照《深圳经济特区政府采购条例》第四十条、第四十八条规定办理相关手续。

12.2 除《中华人民共和国政府采购法》第 49 条、第 50 条第二款规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止合同。

第十三条　争议的解决

13.1 因货物的质量问题发生争议的，应当邀请国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合质量标准的，鉴定费由乙方承担。

13.2 因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决，如果协商不能解决争议，则向甲方所在地有管辖权的人民法院提起诉讼。

第十四条　合同生效及其他

14.1 下列文件均为本合同的组成部分：

（1）招标文件、答疑及补充通知；

（2）乙方的投标文件；

（3）本合同执行中甲乙双方共同签署的补充与修正文件。

14.2 本合同一式_____份，甲、乙方双方各执_____份，具有同等法律效力。本合同自双方签字并盖章之日起生效。

14.3 本合同未尽事宜，双方友好协商，达成解决方案，经双方签字后，可作为本合同的有效附件。

附件：

1、《中标/成交通知书》

2、《投标文件》

3、《招标文件》

4、《分包意向协议书/联合体投标协议》

甲方（采购人）：（盖公章）	乙方（中标人）：（盖公章）
法定代表人（签字或盖私章）：	法定代表人（签字或盖私章）：
委托代理人：	委托代理人：
日期：　　年　　月　　日	日期：　　年　　月　　日

二、政府采购履约情况反馈表

采购人名称： **联系人及电话：**

<table>
<tr><td colspan="3">采购项目名称</td><td></td><td>项目编号</td><td></td></tr>
<tr><td colspan="3">中标供应商名称</td><td></td><td>供应商
联系人及电话</td><td></td></tr>
<tr><td colspan="3">中标金额</td><td></td><td>合同履约时间</td><td>自　　至</td></tr>
<tr><td rowspan="7">履约情况评价</td><td colspan="2">总体评价</td><td colspan="4">☐ 优　☐ 良　☐ 中　☐ 差</td></tr>
<tr><td rowspan="6">分项评价</td><td>质量方面</td><td colspan="4">☐ 优　☐ 良　☐ 中　☐ 差</td></tr>
<tr><td>价格方面</td><td colspan="4">☐ 优　☐ 良　☐ 中　☐ 差</td></tr>
<tr><td>服务方面</td><td colspan="4">☐ 优　☐ 良　☐ 中　☐ 差</td></tr>
<tr><td>时间方面</td><td colspan="4">☐ 优　☐ 良　☐ 中　☐ 差</td></tr>
<tr><td>环境保护</td><td colspan="4">☐ 优　☐ 良　☐ 中　☐ 差</td></tr>
<tr><td>其他</td><td colspan="4">评价内容为：_____
评价等级为：☐ 优　☐ 良　☐ 中　☐ 差</td></tr>
<tr><td colspan="3">具体情况说明</td><td colspan="4"></td></tr>
<tr><td colspan="3">采购人意见
（公章）</td><td colspan="4">日期：　年　月　日</td></tr>
</table>

说明：

履约情况评价分为优、良、中、差四个等级，请在对应的框前打“√”，然后在“具体情况说明”一栏详细说明有关情况。

第五章　附件

一、财政部 工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知

财库〔2020〕46号

各中央预算单位办公厅（室），各省、自治区、直辖市、计划单列市财政厅（局）、工业和信息化主管部门，新疆生产建设兵团财政局、工业和信息化主管部门：

为贯彻落实《关于促进中小企业健康发展的指导意见》，发挥政府采购政策功能，促进中小企业发展，根据《中华人民共和国政府采购法》、《中华人民共和国中小企业促进法》等法律法规，财政部、工业和信息化部制定了《政府采购促进中小企业发展管理办法》。现印发给你们，请遵照执行。

附件：政府采购促进中小企业发展管理办法

财　　政　　部

工业和信息化部

2020年12月18日

附件

政府采购促进中小企业发展管理办法

第一条　为了发挥政府采购的政策功能，促进中小企业健康发展，根据《中华人民共和国政府采购法》、《中华人民共和国中小企业促进法》等有关法律法规，制定本办法。

第二条　本办法所称中小企业，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。

第三条　采购人在政府采购活动中应当通过加强采购需求管理，落实预留采购份额、价格评审优惠、优先采购等措施，提高中小企业在政府采购中的份额，支持中小企业发展。

第四条　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：

（一）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；

（二）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；

（三）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。

第五条 采购人在政府采购活动中应当合理确定采购项目的采购需求，不得以企业注册资本、资产总额、营业收入、从业人员、利润、纳税额等规模条件和财务指标作为供应商的资格要求或者评审因素，不得在企业股权结构、经营年限等方面对中小企业实行差别待遇或者歧视待遇。

第六条 主管预算单位应当组织评估本部门及所属单位政府采购项目，统筹制定面向中小企业预留采购份额的具体方案，对适宜由中小企业提供的采购项目和采购包，预留采购份额专门面向中小企业采购，并在政府采购预算中单独列示。

符合下列情形之一的，可不专门面向中小企业预留采购份额：

（一）法律法规和国家有关政策明确规定优先或者应当面向事业单位、社会组织等非企业主体采购的；

（二）因确需使用不可替代的专利、专有技术，基础设施限制，或者提供特定公共服务等原因，只能从中小企业之外的供应商处采购的；

（三）按照本办法规定预留采购份额无法确保充分供应、充分竞争，或者存在可能影响政府采购目标实现的情形；

（四）框架协议采购项目；

（五）省级以上人民政府财政部门规定的其他情形。

除上述情形外，其他均为适宜由中小企业提供的情形。

第七条 采购限额标准以上，200 万元以下的货物和服务采购项目、400 万元以下的工程采购项目，适宜由中小企业提供的，采购人应当专门面向中小企业采购。

第八条 超过 200 万元的货物和服务采购项目、超过 400 万元的工程采购项目中适宜由中小企业提供的，预留该部分采购项目预算总额的 30%以上专门面向中小企业采购，其中预留给小微企业的比例不低于 60%。预留份额通过下列措施进行：

（一）将采购项目整体或者设置采购包专门面向中小企业采购；

（二）要求供应商以联合体形式参加采购活动，且联合体中中小企业承担的部分达到一定比例；

（三）要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业。

组成联合体或者接受分包合同的中小企业与联合体内其他企业、分包企业之间不得存在直接控股、管理关系。

第九条 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6%—10%（工程项目为3%—5%）的扣除，用扣除后的价格参加评审。适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，评标时应当在采用原报价进行评分的基础上增加其价格得分的3%—5%作为其价格分。

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，采购人、采购代理机构应当对联合体或者大中型企业的报价给予2%-3%（工程项目为1%—2%）的扣除，用扣除后的价格参加评审。适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，评标时应当在采用原报价进行评分的基础上增加其价格得分的1%—2%作为其价格分。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。

价格扣除比例或者价格分加分比例对小型企业和微型企业同等对待，不作区分。具体采购项目的价格扣除比例或者价格分加分比例，由采购人根据采购标的相关行业平均利润率、市场竞争状况等，在本办法规定的幅度内确定。

第十条 采购人应当严格按照本办法规定和主管预算单位制定的预留采购份额具体方案开展采购活动。预留份额的采购项目或者采购包，通过发布公告方式邀请供应商后，符合资格条件的中小企业数量不足3家的，应当中止采购活动，视同未预留份额的采购项目或者采购包，按照本办法第九条有关规定重新组织采购活动。

第十一条 中小企业参加政府采购活动，应当出具本办法规定的《中小企业声明函》（附1），否则不得享受相关中小企业扶持政策。任何单位和个人不得要求供应商提供《中小企业声明函》之外的中小企业身份证明文件。

第十二条 采购项目涉及中小企业采购的，采购文件应当明确以下内容：

（一）预留份额的采购项目或者采购包，明确该项目或相关采购包专门面向中小企业采购，以及相关标的及预算金额；

（二）要求以联合体形式参加或者合同分包的，明确联合协议或者分包意向协议中中小企业合同金额应当达到的比例，并作为供应商资格条件；

（三）非预留份额的采购项目或者采购包，明确有关价格扣除比例或者价格分加分比例；

（四）规定依据本办法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；

（五）采购人认为具备相关条件的，明确对中小企业在资金支付期限、预付款比例等方面的优惠措施；

（六）明确采购标的对应的中小企业划分标准所属行业；

（七）法律法规和省级以上人民政府财政部门规定的其他事项。

第十三条 中标、成交供应商享受本办法规定的中小企业扶持政策的，采购人、采购代理机构应当随中标、成交结果公开中标、成交供应商的《中小企业声明函》。

适用招标投标法的政府采购工程建设项目，应当在公示中标候选人时公开中标候选人的《中小企业声明函》。

第十四条 对于通过预留采购项目、预留专门采购包、要求以联合体形式参加或者合同分包等措施签订的采购合同，应当明确标注本合同为中小企业预留合同。其中，要求以联合体形式参加采购活动或者合同分包的，应当将联合协议或者分包意向协议作为采购合同的组成部分。

第十五条 鼓励各地区、各部门在采购活动中允许中小企业引入信用担保手段，为中小企业在投标（响应）保证、履约保证等方面提供专业化服务。鼓励中小企业依法合规通过政府采购合同融资。

第十六条 政府采购监督检查、投诉处理及政府采购行政处罚中对中小企业的认定，由货物制造商或者工程、服务供应商注册登记所在地的县级以上人民政府中小企业主管部门负责。

中小企业主管部门应当在收到财政部门或者有关招标投标行政监督部门关于协助开展中小企业认定函后 10 个工作日内做出书面答复。

第十七条 各地区、各部门应当对涉及中小企业采购的预算项目实施全过程绩效管理，合理设置绩效目标和指标，落实扶持中小企业有关政策要求，定期开展绩效监控和评价，强化绩效评价结果应用。

第十八条 主管预算单位应当自2022年起向同级财政部门报告本部门上一年度面向中小企业预留份额和采购的具体情况，并在中国政府采购网公开预留项目执行情况（附 2）。未达到本办法规定的预留份额比例的，应当作出说明。

第十九条 采购人未按本办法规定为中小企业预留采购份额，采购人、采购代理机构未按照本办法规定要求实施价格扣除或者价格分加分的，属于未按照规定执行政府采购政策，依照《中华人民共和国政府采购法》等国家有关规定追究法律责任。

第二十条 供应商按照本办法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。

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

第二十一条 财政部门、中小企业主管部门及其工作人员在履行职责中违反本办法规定及存在其他滥用职权、玩忽职守、徇私舞弊等违法违纪行为的，依照《中华人民共和国政府采购法》、《中华人民共和国公务员法》、《中华人民共和国监察法》、《中华人民共和国政府采购法实施条例》等国家有关规定追究相应责任；涉嫌犯罪的，依法移送有关国家机关处理。

第二十二条 对外援助项目、国家相关资格或者资质管理制度另有规定的项目，不适用本办法。

第二十三条 关于视同中小企业的其他主体的政府采购扶持政策，由财政部会同有关部门另行规定。

第二十四条 省级财政部门可以会同中小企业主管部门根据本办法的规定制定具体实施办法。

第二十五条 本办法自 2021 年 1 月 1 日起施行。《财政部 工业和信息化部关于印发〈政府采购促进中小企业发展暂行办法〉的通知》（财库〔2011〕181 号）同时废止。

二、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

各省、自治区、直辖市人民政府，国务院各部委、各直属机构及有关单位：

为贯彻落实《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号），工业和信息化部、国家统计局、发展改革委、财政部研究制定了《中小企业划型标准规定》。经国务院同意，现印发给你们，请遵照执行。

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

二〇一一年六月十八日

中小企业划型标准规定

一、根据《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》(国发〔2009〕36 号)，制定本规定。

二、中小企业划分为中型、小型、微型三种类型，具体标准根据企业从业人员、营业收入、资产总额等指标，结合行业特点制定。

三、本规定适用的行业包括：农、林、牧、渔业，工业（包括采矿业，制造业，电力、

热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。

四、各行业划型标准为：

（一）农、林、牧、渔业。营业收入20000万元以下的为中小微型企业。其中，营业收入500万元及以上的为中型企业，营业收入50万元及以上的为小型企业，营业收入50万元以下的为微型企业。

（二）工业。从业人员1000人以下或营业收入40000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入300万元及以上的为小型企业；从业人员20人以下或营业收入300万元以下的为微型企业。

（三）建筑业。营业收入80000万元以下或资产总额80000万元以下的为中小微型企业。其中，营业收入6000万元及以上，且资产总额5000万元及以上的为中型企业；营业收入300万元及以上，且资产总额300万元及以上的为小型企业；营业收入300万元以下或资产总额300万元以下的为微型企业。

（四）批发业。从业人员200人以下或营业收入40000万元以下的为中小微型企业。其中，从业人员20人及以上，且营业收入5000万元及以上的为中型企业；从业人员5人及以上，且营业收入1000万元及以上的为小型企业；从业人员5人以下或营业收入1000万元以下的为微型企业。

（五）零售业。从业人员300人以下或营业收入20000万元以下的为中小微型企业。其中，从业人员50人及以上，且营业收入500万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（六）交通运输业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入3000万元及以上的为中型企业；从业人员20人及以上，且营业收入200万元及以上的为小型企业；从业人员20人以下或营业收入200万元以下的为微型企业。

（七）仓储业。从业人员200人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（八）邮政业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。

其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（九）住宿业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十）餐饮业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十一）信息传输业。从业人员2000人以下或营业收入100000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业人员10人以下或营业收入50万元以下的为微型企业。

（十三）房地产开发经营。营业收入200000万元以下或资产总额10000万元以下的为中小微型企业。其中，营业收入1000万元及以上，且资产总额5000万元及以上的为中型企业；营业收入100万元及以上，且资产总额2000万元及以上的为小型企业；营业收入100万元以下或资产总额2000万元以下的为微型企业。

（十四）物业管理。从业人员1000人以下或营业收入5000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入1000万元及以上的为中型企业；从业人员100人及以上，且营业收入500万元及以上的为小型企业；从业人员100人以下或营业收入500万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员300人以下或资产总额120000万元以下的为中小微型企业。其中，从业人员100人及以上，且资产总额8000万元及以上的为中型企业；从业人员10人及以上，且资产总额100万元及以上的为小型企业；从业人员10人以下或资产总额100万元以下的为微型企业。

（十六）其他未列明行业。从业人员300人以下的为中小微型企业。其中，从业人员100人及以上的为中型企业；从业人员10人及以上的为小型企业；从业人员10人以下的为微型企业。

五、企业类型的划分以统计部门的统计数据为依据。

六、本规定适用于在中华人民共和国境内依法设立的各类所有制和各种组织形式的企业。个体工商户和本规定以外的行业，参照本规定进行划型。

七、本规定的中型企业标准上限即为大型企业标准的下限，国家统计部门据此制定大中小微型企业的统计分类。国务院有关部门据此进行相关数据分析，不得制定与本规定不一致的企业划型标准。

八、本规定由工业和信息化部、国家统计局会同有关部门根据《国民经济行业分类》修订情况和企业发展变化情况适时修订。

九、本规定由工业和信息化部、国家统计局会同有关部门负责解释。

十、本规定自发布之日起执行，原国家经贸委、原国家计委、财政部和国家统计局2003年颁布的《中小企业标准暂行规定》同时废止。

三、国家统计局关于印发《统计上大中小微型企业划分办法（2017）》的通知

国统字〔2017〕213号

各省、自治区、直辖市统计局，新疆生产建设兵团统计局，国务院各有关部门，国家统计局各调查总队：

《国民经济行业分类》（GB/T 4754—2017）已正式实施，现对2011年制定的《统计上大中小微型企业划分办法》进行修订。本次修订保持原有的分类原则、方法、结构框架和适用范围，仅将所涉及的行业按照《国民经济行业分类》（GB/T 4754—2011）和《国民经济行业分类》（GB/T 4754—2017）的对应关系，进行相应调整，形成《统计上大中小微型企业划分办法（2017）》。现将《统计上大中小微型企业划分办法（2017）》印发给你们，请在统计工作中认真贯彻执行。

附件：《统计上大中小微型企业划分办法（2017）》修订说明

国家统计局

2017年12月28日

统计上大中小微型企业划分办法（2017）

一、根据工业和信息化部、国家统计局、国家发展改革委、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），以《国民经济行业分类》（GB/T4754-2017）为基础，结合统计工作的实际情况，制定本办法。

二、本办法适用对象为在中华人民共和国境内依法设立的各种组织形式的法人企业或单位。个体工商户参照本办法进行划分。

三、本办法适用范围包括：农、林、牧、渔业，采矿业，制造业，电力、热力、燃气及水生产和供应业，建筑业，批发和零售业，交通运输、仓储和邮政业，住宿和餐饮业，信息传输、软件和信息技术服务业，房地产业，租赁和商务服务业，科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，文化、体育和娱乐业等15个行业门类以及社会工作行业大类。

四、本办法按照行业门类、大类、中类和组合类别，依据从业人员、营业收入、资产总额等指标或替代指标，将我国的企业划分为大型、中型、小型、微型等四种类型。具体划分标准见附表。

五、企业划分由政府综合统计部门根据统计年报每年确定一次，定报统计原则上不进行调整。

六、本办法自印发之日起执行，国家统计局2011年印发的《统计上大中小微型企业划分办法》（国统字〔2011〕75号）同时废止。

附件

《统计上大中小微型企业划分办法（2017）》修订说明

一、修订背景

目前执行的《统计上大中小微型企业划分办法》是2011年国家统计局根据工业和信息化部、国家统计局、国家发展改革委、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），同时依据《国民经济行业分类》（GB/T 4754—2011），制定并颁布的。

2017年6月30日，《国民经济行业分类》（GB/T 4754—2017）正式颁布。8月29日，国家统计局印发《关于执行新国民经济行业分类国家标准的通知》（国统字〔2017〕142号），规定从2017年统计年报和2018年定期统计报表起统一使用新分类标准。为此，我们对2011年印发的《统计上大中小微型企业划分办法》进行修订。

二、修订主要内容

本次修订是在2011年《统计上大中小微型企业划分办法》基础上进行的，修订延续原有的分类原则、方法和结构框架，在保持适用范围不变的情况下,依据标准由《国民经济行业分类》（GB/T 4754—2011）修改为《国民经济行业分类》（GB/T 4754—2017），并根据新旧国民经济行业的对应关系，进行了行业所包含类别的对应调整。

将交通运输业中包括的“装卸搬运和运输代理业”修改为“多式联运和运输代理业、装卸搬运”。

仓储业所包括的行业中类，根据《国民经济行业分类》（GB/T 4754—2017）调整为“通用仓储，低温仓储，危险品仓储，谷物、棉花等农产品仓储，中药材仓储和其他仓储业”。

附表

统计上大中小微型企业划分标准

行业名称	指标名称	计量单位	大型	中型	小型	微型
农、林、牧、渔业	营业收入(Y)	万元	Y≥20000	500≤Y＜20000	50≤Y＜500	Y＜50
工业 *	从业人员(X)	人	X≥1000	300≤X＜1000	20≤X＜300	X＜20
	营业收入(Y)	万元	Y≥40000	2000≤Y＜40000	300≤Y＜2000	Y＜300
建筑业	营业收入(Y)	万元	Y≥80000	6000≤Y＜80000	300≤Y＜6000	Y＜300
	资产总额(Z)	万元	Z≥80000	5000≤Z＜80000	300≤Z＜5000	Z＜300
批发业	从业人员(X)	人	X≥200	20≤X＜200	5≤X＜20	X＜5
	营业收入(Y)	万元	Y≥40000	5000≤Y＜40000	1000≤Y＜5000	Y＜1000
零售业	从业人员(X)	人	X≥300	50≤X＜300	10≤X＜50	X＜10
	营业收入(Y)	万元	Y≥20000	500≤Y＜20000	100≤Y＜500	Y＜100
交通运输业 *	从业人员(X)	人	X≥1000	300≤X＜1000	20≤X＜300	X＜20
	营业收入(Y)	万元	Y≥30000	3000≤Y＜30000	200≤Y＜3000	Y＜200
仓储业*	从业人员(X)	人	X≥200	100≤X＜200	20≤X＜100	X＜20
	营业收入(Y)	万元	Y≥30000	1000≤Y＜30000	100≤Y＜1000	Y＜100
邮政业	从业人员(X)	人	X≥1000	300≤X＜1000	20≤X＜300	X＜20
	营业收入(Y)	万元	Y≥30000	2000≤Y＜30000	100≤Y＜2000	Y＜100
住宿业	从业人员(X)	人	X≥300	100≤X＜300	10≤X＜100	X＜10
	营业收入(Y)	万元	Y≥10000	2000≤Y＜10000	100≤Y＜2000	Y＜100
餐饮业	从业人员(X)	人	X≥300	100≤X＜300	10≤X＜100	X＜10
	营业收入(Y)	万元	Y≥10000	2000≤Y＜10000	100≤Y＜2000	Y＜100
信息传输业 *	从业人员(X)	人	X≥2000	100≤X＜2000	10≤X＜100	X＜10
	营业收入(Y)	万元	Y≥100000	1000≤Y＜100000	100≤Y＜1000	Y＜100
软件和信息技术服务业	从业人员(X)	人	X≥300	100≤X＜300	10≤X＜100	X＜10
	营业收入(Y)	万元	Y≥10000	1000≤Y＜10000	50≤Y＜1000	Y＜50
房地产开发经营	营业收入(Y)	万元	Y≥200000	1000≤Y＜200000	100≤Y＜1000	Y＜100
	资产总额(Z)	万元	Z≥10000	5000≤Z＜10000	2000≤Z＜5000	Z＜2000
物业管理	从业人员(X)	人	X≥1000	300≤X＜1000	100≤X＜300	X＜100
	营业收入(Y)	万元	Y≥5000	1000≤Y＜5000	500≤Y＜1000	Y＜500
租赁和商务服务业	从业人员(X)	人	X≥300	100≤X＜300	10≤X＜100	X＜10
	资产总额(Z)	万元	Z≥120000	8000≤Z＜120000	100≤Z＜8000	Z＜100

其他未列明行业 *	从业人员(X)	人	X≥300	100≤X＜300	10≤X＜100	X＜10

说明：

1.大型、中型和小型企业须同时满足所列指标的下限，否则下划一档；微型企业只须满足所列指标中的一项即可。

2.附表中各行业的范围以《国民经济行业分类》（GB/T4754-2017）为准。带*的项为行业组合类别，其中，工业包括采矿业，制造业，电力、热力、燃气及水生产和供应业；交通运输业包括道路运输业，水上运输业，航空运输业，管道运输业，多式联运和运输代理业、装卸搬运，不包括铁路运输业；仓储业包括通用仓储，低温仓储，危险品仓储，谷物、棉花等农产品仓储，中药材仓储和其他仓储业;信息传输业包括电信、广播电视和卫星传输服务，互联网和相关服务；其他未列明行业包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业，以及房地产中介服务，其他房地产业等，不包括自有房地产经营活动。

3.企业划分指标以现行统计制度为准。（1）从业人员，是指期末从业人员数，没有期末从业人员数的，采用全年平均人员数代替。（2）营业收入，工业、建筑业、限额以上批发和零售业、限额以上住宿和餐饮业以及其他设置主营业务收入指标的行业，采用主营业务收入；限额以下批发与零售业企业采用商品销售额代替；限额以下住宿与餐饮业企业采用营业额代替；农、林、牧、渔业企业采用营业总收入代替；其他未设置主营业务收入的行业，采用营业收入指标。（3）资产总额，采用资产总计代替。

四、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

党中央有关部门，国务院各部委、各直属机构，全国人大常委会办公厅，全国政协办公厅，高法院，高检院，各民主党派中央，有关人民团体，各省、自治区、直辖市、计划单列市财政厅（局）、民政厅（局）、残疾人联合会，新疆生产建设兵团财务局、民政局、残疾人联合会：

为了发挥政府采购促进残疾人就业的作用，进一步保障残疾人权益，依照《政府采购法》、《残疾人保障法》等法律法规及相关规定，现就促进残疾人就业政府采购政策通知如下：

一、享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

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

（二）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

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

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

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

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

二、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。任何单位或者个人在政府采购活动中均不得要求残疾人福利性单位提供其他证明声明函内容的材料。

中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。

供应商提供的《残疾人福利性单位声明函》与事实不符的，依照《政府采购法》第七十七条第一款的规定追究法律责任。

三、在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。向残疾人福利性单位采购的金额，计入面向中小企业采购的统计数据。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

四、采购人采购公开招标数额标准以上的货物或者服务，因落实促进残疾人就业政策的需要，依法履行有关报批程序后，可采用公开招标以外的采购方式。

五、对于满足要求的残疾人福利性单位产品，集中采购机构可直接纳入协议供货或者定点采购范围。各地区建设的政府采购电子卖场、电子商城、网上超市等应当设立残疾人福利性单位产品专栏。鼓励采购人优先选择残疾人福利性单位的产品。

六、省级财政部门可以结合本地区残疾人生产、经营的实际情况，细化政府采购支持措施。对符合国家有关部门规定条件的残疾人辅助性就业机构，可通过上述措施予以支持。各地制定的有关文件应当报财政部备案。

七、本通知自2017年10月1日起执行。

财政部　民政部　中国残疾人联合会

2017年8月22日

五、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

党中央有关部门，国务院各部委、各直属机构，全国人大常委会办公厅，全国政协办公厅，高法院，高检院，有关人民团体，中央国家机关政府采购中心，中共中央直属机关采购中心，全国人大机关采购中心，各省、自治区、直辖市、计划单列市财政厅（局）、司法厅（局），新疆生产建设兵团财务局、司法局、监狱管理局：

政府采购支持监狱和戒毒企业（以下简称监狱企业）发展对稳定监狱企业生产，提高财政资金使用效益，为罪犯和戒毒人员提供长期可靠的劳动岗位，提高罪犯和戒毒人员的教育改造质量，减少重新违法犯罪，确保监狱、戒毒场所安全稳定，促进社会和谐稳定具有十分重要的意义。为进一步贯彻落实国务院《关于解决监狱企业困难的实施方案的通知》（国发[2003]7号）文件精神，发挥政府采购支持监狱企业发展的作用，现就有关事项通知如下：

一、监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。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。

二、在政府采购活动中，监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。向监狱企业采购的金额，计入面向中小企业采购的统计数据。

三、各地区、各部门要积极通过预留采购份额支持监狱企业。有制服采购项目的部门，应加强对政府采购预算和计划编制工作的统筹，预留本部门制服采购项目预算总额的30%以上，专门面向监狱企业采购。省级以上政府部门组织的公务员考试、招生考试、等级考试、资格考试的试卷印刷项目原则上应当在符合有关资质的监狱企业范围内采购。各地在免费教科书政府采购工作中，应当根据符合教科书印制资质的监狱企业情况，提出由监狱企业印刷的比例要求。

四、各地区可以结合本地区实际，对监狱企业生产的办公用品、家具用具、车辆维修和提供的保养服务、消防设备等，提出预留份额等政府采购支持措施，加大对监狱企业产品的采购力度。

五、各地区、各部门要高度重视，加强组织管理和监督，做好政府采购支持监狱企业发展的相关工作。有关部门要加强监管，确保面向监狱企业采购的工作依法依规进行。各监狱

企业要不断提高监狱企业产品的质量和服务水平，为做好监狱企业产品政府采购工作提供有力保障。

中华人民共和国财政部

中华人民共和国司法部

2014 年 6 月 10 日

第二册　通用条款（公开招标）

第一章　总则

1. 通用条款说明

1.1 采购代理机构发出招标文件通用条款版本，列出深圳市政府采购项目进行招标采购所适用的通用条款内容。如有需要，采购代理机构可以对通用条款的内容进行补充。

1.2 招标文件分为第一册“专用条款”和第二册“通用条款”。

1.3“专用条款”是对本次采购项目的具体要求，包含招标公告、对通用条款的补充内容及其他关键信息、用户需求书、投标文件格式及附件、合同条款及格式等内容。

1.4“通用条款”是适用于政府采购公开招标项目的基础性条款，具有普遍性和通用性。

1.5 “专用条款”和“通用条款”表述不一致或有冲突时，以“专用条款”为准。

2. 招标说明

本项目按照《深圳经济特区政府采购条例》、《深圳经济特区政府采购条例实施细则》及政府采购其他法律法规，通过公开招标方式确定中标供应商。

3. 定义

招标文件中下列术语应解释为：

3.1“采购人”：指利用财政性资金依法进行政府采购的国家机关、事业单位、团体组织；

3.2 “政府集中采购机构”是指市政府设立的，对纳入集中采购目录内的采购项目组织实施采购，并对政府采购活动提供服务的专门机构；本文件所述的“政府集中采购机构”指深圳公共资源交易中心；

3.3“采购代理机构”是指根据采购人委托，代理政府采购事宜的社会采购代理机构。本招标文件的招标机构特指**深圳市中正招标有限公司；**

3.4“投标人”，即供应商，指参加投标竞争并愿意按照招标文件要求向采购人提供货物、工程或者服务的依法成立的法人、其他组织或者自然人；

3.5“评审委员会”是依据《深圳经济特区政府采购条例》、《深圳经济特区政府采购条例实施细则》等有关规定组建的专门负责本次招标其评审工作的临时性机构；

3.6“日期”指公历日；

3.7“合同”指由本次招标所产生的合同或合约文件；

3.8“电子投标文件”指利用深圳公共资源交易网站提供的深圳智慧采购平台投标文件制作专用软件（以下简称：投标文件制作软件）制作并加密的投标文件,适用于网上投标；（投标文件制作软件可从“下载地址：http://zfcg.szggzy.com/TPBidder/DownLoad/深圳市智慧采购平台投标文件制作专用软件.zip”下载）；

3.9“网上投标”指通过深圳公共资源交易网站上传电子投标文件；

3.10 招标文件中的标题或题名仅起引导作用，而不应视为对招标文件内容的理解和解释。

4. 政府采购供应商责任

4.1 欢迎诚信、有实力和有社会责任心的供应商参与政府采购事业。

4.2 投标人应当遵循公平竞争的原则，不得恶意串通，不得妨碍其他投标人的竞争行为，不得损害采购人或者其他投标人的合法权益。如违反上述要求，经核实后，供应商的投标无效。

5. 投标人参加政府采购的条件

5.1 投标人应在投标前到**深圳公共资源交易中心（具体在深圳交易集团有限公司政府采购业务分公司进行办理）**进行注册并办理电子密钥。《供应商注册及电子密钥新申请指引》详见 http://zfcg.szggzy.com/。

5.2 投标人资格要求

参加本项目的投标人应具备的资格条件详见本项目招标公告中“投标人资格要求”（即申请人的资格要求）的内容。

5.3 联合体投标

5.3.1　以下有关联合体投标的条款仅适用于允许投标人组成联合体投标的项目。

5.3.2　由两个或两个以上的自然人、法人或者其他组织可以组成一个联合体，以一个供应商的身份共同投标时，应符合以下原则：

（1）投标联合体各方参加政府采购活动应当具备下列条件：

1、具有独立承担民事责任的能力；

2、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、法律、行政法规规定的其他条件。

（2）在投标截止前，投标联合体各方均应注册成深圳市政府采购供应商；

（3）联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级；

（4）是否允许联合体参加投标，应当由采购人和采购代理机构根据项目的实际情况和潜在供应商的数量自主决定，如果决定接受联合体投标则应当在招标公告中明示；

（5）投标人的投标文件及中标后签署的合同协议对联合体各方均具法律约束力；

（6）联合体各方应当签订联合体投标协议，明确约定各方拟承担的工作和责任，并将该协议随投标文件一并递交给采购代理机构；

（7）联合体中标后，联合体各方应当共同与采购人签订合同，就中标项目向采购人承

担连带责任；

（8）以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动，出现上述情况者，其投标和与此有关联合体、总包单位的投标将被拒绝；

（9）本通用条款中“投标人”一词亦指联合体各方，专用条款另有规定或说明的除外。

6．政策导向

6.1 政府采购扶持贫困地区、中小企业、监狱企业和残疾人福利性单位发展，支持节能减排、环境保护。

6.2 本项目落实深圳市政府采购供应商诚信管理政策要求。

7．本项目若涉及采购货物，则合格的货物及相应服务应满足以下要求：

7.1　必须是全新、未使用过的原装合格正品（包括零部件），如安装或配置了软件的，须为正版软件。

7.2　国产的货物及其有关服务必须符合中华人民共和国的设计、制造生产标准及行业标准。招标公告有其他要求的，亦应符合其要求。

7.3 进口货物及其有关服务必须符合原产地和中华人民共和国的设计、制造生产标准及行业标准。进口的货物必须具有合法的进口手续和途径，并通过中华人民共和国商检部门检验。招标公告有其他要求的，亦应符合其要求。

7.4 投标人应保证，其所提供的货物通过合法正规渠道供货，在提供给采购人前具有完全的所有权，采购人在中华人民共和国使用该货物或货物的任何一部分时，不会产生因第三方提出的包括但不限于侵犯其专利权、商标权、工业设计权等知识产权和侵犯其所有权、抵押权等物权及其他权利而引发的纠纷。如有纠纷，投标人应承担全部责任。

7.5　投标人应保证，其所提供的货物符合国家强制性标准要求；符合相关行业标准（如具备行政主管部门颁发的资质证书或国家质量监督部门的产品《检验报告》等）。设备到货验收时，还必须提供设备的产品合格证、质量保证文件。若中标后，除非另有约定，投标人必须按合同规定完成设备的安装，并达到验收标准。

7.6　工期要求：投标人在投标时对其所投项目应提交交货进度、交货计划等，在合同规定的时间内完成项目实施工作。

7.7　投标人必须承担的设备运输、安装调试、验收检测和提供设备操作说明书、图纸等其他相关及类似的义务。

8．投标费用

不论投标结果如何，投标人应承担其编制投标文件与递交投标文件所涉及的一切费用。

9．踏勘现场

9.1 如有需要（详见专用条款），采购人或采购代理机构将组织投标人对项目现场及周围环境进行踏勘，以便投标人获取有关编制投标文件和签署合同所需的资料。踏勘现场所发

生的费用由投标人自行承担。投标人应按招标文件所约定的时间、地点踏勘现场。

9.2 投标人及其人员经过采购人的允许，可以进入采购人的项目现场踏勘。若招标文件要求投标人于统一时间地点踏勘现场的，投标人应当按时前往。

9.3 采购人应当通过采购代理机构向投标人提供有关现场的书面资料和数据。

9.4 任何人或任何组织在踏勘现场时向投标人提供的任何书面资料或口头承诺，未经采购代理机构在网上发布或书面通知，均作无效处理。

9.5 未参与踏勘现场不作为否定投标人资格的理由。

10．标前会议

10.1 如采购人或采购代理机构认为有必要组织标前会议，投标人应按照招标文件规定的时间或采购代理机构另行书面通知（包括采购代理机构网站发布方式，如更正公告等）的时间和地点，参与标前会议。

10.2 任何人或任何组织在标前会议时向投标人提供的任何书面资料或口头承诺，未经采购代理机构在网上发布或书面通知，均作无效处理。

10.3 未参与标前会议不作为否定投标人资格的理由。

第二章　招标文件

11．招标文件的编制与组成

11.1 招标文件除以下内容外，采购代理机构在招标期间发出的澄清或修改等相关公告或通知内容，均是招标文件的组成部分，对投标人起约束作用；

招标文件包括下列内容：

第一册　专用条款

关键信息

第一章　招标公告

第二章　对通用条款的补充内容及其他关键信息

第三章　用户需求书

第四章　投标文件格式及附件

第五章　合同条款及格式

第二册　通用条款

第一章　总则

第二章　招标文件

第三章　投标文件的编制

第四章　投标文件的递交

第五章　开标

第六章　评审要求

第七章　评审程序及评审方法

第八章　定标及公示

第九章　公开招标失败的后续处理

第十章　合同的授予与备案

第十一章　质疑处理

11.2 投标人下载招标文件后，应仔细检查招标文件的所有内容，如有疑问应在答疑截止时间之前向采购代理机构提出，否则，由此引起的投标损失自负；投标人同时应认真审阅招标文件所有的事项、格式、条款和规范要求等，如果投标人的投标文件未按招标文件要求提交全部资料或者投标文件未对招标文件做出实质性响应，其风险由投标人自行承担。

11.3 任何人或任何组织向投标人提交的任何书面或口头资料，未经采购代理机构在网上发布或书面通知，均作无效处理，不得作为招标文件的组成部分。采购代理机构对投标人由此而做出的推论、理解和结论概不负责。

12．招标文件的澄清

12.1 招标文件澄清的目的是澄清、解答投标人在查阅招标文件后或现场踏勘中可能提出的与投标有关的疑问或询问。

12.2 投标人如对招标文件内容有疑问，应当在招标公告规定的澄清（提问）截止时间前以网上提问的形式通过网上政府采购系统提交采购代理机构。

12.3 不论是采购代理机构根据需要主动对招标文件进行必要的澄清或是根据投标人的要求对招标文件做出澄清，采购代理机构都将在投标截止日期前以书面形式（包括采购代理机构网站发布方式）答复或发送给所有投标人。答复内容是招标文件的组成部分，对投标人起约束作用，其有效性按照本通用条款第 13.3、13.4 款规定执行。

13．招标文件的修改

13.1 招标文件发出后，在投标截止日期前任何时候，确需要变更招标文件内容的，采购代理机构可主动或在解答投标人提出的澄清问题时对招标文件进行修改。

13.2 招标文件的修改以书面形式（包括采购代理机构网站发布方式，如更正公告等）发送给所有投标人，招标文件的修改内容作为招标文件的组成部分，并具有约束力。

13.3 招标文件、招标文件澄清答复内容、招标文件修改补充内容均以书面形式（包括采购代理机构网站公开发布方式，如更正公告等）明确的内容为准。当招标文件、修改补充通知、招标文件澄清答复内容相互矛盾时，以最后发出的内容为准。

13.4 采购代理机构保证招标文件澄清答复内容和招标文件修改补充内容在投标截止时间前以书面形式（包括采购代理机构网站发布方式，如更正公告等）发送给所有投标人。为使投标人在编制投标文件时有充分时间对招标文件的修改部分进行研究，采购代理机构可以酌情延长递交投标文件的截止日期。

第三章　投标文件的编制

14．投标文件的语言及度量单位

14.1 投标人与采购代理机构之间与投标有关的所有往来通知、函件和投标文件均用中文表述。投标人随投标文件提供的证明文件和资料可以为其它语言，但必须附中文译文。翻译的中文资料与外文资料如果出现差异时，以中文为准，但翻译错误的除外。

14.2 除技术规范另有规定外，投标文件使用的度量单位，均采用中华人民共和国法定计量单位。

15．投标文件的组成

具体内容在招标文件专用条款中进行规定。

16．投标文件格式

投标文件包括本通用条款第 15 条中规定的内容。如招标文件提供了投标文件格式，则**投标人提交的投标文件应毫无例外地使用招标文件所提供的相应格式**（表格均可按同样格式扩展）。

17．投标货币

本项目的投标报价应以人民币计。

18．证明投标文件投标技术方案的合格性和符合招标文件规定的文件要求

18.1 投标人应提交证明文件，证明其投标技术方案项下的货物和服务的合格性符合招标文件规定。该投标技术方案及其证明文件均作为投标文件组成部分。

18.2 投标人提供证明投标技术方案与招标文件的要求相一致的文件，可以是文字资料、图纸、数据或数码照片、制造商公布的产品说明书、产品彩页和我国政府机构出具的产品检验和核准证件等，提供的文件应符合以下要求：

18.2.1 主要技术指标和性能的详细说明。

18.2.2 投标产品从采购人开始使用至招标文件中规定的周期内正常、连续地使用所必须的备件和专用工具清单，包括备件和专用工具的货源及现行价格。

18.2.3 对照招标文件技术规格，逐条说明投标技术方案已对采购人的技术规格做出了实质性的响应，或申明与技术规格条文的偏差和例外。投标人应详细说明投标技术方案中产品的具体参数，不得不合理照搬照抄招标文件的技术要求。

18.2.4 产品说明书或彩页应为制造商公布或出具的中文产品说明书或彩页；提供外文说明书或彩页的，必须同时提供加盖制造商公章的对应中文翻译说明，评标依据以中文翻译内容为准，外文说明书或彩页仅供参考；产品说明书或彩页的尺寸和清晰度要求能够使用电脑阅读、识别和判断；

18.2.5 我国政府机构出具的产品检验和核准证件应为证件正面、背面和附件标注的全部具体内容；产品检验和核准证件的尺寸和清晰度应该能够在电脑上被阅读、识别和判断，

提供原件扫描件。

18.3 相关资料不符合 18.2 款要求的，评审委员会有权认定为投标技术方案不合格响应，其相关分数予以扣减或作投标无效处理。

18.4 投标人在阐述上述第 18.2 时应注意采购人在技术规格中指出的工艺、材料和设备的标准以及参照的牌号或分类号仅起说明作用，并没有任何限制性。投标人在投标中可以选用替代标准、牌号或分类号，但这些替代要实质上满足招标文件中技术规格的要求，是否满足要求，由评审委员会来评判。

18.5 除非另有规定或说明，投标人对同一项目投标时，不得同时提供两套或两套以上的投标方案。

19．投标文件其他证明文件的要求

19.1 采用综合评分法的项目，对项目招标文件《评标信息》评分项中涉及的相关业绩、社保情况等内容以及《资格性审查表》和《符合性审查表》中涉及的证明材料，投标人应提供相关部门出具的证明材料扫描件或照片，原件备查。有关扫描件（或照片）的尺寸和清晰度要求能够使用电脑阅读、识别和判断。若投标人未按要求提供证明材料或提供的是部分证明材料或提供不清晰的扫描件（或照片）的，评审委员会有权认定其投标文件未对招标文件有关需求进行响应，涉及资格性检查或符合性检查的予以投标无效处理，涉及《评标信息》打分项的则该项评分予以 0 分处理。评审委员会对供应商投标资料是否异常、是否有效问题进行核查和判定，如认为供应商投标资料有异常或无效的，若涉及资格性审查或符合性审查条款的，则应作投标无效处理；若涉及评分的，则作不得分处理。

19.2 本项目涉及提供的有关资质（资格）证书，若原有资质（资格）证书处于年审期间，须提供证书颁发部门提供的回执，并且回执须证明该证书依然有效（若在法规范围不需提供的，供应商应做书面说明并提供证明文件，否则该证书无效），则该投标人提供年审证明的可按原资质（资格）投标；若投标人正在申报上一级别资质（资格），在未获批准之前，仍按原级别资质（资格）投标。

20．投标有效期

20.1 投标有效期为从投标截止之日算起的日历天数。在此期限内，所有投标文件均保持有效。

20.2 在特殊情况下，采购代理机构在原定的投标有效期满之前，可以根据需要以书面形式（包括采购代理机构网站公开发布方式）向投标人提出延长投标有效期的要求，对此要求投标人须以书面形式予以答复，投标人可以拒绝采购代理机构此项要求，其投标在原投标有效期满后不再有效。同意延长投标有效期的投标人不能要求也不允许修改其投标文件。

20.3 中标供应商的投标文件有效期，截止于完成本招标文件规定的全部项目内容，并通过竣工验收及保修期结束。

21．关于投标保证金

21.1 根据《深圳市财政局关于明确政府采购保证金管理工作的通知》（深财购[2019]42号）文的规定，本项目不收取投标保证金。

22. 投标人的替代方案

22.1 投标人所提交的投标文件应完全满足招标文件（包括图纸和技术规范所示的基本技术设计）的要求。除非项目明确允许投标人提交替代方案，否则投标人有关替代方案的条款将初审不通过，作投标无效处理。

22.2 如果允许投标人提交替代方案，则准备提交替代方案的投标人除应提交一份满足招标文件（包括图纸和技术规范所示的基本技术设计）要求的投标文件外，还应提交需评审其替代方案所需的全部资料，包括项目方案书、技术规范、替代方案报价书、所建议的项目方案及有关的其它详细资料。

23. 投标文件的制作要求

23.1 投标人应准备所投项目的电子投标文件一份。此电子投标文件须由投标人根据采购代理机构提供的后缀名为.szczf 的电子招标文件，下载并使用相应的深圳智慧采购平台投标文件制作专用软件打开招标文件（.szczf 格式）【下载地址：http://zfcg.szggzy.com/TPBidder/DownLoad/深圳市智慧采购平台投标文件制作专用软件.zip】。

23.2 投标人在使用《投标文件制作软件》编制投标书时须注意：

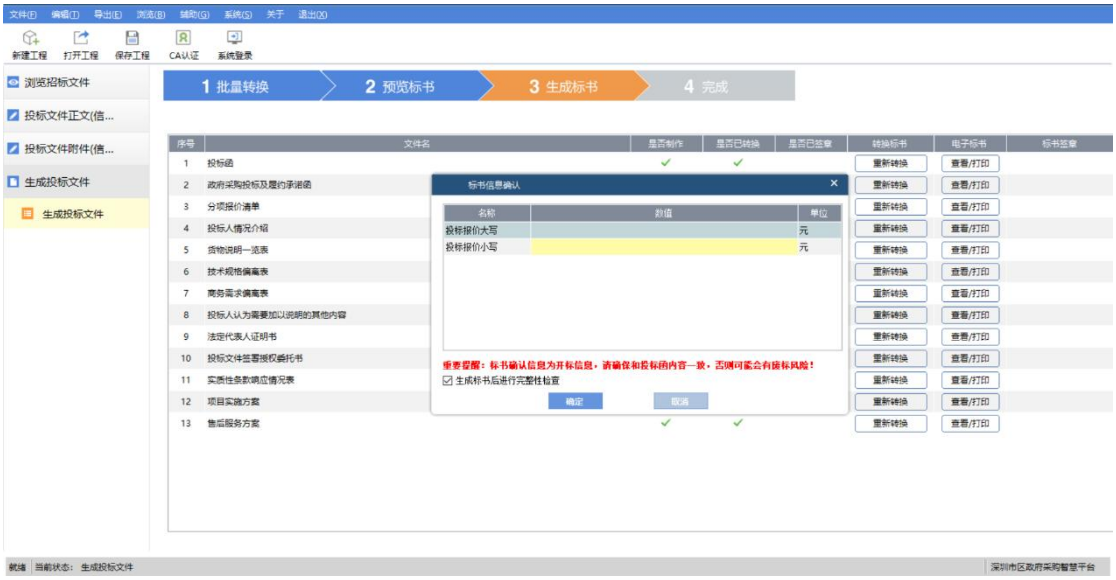
23.2.1 导入《投标文件制作软件》的招标文件项目编号、包号应与以此制作的投标文件项目编号、包号一致。例如，不能将甲项目 A 包的招标书导入《投标文件制作软件》，制作乙项目 B 包的投标书。

23.2.2 不能用非本公司的电子密钥加密本公司的投标文件，或者用其它公司的登录用户上传本公司的投标文件。

23.2.3 要求用《投标文件制作软件》编制投标书的包，不能用其它方式编制投标书。编制投标文件时，电脑须连通互联网。

23.2.4 投标文件不能带病毒。采购代理机构将用专业杀毒软件对投标文件进行病毒检测，如果这两种软件均报告发现病毒，则采购代理机构认为该投标文件带病毒。

23.2.5 完整填写“投标关键信息”，如下图所示：



备注：上述“开标一览表”中的“投标总价”将作为价格分计算依据；其它信息仅是对投标文件相关内容的概括性表述，不作为评审依据。

23.2.6 投标人在编辑投标文件时，**在投标文件目录中属于本节点内容的必须在本节点中填写，填写到其他节点或附件，**一切后果由供应商自行承担。

23.2.7 投标文件编写完成后，**必须用属于投标人的电子密钥进行加密，否则视同未盖公章，将导致投标文件无效。**

23.2.8 采购代理机构不接受投标截止时间后递交的纸质、电子、传真等所有形式的投标文件。由于对网上政府采购系统操作不熟悉或自身电脑、网络等原因导致不能在投标截止时间之前上传投标文件，采购代理机构概不负责。建议于开标前一个工作日完成投标文件的制作与上传，如上传确有困难，请及时咨询。

23.2.9 如果开标时出现网络故障、技术故障，影响了政府采购活动，采购代理机构有权采取措施如延期、接受无法从网上上传的投标书等，以保障政府采购活动的公开、公平和公正。

23.3 电报、电话、传真形式的投标概不接受。

23.4 经投标人电子密钥加密的投标文件无须盖章或签字，专用条款另有要求的除外。

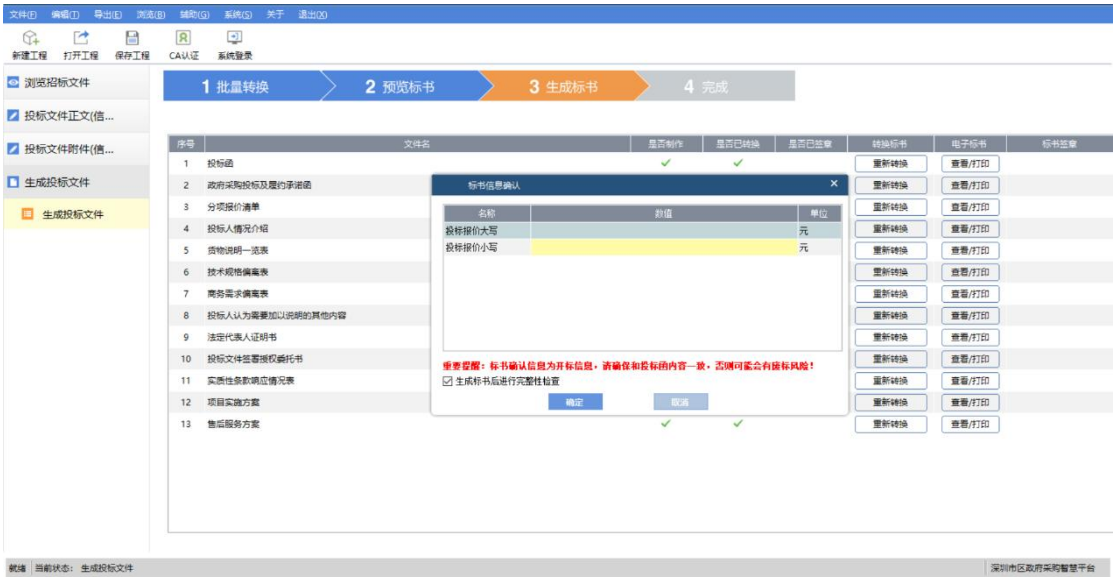
23.5 各类资格（资质）文件提供扫描件，专用条款另有要求的除外。

第四章　投标文件的递交

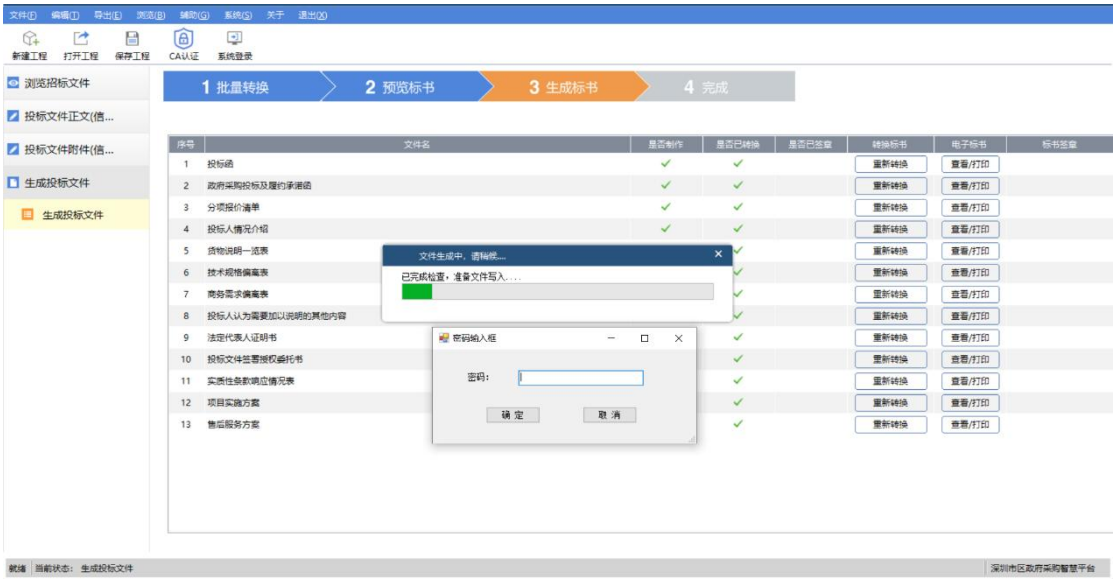
24. 投标书的保密

24.1 在投标文件制作完成后，在投标文件制作软件点击【生成标书】按钮进入【填写开标一览表界面】界面，在该界面填写完开标一览表信息后点击【确定】，进入投标文件生成环节。投标文件制作软件会在投标文件生成过程中，提示用户输入密码，输入密码后对标文件自动进行加密，此加密程序确保投标文件在到达开标时间后才能解密查看。在加密过程

中，请按照软件提示进行操作。加密操作界面如下图所示：



在投标文件制作软件点击【生成标书】按钮进入【填写开标一览表界面】界面，在该界面填写完开标一览表信息后点击【确定】，进入投标文件生成环节。



投标文件制作软件会在投标文件生成过程中，提示用户输入密码，输入密码后对标文件自动进行加密。

24.2 若采购项目出现延期情况：

如果供下载的招标文件（后缀名为.szczf）有更新，投标人必须重新下载招标文件、重新制作投标文件、重新加密投标文件、重新上传投标文件；如果供下载的招标文件（后缀名为.szczf）没有更新，投标人必须重新加密投标文件、重新上传投标文件（是否重新制作投标文件根据项目实际情况定）。否则，投标人自行承担投标文件无法解密导致投标无效的后果。

25. 上传投标文件及投标截止日期

25.1 实行网上投标，投标人必须在招标文件规定的投标截止时间前用电子密钥登录“深圳政府采购智慧平台用户网上办事子系统（http://zfcg.szggzy.com/TPBidder/memberLogin）”，用“【我的项目】→【项目流程】→【递交投标(应答)文件】”功能点上传投标文件。

25.2 采购代理机构可以按本通用条款第 13 条规定，通过修改招标文件自行决定酌情延长投标截止期。在此情况下，采购代理机构、采购人和投标人受投标截止期制约的所有权利和义务均应延长至新的截止期。

25.3 投标截止时间以后不得上传投标文件。

25.4.投标人须在开标当日的开标时间至解密截止时间内进行解密，逾期未解密的作无效处理。解密方法：登录“深圳政府采购智慧平台用户网上办事子系统（http://zfcg.szggzy.com/TPBidder/memberLogin）”，使用本单位制作电子投标文件同一个电子密钥，在“【我的项目】→【项目流程】→【开标及解密】”进行在线解密、查询开标情况。

26. 样品、现场演示、方案讲解

26.1 样品、现场演示、方案讲解等事项在招标文件专用条款中进行规定。

27．投标文件的修改和撤销

27.1 投标方在提交投标文件后可对其投标文件进行修改并重新上传投标文件或在网上进行撤销投标的操作。

27.2 投标截止时间以后不得修改投标文件。

27.3 从投标截止期至投标人在投标文件中确定的投标有效期之间的这段时间内，投标人不得撤回其投标。

27.4 采购代理机构不退还投标文件，专用条款另有规定的除外。

第五章　开标

28．开标

28.1 投标人须在开标当日的开标时间至解密截止时间内进行解密，逾期未解密的作无效处理。解密方法：登录“深圳政府采购智慧平台用户网上办事子系统（http://zfcg.szggzy.com/TPBidder/memberLogin）”，使用本单位制作电子投标文件同一个电子密钥，在“【我的项目】→【项目流程】→【开标及解密】”进行在线解密、查询开标情况。

28.2 采购代理机构将在满足开标条件（①解密时间结束，解密后的投标供应商数量满足开标要求或②解密时间结束前所有投标供应商均完成投标文件解密）后，对投标文件进行开标，并在网上公布开标结果。

第六章　评审要求

29．评审委员会组成

29.1 网上开标结束后召开评审会议，评审委员会由采购代理机构依法组建，负责评审活动。

评审委员会由采购人代表和评审专家组成，成员人数应当为 5 人以上单数（部分条件下为 7 人以上单数），其中评审专家不得少于成员总数的三分之二。评定分离项目评审专家均由评审专家组成。评审专家一般是从深圳市政府采购评审专家库中随机抽取。采购人代表须持本单位签发的《评审授权书》参加评审。

29.2 评审定标应当遵循公平、公正、科学、择优的原则。

29.3 评审活动依法进行，任何单位和个人不得非法干预评标过程和结果。

29.4 评审过程中不允许违背评标程序或采用招标文件未载明的评标方法或评标因素进行评标。

29.5 开标后，直到签订合同为止，凡属于对投标文件的审查、澄清、评价和比较的有关资料以及中标候选人的推荐情况、与评审有关的其他任何情况均严格保密（信息公开的内容除外）。

30．向评审委员会提供的资料

30.1 公开发布的招标文件，包括图纸、服务清单、答疑文件等；

30.2 其他评标必须的资料。

30.3 评审委员会应当认真研究招标文件，至少应了解熟悉以下内容：

（1）招标的目的；

（2）招标项目需求的范围和性质；

（3）招标文件规定的投标人的资格、财政预算限额、商务条款；

（4）招标文件规定的评标程序、评标方法和评标因素；

（5）招标文件所列示的资格性审查表及符合性审查表。

31．独立评审

31.1 评审委员会成员的评标活动应当独立进行，并应遵循投标文件初审、澄清有关问题、比较与评价、确定中标供应商、编写评审报告的工作程序。

第七章　评审程序及评审方法

32．投标文件初审

32.1 投标文件初审包括资格性审查和符合性审查。

资格性审查：依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标供应商是否具备投标资格。

符合性审查：依据招标文件的规定，对投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否满足符合性审查的要求。

32.2 投标文件初审内容请详见《资格性审查表》和《符合性审查表》部分。投标人若有一条审查不通过则按投标无效处理。

32.3 投标文件初审中关于供应商家数的计算:

32.3.1 采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评审委员会按照招标文件规定的方式确定一个参加评审的投标人，招标文件未规定的采取随机抽取方式确定，其他投标无效。

32.3.2 采用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评审委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

32.3.3 非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前两款规定处理。

32.4 投标人投标文件作无效处理的情形，具体包括但不限于以下：

32.4.1 不同投标人的投标文件由同一单位或者同一个人编制，或者由同一个人分阶段参与编制；

32.4.2 不同投标人委托同一单位或者个人办理投标事宜；

32.4.3 不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

32.4.4 不同投标人的投标文件异常一致或者投标报价呈规律性差异；

32.4.5 不同投标供应商的投标文件或部分投标文件相互混装；

32.4.6 投标供应商之间相互约定给予未中标的供应商利益补偿；

32.4.7 不同投标供应商的法定代表人、主要经营负责人、项目投标授权代表人、项目负责人、主要技术人员为同一人、属同一单位或者同一单位缴纳社会保险；

32.4.8 不同投标供应商的投标文件内容存在非正常一致；

32.4.9 在同一单位工作人员为两家以上（含两家）供应商进行同一项投标活动；

32.4.10 主管部门依照法律、法规认定的其他情形。

32.5 对不属于《资格性审查表》和《符合性审查表》所列的其他情形，除专用条款另有规定和 32.4 条款所列情形外，不得作为投标无效的理由。

33．澄清有关问题

33.1 对招标文件中描述有歧义或前后不一致的地方（不含招标文件存在歧义、重大缺

陷导致评审工作无法进行的情况），评审委员会有权进行评判，但对同一条款的评判应适用于每个投标人。

33.2 评审委员会发现招标文件存在歧义、重大缺陷导致评审工作无法进行，或者招标文件内容违反国家有关强制性规定的，应当停止评审工作，与采购代理机构沟通并作书面记录。经确认后，项目应当修改招标文件，重新组织采购活动。

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

投标人的澄清、说明或者补正应当采用书面形式【书面形式是指文书、信件（含电子邮件）、电报、电传、传真等形式】，并加盖公章（或者由法定代表人或其授权的代表签字）。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

根据本通用条款第 34 条，凡属于评审委员会在评审中发现的算术错误进行核实的修改不在此列。

34．错误的修正

投标文件报价出现前后不一致的，除专用条款另有规定外，按照下列规定修正：

34.1 投标文件中开标一览表投标报价内容与投标文件中投标报价相应内容不一致的，以开标一览表为准；

34.2 大写金额和小写金额不一致的，以大写金额为准；

34.3 单价金额小数点或者百分比有明显错位，以开标一览表的总价为准，并修改单价；

34.4 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。

34.5 同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照本通用条款 33 条的规定，经投标人确认后产生约束力，投标人不确认的，其投标无效。

35．投标文件的比较与评价

评审委员会将按照《深圳经济特区政府采购条例》、《深圳经济特区政府采购条例实施细则》、《深圳市政府采购评标定标分离管理办法》及政府采购其他法律法规，仅对通过资格性审查和符合性审查的投标文件进行综合比较与评价。

评审委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的评审委员会成员应当书面作出说明，否则视为无异议。

36. 实地考察或资料查验

36.1 在评审过程中，评审委员会有权决定是否对本项目投标人进行实地考察或资料查验（原件）。投标人应随时做好接受实地考察或资料查验的准备。

37．评审方法

37.1.1 最低价法

最低价法，是指完全满足招标文件实质性要求，按照报价由低到高的顺序，依据招标文件中规定的数量或者比例推荐候选中标供应商。

37.1.2 综合评分法

综合评分法，是指在满足招标文件全部实质性要求的前提下，按照招标文件中规定的各项因素进行综合评审，评审总得分排名前列的投标人，作为推荐的候选中标供应商。

37.2 本项目采用的评审方法见本项目招标文件第一册“专用条款”的相关内容。

37.3 重新评审的情形

评审结果汇总完成后，除下列情形外，任何人不得修改评审结果：

37.3.1 分值汇总计算错误的；

37.3.2 分项评分超出评分标准范围的；

37.3.3 评审委员会成员对客观评审因素评分不一致的；

37.3.4 经评审委员会认定评分畸高、畸低的。

评审报告签署前，经复核发现存在以上情形之一的，评审委员会应当当场修改评审结果，并进行书面记载；评审报告签署后，采购人或者采购代理机构发现存在以上情形之一的，应当组织原评审委员会进行重新评审，重新评审改变评审结果的，书面报告本级财政部门。

投标人对本条第一款情形提出质疑的，采购人或者采购代理机构可以组织原评审委员会进行重新评审，重新评审改变评审结果的，应当书面报告本级财政部门。

37.4 重新组建评审委员会的情形

评审委员会或者其成员存在下列情形导致评审结果无效的，重新组建评审委员会进行评标，并书面报告本级财政部门：

37.4.1 评审委员会组成不符合《政府采购货物和服务招标投标管理办法》规定的；

37.4.2 有《政府采购货物和服务招标投标管理办法》第六十二条第一至五项情形的；

37.4.3 评审委员会及其成员独立评标受到非法干预的；

37.4.4 有政府采购法实施条例第七十五条规定的违法行为的。

有违法违规行为的原评审委员会成员不得参加重新组建的评审委员会。

第八章　定标及公示

38．定标方法

38.1 非评定分离项目定标方法

38.1.1 评审委员会依据本项目招标文件所约定的评审方法进行评审和比较，向采购代理机构提交书面评审报告，并根据评审方法比较评价结果从优到劣进行排序，确定候选中标供应商。

38.1.2 采用最低价法的，评审结果按投标报价由低到高顺序排列。投标报价相同的并列。投标文件满足招标文件全部实质性要求且投标报价最低的投标人为中标供应商（排名第二的投标人为第一替补中标候选人、排名第三的投标人为第二替补中标候选人）。

38.1.3 采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，

按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标供应商（中标候选人如不止一名，则推选排名第二的投标人为第一替补中标候选人、排名第三的投标人为第二替补中标候选人）。出现得分且投标报价相同的并列情况时，采取随机抽取的方式确定，具体操作办法及流程由评审委员会确定。

38.2 评定分离项目定标方法

38.2.1 评定分离是指在政府集中采购程序中，以公开招标方式执行采购，评审委员会负责对投标文件进行评审、推荐候选中标供应商并出具书面评审报告，由采购人根据评审委员会出具的评审报告从推荐的候选中标供应商中确定中标供应商。单个项目需要确定多家中标供应商的，不适用评定分离。

38.2.2 适用评定分离的政府采购项目，采用综合评分法评审。评审委员会按照评审结果，推荐三个合格的候选中标供应商。

38.2.3 适用评定分离的政府采购项目，按照自定法确定中标供应商：自定法是指采购人组织定标委员会，由定标委员会在三家候选中标供应商中确定中标供应商。

38.2.4 采购代理机构应当自评审结束之日起两个工作日内将候选中标供应商名单及其投标文件、评审报告送交采购人。采购人应当安排专人对定标过程进行书面记录，形成定标报告，作为采购文件的组成部分存档，并及时将定标结果反馈采购代理机构。具体定标程序及相关要求以按照《深圳市财政局关于印发〈深圳市政府采购评标定标分离管理办法〉的通知》（深财规【2020】1 号）执行。

说明：采购人及投标供应商应按照上述方法提前做好相关准备。

38.3 专用条款另有规定的，按专用条款相关要求定标。

39. 编写评审报告

评审报告是评审委员会根据全体评标成员签字的原始评审记录和评审结果编写的报告，评审报告由评审委员会全体成员签字。对评审结论持有异议的评审委员会成员可以书面方式阐述其不同意见和理由。评审委员会成员拒绝在评审报告上签字且不陈述其不同意见和理由的，视为同意评审结论。评审委员会应当对此作出书面说明并记录存档。

40. 中标公告

40.1 为体现“公开、公平、公正”的原则，评审结束后经采购人确认（确定）评审结果，采购代理机构将在“深圳政府采购智慧平台（http://zfcg.szggzy.com/）”上发布中标结果公告。供应商如对评审结果有异议，可在发布公示日期起七个工作日内向采购代理机构提出。 监督电话：0755-83948143。若在公示期内未提出质疑，则视为认同该评审结果。

40.2 质疑、投诉供应商应保证质疑、投诉内容的真实性和可靠性，并承担相应的法律责任。

41. 中标通知书

41.1 中标公告公布以后无异常的情况下,采购代理机构将向中标供应商和采购人发出中标通知书。

41.2 中标通知书是合同的重要组成部分。

41.3 因质疑投诉或其它原因导致项目结果变更或采购终止的，采购代理机构有权吊销中标通知书。

41.4 中标服务费

中标人须在中标公告公示期结束后，向采购代理机构缴纳中标服务费。中标服务费收费标准根据《深圳市财政委员会关于规范深圳市社会采购代理机构的管理有关事项的补充通知（深财购[2018]27 号）》文件相关规定，按照差额定率累进法计算。具体收费标准详见下表：

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	1.500%	1.500%	1.000%
100～500	1.100%	0.800%	0.700%
500～1000	0.800%	0.450%	0.550%
1000～5000	0.500%	0.250%	0.350%
5000～10000	0.250%	0.100%	0.200%
10000～50000	0.050%	0.050%	0.050%
50000～100000	0.035%	0.035%	0.035%
100000～500000	0.008%	0.008%	0.008%
500000～1000000	0.006%	0.006%	0.006%
1000000 以上	0.004%	0.004%	0.004%

第九章　公开招标失败的后续处理

42．公开招标失败的处理

42.1 本项目公开招标过程中若由于投标截止后实际递交投标文件的供应商数量不足、经评审委员会评审对招标文件作实质响应的供应商不足等原因造成公开招标失败，可由采购代理机构重新组织采购。

42.2 对公开招标失败的项目，评审委员会在出具该项目招标失败结论的同时，可以提出重新采购组织形式的建议，以及进一步完善招标文件的资格、技术、商务要求的修改建议。

42.3 重新组织采购有以下两种组织形式：

（1）由采购代理机构重新组织公开招标；

（2）根据实际情况需要向同级财政部门提出非公开招标方式申请的，经同级财政部门批准，公开招标失败采购项目可转为竞争性谈判或单一来源谈判方式采购。

42.4 公开招标失败的采购项目重新组织公开招标，由采购代理机构重新按公开招标流程组织采购活动。

42.5 公开招标失败的采购项目经同级财政部门批准转为竞争性谈判或单一来源谈判方式采购的，按规定要求组织政府采购工作。

第十章　合同的授予与备案

43．合同授予标准

本项目的合同将授予经本招标文件规定评审确定的中标供应商。

44．接受和拒绝任何或所有投标的权力

采购代理机构和采购人保留在投标之前任何时候接受或拒绝任何投标或所有投标，以及宣布招标无效的权力，对受影响的投标人不承担任何责任，也无义务向受影响的投标人解释采取这一行动的理由。

45．合同的签订

45.1 中标人将于中标通知书发出之日起十个工作日内，按照采购文件（招标文件和投标文件等）内容与采购人签订政府采购合同；合同的实质性内容应当符合招标文件的规定；

45.2 中标人如不按本通用条款第 45.1 款的规定与采购人签订合同，情节严重的，由同级财政部门记入供应商诚信档案，予以通报；

45.3 中标人应当按照合同约定履行义务，完成中标项目，不得将中标项目转让（转包）给他人。

46．履约担保

46.1 在签订项目合同的同时，中标人应按“对通用条款的补充内容”中规定的金额向采购人提交履约担保；

46.2，允许供应商自主选择以支票、汇票、本票、保函等非现金方式提交履约担保；中标人提交履约担保不是合同签订的前提条件，不要求中标人提供除法律、法规明确规定外的其他担保。

47．合同备案

采购人与中标人应于合同签订之日起十日内，由采购人或委托中标人将采购合同副本抄送合同备案工作实施机构备案。

48．合同变更

合同变更事宜按《深圳市财政局 深圳市政府采购中心关于进一步加强市本级政府采购合同备案管理工作的通知》（深财购〔2019〕43 号）相关规定执行。

49．项目验收

49.1 采购人应当按照招标文件和合同规定的标准和方法，及时组织验收。

50. 宣传

凡与政府采购活动有关的宣传或广告，若当中提及政府采购，必须事先将具体对外宣传方案报同级财政部门和采购代理机构，并征得其同意。对外市场宣传包括但不限于以下形式：

a.名片、宣传册、广告标语等；

b.案例介绍、推广等；

c.工作人员向其他消费群体宣传。

51. 供应商违法责任

51.1《深圳经济特区政府采购条例》第五十七条 供应商在政府采购中，有下列行为之一的，一至三年内禁止其参与本市政府采购，并由主管部门记入供应商诚信档案，处以采购金额千分之十以上千分之二十以下的罚款；情节严重的，取消其参与本市政府采购资格，处以采购金额千分之二十以上千分之三十以下的罚款，并由市场监管部门依法吊销其营业执照；给他人造成损失的，依法承担赔偿责任；构成犯罪的，依法追究刑事责任：

（1）在采购活动中应当回避而未回避的；

（2）未按本条例规定签订、履行采购合同，造成严重后果的；

（3）隐瞒真实情况，提供虚假资料的；

（4）以非法手段排斥其他供应商参与竞争的；

（5）与其他采购参加人串通投标的；

（6）恶意投诉的；

（7）向采购项目相关人行贿或者提供其他不当利益的；

（8）阻碍、抗拒主管部门监督检查的；

（9）其他违反本条例规定的行为。

51.2 根据《深圳市财政局关于明确政府采购保证金管理工作的通知》（深财购[2019]42号）的要求，供应商在政府采购活动中出现《深圳经济特区政府采购条例实施细则》第八十四条所列情形的，采购人或采购代理机构可将有关情况报同级财政部门，由财政部门根据实际情况记入供应商诚信档案，予以通报：

（1）投标截止后，撤销投标的；

（2）中标后无正当理由未在规定期限内签订合同的；

（3）将中标项目转让给他人、或者在投标文件中未说明且未经采购人、采购招标机构同意，将中标项目分包给他人的；

（4）拒绝履行合同义务的。

第十一章 质疑处理

52.质疑提出与答复

52.1 提出质疑

参与政府采购活动的供应商认为自己的权益在采购活动中受到损害的，应当自知道或者应当知道其权益受到损害之日起七个工作日内向采购人、采购代理机构以书面形式提出质疑。

52.2 法律依据

《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《深圳经济特区政府采购条例》、《深圳经济特区政府采购条例实施细则》、《政府采购质疑和投诉办法》（财政部令第 94 号）和其他有关法律法规规定。

52.3 质疑条件

52.3.1 提出质疑的供应商应当是参与所质疑项目采购活动的供应商；以联合体形式参与的，质疑应当由组成联合体的所有成员共同提出；

52.3.2 应当在法定质疑期内一次性提出针对同一采购程序环节的质疑，法定质疑期为自知道或应当知道权益受到损害之日起 7 个工作日内。应当知道其权益受到损害之日是指：对招标文件的质疑，为招标文件公布之日；对采购过程的质疑，为各采购程序环节结束之日；对中标结果以及评审委员会组成人员的质疑，为中标结果公示之日；

52.3.3 应提交书面质疑函，质疑函应当包括以下内容：

（1）供应商的名称（或者姓名）、地址、邮编、邮箱、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑对象、质疑事项和质疑请求；

（4）因质疑事项而受损害的权益；

（5）事实依据；

（6）必要的法律依据；

（7）提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人（负责人），或者其授权代理人签字或者盖章，并加盖公章。

52.4 提交材料

供应商质疑实行实名制。供应商为自然人的，应当提交本人身份证复印件；供应商为法人或者其他组织的，应当根据自身性质提交营业执照复印件或者其他证明文件（如事业单位法人证书等）复印件。

供应商可以委托代理人进行质疑。其授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

52.5 提交方式

52.5.1 供应商登录“深圳政府采购智慧平台用户网上办事子系统（http://zfcg.szggzy.com/TPBidder/memberLogin）”，在“【我的项目】→【项目流程】→【质疑】”中提出质疑。

52.5.2 同时，请质疑供应商根据深圳政府采购智慧平台（http://zfcg.szggzy.com/）所发布的质疑指引、质疑函模板填写质疑函并提交质疑材料。地址：深圳市中正招标有限公司（深圳市福田区民田路 171 号新华保险大厦 903），质疑咨询电话：0755-83026699。

52.6 收文办理程序

52.6.1 供应商提交的质疑符合受理条件的，采购代理机构自收到质疑材料之日起即为受理，应当向供应商出具质疑函收文回执并可以要求其递交质疑的法定代表人（负责人）或者授权代理人签署质疑文书送达地址确认书。

52.6.2 供应商提交的质疑材料不符合质疑条件的，视情况处理：

供应商提交的质疑材料不全或者未按要求签字或者盖章的，采购代理机构应当一次性告知供应商需补正的内容和补正期限。

供应商提交的质疑存在下列情形之一的，不予受理：

（1）质疑主体不满足要求的；

（2）供应商自身权益未受到损害的；

（3）供应商未在法定质疑期限内提出质疑的；

（4）质疑材料不全或者未按要求签字或者盖章的情况下，要求补正后，逾期未补正或者补正后仍不符合规定的；

（5）其他不符合受理条件情形的。

质疑事项不予受理的，采购代理机构应当向供应商出具不符合质疑条件告知书。

52.7 质疑答复时限

自收文之日起七个工作日内。

52.8 投诉

对质疑答复不满意或者未在规定时间内答复的，提出质疑的供应商可以在答复期满后 15 个工作日内向同级财政部门投诉。