## 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“投标人资格要求”部分的相关内容 |
| 2 | 投标有效期 | 120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 | 本项目实行网下投标，按照投标文件的要求提交纸质文件正本1份，副本4份，电子文件1份（WORD和PDF格式电子文档各1份）电子文档要求U盘，PDF格式有签字盖章，不留密码，无病毒，不压缩，密封提交），所有应答文件应于递交截止时间之前送达招标文件规定的地址。 |
| 5 | 履约保证金 | \_\_\_\_\_万元或合同金额的\_\_\_\_\_%，缴纳方式： |
| 6 | 中标服务费 | 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管理有关事项的补充通知(深财购[2018]27号)”的规定执行。招标代理服务收费以中标/成交通知书公布的中标金额为计算基准,按差额定率累进法计算,作为招标代理服务费。不足陆仟元的按陆仟元收取。 |

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 | 采购计划编号 | 货物名称 | 数量 | 单位 | **备注** | **财政预算限额（元）** |
| 1 |  | 移动应用安全检测设备（含安全漏洞模块和 个人信息安全影响评估模块） | 1 | 套 | 拒绝进口 | 90万 |
| 测试终端 | 6 | 台 | 拒绝进口 |

**备注：1.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。**

**2、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。**

**3、本项目核心产品为：无。**

### 三、实质性条款

|  |  |
| --- | --- |
| 序号 | 具体内容 |
| 1 | 投标文件载明的交货期不超过招标文件规定的期限 |
| 2 | 投标文件载明的免费保修期不低于招标文件规定的期限 |
| 3 | 具体技术要求、商务需求中带“★”要求 |
| 4 | 签订合同后15天（日历日）内交货。提供承诺函（格式自拟）。 |
| 5 | 投标文件载明的免费保修期为3年，时间自最终验收合格并交付使用之日起计算；免费提供5年相关的软件系统打补丁、升级服务及介质，支持系统功能升级和规则库升级。提供承诺函（格式自拟）。 |
| 6 | 免费保修期外，提供远程技术支持服务，对工具使用和报告分析结果进行解答。提供承诺函（格式自拟）。 |
| 7 | 按照合同条款、保密协议格式签订合同、保密协议，按照安全服务承诺书格式签订安全服务承诺书。 |

**注：上表所列内容为不可负偏离条款**

### 四、具体技术要求

**说明：1、带“★”指标项为实质性条款，如出现负偏离，将被视为未实质性满足招标文件要求作投标无效处理。带“▲”指标项为重要参数，负偏离时依相关评分准则内容作重点扣分处理。**

**2、招标技术要求中，用红色加粗字体标注的技术条款为要求提供证明资料的条款，共9项，需提供具有国家级第三方检测机构或者国家部委主管单位检测机构的检测报告，要求提供报告扫描件（原件备查）作为得分依据；其余为未要求提供证明资料的条款，无需提供相关证明资料。**

**3、评分时，如对一项招标技术要求（以划分框为准）中的内容存在两处（或以上）负偏离的，在评分时只作一项负偏离扣分。**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物名称 | 分类 | 招标技术要求 |
| **1** | 移动应用安全检测设备 | 基本要求 | 1.1 系统综述:移动应用安全检测设备集成安全漏洞模块和个人信息安全影响评估模块，任务提交和结果查看可在统一平台完成，模块也可独立使用。安全漏洞模块支持覆盖移动应用的客户端自身安全、业务动态安全、通讯链路安全、服务器端安全，能出具安全检测报告；个人信息安全影响评估模块支持App违法违规、个人信息安全、SDK安全、合规项目的自动化检测，全自动化快速识别App潜在的安全风险包括个人信息窃取、个人信息出境等。 |
| 1.2 系统具有公安部颁发的销售许可证 |
| 1.3计算机软件著作权登记证书 |
| 安全漏洞 | **▲2.1 测试应用：单台系统同时支持Android/iOS/鸿蒙应用和微信公众号、小程序的测试，以及WEB主动和WEB被动测试。** |
| **▲2.2测试范围：检测覆盖客户端自身安全、业务动态安全、通讯链路安全、服务器端安全。** |
| 2.3测试报告：支持自动导出报告，报告格式至少包括.doc、.pdf、.xml。报告内容至少包括所有检测项以及所发现问题的漏洞名称、风险内容、风险级别、检测详情、修复建议等。 |
| 2.4规则库：系统应至少包含恶意代码规则库、恶意URL规则、恶意行为规则库、主机漏洞规则库、应用漏洞规则库。必须要在五个工作日内将业界最新发现的病毒和漏洞更新到检测工具的病毒库和规则库内。 |
| 2.5移动应用安全检测工具扫描报告中漏洞名称及风险级别等须与国家信息安全漏洞库（CNNVD）相兼容, 具备国家信息安全漏洞库（CNNVD）兼容性资质证书 |
| **▲2.6自动脱壳：支持至少5种加固厂商（具有公安部移动APP加固产品销售许可的安全厂商）加固后APP的脱壳，解密还原加固前程序文件，支持脱壳包一键导出。** |
| 2.7通用测试项：测试项目包括但不限于拒绝服务攻击风险，应用完整性检测，程序签名保护检测，应用二次打包风险，Activity、Service、Content Provider、Broadcast Receiver、Intent等组件检测项。包括但不限于Java代码动态调试风险，动态注入攻击风险等检测项。包括但不限于Webview明文存储密码漏洞，WebView远程代码执行漏洞，WebView组件忽略SSL证书验证错误漏洞，数据库注入漏洞等检测。包括但不限于内存Dump风险，RSA加密算法使用不当风险，密钥硬编码漏洞，动态注册Receiver风险等检测；包括但不限于系统键盘使用风险，关键界面劫持风险，SSL证书有效性风险，HTTP传输通道风险等检测。 |
| ▲2.8**图形验证码：可对被测 APP 的身份鉴别图形验证码进行截图并上传后台服务器自动识别。可人工参与图像验证码标记，系统后台自动比对分析输出图形验证码安全分析结果。** |
| **▲2.9 API漏洞检测：支持对应用服务端进行检测，包括但不限于：SQL注入检测；XSS漏洞；CSRF漏洞；文件漏洞、后门检测等。** |
| 个人信息安全影响评估 | 3.1检测内容：支持App基本信息分析、应用类型识别、恶意程序检测、违规内容检测、SDK安全、隐私合规、敏感行为、网络流量的自动化检测。 |
| 3.2通用分析项：根据《信息安全技术 个人信息安全规范（GB/T 35273-2020）》和《App违法违规收集使用个人信息行为认定方法（国信办秘字〔2019〕191号）》，分析类别包括违规收集使用个人信息行为分析，App权限使用检查，App敏感行为分析，未公开收集使用规则，未明示收集目的方式和范围、违规收集个人信息、违规使用个人信息，违反必要原则，超范围收集个人信息，设置障碍、频繁骚扰用户，欺骗误导用户，删除、更正个人信息难等分类，持个人信息安全项目支持不低于114项。 |
| 3.3加密数据导入：支持自定义配置压缩包密码功能，可对导入重要数据压缩密码进行定制配置。 |
| 3.4支持任务结果对比功能，选择隐藏相同项目、高亮显示差异项目。 |
| 3.5任务管理：支持对任务暂停操作便于停止测试，支持对子任务（静态分析、动态分析、数据分析等）手动重启和手动完成操作，满足针对模块重测和跳过的需求。检测过程支持自动、半自动、手动测试模式。 |
| 3.6结果过滤：支持对分析结果的过滤规则配置，支持域名、sdk、关键词等进行过滤，支持单个任务过滤规则，支持全局过滤规则。 |
| 3.7系统管理:a)测试终端管理：支持对接入测试终端的管理，支持对测试终端的认证，测试终端支持web远程操作。  b)知识库管理：支持对个人信息检测知识库进行调整。  c)网络配置：模块支持独立部署，支持usb网络共享、wifi和有线三种部署模式。 |
| 3.8合规识别行为：支持对敏感行为识别包括获取ANDROID\_ID、获取MEID、获取定位、获取安装包名、获取ip、获取mac等行为，记录敏感行为函数调用栈，分析行为涉及个人信息，超过250敏感接口。 |
| **▲3.9APP组件成分分析：应用支持成分分析，覆盖主流语言公开组件库的识别。** |
| **▲3.10APP组件许可证分析：支持开源许可证合规性分析，支持超过400个开源许可证。** |
| **▲3.11代码补全技术：支持对不完整代码进行自动分析和代码依赖性自动补全，为逆向分析提供技术支撑。** |
| **▲3.12数据流分析技术：支持对系统可执行文件进行数据流分析，识别和分析数据中存在的个人信息泄露、通信数据未加密等安全隐患。** |
| **2** | 测试终端 | | 4.1 测试终端需满足检测所需Android、iOS及鸿蒙操作系统环境。  4.2测试终端需为检测设备定制系统，安装agent与系统后台联动完成测试，提供测试必须的测试框架、数据提取和分析工具，与后台通过标准API进行任务执行、过程数据回传、结果数据回传等。 |

### 五、检测报告

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物名称 | 检测机构要求 | 检测指标 |
| 1 | 移动应用安全检测设备 | 国家级第三方检测机构或者国家部委主管部门检测机构 | 证明支持对移动应用安全漏洞检测和个人信息安全影响评估检测能力。 |

**备注：**

**1、投标文件应按要求提供相应检测报告。**

**2、检测报告（均为原件扫描件）的提供要求：**

**（1）检测报告内容中若涉及外文说明，必须同时提供对应中文翻译说明，评标依据以中文翻译内容为准，外文说明仅供参考；检测报告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测报告应为报告正面、背面和附件标注的全部具体内容；产品检验报告的尺寸和清晰度应该能够在电脑上被阅读、识别和判断。**

### 六、样品要求

（一）一般性规定和要求

1、投标样品上必须标注“项目名称及项目编号、样品编号、样品名称”等信息，但不得显示指向任何投标供应商的信息、生产厂家的商标，或者其他的标记标识。需要安装的投标样品必须为安装完整的成品，由投标供应商自行组织安装。

2、样品递交签到：

投标供应商授权人需在本项目投标截止时间前，提供法定代表人证明书（盖公章）、法定代表人授权委托书（盖公章）、授权委托人身份证原件和复印件、样品清单（加盖公章），到深圳市瑞凝信招标咨询有限公司，按工作人员指引进行样品递交签到。

特别注意事项：（1）上述资料提供不齐全的，不予签到；（2）本项目投标截止时间后，不再受理签到；（3）未进行签到的，样品不予接收。

3、本项目投标截止时间后进行投标样品接收。投标样品接收必须进行身份核对、样品核对、登记确认、顺序编号。

（1）身份核对。代理机构核对投标供应商授权委托人提供的“法定代表人证明书（盖公章）、法定代表人授权委托书（盖公章）、授权委托人身份证原件和复印件”。资料不齐全的，不得接收投标样品。

（2）样品核对。工作人员将投标样品与投标供应商提供的《样品清单》（盖公章）进行一一核对。有不一致的或损坏情况的，将要求供应商授权委托人在《样品清单》上注明。

（3）登记确认。在完成身份核对及样品核对后，投标供应商授权委托人必须在《样品接收登记表》上登记确认。

（4）顺序编号。工作人员按投标样品接收的先后顺序进行编号。

4、代理机构工作人员负责组织投标样品摆样，指引供应商授权委托人将投标样品搬运到指定地点摆放、拆除包装，按要求摆放整齐。完成样品摆样后，供应商授权委托人应及时立场，不得在摆样现场滞留。

5、样品的退回：（1）未中标的供应商投标样品，代理机构工作人员将按规定进行通知，并要求供应商授权委托人在项目完成评审后的三个工作日内凭身份证及样品受理回执原件办理退回手续。（2）中标的供应商投标样品，工作人员将按规定进行通知，并要求采购人代表在中标通知书发放后三个工作日内凭中标通知书复印件及身份证原件办理领取手续。

投标样品移交时，代理机构工作人员将再次核对供应商授权委托人或采购人代表身份、核对《样品清单》，签字确认后并取走样品。

6、未能及时退回的样品的处理：

（1）未中标供应商未在规定时间内（项目完成评审后三个工作日）内取回投标样品的，视为放弃取回，代理机构将定期清理。

（2）采购人未在规定时间内（中标通知书发放后三个工作日内）内领取中标供应商投标样品的，代理机构工作人员将发函或电话敦促。经敦促仍拒不领取的，将按规定内容在代理机构网站发布通报。对于拒不领取的中标样品，视同采购人放弃取回，将定期清理。

（二）样品清单：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **数量** | **单位** | **规格** |
| **1** | **移动应用安全检测设备** | **1** | **套** | **安全漏洞检测模块、个人信息安全影响评估检测模块、测试终端** |

备注：投标样品将作为验收产品的主要依据之一。

### 七、演示要求

（一）总体要求：

各投标人应按照招标公告规定的时间和地点参加现场演示。

演示地点提供电源、带VGA接口的液晶显示器及宽带上网环境（无WIFI环境），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10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）具体程序：

1.现场演示人员须在招标公告规定的现场演示签到截止时间前，携带法定代表人证明书（盖公章）、授权委托书（盖公章）、现场演示人员的身份证原件和复印件，到达代理机构，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）招标公告规定的截止时间后，不再受理签到；（3）未签到的人员，不能参与现场演示。

2.招标公告规定的现场演示签到截止时间后正式进行现场演示。现场演示正式开始前将进行身份核对；核对内容为现场演示人员提供的“授权委托书（盖公章）、现场演示人员的身份证原件和复印件”。资料不齐全的人员，不得参与现场演示。

（三）其它要求：

1.参加本次现场演示的各投标人，视为认可本次现场演示的程序和环境能够满足现场演示基本条件，并对本现场演示方案要求内的各项规定不做事后异议，且能够严格遵守相关规定。

2.现场演示在正式评标环节前进行。现场演示原则上按签到顺序依次进行（经评委同意，可以酌情进行调整）。一个投标人一次性现场演示完毕。一个投标人在进行现场演示时，其他投标人不得进入现场。现场演示期间，评委可视情况现场提问。

3.投标人对本次现场演示条件的不确定性疑虑应在现场演示开始前做书面陈述，若疑虑不能完全消除，并认为现场演示结果仍会产生误判，则可退出现场演示。

4.参加本次现场演示的各投标人，视为同意承担其演示结果不确定性的风险，即同意专家以现场演示情况的判定结论。

5.各项费用由投标人自理、风险自负。

**（四）演示内容：**

**1. 安全漏洞演示:支持Android/iOS/鸿蒙应用和微信公众号、小程序的测试，以及WEB主动和WEB被动测试。**

**2. 图形验证码测试：可对被测 APP 的身份鉴别图形验证码进行截图并上传后台服务器自动识别。可人工参与图像验证码标记，系统后台自动比对分析输出图形验证码安全分析结果。**

**3、合规检测模式：支持自动、半自动、手动测试模式等。**

### 八、商务需求

**说明：1、带“★”指标项为实质性条款，如出现负偏离，将被视为未实质性满足招标文件要求作投标无效处理。**

**2、评分时，如对一项招标商务需求（以划分框为准，一个划分框是作为一项招标商务需求）中的内容存在两处（或以上）负偏离的，在评分时只作一项负偏离扣分。**

|  |  |  |
| --- | --- | --- |
| **序号** | **目录** | **招标商务需求** |
| **（一）免费保修期内售后服务要求** | | |
| **1** | 维修响应及故障解决时间 | 在保修期内，一旦发生质量问题，投标人保证在接到通知24小时内赶到现场进行修理或更换。 |
| **2** | 技术解答 | 对检测结果进行解释；系统发生技术问题导致无法检测时，支持团队需在30分钟内提供现场支持，4小时内解决问题 |
| **3** | 技术培训 | 提供至少2场培训，采取现场演示和功能讲解的方式，协助掌握工具的参数配置、功能应用、故障诊断和日常管理，提供对技术工具手段的认识程度、应用能力和维护能力。 |
| **4** | 现场服务 | 保修期内，投标人应提供系统现场技术服务支持，每年不超过20次，协助完成相应项目的检测工作。并应根据招标人工作需要，安排技术人员辅助完成检测报告。 |
| **（二）免费保修期外售后服务要求** | | |
| **1** | 维修响应 | 投标人保证对发生故障的合同设备按照优惠价格进行修理和技术服务。如果合同设备的性能和质量与合同规定不符或出现质量问题，投标人应予以免费更换或修理，如因此造成招标人损失，由投标人承担。 |
| **2** | 系统升级 | 免费提供相关的软件系统打补丁、升级服务及介质，支持系统功能升级。 |
| **（三）其他商务要求** | | |
| **1** | 关于交货 | 1.1交货地点：深圳市 |
| 1.2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、图纸等其他类似的义务。 |
| 1.3签订合同后15天（日历日）内交货。 |
| **2** | 关于验收 | 2.1投标人货物经过双方检验认可后，签署验收报告，产品保修期自验收合格之日起算，由投标人提供产品保修文件。 |
| 2.2当满足以下条件时，采购人才向中标人签发货物验收报告：  a、中标人已按照合同规定提供了全部产品及完整的技术资料。  b、货物符合招标文件技术规格书的要求，性能满足要求。  c、货物具备产品合格证。 |
| **3** | 关于违约 | 以合同签订为准 |
| **4** | 关于付款 | 1、设备到货完成安装、部署和调试，并免费在现场对采购技术人员进行设备操作培训，保证使用人员能够梳理掌握使用方法，以及小故障的判断余解决，采购人向中标供应商支付不超过合同总金额70%；  2、完成约定的至少2次技术培训，支付合同剩余款项。 |
| **5** | 投标人资质认证情况 | 1、具备信息安全管理体系ISO27001、隐私信息管理体系ISO27701；  2、具有国家级信息安全相关机构颁发的信息安全服务资质证书（风险评估或软件安全开发）。 |
| **6** | 投标人自主知识产权产品（创新、设计）情况 | 1、具有自主研发源代码扫描、开源组件扫描、开发安全产品。  2、移动应用安全检测系统通过龙芯、飞腾/麒麟软件或统信等信创平台兼容性认证； |
| **7** | 投标人服务能力 | 1、信创政务产品安全漏洞专业库技术支撑单位。  2、省厅级及以上网信办或公安机关网络与信息安全信息通报中心技术支撑单位。  3、提供完成的省部级以上（含国家级）移动应用安全案例。  4、荣获公安部网络安全保卫局颁发优秀团队不少于3次。 |
| **8** | 拟安排的项目主要团队成员情况 | 需具备有效期内的CISP证书或者CISAW证书 |

### 九、政策导向

1、2014年起，政府部门、国有企业在进行设备或工程采购时，应在招标文件中明确要求工程机械、装卸机械满足国家现阶段非道路移动机械用柴油机排放标准，并鼓励使用LNG或电动工程机械、装卸机械。2015年起，政府部门、国有企业采购设备或工程项目中选用LNG或电动工程机械、装卸机械的比例不低于30%。

2、根据《深圳市人民政府关于印发深圳市贯彻落实守信联合激励和失信联合惩戒制度实施方案的通知》（深府〔2017〕57号）的要求，对列入失信“黑名单”的供应商限制参与政府采购。

3、“信用中国”、“中国政府采购网”以及“深圳市政府采购监管网”为供应商信用信息的查询渠道，相关信息以中标通知书发出前的查询结果为准。