内蒙古广播电视台奔腾OA移动APP加固服务项目（二次）招标公告

招标项目编号（X15000000EW020264001001）

项目所在地：内蒙古自治区,呼和浩特市,回民区

一、招标条件

本**内蒙古广播电视台奔腾OA移动APP加固服务项目（二次）已由项目审批/核准/备案机关批准，项目资金来源其他资金:9万元**，招标人为**内蒙古广播电视台**。本项目已具备招标条件，招标方式为**其他**。

二、项目概况和范围

规模：**详见附件**；

范围：本招标项目划分为**1**个标段，本次招标为其中的：

内蒙古广播电视台奔腾OA移动APP加固服务项目（二次）

三、投标人资格要求：

【1】内蒙古广播电视台奔腾OA移动APP加固服务项目（二次）的投标人资格能力要求：

详见附件；

本项目是否允许联合体投标：**否。**

四、招标文件获取

获取时间：**从2025-12-15 17:30:00到2025-12-18 17:00:00。**

获取方式：**详见附件。**

五、投标文件递交

递交截止时间：**2025-12-19 15:30:00。**

递交方式：**其他方式，详见附件。**

六、开标时间及地点

开标时间：**2025-12-19 15:30:00。**

开标地点：**详见附件。**

七、其他

详见附件；

公告发布媒介：中国招标投标公共服务平台(http://www.cebpubservice.com/)，内蒙古招投标公共服务平台(https://www.nmgztb.com.cn/)；

八、监督部门

本项目监督部门为**内蒙古广播电视台。**

九、联系人

招标人：**内蒙古广播电视台**

地址：**/**

联系人：**梁慧**

电话：**15848192900**

邮件：**nmtvlianghui@163.com**

招标代理机构:**内蒙古广播电视台**

地址：**/**

联系人：**梁慧**

电话：**15848192900**

邮件：**nmtvlianghui@163.com**

招标人或其代理机构主要负责人（项目负责人）：梁慧（签名）

招标人或其代理机构：________（盖章）

内蒙古广播电视台奔腾 OA 移动 APP 加固服务项目（二次）采购公告

内蒙古广播电视台采用竞争性谈判采购方式，采购奔腾 OA 移动 APP 加固服务项目（二次）欢迎符合资格条件的供应商前来报名参加。

一、项目概述：

（一）项目名称： 内蒙古广播电视台奔腾 OA 移动 APP 加固服务项目（二次）

（二）预算金额： 90000 元

（三）系统介绍： 依据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规要求，全面贯彻总体国家安全观，提升移动政务一体化安全防护能力，强化对奔腾 OA 移动 APP 中重要政务数据、敏感个人信息等的保护，解决奔腾 OA 移动 APP 存在的移动应用安全及合规风险问题。

二、采购内容要求

本项目为内蒙古广播电视台奔腾 OA 客户端安全整改项目，供应商需对所投项目完全响应，不得分解后响应。

序号	服务名称	数量	服务期限	备注
1	Android 加固服务	1	合同日起 1 年内同一 APP 不限次加固	不可使用进口技术加固
2	IOS 加固服务	1	合同日起 1 年内同一 APP 不限次加固	不可使用进口技术加固
3	鸿蒙应用加固服务	1	合同日起 1 年内同一 APP 不限次加固	不可使用进口技术加固
4	安卓、iso、鸿蒙应用测评服务	1	合同日起 1 年内同一 APP 不限次加固	不可使用进口技术加固
5	安卓、iso、鸿蒙应用合规服务	1	合同日起 1 年内同一 APP 不限次加固	不可使用进口技术加固

三、技术服务要求：

1. Android 加固服务（一年）　是否允许进口：否

要求项	子项	具体要求参数
Android 应用防代码逆向要求	DEX 加壳保护	支持对 DEX 文件进行整体加壳保护
	DEX 字符串加密	支持对 DEX 内的明文字符串进行加密保护
	DEX 类动态保护技术	支持对 DEX 内的代码进行动态抽取加密，并且在类被执行时不解密类内全部代码，只对被执行到的方法函数进行解密
	DEX 虚拟化保护技术	支持 DEX 虚拟化技术（VMP），能够将 DEX 代码转换为自定义的虚拟机指令，并以自定义虚拟机进行解释运行
	DEX 全量虚拟化保护技术	★支持 DEX 全量虚拟化技术（ALL-VMP），能够将 DEX 代码的通过 DEX 虚拟化技术进行全量保护
	SO 加壳保护	支持对 SO 进行加壳保护，防止反编译
	防查看伪代码	★支持对 SO 代码进行加密混淆，防止 IDA 的查看伪代码功能（IDA F5 功能）
	导入/导出函数隐藏	支持对 SO 内的函数表信息进行加密
	SO 动态清除	★支持 SO 动态清除技术，能够在 SO 执行过程中动态清除内存中的函数符号
	SO 防盗用绑定	★支持将 SO 文件同应用进行绑定，防止 SO 文件被非法盗用
Android 应用防二次打包要求	完整性保护	支持 APK 完整性验证，防止被非法篡改、二次打包
	资源文件加密	支持对应用内的资源文件、配置文件进行完整性保护，防止被篡改
	签名验证	支持对 APP 的开发者签名进行验证，防止被篡改签名、非法发布
Android 应用防数据泄露要求	数据加密	支持对本次存储的数据库文件、JS 文件、证书文件、配置文件等进行透明加密保护，防止查看和修改
Android 应用防调试要求	防动态调试	支持防动态调试，防止利用调试技术或工具对应用进行内存动态调试
	防内存注入	支持防内存注入，防止利用内存注入技术对应用进行恶意代码注入
	防内存 dump	支持防内存 dump，防止通过内存 dump 的方式分析内存数据
	防 xposed hook 攻击	支持防止利用 Xposed 工具进行 Hook 攻击
	防 Frida hook 攻击	支持防止利用 Frida 工具进行 Hook 攻击
Android 应用环境风险	防截屏	支持防止在应用运行过程中通过截屏非法窃取、捕获敏感数据，保护用户隐私数据安全、交易安全

检测与防护要求	防日志泄露	支持防止攻击者通过分析应用日志信息获取敏感信息
	防设备 root	支持设备 Root 检测，对应用运行环境进行检测，判断设备是否已经 Root 进，确认后能够阻止应用运行
	防模拟器	支持防止模拟器运行，对应用运行环境进行检测，判断是否运行在模拟器上，确认后能够阻止应用运行
	防应用多开	支持防 APP 多开，对应用运行环境进行检测，判断是否通过 VirtualApp 等工具双开、多开应用，确认后能够阻止应用运行
	防 USB 调试攻击	★支持防止通过 USB 连接电脑对手机应用进行调试
	防网络代理	★支持防止应用在开启网络代理的设备上运行
	防 VPN	★支持防止应用在开启 VPN 的设备上运行
	防屏幕模拟点击	★支持防止屏幕模拟点击脚本执行
	防定制化 ROM	★支持防止应用在定制化 ROM 运行
	防 Android 原生模拟器	防止 APP 在 Android 原生模拟器上运行
	防屏幕共享	★防止通过会议软件、远控软件共享应用屏幕
加固服务统计报告	自动生成加固服务报告	自动生成包含指定时间范围内的加固各种数据的服务统计报告
服务形式要求	交付形式	支持 SaaS 在线云交付、支持私有云软件交付、支持本地一体机交付
	使用方式	支持基于 Web 浏览器加固、支持 API 自动化集成工具加固、桌面客户端软件加固
	多语言系统	■支持简体、繁体、英语、韩语系统语言。

2. IOS 加固服务（一年）　是否允许进口：否

要求项	子项	具体要求参数
iOS 应用加固支持语言要求	Object-C/Object-C++	支持对 Object-C/Object-C++代码的源到源加固
	★Swift	支持对 Swift 代码的源到源加固
	C/C++	支持对 C/C++代码的源到源加固
iOS 防代码逆向要求	★控制流平坦化	支持在不改变语义的前提下，通过控制流平坦化将控制流进行混淆处理
	★不透明谓词	支持对跳转逻辑的判断值进行隐藏，增加攻击者逆向分析的难度
	符号混淆	支持对代码内的类名、方法名、函数名进行加密混淆
	★字符串加密	支持对字符串进行加密
	★虚假控制流	支持增加新的虚假控制分支，加大破解和分析原始控制流的难度
	多样性混淆	支持随机化混淆，每次混淆代码不一样

	★防反编译	防基于 IDA、Hooper 工具对 iOS 应用的反编译
	防 chatGPT 逆向	防止通过 chatGPT AI 工具对加固后的代码进行逆向
iOS 应用防调试要求	★静态防调试	在源代码内添加防调试校验代码，在函数执行时触发该保护功能，防止继续调试
	★静态防 Inline Hook	在源代码内添加防 Inline Hook 校验代码，在函数执行时触发该保护功能，防止 Inline Hook 攻击
	★静态防 Swizzling Hook	在源代码内添加防 Swizzling Hook 校验代码，在函数执行时触发该保护功能，防止 Swizzling Hook 攻击
	★静态防 Frida hook 攻击	在源代码内添加防 Frida hook 校验代码，在函数执行时触发该保护功能，防止 Frida hook 攻击
	★静态防 Cycript 注入	在源代码内添加防 Cycript 校验代码，在函数执行时触发该保护功能，防止 Cycript 攻击
	★静态防 Reveal 注入	在源代码内添加防 Reveal 校验代码，在函数执行时触发该保护功能，防止 Reveal 攻击
	★静态代码完整性保护	在源代码内添加防代码篡改校验代码，在函数执行时触发该保护功能，防止代码完整性被破坏
	■实时防调试	在 APP 运行时开启自动守护功能，随时对调试行为进行监测和阻断
	■实时防 hook	在 APP 运行时开启自动守护功能，随时对 hook 行为进行监测和阻断 支持防 Inline Hook 支持防 Swizzling Hook 支持防 fishhook
	■实时完整性保护	在 APP 运行时开启自动守护功能，对代码段进行完整性
iOS 应用防二次打包要求	绑定 App 包名	支持绑定 app 包名，篡改 App 包名将会导致应用运行闪退
	绑定 App 签名	支持绑定 app 签名，篡改 App 签名将会导致应用运行闪退
iOS 应用环境风险检测与防护要求	防设备越狱	支持自动检测设备是否越狱，在已越狱的设备上自动阻止 App 运行
	★防 AirPlay 投屏	支持对 AirPlay 投屏行为进行检测，当存在 AirPlay 投屏行为时阻断 App 的运行，防止用户被进行远程诱导性欺诈。
	防日志泄露	支持对代码内的系统日志输出进行阻断，防止敏感信息泄漏
	★APP 模糊化保护	支持 App 后台切换过程的屏幕模糊化，防止信息泄漏
	★https 证书校验	校验 https 证书的合法性，防止中间人攻击
	★防位置伪造	支持自动检测设备是否进行了位置伪造，当 APP 在伪造位置的设备上运行时，APP 会闪退处理，保护 APP 内依赖精准位置的业务不受位置信息篡改影响。
	防网络代理	支持自动检测是否存在网络代理设置，当发现 APP 在启用网络代理的环境上运行时，APP 会闪退处理，防止基

		于代理的抓包分析。
	★防共享屏幕	支持自动检测是否存在软件共享屏幕行为，在共享屏幕时运行 APP 会闪退处理，防止基于屏幕共享软件的远程信息窃取、诈骗攻击。
	防模拟器	支持自动检测是否在苹果电脑模拟器上运行，当 APP 运行在模拟器上时会闪退处理，防止基于模拟器的各种越权攻击。
	★证书文件加密	支持对证书文件加密，防止对证书文件的非法读取
	★证书文件绑定	支持对证书文件的绑定，自动绑定应用包名和签名，防止被非法盗用
	防截屏	支持检测截屏行为并弹窗提醒
	防 VPN	★防止通过 VPN 环境抓包分析
	防苹果电脑运行	★防止应用在苹果电脑（M 芯片）上运行
	防屏幕点击	★防止模拟屏幕点击脚本
操作要求	文本配置黑白名单	支持通过文本框形式直接快速输入黑白名单参数
	树装配置黑白名单	支持通过树状目录形式直接选择黑白名单范围
iOS 应用加固后审计与定位要求	■加固结果可视化	支持加固后输出的是混淆加密的源代码，能够直观查看加固后的代码。
	■代码逐行定位问题	支持代码逐行调试代码，准确、快速定位问题
	★SourceMap 源代码溯源功能	加固后支持查看出问题的加固代码所对应的原始代码行号
服务形式要求	■交付形式	支持 SaaS 在线云交付、支持私有云软件交付、支持本地一体机交付
	使用方式	支持基于桌面软件加固、支持命令行自动化加固
	■多语言系统	支持简体、英语系统语言。

3. 鸿蒙应用加固服务（一年）　是否允许进口：否

要求项	子项	具体要求参数
方舟 TypeScript 代码加固（ArkTS）	鸿蒙 ArkTS 代码文件整体混淆	支持对 ArkTS 代码文件进行整体的深度混淆加固，防止攻击者对 ArkTS 代码文件的逆向破解。
	鸿蒙 ArkTS 代码控制流平坦化混淆	支持对 ArkTS 代码内的代码分支、控制流程进行扁平化、平坦化混淆，让攻击者无法理解原代码处理流程和逻辑关系，防止攻击者对 ArkTS 代码的逆向破解。
	鸿蒙 ArkTS 代码变量字符串加密	支持对 ArkTS 代码内通过全局变量赋值的字符串内容进行加密处理，防止如 url、密钥等敏感字符串信息被攻击者读取和恶意利用。
	鸿蒙 ArkTS 代码函数字符串加密	支持对 ArkTS 代码函数体内引用的字符串内容进行加密处理，防止如用户名、姓名、账号等敏感字符串信息被攻击

		者读取和恶意利用。
	鸿蒙 ArkTS 代码参数名称混淆	支持对 ArkTS 代码的参数名称进行混淆处理，增加代码的不可阅读性，防止攻击者对 ArkTS 代码文件的逆向破解。
	鸿蒙 ArkTS 代码变量名称混淆	支持对 ArkTS 代码的变量名称进行混淆处理，增加代码的不可阅读性，防止攻击者对 ArkTS 代码文件的逆向破解。
	鸿蒙 ArkTS 文件加固范围自定义功能	支持指定不参与加固处理的 ArkTS 文件，支持正则表达式匹配规则，通过屏蔽无必要加固的文件，提高鸿蒙应用加固处理效率。
	鸿蒙 ArkTS 字符串加密范围自定义功能	支持指定 ArkTS 代码内不参与字符串加密的字符串，支持正则表达式匹配规则，通过屏蔽无必要加固的字符串，提高鸿蒙应用加固处理效率。
标准 TypeScript 代码加固（TS）	标准 TS 代码文件整体混淆	支持对 TS 代码文件进行整体的深度混淆加固，防止攻击者对 TS 代码文件的逆向破解。
	标准 TS 代码控制流平坦化混淆	支持对 TS 代码内的代码分支、控制流程进行扁平化、平坦化混淆，让攻击者无法理解原代码处理流程和逻辑关系，防止攻击者对 TS 代码的逆向破解。
	标准 TS 代码变量字符串加密	支持对 TS 代码内通过全局变量赋值的字符串内容进行加密处理，防止如 url、密钥等敏感字符串信息被攻击者读取和恶意利用。
	标准 TS 代码函数字符串加密	支持对 TS 代码函数体内引用的字符串内容进行加密处理，防止如用户名、姓名、账号等敏感字符串信息被攻击者读取和恶意利用。
	标准 TS 代码参数名称混淆	支持对 TS 代码的参数名称进行混淆处理，增加代码的不可阅读性，防止攻击者对 TS 代码文件的逆向破解。
	标准 TS 代码变量名称混淆	支持对 TS 代码的变量名称进行混淆处理，增加代码的不可阅读性，防止攻击者对 TS 代码文件的逆向破解。
	标准 TS 文件加固范围自定义功能	支持指定不参与加固处理的 TS 文件，支持正则表达式匹配规则，通过屏蔽无必要加固的文件，提高鸿蒙应用加固处理效率。
	标准 TS 字符串加密范围自定义功能	支持指定 TS 代码内不参与字符串加密的字符串，支持正则表达式匹配规则，通过屏蔽无必要加固的字符串，提高鸿蒙应用加固处理效率。
C/C++代码加固	SO 文件高级防逆向加固	支持对 C/C++开发的 SO 文件的高级防逆向保护处理，防止对核心 SO 文件的逆向破解。

4. 应用测评 （含安卓、iso、鸿蒙 一年不限检测次数） 是否允许进口：否

要求项	子项	具体要求参数

检测能力	检测对象	★产品具备 Android、iOS、Android SDK、iOS SDK、鸿蒙、微信小程序、微信公众号、web 应用、源码的漏洞扫描能力。
	检测方式	支持静态代码反编译与动态沙箱模拟攻击相结合的方式进行检测
	动态检测	支持至少 18 项动态检测项，包括但不限于：篡改二次打包风险、应用签名未校验风险、数据库注入漏洞、动态调试攻击风险、http 报文信息泄露风险、界面劫持风险、本地端口开放越权漏洞、ContentProvider 数据泄漏漏洞、动态注入攻击、root 设备运行检测、模拟器运行检测等、★Content Provider 导出组件目录遍历漏洞、★SharedPreferences 文件中存储敏感信息、★SQLite 数据库中明文存储敏感信息、Activity 导出组件拒绝服务漏洞、Service 导出组件拒绝服务漏洞、Broadcast Receiver 导出组件拒绝服务漏洞、Frida HOOK 运行风险。
Android 检测	覆盖检测对象	支持提交 apk、aab 格式的应用提交检测
	检测项数量及覆盖类别	支持至少 150 项测评项，覆盖自身安全、程序源文件安全、本地数据存储安全、通信数据传输安全、身份认证安全、内部数据交互安全、恶意攻击防范能力、第三方 SDK 信息、内容安全、应用优化建议等十项类别。
	基本信息	支持全自动化识别应用基本信息，信息维度包括但不限于 APK 文件名、软件名称、包名、软件大小、软件版本、MD5、签名信息、targetSdkVersion、minSdkVersion、分析时间等。
	权限信息	支持全自动化识别检测 App 的权限信息，包括申请的权限范围和使用权限范围，需要提供敏感权限、普通权限、自定义权限三大类别权限结果。
	行为信息	支持 app 行为信息检测，并输出行为函数名称、行为描述、行为风险等级、行为信息定位等信息。 可识别行为包括但不限于动态加载、删除文件、读写文件、反射调用等
	病毒扫描	★具备至少 3 种病毒引擎的检测能力，支持提供检测出的病毒信息及具体定位。
	第三方 SDK 信息	★SDK 分类基于《网络安全标准实践指南-移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》的常见 SDK 类型的标准分类。 SDK 信息可单独显示，报告显示信息至少包含 SDK 名称、开发者、类别、包名、描述、来源地址等 6 个维度信息。
	加固壳识别	能够识别至少 15 家主流加固厂商的加固特征
	界面劫持风险	★支持动态运行检测应用是否存在界面劫持风险，并可以提供界面劫持成功截图或日志信息

	自身安全检测	检测移动应用程序的基本信息，全景化呈现应用基本权限行为的声明和使用状态。检测项包括但不限于：基本信息、权限信息、行为信息、资源文件中的apk文件、权限过度声明风险、未保护的自定义权限风险、★应用测试模式发布风险、★来源安全检测、★应用权限安全、★控制力安全检测、越权行为检测等
	程序源文件安全	检测移动应用程序的源文件可能面临的安全风险。平台检测项包括但不限于：加固壳识别、java代码反编译风险、so文件破解风险、篡改和二次打包风险、Janus签名机制漏洞、资源文件泄露风险、应用签名未校验风险、代码未混淆风险、使用调试证书发布应用风险、仅使用Java代码风险、启动隐藏服务风险、应用签名算法不安全风险、单元测试配置风险、xml资源文件泄露风险、★友盟SDK越权漏洞、★恶意URL检测、txt资源文件敏感信息泄露风险、lua资源文件敏感信息泄露风险、html资源文件敏感信息泄露风险、★SharedPreferences文件中存储敏感信息、★SQLite数据库中明文存储敏感信息、★SQLite数据库缺少加密保护等。、★SO库导出符号泄露风险检测
	本地数据存储安全	检测移动应用本地数据存储可能面临的安全风险及漏洞。平台检测项包括但不限于：Webview明文存储密码风险、WebView存在潜在跨站脚本攻击风险、允许Webview访问本地任意脚本、明文数字证书风险、调试日志函数调用风险、数据库注入漏洞、RSA加密算法不安全使用漏洞、密钥硬编码漏洞、动态调试攻击风险、Webview远程调试风险、应用数据任意备份风险、敏感函数调用风险、数据库文件任意读写漏洞、全局可读写的内部文件漏洞、SharedPreferences数据全局可读写漏洞、SharedUserld属性设置漏洞、Internal Storage数据全局可读写漏洞、getDir数据全局可读写漏洞、FFmpeg文件读取漏洞、Java层动态调试风险、剪切板敏感信息泄露漏洞、内网测试信息残留漏洞、随机数不安全使用漏洞、代码残留URL信息检测、残留账户密码信息检测、残留手机号信息检测、残留Email信息检测、★明文泄漏风险、StrandHogg漏洞、ECB模式的AES/DEA加密方法不安全使用漏洞、OFB模式的AES/DEA加密方法不安全使用漏洞、外部储存卡存储数据风险、★私有IP地址暴露风险、★字节数组与字符串转换风险、★允许用户控制密钥长度风险、★初始化向量硬编码风险、SD卡数据泄露风险检测、★TDES加密算法不安全使用风险等
	通信数据传输安全	检测移动应用的通信数据传输中可能面临的安全隐患。平台检测项包括但不限于：HTTP传输数据风险、HTTPS未校验服务器证书漏洞、HTTPS未校验主机名漏洞、HTTPS允许任意主机名漏洞、Webview绕过证书校验漏洞、HTTP报文信息泄露风险、互联网环境检测、启用VPN服务检测、访问非中国内地服务器风险、★通信套接字安全等。
	身份认证安全	检测移动应用在身份认证上可能存在关键信息泄露的风险。平台检测项包括但不限于：界面劫持风险、输入监听风险、截屏攻击风险等

	内部数据交互安全	检测移动应用内部数据在内部组件交互过程中可能面临的风险漏洞。平台检测项包括但不限于：动态注册 Receiver 风险、Content Provider 数据泄露漏洞、本地端口开放越权漏洞、PendingIntent 错误使用 Intent 风险、Intent 组件隐式调用风险、反射调用风险、用户隐私信息检测、Activity 组件导出风险、Service 组件导出风险、Broadcast Receiver 组件导出风险、Content Provider 组件导出风险、Android-gif-Drawable 远程代码执行漏洞、Fragment 注入攻击漏洞、Intent Scheme URL 攻击漏洞、★覆盖权限验证风险、★仅定义 Provider writePermission 风险、★混淆代理人攻击风险、★未配置网络安全属性风险、★Receiver 权限未指定风险、★Broadcaster 权限未指定风险、★缺少导出的标志或组件权限、★ContentProvider 访问路径不安全配置风险、★粘滞广播使用风险、★so 包含执行命令函数风险等
	恶意攻击防范能力	通过动静态检测手段，分析移动应用对于恶意攻击手段的防范能力。平台检测项包括但不限于："应用克隆"漏洞攻击风险、动态注入攻击风险、Webview 远程代码执行漏洞、未移除有风险的 Webview 系统隐藏接口漏洞、zip 文件解压目录遍历漏洞、下载任意 apk 漏洞、Activity 导出组件拒绝服务漏洞、Service 导出组件拒绝服务漏洞、Broadcast Receiver 导出组件拒绝服务漏洞、从 sdcard 加载 dex 风险、从 sdcard 加载 so 风险、未使用编译器堆栈保护技术风险、未使用地址空间随机化技术风险、模拟器运行风险、Root 设备运行风险、不安全的浏览器调用漏洞、"寄生体"云控风险检测、★运行其他可执行程序漏洞、★libupnp 缓冲区溢出漏洞 ★Intent 重定向漏洞、★Content Provider 导出组件目录遍历漏洞、★fastjson 反序列化远程代码执行漏洞、★fastjson 远程命令执行漏洞、★UnityGhost 漏洞、★阿里云 OSS 凭证泄露、Frida hook 运行风险（动态检测）等
	HTML5 安全	支持检测集成 Html5 语言框架开发的 app。平台检测项包括但不限于：Web Storage 数据泄露风险、WebSQL 注入漏洞、InnerHTML 的 XSS 攻击漏洞等
	内容安全	支持检测应用代码层面的敏感信息。检测项包括但不限于：敏感词信息、敏感图片检测、敏感文本检测
	优化建议	支持检测应用在开发规范、加密等级升级等配置情况。检测项包括但不限于：全局异常检测、IP 地址检测、国密算法检测、SharedPreferences 使用 commit 提交数据检测、自启行为检测
iOS 检测	检测项数量及覆盖类别	★支持至少 68 项测评项，覆盖自身安全、二进制代码保护、客户端数据存储安全、数据传输安全、加密算法及密码安全、程序源文件安全和 iOS 应用安全规范、内容安全、HTML5 安全、第三方 SDK、身份认证安全等检测类别。
	自身安全检测	支持检测移动应用基本信息，全量化输出应用权限、行为、架构等信息。检测项包括但不限于：基本信息、权限信息、行为信息、证

		书类型检测、无法上架 App Store 风险、编译架构检测等。
	二进制代码保护	支持检测移动应用二进制代码保护情况。检测项包括但不限于：代码未混淆风险、未使用地址空间随机化技术风险、未使用编译器堆栈保护技术风险、注入攻击风险、可执行文件被篡改风险。
	客户端数据存储安全	支持检测移动应用客户端数据存储安全。检测项包括但不限于：动态调试攻击风险、输入监听风险、调试日志函数调用风险、webview 组件跨域访问风险、越狱设备运行风险、数据库明文存储风险、动态库信息泄露风险、★FFmpeg 文件读取漏洞、★出口合规证明、★明文泄漏风险、★残留 Email 信息检测、★残留手机号信息检测、★日志泄漏风险检测、★cer 证书文件未加密风险、★私钥存储文件未加密风险
	数据传输安全	支持检测移动应用数据传输安全情况。检测项包括但不限于：HTTP 传输数据风险、HTTPS 未校验服务器证书漏洞、URL Schemes 劫持漏洞、联网环境检测
	加密算法及密码安全	检测项包括但不限于:AES/DES 加密算法不安全使用漏洞、弱哈希算法使用漏洞、随机数不安全使用漏洞
	程序源文件安全	检测项包括但不限于：明文字符串泄露风险、外部函数显式调用风险、系统调用暴露风险、创建可执行权限内存风险、篡改和二次打包风险、SQLite 内存破坏漏洞、格式化字符串漏洞、txt 资源文件敏感信息泄露风险、★lua 资源文件敏感信息泄露风险、html 资源文件敏感信息泄露风险、xml 资源文件敏感信息泄露风险、js 资源文件敏感信息泄露风险、★资源文件泄漏风险、★代码反编译风险
	iOS 应用安全开发规范	检测项包括但不限于：XcodeGhost 感染漏洞、不安全的 API 函数引用风险、Private Methods 使用检测、ZipperDown 解压漏洞、iBackDoor 控制漏洞、未使用自动管理内存技术风险、内存分配函数不安全风险、自定义函数逻辑过于复杂风险、★UnityGhost 漏洞、★xcode 版本检查、★使用企业证书发布应用风险检测、★Intel 模拟器运行风险
	HTML5 安全	检测项包括但不限于：Web Storage 数据泄露风险、 InnerHTML 的 XSS 攻击漏洞
	第三方 SDK	★SDK 分类基于《网络安全标准实践指南-移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》的常见 SDK 类型的标准分类。 SDK 信息可单独显示，报告显示信息至少包含 SDK 名称、开发者、类别、描述、来源地址等 5 个维度信息。
	身份认证安全	检测 iOS 应用在★共享屏幕和★airplay 投屏场景下的信息泄露的风险。
	内容安全	支持检测应用代码层面的敏感信息。检测项包括但不限于：敏感词信息

	检测对象	支持上传 aar、★zip、★rar、★jar 格式的 SDK 文件进行检测
★鸿蒙检测	检测对象	支持上传 hap 格式的鸿蒙应用文件进行检测，
	检测项数量及覆盖类别	支持不少于 100 项检测项，检测类别覆盖本地数据存储安全、内部数据交互安全、通信数据传输安全、程序源文件安全、自身安全、恶意攻击防范、优化建议、HTML5 安全、身份认证安全
	自身安全	检测项包括但不限于：基本信息、权限信息、★缺少权限申请理由、★应用使用的权限未定义、★自定义权限以 ohos 开头风险、★动态类加载路径检测等、第三方 SDK 检测、控制力安全、未保护的自定义权限风险、应用权限安全、权限过度声明、敏感词检测等。
	通信数据传输安全	检测项包括但不限于：HTTPS 未检验主机名漏洞、明文流量传输、HTTPS 未校验服务器证书漏洞、WebView 绕过证书校验漏洞、WebView 加载任意 url 风险、HTTPS 允许任意主机名漏洞、互联网环境检测、访问境外服务器检测、通信套接字安全、HTTP 传输数据风险、启用 vpn 服务检测、WebView 绕过证书校验风险等。
	程序源文件安全	检测项包括但不限于：★初始化向量硬编码风险、代码未混淆风险、so 文件破解风险、未使用地址空间随机化技术风险、未使用编译器堆栈保护技术风险、Java 代码反编译风险、仅使用 Java 代码风险、恶意 URL 检测、加固壳识别、应用签名算法不安全风险、单元测试配置风险、友盟 SDK 越权漏洞等。
	本地数据存储	检测项包括但不限于： 应用数据任意备份风险、密钥硬编码漏洞、调试日志函数调用风险、RSA 加密算法不安全、随机数不安全使用漏洞、剪切板敏感信息泄露、代码残留 URL 信息检测、内网测试信息残留漏洞、明文数字证书风险 数据库文件任意读写漏洞、 允许用户控制密钥长度风险、 ECB 模式的 AES/DEA 加密方法不安全使用漏洞、 ffmpge 文件读取漏洞、 getDir 数据全局可读写漏洞、 全局可读写的内部文件漏洞、 Hash 算法不安全、 Internal Storage 数据全局可读写漏洞、 OFB 模式的 AES/DEA 加密方法不安全使用漏洞、 内网 IP 地址泄露风险、 残留 Email 信息、 敏感函数调用风险、

		残留账户密码信息检测、 残留手机号信息检测、 SharedPreferences 数据全局可读写漏洞、 外部储存卡存储数据风险、 字节数组与字符串转换风险、 WebView BadKernel 远程代码执行漏洞、 Webview File 域同源策略绕过、 WebView 远程调试风险、 WebView 明文存储密码风险等。
	内部数据交互安全	检测项包括但不限于：★Page 组件导出风险、Data 组件导出风险、★Service 组件导出风险、★公共事件劫持风险、★公共事件订阅检测、★DataAbility 设置合理的读写权限、 Android-gif-Drawable 远程代码执行漏洞、 Intent Scheme URL 攻击漏洞、 覆盖权限验证、 ★page 劫持检测、 PendingIntent 错误使用 Intent 风险、 权限检查、 反射调用风险等
	恶意攻击防范能力	检测项包括但不限于：zip 文件解压目录遍历漏洞、“寄生推”云控风险、不安全的浏览器调用、运行其他可执行程序漏洞、从 sdcard 加载 dex 风险、从 sdcard 加载 so 风险、libupnp 缓冲区溢出漏洞、未移除有风险的 Webview 系统隐藏接口漏洞、Webview 远程代码执行漏洞等。
	优化建议	检测项包括但不限于：全局异常捕获处理、IP 地址检测、SharedPreferences 使用 commit 提交数据检测、自启行为、SM2 国密算法检测、SM3 国密算法检测、SM4 国密算法检测等。
	HTML5 安全	检测项包括但不限于：innerHTML 的漏洞、Web Storage 数据泄露风险、 WebSQL 漏洞
	身份认证安全	检测项包括但不限于：使用调试证书发布应用风险、截屏攻击风险
平台功能	数据统计	■支持统计账号提交总任务数量、月度任务数量、风险总数量、问题总数量等数据信息。 ■任务数据与样本统计支持以图表方式展现近一个月内数据趋势。
		■支持以日、周、月维度统计应用安全性，应用平均得分

		■支持以月度为单位，以图表形式体现应用得分分布图 ■支持以月度为单位，图表形式展示各个检测项目的风险检出率 ■支持以月度为单位查询单个检测项的风险检出率，及存在此风险的相关被检测应用信息。
	批量操作	★支持批量下载 word、excel、pdf 格式的检测报告
		支持批量提交不少于 50 个应用进行检测
		支持批量下载被检测应用源文件（apk、ipa、aar、zip、jpg、png 等）
		■支持批量统计分析，可对至少 50 个应用的测评结果统计分析，并且以报告的形式展示，包括应用得分、问题项目发生占比等。
	任务日志	
	版本管理	■支持应用安全性版本管理，支持应用不同版本之间安全性对比图表展示，支持输出版本对比分析报告;
	检测结果编辑	★支持在线编辑检测结果，可编辑内容包括但不限于安全与否、存在漏洞的文件详情、人工验证截图上传等，支持输出编辑完成后的最终版报告。
	检测源数据导出	支持 Android 检测结果源数据导出，支持根据用户账号、检测时间进行筛选，导出相应的检测结果源数据 excel。
	检测模板	支持系统自带模板 支持用户自定义增删检测模板 ★检测模板可根据检测方式（动态、静态）、报告语言、报告输出类型等维度灵活配置检测项目。 ★支持导出检测模板
	用户管理	支持用户在授权范围内自定义角色分工，并自主创建账号，实现多用户管理功能，至少提供管理员和普通用户两种角色
	管理功能（仅支持私有化部署场景交付）	★支持自定义检测规则，根据业务需求自主更改检测项分值、分级标准、风险等级、风险描述、检测步骤、修复建议等信息，并支持导入导出备份功能
		★支持 Android 应用通过路径匹配、模糊匹配、文件匹配等方式，对部分检测项或全局检测项设置白名单，并提供相关增删改查管理功能
		支持设置 Android/iOS 应用敏感词库管理功能，可自定义增删改敏感词库内容。
		支持自定义修改平台界面 UI 设置，包括但不限于：平台登录背景图、logo、平台介绍、平台名称等信息

		支持自定义报告内容，包括但不限于：报告标题、logo、水印、附录、公司介绍信息等。
		支持产品授权更新功能
		支持磁盘管理功能，可通过平台定期自动/手动清理系统各类缓存信息，释放系统空间，维持系统运行内存稳定。
		支持检测任务队列调整，管理员可一键置顶或取消某项排队中任务。
		★支持 Android SDK 的后台配置管理，可自主添加或删除第三方 SDK，添加后的 SDK 支持在 App 中进行识别和安全检测。
	日志管理	★支持查看导出用户操作日志
		★支持单个任务运行日志信息下载。适用检测对象：Android、aab、iOS、Android SDK、iOS SDK、鸿蒙、小程序/公众号
	报告输出	支持在线预览查看报告内容，报告内容包括：检测评分、检测数据总览、检测数据图表、检测结果详情等信息
		检测项支持查看风险描述、风险等级、检测结果、检测步骤、检测详情（定位至文件，可输出有风险代码段或日志信息）、修复建议等信息
		★支持在线编辑报告内容，并重新生成编辑后的报告。
		★提交 apk 检测时，支持单独输出其集成的第三方 SDK 风险信息。第三方 SDK 风险报告支持在线查看及报告下载。
		★支持按风险等级、检测结果维度显示报告信息，并生成对应的简版测评报告
		★支持输出单个应用多版本安全检测结果分析报告
		★支持自动化输出对标 OWASP Mobile TOP10 的检测报告。
底层引擎支持	SDK 库	★Android SDK 信息库存量至少 6000+ ★iOS SDK 信息库存量至少 1000+

5. 应用合规（含安卓、iso、鸿蒙 一年不限检测次数） 是否允许进口：否

要求项	子项	具体要求参数
App 基本信息检测	Android 基本信息	支持检测并列出 Android App 的基础信息，包括但不限于：软件名称、包名、类型、软件大小、软件版本、targetSdkVersion、minSdkVersion、签名信息，安装包文件名、散列值（MD5、SHA-1、SHA-256）、App 是否加固

	iOS 基本信息	支持检测并列出 iOS App 的基础信息，包括但不限于：软件名称、包名、类型、软件大小、软件版本、签名信息，安装包文件名、散列值（MD5、SHA-1、SHA-256）
静态权限检测	Android 声明权限	■分析列出 Android App 声明的权限，提供权限名称、权限含义、权限类型、保护级别、是否为敏感权限、是否使用、是否为可收集个人信息权限
	iOS 声明权限	分析列出 iOS App 声明的权限，提供权限名称、权限含义、是否使用、是否为可收集个人信息权限等信息；
	使用权限	列出 App 及 SDK 在运行过程中可能使用的权限（静态分析）
		列出使用权限所对应的代码路径、关键代码、代码片段（仅适用 Android）
	声明权限但未使用情况	检测并列出 App 声明但在运行期间可能未使用的权限，提供权限含义、权限类型、保护级别、是否为敏感权限等信息；
成分检测	Android SDK 信息	检测并列出 Android App 集成的 SDK 的名称、包名、开发者、类别、描述、来源等信息；
	iOS SDK 信息	检测并列出 iOS App 中集成的 SDK 的名称、开发者、类别、描述、来源等信息；
行为检测	数据通信情况	提供 App 进行数据通信的域名、IP 地址、IP 归属地、检测状态、协议、通信次数等信息，支持查看数据通信的具体内容；
	个人信息明文传输行为	支持检测 App 的网络数据通信及 cookie 中是否明文传输了个人信息
	数据跨境传输行为	检测 App 是否存在数据跨境传输行为；
	个人信息明文存储行为	列出 App 存储明文个人信息的情况，包括：时间、代码片段、存储位置、明文个人信息、个人信息类别，明文个人信息以红色区分；
	个人信息采集行为	列出 App 在检测过程中的个人信息采集行为，行为所依赖的权限、行为发生的时间、总次数、平均每分钟发生的最高次数，提供对应行为的堆栈信息，便于问题定位；
		支持根据行为名称进行筛选；支持根据检测状态进行筛选；支持从“行为”“主体”两种维度展示个人信息采集行为；
	声明权限但未使用情况	检测并列出 App 声明但在运行期间可能未使用的权限，提供权限含义、权限类型、保护级别、是否为敏感权限等信息；
	自启动/	检测 App 是否存在自启动/关联启动行为（Android）

	关联启动行为	
	热更新能力检测	支持检测 App 是否存在热更新能力（Android）
	一揽子授权行为	检测 App 是否存在一揽子授权行为（Android）
合规检测	隐私政策	自动合规检测时支持对 App 隐私政策文本进行自动化获取及显示，支持手动上传 App 隐私政策
	合规评估	★内置 191 号文、164 号文、165 号文、292 号文、26 号文、自评估指南、国标 35273、国标 41391 等多套合规检测模板，可依据检测模板对移动应用程序进行合规检测，输出 word、pdf 报告 （2）支持在 Web 页面进行人工检测并编辑合规检测结果，输出全量合规检测报告
深度	自动化脱壳	
产品基础功能	首页统计视图	■支持展示应用检测数据统计信息，对检测趋势及问题情况进行统计预览，方便呈现总体检测情况：支持显示最近 7 天/最近 30 天/最近 90 天/全部时间检测的 APP 数量；支持统计显示被测 APP 总数、已完成检测的 App 总数、待检测任务总数、待人工介入的应用数；支持统计显示 App 中集成的 SDK、使用权限、不合规行为 TOP10 排行；
	样本管理	新增样本上传方式：支持本地单个/批量上传与 URL 单个/批量下载方式上传，支持显示上传进度；
		支持根据时间、应用名称、应用类型、平台类型进行查询；
		支持单个/批量应用的下载、删除；
	任务管理	支持进行单个/批量检测，每个检测应用支持显示子任务状态，
		★支持查看实时检测详情， 方便用户在测试过程中实时查看应用行为，能够提升测试效率及合规评估效果（截图）
		支持对任务进行单个/批量终止、删除、重新检测、下载报告；
		支持根据任务名称、应用名称、创建者、检测时间、平台类型、任务类型、任务状态等条件进行筛选；
		人工检测时支持页面录屏功能，用于证据留存；
		人工检测时支持横竖屏切换

		★任务类型支持：全自动、自动+人工、纯人工 三种方式，满足批量自动化检测与人工深度检测场景，人工可对自动化合规检测结果进行审核修订，大大降低提升合规检测效率；（iOS 目前只支持纯人工任务类型）（截图）
		支持对应用不同版本之间检测结果进行对比，帮助用户分析不同版本的集成 SDK、权限及合规结果的差异。
	报告管理	支持对已完成任务生成的报告进行统一管理，支持单个/批量下载已完成任务的报告，含 Word 与 PDF 格式；支持重新生成报告，自定义输出检测内容；
		报告模板配置，支持创建报告模板，自定义报告模板名称、报告标题、logo、封面、页眉、页脚、单位名称、公司介绍；
	真机管理	■支持对平台所连接的检测真机进行管理查看，修改用途，方便用户及时了解真机资源使用情况，并及时配置真机属性
	知识库管理	支持查询下载常见合规标准政策原文
	内容识别配置	（1）内容识别配置支持自定义内容识别关键字 （2）支持对内置规则进行编辑、删除、启用、禁用
	合规检测策略配置	★支持自定义合规检测项、检测点
	合规检测模板配置	★支持自定义配置增加合规检测模板
	SDK 配置	支持自定义添加 SDK，提升 SDK 识别能力
	IP 地址归属地配置	支持用户自主配置 IP 地址与归属地映射关系，形成适合用户的 IP 库
	网站设置	支持自定义网站 logo、网站 icon、产品名称；
	磁盘管理	■支持通过手动/自动方式清理磁盘空间，便于用户维护系统空间，提升运维效率；
	系统日志	支持记录用户操作日志，包括账号登录、上传样本、创建任务等；便于管理员对系统使用情况进行回溯审查，排查可疑 IP 登录操作行为
	API 管理	（1）支持 API 对接，可通过 API 进行新建任务、上传 App、查询任务列表、查询任务详情、下载报告等操作 （2）支持对用户进行 API 权限控制，可限定其 API 权限调用范围
	系统升级	支持在页面进行系统升级，上传升级包即可进行

	客户端升级	■客户端升级，支持在页面上传合规检测客户端，方便对真机客户端检测软件进行统一升级

四、商务要求

支付方式：项目交付完成并经采购人验收合格后，供应商开具并交付与应付金额相符的合法有效增值税专用发票，采购人应在收到发票后十个工作日内，向中标供应商一次性支付全部费用。是否缴纳履约保证金：是。

“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

技术参数（服务）解答联系人：王猛

联系电话：18604713809

五、供应商的资格要求

1.供应商须符合《中华人民共和国政府采购法》第二十二条规定条件；

2.具有有效的营业执照；

3.根据《财政部关于在政府采购活动中查询及使用信用信息记录有关文件的通知》（财库【2016】125号），通过信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询信息，对列入“失信被执行人”“重大税收违法案件当事人名单”“政府采购严重违法失信名单”的供应商，拒绝参与采购活动；

4.中国裁判文书网(http://wenshu.court.gov.cn/）无行贿犯罪记录；

5.供应商须提供参加采购活动前三年内，在经济活动中无重大违法记录的承诺书；

6.供应商须提供近一年任意一个月的纳税凭证；

7.供应商须提供近一年经会计师事务所或审计机构审计的财务报

告，或基本开户行出具的资信证明；

8.本项目不接受联合体响应，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招标活动。

六、获取谈判文件方式

本公告内容为包含所有技术参数与配置，不需要现场报名，供应商按要求直接递交响应文件。

七、响应文件内附资料如下

1.法定代表人身份证正、反面，加盖公章；

2.非法定代表人报名，出具经法定代表人签字、公司盖章的“授权委托书”及本人身份证复印件，加盖公章；

3.营业执照加盖公章；

4.银行开户许可证（银行开户信息）加盖公章；

5.信用中国截图加盖公章；

6.在“国家企业信用信息公示系（http://gsxt.saic.gov.cn/）中未被列入严重违法失信名单（黑名单）信息加盖公章；

7.中国裁判文书网(http://wenshu.court.gov.cn/）无行贿犯罪记录加盖公章；

8.供应商须提供近一年任意一个月的纳税凭证加盖公章；

9.供应商须提供参加采购活动前三年内，在经济活动中无重大违法记录的承诺书加盖公章；

10.供应商须提供近一年经会计师事务所或审计机构审计的财务报告或基本开户行出具的资信证明加盖公章；

11.响应文件方案及报价。

以上材料加盖公章，胶装正本一份、副本两份。材料不完整，视为无效投标。

供应商提供营业执照副本扫描件、授权委托书、法定代表人身份证及授权委托人身份证正反面、企业联系单（包括公司名称、联系人、联系电话、电子邮箱、联系地址等），2025 年 12 月 18 日 17 时前以电子版方式发送邮箱 nmtvlianghui@163.com 进行报名资料审核（未在上述时间发送资料到指定邮箱的，视为无效报名，不接受其报价），邮件注明：公司名称、项目名称、联系方式。

响应文件需在信封的封装处粘贴采购公告中指明的项目名称并加盖供应商公章。

开标时，供应商需携带身份证到现场。本项目预算金额即为报价的最高限价，报价超出最高限价的将被视为无效投标。

八、响应文件递交截止时间、开标时间、地点

1.响应文件现场递交截止时间：2025 年 12 月 19 日 15 时 30 分；

2.开标时间：2025 年 12 月 19 日 15 时 30 分；

3.开标地点：内蒙古广播电视台。

采购单位名称：呼和浩特市成吉思汗西街 1 号院内蒙古广播电视台 B 座 13 楼 1312 会议室

递交地址：呼和浩特市回民区成吉思汗西街 1 号

邮政编码：010010

联系人：梁慧

联系电话:15848192900

内蒙古广播电视台

2025 年 12 月 15 日