第六章　技术需求

货物需求一览表

包号	系统名称	具体标的名称	数量	交付期	试运行期	交付地点
1	数据安全风险识别及漏洞扫描系统	数据安全风险识别及漏洞扫描系统开发	1 套	120 日历日	180 日历日	北京市海淀区温泉镇高里掌路 1 号院 21 号楼 304 号 中国信通院翠湖办公区大数据应用与安全创新实验室
2	异常行为识别与数据流量分析系统	异常行为识别与数据流量分析系统开发	1 套			

注：

1.交付期从合同签订之日开始起算，至软件/系统通过初步验收，具备上线试运行条件为止。

2.运行期从交付期第二日开始算起，到可以终验为止。试运行期内所有出现的问题应得到解决，软件系统运行稳定。

3.质保期自买卖双方验收签署“验收报告”的日期开始计算。

技术规格

注：

1、本章中加注“*”或“★”号的条款，投标人应完全满足并提供相关正面应答或承诺，否则将被视为实质性不响应，其投标将被拒绝；若技术规格中对“*”或“★”号条款还有证明材料要求的，投标人还应按照招标文件要求提供相应的证明材料，否则也将被视为实质性不响应，其投标将被拒绝。

2、本章中未加注“*”或“★”号的条款，投标人应进行响应并提供相关正面应答或承诺，否则将被视为不满足招标文件要求；如技术规格中对未加注“*”或“★”号的条款有证明材料要求的，投标人应按照招标文件要求提供相应的证明材料，否则也将被视为不满足招标文件要求。

3、以上 2 条所指的证明材料，如没有特殊说明，指生产厂家官方网站截图或产品白皮书或所投产品在相应系统上正常运行截图或第三方机构检验报告或产品彩页，并加盖投标人公章。招标文件中有其他证明材料要求的，以具体要求为准。

第 1 包

一、详细技术需求

1.1 采购用途

现有不良移动应用（App）数据安全风险扫描工具，一般仅支持静态扫描、代码特征识别等通用识别技术，已无法适应不良移动应用形态日益复杂、行为高度隐蔽、技术对抗不断升级的现状。依据行业标准《不良移动应用程序分类及判定方法》相关要求，针对金融、视频、通信等特定应用场景，定制开发深度数据安全识别模块，建成覆盖不良 App 及相关 SDK、小程序、API 数据安全风险、漏洞的扫描识别与取证能力，将为不良移动应数据治理工作提供急需的工具支持，也为移动互联网数据安全研究工作提供基础科研环境，填补针对不良移动应用动态攻击、流量分析以及技术对抗能力验证技术的空白，为提升行业数据安全治理水平提供助力。

1.2 需实现的功能要求

系统需实现针对 Android App、iOS App、SDK 产品、鸿蒙应用、微信公众号/小程序的自动化安全风险及漏洞扫描，通过深度静态代码扫描、动态模拟攻击等技术识别相关载体内存在的数据安全风险漏洞，实现针对不良移动应用产品数据安全情况的全面评估，准确定位问题根源，呈现详细的问题详情，并提供代码修复示例，充分结合国家法律法规、标准要求，满足不良移动应用监管支撑工作需要，促进移动应用行业数据安全生态良性发展，维护国家、社会数据安全及人民群众合法利益。

1.3 详细技术要求

1.3.1 基本要求

1.3.1.1 ★ 扫描对象要求

具备针对 Android App、iOS App、SDK、鸿蒙系统 App、微信小程序、微信公众号的数据安全风险及漏洞识别能力。

1.3.1.2 △ 扫描方式要求

具备包含静态代码反编译与动态沙箱模拟攻击相结合在内的多种扫描方式，并提供风险定位及代码详情展示、证据记录留存能力。

1.3.1.3 △ 误报率要求

系统数据安全风险识别及漏洞扫描结果整体误报率不超过 5%。

1.3.2Android 扫描

1.3.2.1 △ 界面劫持风险识别能力

具备动态运行检测应用是否存在界面劫持风险能力，并提供界面劫持成功截图或日志信息。

1.3.2.2 # 恶意程序/病毒识别能力

具备至少 3 种病毒引擎的识别能力，并提供病毒信息。

1.3.2.3 △ 行为风险识别能力

具备呈现 App 基本权限行为声明和使用状态能力，包括但不限于：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、App 测试模式发布风险、来源安全、App 权限安全、控制力安全、越权风险等。

1.3.2.4 # 程序源文件扫描能力

具备识别 App 源文件可能面临的安全风险能力，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、App 签名未校验风险、代码未混淆风险、使用调试证书发布 App 风险、仅使用 Java 代码风险、启动隐藏服务风险、App 全名算法不安全风险、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 识别、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、SO 库导出符号泄露风险识别等。

1.3.2.5 # 数据传输风险识别能力

具备识别 App 数据传输中可能面临的安全隐患能力，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、联网环境识别、启用 VPN 服务识别、访问非中国内地服务器风险、通信套接字安全等。

1.3.2.6 △ 身份认证风险识别能力

具备识别 App 身份认证上可能存在关键信息泄露风险的能力，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。

1.3.2.7 △ 攻击防范机制扫描能力

具备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，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、"寄生推"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。

1.3.3iOS 扫描

1.3.3.1 △ 基本信息识别能力

具备自动化 App 基本信息识别能力，包括但不限于识别 IPA 文件名、软件名称、包名、软件大小、软件版本、MD5、签名信息、分析时间等。

1.3.3.2 # 本地安全风险识别能力

具备识别 App 本地数据安全风险能力，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、残留手机号信息。

1.3.3.3 △ 程序源文件扫描能力

具备识别 App 代码源文件内安全风险、漏洞能力，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。

1.3.4SDK 风险扫描

1.3.4.1 # 扫描对象要求

支持 aar、zip、rar、jar 格式的 SDK 文件安全风险识别及漏洞扫描。

1.3.4.2 △ 可识别风险项要求

具备针对 SDK 产品的安全风险、漏洞识别能力，包括但不限于 SDK 自身安全、程序源文件安全、本地数据存储安全、内部数据交互安全、恶意攻击防范能力等安全风险类别，可识别风险、漏洞种类不少于 80 种。

1.3.5 鸿蒙系统扫描

1.3.5.1 △ 基本安全扫描能力

具备鸿蒙系统 App 基本信息、权限信息、缺少权限申请理由、使用的权限未定义、自定义权限以 ohos 开头、动态类加载路径识别、第三方 SDK 识别、控制力安全、未保护的自定义权限、权限过度声明等风险的识别能力。

1.3.5.2 △ 程序源文件安全风险识别能力

具备鸿蒙系统 App 初始化向量硬编码、代码未混淆、so 文件破解、未使用地址空间随机化技术、未使用编译器堆栈保护技术、Java 代码反编译、仅使用 Java 代码、恶意 URL 识别、加固壳识别、签名算法不安全、单元测试配置、SDK 越权漏洞等风险的识别能力。

1.3.5.3 △ 内部数据交互风险识别能力

具备鸿蒙系统 App Page 组件导出、Data 组件导出、Service 组件导出、公共事件劫持、公共事件订阅识别、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 劫持识别、PendingIntent 错误使用 Intent、权限检查、反射调用等风险的识别能力。

1.3.5.4 △ HTML5 安全风险识别能力

具备鸿蒙系统 App innerHTML 的漏洞、Web Storage 数据泄露风险、WebSQL 漏洞等风险的识别能力。

1.3.5.5 △ 身份认证安全风险识别能力

具备鸿蒙系统 App 调试证书发布、截屏攻击等风险的识别能力。

1.3.6 微信公众号级小程序安全风险扫描

1.3.6.1 # 数据泄露风险识别能力

具备针对微信公众号、小程序 Robots 敏感目录泄露、服务器端 Banner 泄漏、备份文件泄漏。ELMAH elmah.axd/errorlog.axd 信息泄露、CVS 文件泄露、SVN 文件泄漏、DS_Store 文件泄漏、Apache 不安全配置漏洞、Web 页面源代码敏感信息识别、Web 页面源代码注释信息识别、不存在的 URL 异常处理识别、非法字符异常处理等安全风险、漏洞的识别能力。

1.3.6.2 △ 组件漏洞扫描能力

具备针对微信公众号、小程序破壳（ShellShock）漏洞、心脏滴血漏洞、SSL POODLE 漏洞、SSL DROWN 攻击漏洞、SSL FREAK 漏洞等风险的识别能力。

1.3.6.3 △ HTTP 不安全配置识别能力

具备针对微信公众号、小程序不安全跨域资源共享配置、HTTP 传输不安全策略等风险的识别能力。

1.3.7 辅助功能

1.3.7.1 △ 数据统计功能

具备统计扫描任务数量、月度任务数量、发现风险总量、风险分布情况等数据信息统计能力，支持以图表方式展现近一个月内数据趋势，以日、周、月维度统计 App 安全性，以月度为单位，图表形式展示各个识别项目的风险检出率、以月度为单位查询单个识别项的风险检出率，并关联历史扫描中发现存在此风险的 App 信息能力。

1.3.7.2 △ 日志管理功能

具备单个任务运行日志信息下载功能，适用 Android、iOS、SDK、鸿蒙、小程序/公众号等全部扫描识别任务。

1.3.7.3 △ 报告输出功能

具备按风险等级、识别结果维度显示报告信息并生成对应的扫描报告功能，支持输出单个 App 多版本安全扫描结果分析报告、对标 OWASP Mobile TOP10 分

析报告等多类型报告。

1.3.7.4 △ 管理功能

具备自定义检测规则机制，可自主更改分值、分级标准、风险等级、风险描述、检测步骤、修复建议等信息。

支持自定义修改系统界面 UI 设置，包括但不限于：系统登录背景图、logo、系统介绍、系统名称等信息。

支持自定义报告内容，包括但不限于：报告标题、logo、水印、附录、介绍信息等。

1.4 性能要求

本次采购软件系统需要满足如下性能要求：

1.批量上传不良移动应用样品文件时（10 个以内），CPU 占用率不超过 20%，内存占用率不超过 70%；

2.批量扫描、识别时（10 个以内），CPU 占用率不超过 60%，内存占用比不超过 70%；

3.CPU 平均消耗不超过 40%，内存平均消耗不超过 60%。

1.5 安全要求

本系统不与院业务系统产生交集，线下运行，内网、外网均无访问接口，为独立运作的安全扫描类工具，无需等保定级。但系统需要遵循“网络安全法”的相关要求，部署前开展渗透测试，确保不存在高危漏洞，并提供渗透测试报告。

1.6 其他要求

产品支持部分国产化服务器、中间件、数据库等，并能够提供适配证书。

二、服务需求

1.★质保期

1.1 质保期自买卖双方在签署的终验验收单的日期开始计算，卖方提供免费质保期为(3)年。

1.2 在质保期内，如果卖方出售的相同型号产品发生硬件和软件更新/升级，卖方应将新发布的硬件和软件更新/升级在一个月内提供给买方，并到现场给予支持。

1.3 卖方需在投标总价以外单独列出质保期后的年度质保费用，卖方承诺买

方可在过质保期后以此价格向卖方购买保修服务。

2、培训内容及要求

提供不少于 3 人天的培训，培训内容包括但不限于系统使用培训、系统运维培训、Android App 风险识别培训、iOS App 风险识别培训、微信小程序、公众号风险识别培训等。培训费用均由投标人负责。

3、项目文档要求

序号	文档名称	说 明	提交阶段
1	需求规格说明书	系统开发最依据	需求完成后提交
2	设计文档	说明系统结构、业务流程、系统功能	实施开发前提交
3	测试用例	试运行测试用例	初验提交
4	初验报告	按照初验要求提交	初验提交
5	终验报告	按照终验要求提交	终验提交
6	用户手册/使用手册	按照终验要求提交	终验提交
7	培训资料文档	按照培训前提交	培训前提交
8	源代码	作为项目交付物提供	终验提交

4、项目团队要求

项目团队需包括但不限于项目经理、技术负责人、开发运维人员，项目团队人数不少于 4 人。

5、项目进度要求

项目启动后 60 日历日内完成该模块应基本架构、样品基本信息识别、自动化代码反编译、化代码脱壳等核心功能开发；

120 日历日内完成静态风险识别引擎、动态沙箱模拟攻击检测等功能开发并进入试运行阶段。

试运行期不应少于 180 日历日，期间对系统运行效率、误报率、稳定性等指标进行测试、评估，并接入至少 3 种病毒引擎检测能力，能够识别至少 10 家主流加固厂商的加固特征。并根据试运行情况及漏洞库、风险库升级情况增补、完善引擎规则及脱壳工具能力、识别规则自定义、风险分析报告自动生成等辅助功能。

6、★所有权、知识产权归属及要求

本次采购所产生的全部技术成果及衍生品的所有权及知识产权归属买方所有。

7、技术支持及服务响应

7.1 甲方可以通过访问网页接入的方式获得最新的技术信息以及其他资料。

7.2 乙方将最新的技术信息和资料及时主动提供给甲方。

7.3 技术响应时间要求：

1.质保期内，乙方免费为甲方提供技术指导和维修服务。

2.# 质保期内，乙方保证在合同标的物出现故障和缺陷时，或接到甲方提出的技术服务要求后（ 4 ）小时内予以答复，如甲方有要求或必要时，乙方应在接到甲方通知后（ 24 ）小时内派员至甲方免费维修和提供现场指导；如果出现紧急技术问题，乙方的技术人员应在（ 1 ）小时内予以答复；如果要求紧急处理，乙方应在收到甲方通知后的（ 4 ）小时内赶到现场解决问题。如乙方未按照以上要求响应的，甲方有权委托第三方对合同标的物进行维修或提供技术服务，因此产生的相关费用由乙方承担。

3.质保期届满后，如果因标的物硬件或软件的固有缺陷和瑕疵出现紧急故障和事故，卖方应在接到买方通知之后(4)小时内到达现场。

8、其他

8.1 投标人应提供详尽的售后服务方案。

8.2 投标人应提供详细的培训方案。

8.3 投标人应提供投标产品的软件开发著作权

三、履约验收方案

1.验收方式及程序

乙方完成系统开发及部署后，甲方进行现场项目初验，乙方需配合甲方的验收工作。

系统经过初验后进入试运行期，所有性能指标达到技术要求时，可进行最终验收。

在试运行期间，如系统出现重大问题，则试运行期从系统故障修复之日起重新计算，顺延 1 个月，若仍达不到要求，继续顺延，直到系统连续 1 个月无故障

时为止。在全部达到要求时，双方签署最终验收文件。

（1）乙方自行携带测试所需仪器、仪表及专用工具至甲方现场，并提供测试手册给甲方。测试手册经甲方确认后作为移交测试的依据。

（2）移交测试应由甲方的技术人员在乙方人员的指导和协助下按照有关测试规定进行。

在上线完成后，系统进入试运行阶段。对于系统在试运行阶段出现的问题乙方应在 5 个工作日内解决。试运行问题全部解决后，乙方应配合甲方对该期系统进行竣工验收。

（3）在甲方同意的前提下，如果因乙方原因导致合同系统存在无实质性影响的微小故障，且乙方及时采取措施进行修复或改进，并达到本合同约定及甲方要求的，双方仍将按上述约定签署竣工验收报告。

（4）如果由于乙方的原因，使系统中的任何一部分不能按合同开发进度通过验收，双方签订验收证书并如实记载验收过程中存在的问题。乙方应及时对验收过程中存在的问题进行改正后再次通知甲方进行验收，再次验收的所有费用由乙方负担。

（5）验收证书为乙方履行其义务的必要证据，但是无论如何验收证书的签署不免除乙方对于合同系统的瑕疵担保责任和保修责任。

2.验收标准

（1）软件错误的严重性等级定义

1 级：不能执行正常功能或重要功能,或者危及人身安全；

2 级：严重地影响系统要求或基本功能的实现,且没有办法解决；

3 级：严重地影响系统要求或基本功能的实现,但存在合理的解决办法；

4 级：使操作者不方便或遇到麻烦,但不影响执行正常功能或重要功能；

5 级：其它错误；

以下 1、2、3、4 项验收标准是结合软件行业惯例所提出的对于软件系统质量的推荐要求，所有交付的软件须首先满足以下 1、2、3、4 项验收标准要求，同时再满足本项目其他具体初验标准要求，才能通过初验。

（2)验收合格标准(以下比例为测试用例不通过数占总测试用例数的比例）

项目验收合格应同时满足以下要求：

1）测试用例不通过数的比例<1.5%；

2）不存在错误等级为 1 的错误；

3）不存在错误等级为 2 的错误；

4）错误等级为 3 的错误数量≤5；

在系统初验合格之后即可开始试运行，在试运行期内应用软件开发人员共同负责系统的维护；在试运行期间须对进行有关维护和使用的授课培训；试运行结束时乙方协助甲方生成试运行报告后提出项目终验申请。

3.项目终验验收标准

1、软件产品符合“合同”或“验收标准”规定的全部功能和质量要求

2、文档齐全、符合“合同”或“验收标准”要求及有关标准的规定。

3、对被验收软件的可执行代码，在验收测试中查出的错误总数，依错误严重性不超过位事先约定的限定值

4、提供全部项目文档，交付文档中的错误总数不超过事先约定的限定值。

第 2 包

一、详细技术需求

1.1 采购用途

随着移动互联网安全技术的发展，现有移动应用合规检测相关工具无法全面覆盖不良移动应用各类违法违规行为，针对数据流量的抓取难度大幅提高，依据行业标准《不良移动应用程序分类及判定方法》相关要求，针对金融、视频、通信等应用场景，定制开发不良 App 异常行为识别及流量分析工具，建成覆盖 Android App、iOS App、微信小程序、SDK 的数据安全合规异常行为、数据流量截取、识别、取证等能力，可为不良移动应数据治理工作提供急需的工具支持，为移动互联网数据安全研究工作提供基础科研环境，为提升产业数据安全治理水平提供助力。

1.2 需实现的功能要求

系统需具备针对移动应用软件（包括安卓及 iOS）、微信小程序、SDK 堆栈访问、权限使用、数据传输等各类基本行为的识别能力，并依据需《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》《不良移动应用程序分类及判定方法》《信息安全技术—个人信息安全规范》等法律法规、技术标准等，实现对 App 收集、传输、使用、销毁数据行为的深度分析，发现其中违法违规行为，并针对违法违规采集、传输、使用及存储用户数据，危害用户合法权益等行为进行取证，挖掘违法违规证据链，支撑工信部不良 App 治理相关工作。

1.3 详细技术要求

1.3.1 基本要求

1.3.1.1 ★ 识别对象要求

具备 Android App、iOS App、微信小程序、App 内第三方 SDK 的数据安全合规异常行为及数据传输识别、分析。

1.3.1.2 △ 基本信息识别能力

具备自动化静态识别获取样品基本信息，如 App 名称、包名、版本、证书等。

1.3.1.3 △ 加固技术对抗能力

具备针对加固后的移动应用识别、分析能力，可以正常遍历功能，并对收集、传输敏感数据的行为进行监控。

1.3.2 识别方式要求

1.3.2.1 # 人工半自动识别能力

具备识别流程指引功能，遵循法律法规要求和移动应用收集使用敏感数据的周期进行识别，包括授权前阶段、前台行为阶段、功能深度遍历及行为深度挖掘阶段、数据安全识别阶段、文本分析阶段、权限专项识别、个人信息相关数据专项识别等多种场景。

1.3.2.2 # 全自动识别能力

具备异常行为全自动化识别能力，可对 App 进行快速的静态代码特征识别以及动态的授权前、前台、后台、退出阶段的行为监控，通过自动化脚本、合规库、静态动态结果对比等方式输出报告。

1.3.2.3 # 动态行为识别能力

具备动态行为沙箱运行能力，支持 Android、iOS 应用自动化安装、启动、功能遍历、行为监控，并支持区分主程序及第三方 SDK 行为机制，可导出详细的行为堆栈数据作为不良移动应用违法违规行为证据。同时支持对微信小程序的动态识别，在小程序登录后进行功能遍历，实现小程序违法违规行为、传输数据等问题发现。

1.3.2.4 △ 任务复测能力

具备在已完成任务基础上进行特定问题的针对性复测，并根据历史识别结果智能标记重要识别点。

1.3.2.5 △ 违规取证能力

具备识别过程中对样品的不合规内容、违规行为等进行截图取证能力，并支持在自动生成的报告中展示。

1.3.3 可识别内容要求

1.3.3.1 # 基础识别能力

支持动态行为分析，系统需支持通过沙箱系统监测 App 运行过程中数据行为，通过行为函数调用栈对行为主体进行分析，能够定位行为触发的代码位置。

支持通信传输分析，系统需支持通过 DPI 技术对 App 运行过程中传输的数据

信息进行抓取，并解析通讯访问的域名、IP、地理位置等，分辨境内外地址，通过函数调用栈定位具体触发位置和触发主体。

支持 SDK 分析，系统需通过静态+动态运行，以 SDK 库为依托，分析 App 中包含的 SDK，及 SDK 使用的权限及权限次数。

支持声明权限识别，系统需支持分析 App 中 Androidmanifest.xml 文件，解析谷歌定义权限及开发企业自定义权限。

支持尝试使用未声明权限识别，系统需支持根据 App 运行行为，分析未声明但尝试使用的权限。

支持关联启动分析，系统需支持识别 iOS App 是否存在关联启动的行为。

支持权限过度声明分析，系统需支持识别 App 是否存在过度声明权限的情形。

支持 App 安全加固情况分析，系统需支持识别识别 Android App 是否进行加固及加固厂商。

1.3.3.2 △ 深度识别能力

具备覆盖国内不良 App 治理、数据安全、个人信息保护相关法律法规要求的深度识别能力，依据各场景阶段识别点结果和部分自动化判断，输出各评估点最终结论并提供取证依据，包括图片，隐私政策片段、触发行为、行为主体、代码片段等内容。总体法规识别条目总数不得少于 60 项。

1.3.3.2 △ 全自动化识别能力

全自动化识别模式支持《信息安全技术 个人信息安全规范》《不良移动应用程序分类及判定方法》《工业和信息化部关于开展纵深推进 App 侵害用户权益专项整治行动的通知》《App 违法违规收集使用个人信息行为认定方法》等标准规范，并根据不同的技术标准输出识别结果。

1.3.3.3 △ 微信小程序识别能力

支撑通过添加 App ID 的方式对微信小程序进行正常访问，实现遍历小程序功能，并依照相关法规标准标准识别异常行为及违规传输情形。

1.3.4 辅助功能

1.3.4.1 △ 数据统计功能

具备任务数量、月度任务数量、发现风险总量、风险分布情况等数据信息统

计能力。

1.3.4.2 △ 日志管理功能

具备单个任务运行日志信息或扫描数据下载功能，且适用 Android、iOS、SDK、小程序等全部扫描识别任务。

1.3.4.3 △ 报告输出功能

具备自动输出包含整体评价、安全风险等级、法规依据、异常行为截图、数据传输情况分析、整改建议等内容的识别报告。

1.3.4.4 △ 管理功能

具备自定义识别规则机制，可自主更改识别项、描述、修复建议等信息。

支持自定义修改系统界面 UI 设置，包括但不限于：系统登录背景图、logo、系统介绍、系统名称等信息。

支持自定义报告内容，包括但不限于：报告标题、logo、水印、介绍信息等。

1.4 性能要求

本次采购软件系统需要满足如下性能要求：

1.批量上传不良移动应用样品文件时（10 个以内），CPU 占用率不超过 20%，内存占用率不超过 70%；

2.批量扫描、识别时（10 个以内），CPU 占用率不超过 60%，内存占用比不超过 70%；

3.CPU 平均消耗不超过 40%，内存平均消耗不超过 60%。

1.5 安全要求

本系统不与院业务系统产生交集，线下运行，内网、外网均无访问接口，为独立运作的安全扫描类工具，无需等保定级。但系统需要遵循“网络安全法”的相关要求，部署前开展渗透测试，确保不存在高危漏洞，并提供渗透测试报告。

1.6 其他要求

产品支持部分国产化服务器、中间件、数据库等，并能够提供适配证书。

二、服务需求

1、★质保期

1.1 质保期自买卖双方在签署的终验验收单的日期开始计算，卖方提供免费质保期为(3)年。

1.2 在质保期内，如果卖方出售的相同型号产品发生硬件和软件更新/升级，卖方应将新发布的硬件和软件更新/升级在一个月内提供给买方，并到现场给予支持。

1.3 卖方需在投标总价以外单独列出质保期后的年度质保费用，卖方承诺买方可在过质保期后以此价格向卖方购买保修服务。

1.4 在设备维修期间，卖方应无偿提供替代设备。

2、培训内容及要求

提供不少于 3 人天的培训，培训内容包括但不限于系统基本功能使用培训、Android App 识别培训、iOS App 识别培训、微信小程序识别培训。培训费用均由投标人负责。

3、项目文档要求

序号	文档名称	说 明	提交阶段
1	需求规格说明书	系统开发最依据	需求完成后提交
2	设计文档	说明系统结构、业务流程、系统功能	实施开发前提交
3	测试用例	试运行测试用例	初验提交
4	初验报告	按照初验要求提交	初验提交
5	终验报告	按照终验要求提交	终验提交
6	用户手册/使用手册	按照终验要求提交	终验提交
7	培训资料文档	按照培训前提交	培训前提交
8	源代码	作为项目交付物提供	终验提交

4、项目团队要求

项目团队需包括但不限于项目经理、技术负责人、开发运维人员，项目团队人数不少于 4 人。

5、项目进度要求

项目启动后 60 日历日内完成该模块基本架构及样品信息识别、后台行为抓取、分析等核心功能开发。

120 日历日内完成样品通讯传输行为、软件和技术供应链情况、数据采集规范性方面识别功能开发，并进入试运行阶段。

试运行期不应少于 180 日历日，期间应对系统运行效率、误报率、稳定性等指标进行测试、评估，并根据法律法规及各类标准规范升级、完善软件系统功能，增补、调整可识别异常行为种类，完善识别规则自定义、自动化报告输出等辅助功能。

6、★所有权、知识产权归属及要求

本次采购因项目特殊需要定制开发部分的所有权及知识产权归属买方所有。

7、技术支持及服务响应

7.1 甲方可以通过访问网页接入的方式获得最新的技术信息以及其他资料。

7.2 乙方将最新的技术信息和资料及时主动提供给甲方。

7.3 技术响应时间要求：

1.质保期内，乙方免费为甲方提供技术指导和维修服务。

2.# 质保期内，乙方保证在合同标的物出现故障和缺陷时，或接到甲方提出的技术服务要求后（ 4 ）小时内予以答复，如甲方有要求或必要时，乙方应在接到甲方通知后（ 24 ）小时内派员至甲方免费维修和提供现场指导；如果出现紧急技术问题，乙方的技术人员应在（ 1 ）小时内予以答复；如果要求紧急处理，乙方应在收到甲方通知后的（ 4 ）小时内赶到现场解决问题。如乙方未按照以上要求响应的，甲方有权委托第三方对合同标的物进行维修或提供技术服务，因此产生的相关费用由乙方承担。

3.质保期届满后，如果因标的物硬件或软件的固有缺陷和瑕疵出现紧急故障和事故，卖方应在接到买方通知之后(4)小时内到达现场。

8、其他

8.1 投标人应提供详尽的售后服务方案。

8.2 投标人应提供详细的培训方案。

8.3 投标人应提供投标产品的软件开发著作权。

三、履约验收方案

1.验收方式及程序

乙方完成系统开发及部署后，甲方进行现场项目初验，乙方需配合甲方的验收工作。

系统经过初验后进入试运行期，所有性能指标达到技术要求时，可进行最终验收。

在试运行期间，如系统出现重大问题，则试运行期从系统故障修复之日起重新计算，顺延 1 个月，若仍达不到要求，继续顺延，直到系统连续 1 个月无故障

时为止。在全部达到要求时，双方签署最终验收文件。

（1）乙方自行携带测试所需仪器、仪表及专用工具至甲方现场，并提供测试手册给甲方。测试手册经甲方确认后作为移交测试的依据。

（2）移交测试应由甲方的技术人员在乙方人员的指导和协助下按照有关测试规定进行。

在上线完成后，系统进入试运行阶段。对于系统在试运行阶段出现的问题乙方应在 5 个工作日内解决。试运行问题全部解决后，乙方应配合甲方对该期系统进行竣工验收。

（3）在甲方同意的前提下，如果因乙方原因导致合同系统存在无实质性影响的微小故障，且乙方及时采取措施进行修复或改进，并达到本合同约定及甲方要求的，双方仍将按上述约定签署竣工验收报告。

（4）如果由于乙方的原因，使系统中的任何一部分不能按合同开发进度通过验收，双方签订验收证书并如实记载验收过程中存在的问题。乙方应及时对验收过程中存在的问题进行改正后再次通知甲方进行验收，再次验收的所有费用由乙方负担。

（5）验收证书为乙方履行其义务的必要证据，但是无论如何验收证书的签署不免除乙方对于合同系统的瑕疵担保责任和保修责任。

2.验收标准

（1）软件错误的严重性等级定义

1 级：不能执行正常功能或重要功能,或者危及人身安全；

2 级：严重地影响系统要求或基本功能的实现,且没有办法解决；

3 级：严重地影响系统要求或基本功能的实现,但存在合理的解决办法；

4 级：使操作者不方便或遇到麻烦,但不影响执行正常功能或重要功能；

5 级：其它错误；

以下 1、2、3、4 项验收标准是结合软件行业惯例所提出的对于软件系统质量的推荐要求，所有交付的软件须首先满足以下 1、2、3、4 项验收标准要求，同时再满足本项目其他具体初验标准要求，才能通过初验。

（2)验收合格标准(以下比例为测试用例不通过数占总测试用例数的比例）

项目验收合格应同时满足以下要求：

1）测试用例不通过数的比例<1.5%；

2）不存在错误等级为 1 的错误；

3）不存在错误等级为 2 的错误；

4）错误等级为 3 的错误数量≤5；

在系统初验合格之后即可开始试运行，在试运行期内应用软件开发人员共同负责系统的维护；在试运行期间须对进行有关维护和使用的授课培训；试运行结束时乙方协助甲方生成试运行报告后提出项目终验申请。

3.项目终验验收标准

1、软件产品符合“合同”或“验收标准”规定的全部功能和质量要求

2、文档齐全、符合“合同”或“验收标准”要求及有关标准的规定。

3、对被验收软件的可执行代码，在验收测试中查出的错误总数，依错误严重性不超过位事先约定的限定值

4、提供全部项目文档，交付文档中的错误总数不超过事先约定的限定值。