移动应用安全服务项目需求

根据《网络安全法》要求，为加强广东省人民医院APP应用程序的安全，拟采购移动APP安全服务对省医的APP程序进行加固。具体需求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **详细描述** | **服务方式** |
| 1 | APP个人信息安全检测服务 | 对标监管部门相关政策要求，依据《APP违法违规收集使用个人信息自评估指南》为检测内容，检测覆盖范围包括但不限《工信部发布信管函[2019]337号《关于开展APP侵害用户权益专项整治工作的通知》、《App违法违规收集使用个人信息行为认定方法》、《工业和信息化部《关于开展纵深推进 APPAPP 侵害用户权益 专项整治行动的通知（工信部信管函〔 2020〕164号》等检测要点，对APP进行个人信息违法违规检测，并提供相应评估报告及修复意见，包含初测、整改咨询、复测服务。 | 单款APP，一次个人信息安全检测服务，远程及现场服务 |
| 2 | APP安全加固服务 | **一、Android安全加固：** 1、Android基础加固项：含DEX函数分离+DEX整体加壳、资源防篡改、代码防篡改、防dump、动态调试、防注入、防二次打包； 2、资源文件加密：对应用中assets、res目录下的资源进行加密，防止资源查看以及盗用； 3、SO库加壳：利用自主研发的加密算法对C/C++源码编译出来的so文件进行加壳，使加壳后的so文件无法通过ida反编译工具查看导出符号，并在加壳的过程中对数据段进行加密压缩，从而加壳后的so文件具备无法正确反编译和反汇编并体积会有减小的趋势； 4、签名文件保护：对应用签名信息进行校验，防止APK被其他签名证书签名； 5、本地数据加密：对应用中本地数据读写接口进行自动拦截加密出来，防止应用缓存数据明文落地； **二、IOS安全加固：** 对C/C++/OC代码进行混淆加固，包括字符串加密、指令多样化、基本块分裂、控制流引入、跳转指令插入、控制流扁平化、控制流间接化等功能。 | 单款APP，一年服务期内无限版本安全加固 |
| 3 | APP自动化平台检测服务 | APP加固完成后对APP进行自动化平台检测，针对Android和iOS移动应用通过静态反编译技术对APK文件进行反编译，通过词法分析、语法分析、控制流、数据流分析等技术对移动应用程序代码和配置文件进行扫描，验证移动应用是否满足规范性、安全性、可靠性、可维护性等进行检测，同时通过沙箱模型、云手机等方式对移动应用的安装、运行过程中的行为进行监测分析，验证应用是否存在安全性问题。 | Android、IOS加固完成后，对已加固app分别进行一次自动化平台检测，并提供自动化平台检测报告 |
| 4 | 移动应用安全培训服务 | app个人信息安全检测报告解读培训 | 提供一次个人信息安全检测报告解读培训服务，现场培训 |

报名资质要求：

1、具备中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质认证；

2、具备中国网络安全审查技术与认证中心颁发的信息系统安全运维服务资质认证；

3、具备ISO27001信息安全管理体系认证证书及ISO9001质量管理体系认证证书；

4、广州市内拥有分子公司或办事处，并提供营业执照或不少于一年的场地租赁合同；

5、具备移动应用安全服务类案例不少于1个。