国家标准《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》（征求意见稿）编制说明

一、工作简况

1.1 任务来源

根据国家标准化管理委员会 2021 年下达的国家标准制修订计划，《信息安全技术 移动互联网应用程序安全开发和生命周期管理指南》由武汉安天信息技术有限责任公司（以下简称“武汉安天”）负责承办，计划号：20210992-T-469。该标准由全国信息安全标准化技术委员会归口管理。

1.2 主要起草单位和工作组成员

武汉安天信息技术有限责任公司负责主要起草，华为技术有限公司、北京赛西科技发展有限责任公司、维沃移动通信有限公司、三六零科技集团有限公司、OPPO 广东移动通信有限公司、北京小米移动软件有限公司、公安部第三研究所、国家计算机病毒应急处理中心、中国软件评测中心、国家计算机网络应急技术处理协调中心、中国科学院信息工程研究所、启明星辰信息技术集团股份有限公司、联想（北京）有限公司、海信集团有限公司、蚂蚁科技集团股份有限公司、南方电网数字电网研究院有限公司、北京智游网安科技有限公司（爱加密）、深圳市腾讯计算机系统有限公司、杭州安恒信息技术股份有限公司、北京指掌易科技有限公司、北京百度网讯科技有限公司、北京版信通技术有限公司等单位共同参与了该标准的起草工作。

主要起草人包括：潘宣辰、许玉娜、陈诚、衣强、成明江、姚一楠、李腾、陆伟、水晶、张艳、刘彦、蔡一鸣、孙海燕、何能强、杜丹、史景、李汝鑫、张淯易、王昕、母天石、陈家林、韩云、刘海涛、李献振、李彪、吴月升、董宏、陈牧、潘正泰、王克、方宁等。

1.3 工作过程

1、2020 年 5 月至 8 月，武汉安天组织启动标准研制工作，并公开征集标准参编单位，组建标准编制组，制定工作计划并确定编制组人员。

2、2020 年 10 月至 11 月，组织召开项目启动会和两次编制组研讨会。编制

组根据 WG6 工作组、业内专家的意见，厘清标准边界，完善标准结构和具体条款，形成标准草案。

3、2020 年 11 月 12 日，在信安标委工作组会议周上进行汇报。会后，根据工作组成员单位意见对标准草案进行进一步完善，主要将第五章的总体原则修改成了安全目标和总体框架，标准内容根据总体框架进行展开描述。

4、2020 年 12 月至 2021 年 2 月，组织召开三次编制组研讨会。经研讨，参考个人信息、软件开发、数据和密码等相关标准对标准具体条款进行完善。

5、2021 年 3 月 10 日，参加信安标委秘书处组织的项目中期检查。会后，针对专家提出的基础编码安全的完整性、代码的安全检测、密码算法条款及章节的关联性相关建议，对标准草案进行修改完善，重点完善了安全开发技术章节。

7、2021 年 5 月，在信安标委工作组会议周上进行汇报，根据会议决议，修改完善后形成标准征求意见稿。主要修改内容：将第七章中的“生命周期模型与角色关注域”纳入了第五章，将第八章检测部分纳入到了第七章第二节，并对标准文本的框架逻辑和条款准确性表述等进行完善。

8、2021 年 11 月，在信安标委工作组会议周上汇报标准征求意见稿。会后，根据工作组成员单位意见重点对侵害用户权益关于行为风险处置部分进行了完善，并将移动生态中需要协同管理的部分进行了厘清，并在生命周期管理中对风险行为检测处置做了关联。

9、2021 年 12 月 2 日，信安标委秘书处组织召开了标准征求意见稿专家审查会。根据专家意见，由于“生命周期”包含“开发”环节，存在重复，建议将标准名称调整为《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》，在附录 B 中补充风险与管理和技术活动关联性，并将安全开发章节内容纳入附录 C，修改完善后形成了目前版本的标准征求意见稿。

二、标准编制原则和确定主要内容的论据及解决的主要问题

2.1 编制原则

本标准的修订工作遵循以下原则：

以风险防控为核心：坚持维护移动互联网应用程序安全为根本理念，提高开发过程和全生命周期管理过程中应用程序的风险防范能力，规避恶意代码攻击、应用程序漏洞、损害用户利益的风险行为、个人隐私和敏感数据泄露等风险。

以协调一致为基础：以推进标准应用为前提，确保标准与现有移动互联网应用程序开发和生命周期管理模式相协调，与现行政策标准相兼容。

以规范适应为目标：以促进移动互联网应用程序发展为宗旨，提炼安全共性、基础性安全要求，兼顾部委、企业等对移动互联网应用程序安全监管的需求，提升标准适用性。

2.2 主要内容及其确定依据

本标准提供了移动互联网应用程序（App）生命周期安全管理的建议，适用于 App 开发者对 App 的开发、运营，也适用于移动应用分发平台厂商和移动智能终端厂商对 App 的管理，也可作为第三方机构对 App 进行安全检测时的参考。

本标准共包含 6 章内容，分别为：范围、规范性引用文件、术语和定义、缩略语、概述、生命周期管理，给出了 App 生命周期安全需求、App 生命周期安全保证框架、角色及安全建议。

该标准编制过程中，编制组主要研究参考了以下标准或文件：

GB/T 22032-2008 系统工程 系统生存周期过程

GB/T 34978-2017 信息安全技术 移动智能终端个人信息保护技术要求

GB/T 37952-2019 信息安全技术 移动终端安全管理平台技术要求

GB/T 35278-2017 信息安全技术 移动终端安全保护技术要求

GB/T 37729-2019 信息技术 智能移动终端应用软件（App）技术要求

GB/T 30284-2020 信息安全技术 移动通信智能终端操作系统安全技术要求

YD/T 3437-2019 移动智能终端恶意推送信息判定技术要求

TC260-PG-20191A 网络安全实践指南—移动互联网应用基本业务功能必要信息规范

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

2.3 解决的主要问题

1）如何规避开发引入的恶意代码攻击、应用程序漏洞等风险；

2）如何规避应用程序管理不当造成的个人隐私和敏感数据泄露等风险；

3）及时发现侵害用户权益的行为，如私自收集个人信息、强制用户使用定向推送功能、过度索取权限、欺骗误导用户等；

4）如何采取措施避免安全漏洞信息传播而产生危害的风险。

三、主要试验[或验证]情况分析

暂无。

四、知识产权情况说明

暂未发现本标准涉及相关知识产权问题。

五、产业化情况、推广应用论证和预期达到的经济效果

本标准发布后，计划用于指导移动互联网应用程序的开发者和运营者建立健生命周期管理机制，提高移动互联网应用程序的安全防护能力，满足应用程序安全、个人隐私保护和数据合规等方面的需求。通过与移动互联网应用程序开发商、手机厂商、移动应用渠道、互联网厂商、安全厂商等产业链企业以及监管部门等组织机构的共同努力，提升网络安全保护能力，促进产业化的健康发展。

六、采用国际标准和国外先进标准情况

不涉及。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准与现行《中华人民共和国网络安全法》《移动互联网应用程序信息服务管理规定》《移动智能终端应用软件预置和分发管理暂行规定》《电信和互联网用户个人信息保护规定》《App 违法违规收集使用个人信息行为认定方法》和《网络产品安全漏洞管理规定》等法律法规相协调配套。

本标准与现行相关标准无冲突和矛盾的地方。

八、重大分歧意见的处理经过和依据

本标准编制过程中未出现重大分歧。

九、标准性质的建议

建议本标准作为推荐性国家标准发布实施。

十、贯彻标准的要求和措施建议

本标准为移动互联网应用程序（App）生命周期管理提供安全指导。移动互联网应用程序的开发者可依据本标准开展安全开发活动，建立健全安全开发管理机制，提升安全技术保障能力，以提供安全的移动互联网应用程序，也可以此开展安全自评估；移动互联网应用程序的运营者可依据本标准开展全生命周期安全

管理，并实施生命周期过程和风险监测处置过程中的相应措施；第三方安全评估机构可借鉴本标准开展安全评估工作。

十一、替代或废止现行相关标准的建议

无。

十二、其它应予说明的事项

由于“安全开发”是“生命周期安全管理”的环节之一，存在重复。经征求意见稿审查会讨论评议，标准名称调整为《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》。

国家标准《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》

编制工作组

2022 年 2 月 8 日