国家标准《信息安全技术 软件产品开源代码安全评价方法》（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2023年下达的国家标准制修订计划,《信息安全技术 软件产品开源代码安全评价方法》由中国信息通信研究院负责承办，计划号：20230259-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 制定背景

当前开源代码应用广泛，超过 90%的企业使用的软件产品中涉及开源代码。与此同时开源安全问题凸显,开源代码自身存在的安全隐患被黑客利用攻击导致一系列安全事件，Log4j等开源代码暴露的安全问题极大程度影响软件产品正常稳定运行。市场亟需标准化的软件产品开源代码安全评价方法。本标准为保障开源代码安全性，针对软件产品开源代码提出安全评价要素，给出评价方法，旨在降低软件产品中的开源代码安全风险。

1.3 起草过程

（1）标准草案阶段

2022.3-2022.6成立标准编制组，组织华为、腾讯、小米、京东、奇安信等国内头部科技企业和安全厂商开展多轮讨论，针对开源代码安全相关政策、标准规范、技术实现开展研究，形成《信息安全技术 软件产品开源代码安全评价方法》标准草案初稿。

2022年6月-2022年10月组织产业调研，调研国内外多家软件产品开源代码安全治理情况。根据调研测试结果和相关国家、行业、团体标准的基础上改进标准草案，形成草案第二稿。

2022年10月以多种形式征求主管部门、专家和相关单位意见，完善标准草案、编制说明、意见处理汇总表。

2022年11月13日，下发《关于征集<信息安全技术 软件产品开源代码安全评价方法>标准参编单位的通知》，广泛征集标准编制组成员。

2022年11月-12月，组织标准编写组成员完成3次标准草案研讨会，根据

各单位的意见持续完善标准草案内容，对标准草案编写格式和内容呈现均进行修改，形成草案第三、四、五稿。

2022 年 12 月 7 日，完成 WG5 工作组 2022 年第三次全体会议标准汇报，根据工作组、责任编辑、专家评审会等提出的意见，修改完善标准草案、编制说明、意见处理汇总表后形成标准征求意见稿。

（2）标准征求意见稿阶段

2022 年 12 月 8 日-2023 年 2 月，根据工作组成员单位意见修改，并多次组织编制组内部研讨，修改完善后形成当前的征求意见稿版本。

2023 年 2 月 16 日，秘书处组织召开标准征求意见稿专家评审会，与会专家听取了编制组的汇报，经质询和讨论，建议编制组根据本次会议意见修改完善后，发起公开征求意见。

二、标准编制原则、主要内容及其确定依据

2.1 标准编制原则

（1）普适性原则

本标准充分立足我国软件产品开源代码安全特点，充分调研不同行业软件产品开源代码安全治理实践经验，对软件产品开源代码引入方提出开源代码来源、开源代码质量、开源代码知识产权和开源代码管理能力四方面指标要求并针对指标给出评价方法。

（2）合规性原则

本标准遵从软件产品开源代码安全有关法律法规的规定，标准条款内容符合我国法律法规和相关政策要求。

（3）一致性原则

本标准与国内外相关技术标准协调一致，与我国软件产品开源代码安全相关标准不矛盾。

2.2 主要内容及其确定依据

本标准针对软件产品开源代码给出安全评价方法，分为开源代码来源、开源代码质量、开源代码知识产权和开源代码管理能力四部分，每个部分提取关键安全要素，推动各单位对开源代码安全性进行审查，为各单位选取安全性较高的开源代码提供选型依据。

标准制定的依据为：

a）标准格式按照 GB/T 1.1—2020 标准要求编写。

b）本标准制定参考以下政策文件与国家标准：

《中华人民共和国网络安全法》

《关键信息基础设施安全保护条例》

《“十四五”国家信息化规划》

《国家网络安全事件应急预案》

GB/T 24420-2009《供应链风险管理》

GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》

GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》

GB/T 25069-2022《信息安全技术 术语》

开源代码来源评价类评价对象为软件产品中开源代码部分，通过考察开源代码规模占比、开源代码编码语言、开源代码著作权持有者、开源代码贡献量、开源代码丰富度、开源社区安全管理、开源代码托管平台、开源代码下载平台 8 个指标项达到可控性目的。本类指标项通过对 50 余家企事业单位进行调研，结合行业最佳实践和信通院前期开源产业研究和标准化积累得出。

开源代码质量评价类评价对象为软件产品中开源代码部分，主要通过考察开源代码漏洞率、开源代码漏洞严重性、开源代码漏洞影响范围、开源代码漏洞攻击复杂性、开源代码漏洞修复率、开源代码版本更新情况 6 个指标项达到安全性目标。本类指标项通过对 50 余家企事业单位进行调研，结合 GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》中的相关漏洞分类分级依据得出。

开源代码知识产权评价类评价对象为软件产品中开源代码部分，主要通过考察开源许可证规范性、开源许可证传染性、开源许可证兼容性、开源许可证专利权情况、开源许可证适用范围 5 个指标项达到合规性目标。本类指标项通过对 50 余家企事业单位进行调研，结合行业最佳实践和在研国标《信息技术 开源 开源许可证框架》得出。

开源代码管理能力评价类评价对象为软件产品，主要通过考察开源代码物料清单、开源代码设计、开源代码生成、开源代码管理团队 4 个指标项达到稳定性目标。本类指标项通过对 50 余家企事业单位进行调研，结合 GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》中组织和人员管理指标项得出。

本标准中的附录为一个规范性附录，给出了开源代码安全风险。

2.3 修订前后技术内容的对比[适用于国家标准修订项目]

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

3.1 试验验证的分析、综述报告

标准在编制过程中，对涉及软件产品开源代码引入的相关单位进行了多次调研，同时组织金融、运营商、汽车、软件等 20 多家单位进行标准验证工作，以保证标准条款的可实施落地。后续，标准还将由参与标准编制的各单位积极进行试验应用，针对不同的行业，如金融、汽车、运营商等，最后将实施经验转化为标准的具体内容，以增加标准的实用性。

3.2 技术经济论证

本标准在制定过程中，对标准进行技术经济论证，选出技术上可行和经济上合理的技术方案，为标准内容设置提供科学依据。

3.3 预期的经济效益、社会效益和生态效益

本文件适用于软件产品开源代码安全评价工作，为各企事业单位对于软件产品中的开源代码进行安全性自评价提供参考，为第三方机构开展此类工作提供依据。

本标准拟形成软件产品开源代码安全评价方法，研究开源代码面临的安全风险，明确开源代码度量基线。标准的制定与应用过程中，一是摸清软件产品开源代码安全现状；二是给出开源代码安全指引，解决开源代码安全性较弱的问题；三是降低开源使用的安全风险问题。

针对各企事业单位软件产品开源代码使用广泛的现状，本标准的应用降低开源代码安全风险，降低开源代码安全风险对我国国家和企业造成的信息安全威胁，推动我国软件产品开源代码安全发展。

四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况

国内其他开源相关国家标准尚未聚焦开源代码安全性评价，《信息技术 开源开源许可证框架》聚焦开源许可证合规和开源术语定义，《金融行业开源软件评

测规范》聚焦开源软件自身技术评价，与本项标准内容并不冲突，同时本项标准在术语描述上与《信息技术 开源 开源许可证框架》保持一致，在相关内容描述上与《金融行业开源软件评测规范》保持一致。

五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

无

六、与有关法律、行政法规及相关标准的关系

本标准与现行法律、法规、强制性国家标准及相关标准协调一致。本标准在同《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《“十四五”国家信息化规划》《国家网络安全事件应急预案》等相关法律法规和政策文件及现行国家标准 GB/T 24420-2009《供应链风险管理》、GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》、GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》、GB/T 25069-2022《信息安全技术 术语》相关内容协调一致基础上，在研过程中引用了在研阶段的国家标准《信息安全技术 软件供应链安全要求》、《信息技术 开源 开源许可证框架》、《金融行业开源软件测评规范》相关内容，同时针对软件产品开源代码安全特性提出具体要求。

七、重大分歧意见的处理经过和依据

无。

八、涉及专利的有关说明

本标准未涉及专利。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

基于开源代码的软件产品提供方应用本标准提高开源代码安全管控能力；基于开源代码的软件产品使用方应用本标准选择风险可控的开源代码；第三方评测机构梳理应用广泛的开源代码，应用本标准对开源代码进行评价。标准实施过程中建立反馈机制，针对标准不适用情况进行及时追踪、修订，不断提升标准的可操作性和先进性。

十、其他应当说明的事项

无