国家标准《网络安全技术 软件物料清单数据格式》（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年下达的国家标准需求，《网络安全技术 软件物料清单数据格式》由水利部信息中心负责承办。本标准由全国网络安全标准化技术委员会归口管理。

**1.2 制定背景**

软件供应链复杂、开源软件使用增加、软件升级补丁的保障措施不够完善等，都是造成软件供应链安全风险上升、监管难度较大的主要原因。针对软件供应链愈发复杂、软件嵌套引用组件数量庞大、国内的软件物料清单建设没有统一规范等问题，制定软件物料清单（SBOM）格式规范，识别软件组件及其依赖关系，提高软件全生命周期的可见性和透明度，增强软件供应链安全管理能力。软件物料清单能够支撑软件供应链供方、需方和监管方发现软件中存在的安全漏洞风险和知识版权风险。

**1.3 起草过程**

（1）标准立项申报

2023年7月-2023年8月，成立标准编制组，组内开展多轮讨论，针对软件物料清单相关政策、标准规范、技术实现开展研究，形成《网络安全技术 软件物料清单数据格式》标准草案初稿。按照网安标委2023年国家标准项目申报要求提交了国家标准制定项目立项申请。

（2）草案阶段

2023年8月，在2023年WG7工作组第二次全体会议立项申报项目初审会进行汇报，根据评审专家意见完善标准草案。

2023年9月，在网安标委2023年第二批网络安全国家标准立项专家评审会进行汇报，根据评审专家意见完善标准草案。

2023年10月-2024年2月，在水利部信息中心和南方电网初步开展试点验证，根据验证实践活动制定正式试点验证方案，开展组内试点验证单位征集。

2024年2月根据《全国网络安全标准化技术委员会 关于17项网络安全国家标准项目立项的通知》（网安字[2024]2号）通知，本标准正式获批为网络安全标准制定项目。

2024年3月13日，在WG7工作组专家评审会进行汇报，与会专家进行研讨，根据专家意见修改重点完善数据模型图和标准字段描述。

（2）征求意见阶段

2024年3月27日至4月1日，WG7组织成员单位对该标准进行了转阶段投票，经成员单位投票决定该标准转为征求意见稿。

2024年4月11日，在TC260专家评审会进行汇报，根据专家意见，进一步修改完善标准框架图，梳理元素分类；完善标准模型图，精简模块中文字并添加图例等信息；针对标准引言、术语等进一步完善、补充；补充关于组件重要性相关信息。

2024年4月21日，水利部组织专家质询会，向与会专家汇报标准内容，根据专家意见，修改标准引言、修改清单组成逻辑结构及说明、增加缩略语定义、统一部分内容在上下文中的表述、进一步明确部分字段定义。

**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

数据字段选择满足供需监管等各相关方的需求，包括需方的软件供应链风险管理需求，供方的软件物料清单管理需求和监管方的行业和多级监管需求。

（2）合规性原则

本标准遵从软件供应链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，与我国软件供应链安全相关标准不 矛盾。

（4）兼容性原则

与现有标准良好兼容，覆盖现有标准的必要字段，提供国际标准格式转化的指导。

（5）可操作性：标准能够支持自动化手段生成和交换清单。

**2.2 主要内容及其确定依据**

本标准规定了一种通用的软件物料清单数据交换格式，包括软件物料清单组成、清单文件格式要求和软件物料清单元素。软件物料清单组成规定了软件物料清单包含哪些元素，以及各元素的含义和内容。清单文件格式要求规定了软件物料清单文件应符合的格式规范。软件物料清单元素规定了软件物料清单各元素的字段和字段值格式，并给出了各个字段的含义说明。

标准制定的依据为：

1. 标准格式按照 GB/T 1.1—2020 标准要求编写。
2. 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》

《网络安全审查办法》

GB/T 24420-2009《供应链风险管理》

GB/T 25069-2022《信息安全技术 术语》

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

《信息安全技术 软件供应链安全要求》（报批稿）

软件物料清单组成规定了清单由基本信息、软件组成信息、外部依赖信息、安全信息、扩展信息和签名信息六大类信息17个元素组成，规定了支持清单基本功能的最小元素集。

清单文件格式要求规定了软件物料清单为承载软件物料清单信息的一个或一组文本文件，对文件的格式、命名提出具体要求。

软件物料清单元素对元素的字段及字段值格式进行格式规范。包括概述、基本信息类别、软件组成信息类别、外部依赖信息类别、安全信息类别、扩展信息类别、签名信息类别7个章节。概述部分对本章节软件物料清单字段描述提出统一规范，应包括字段名、字段描述、字段类型和字段必要性。基本信息类别包括软件信息和清单信息两个章节，软件信息包含软件所涉及的标识、供应商、来源、授权、完整性等信息；清单信息包含软件物料清单所涉及的版本、标识、创建、获取等信息。软件组成信息类别包括组件信息、文件信息、代码片段信息、内部依赖信息四个章节，组件信息提供软件包含的所有组件列表，每个组件包含组件标识、供应商、许可协议、完整性校验等组件信息；文件信息描述软件的第一层解压和镜像加载的制品文件列表，包含文件名称、路径、用途、完整性校验等信息；代码片段信息描述自研源代码中所包含的从社区、论坛等其他渠道获取的源代码片段列表，包含片段标识、位置、来源、许可证等信息。内部依赖信息描述组件、文件、代码片段之间依赖关系的信息。

外部依赖信息类别包括外部网络服务信息、基础环境信息和开发工具信息三个章节，外部网络服务信息描述为软件运行提供必要功能的外部网络服务列表（例如：域名服务、CDN服务、邮件发送、短信发送、支付接口等），包含服务名称、可替代性、供应商、服务环境、服务数据等信息；基础环境信息描述支撑软件运行的数据库管理系统、web应用框架、中间件、操作系统、BIOS等基础运行环境的列表，包含基础环境名称、版本、可替代性、供应商等信息；开发工具信息描述能够生成或影响最终软件代码的开发工具的列表，包含开发工具名称、版本、用途等信息。

安全信息类别包括网络服务接口信息、补丁信息、许可证信息、安全漏洞、配置风险、生命周期维护中断风险六个章节。网络服务接口信息描述软件提供的可被访问或调用的网络服务接口列表，包含接口描述、协议、地址、请求方式等信息；补丁信息描述从软件发布到生成软件物料清单期间为了修复问题和漏洞、优化性能而发布的补丁列表，包含补丁名称、原厂标识、用途描述等信息；许可证信息描述软件及其组件和代码片段中使用的许可证列表，包含许可证名称、内容、风险等信息；安全漏洞描述生成清单之前已修复的组件安全漏洞信息列表，包含漏洞名称、相关编号、影响对象、修复情况等信息；配置风险描述从软件发布到生成软件物料清单期间发现的软件默认配置项可能存在的已知配置风险信息列表，包含风险名称、受影响配置项、处置建议等信息。生命周期维护中断风险描述软件生命周期中可能发生的维护服务终止的风险列表，包含中断类型、描述、预计中断时间、处置情况等信息。

扩展信息描述本文件中未定义的其他软件物料信息列表，包括扩展信息的属性名称和属性值。

签名信息描述清单的数字证书和签名文件信息，应使用符合国家或行业规定的机构签发的数字证书。

**2.3 修订前后技术内容的对比**[仅适用于国家标准修订项目]

不涉及。

**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 试验验证分析**

标准在编制过程中，对软件物料清单的基本概念、应用价值、相关国际标准进行了全面研究，对涉及软件产品采购或定制化开发的相关单位进行了多次调研，并形成了研究报告，制定了初步的验证方案，在水利和能源行业，对38个系统/子系统开展试点验证，针对可行性、安全效益进行了验证，以论证部分核心标准条款的可实施落地，研究试点工作方案。

标准目前必选字段27个，非必选字段97个。本次初步测试验证覆盖必选字段27个本，水利行业自动化获取字段23个，自动化率85%；能源行业自动化获取字段24个，自动化率89%。

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、交通、政府、电信等，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。

目前已经制定了正式的试点验证方案，初步计划对以下层面进行验证：

1、标准可行性验证：

（1）标准字段采集可行性，是否可以通过技术或非技术手段获取；

（2）标准字段获取的便利性，是否能够自动化技术采集；

（3）采集到的标准字段的可靠性；

（4）采集的过程验证，软件生命周期每个阶段通过哪些手段获取哪些字段；

2、安全效益验证：

（1）标准字段能够重点解决哪些问题，例如对漏洞修复的作用、对应急处置的作用等；

3、兼容性验证

（1）与国际标准的兼容性，是否能实现两种格式的互相转换；

**3.2 技术经济论证**

国际标准及相关组织已经逐步建立软件物料清单标准格式共识，包括英特尔、微软、西门子、索尼、新思科技、VMware 和 WindRiver 在内的众多公司已经使用软件物料清单在政策或工具中传达软件物料清单信息，国内大部分的主流软件成分分析系统基于国际标准实现了软件物料清单的生成和验证等功能。软件物料清单生成包括两个主要步骤，一个是清单数据的获取，另一个是清单文件的生成。前者依赖软件成分分析、安全管理平台、三方数据共享等技术手段获取，后者使用格式转换的引擎能够实现。从目前国内外的管理和产品实践分析，基于标准化格式的软件物料清单具备技术可行性，从软件物料清单实现原理分析，技术实现难度不大，但是要实现较高的自动化水平，以及实现符合国内软件供应链安全管理实际需求的清单数据的获取，还有待进一步技术经济论证和验证，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 预期的经济效益和社会效益**

本标准的制定，将填补我国在软件物料清单方面国家标准领域的空白，促进软件供应链供方、需方和监管方之间进行软件物料清单信息的生成、共享和使用的规范化，支撑软件供应链相关监管政策规则的落地实施，推动我国软件供应链安全管理体系的逐步完善，助力关键信息基础设施解决大国博弈中的“卡脖子”问题，为我国经济高质量发展提供保障，维护社会稳定和国家安全。规范软件物料清单格式有助于减少因格式不统一而导致的额外成本，如转换格式、修复错误等，从而降低软件开发的整体成本。软件物料清单标准的推广应用，将有效提升软件供应链透明度，极大地便利软件组件溯源、软件产品依赖关系梳理、已知漏洞的影响范围判断、及时发现恶意软件渗透等，能够有效降低软件物料清单管理成本、降低漏洞修复成本、减少网络安全事件造成经济损失，从而增加企业经济效益。

**四、与国际、国外同类标准技术内容的对比情况**

关于软件物料清单的研究，国外起步较早，美国关于SBOM的研究一直是软件供应链安全研究的重点，已经形成完善的知识和标准，在能源、医疗、制造等行业进行了应用形成实践经验，美国国内已经对SBOM形成共识，并广泛使用。

国外针对软件物料清单相关的标准包括ISO/IEC 19770-2:2015《信息技术.软件资产管理.第2部分：软件识别标签》和ISO/IEC 5962:2021《信息技术-SPDX规范 V2.2.1》。

ISO/IEC 19770-2:2015规定了一种用于描述软件产品的结构化元数据格式SWID，在SWID格式规范中，除了标签ID、软件名称、相关组织名称和角色、相关链接等少数几个必须的字段外，其他的元素和属性都是可选的，并且未包含软件依赖的三方组件信息以及组件之间的依赖关系，对于使用者来说虽然灵活性较大，但是标准化程度不足，不能保证清单信息的全面性，不能满足系统运营者以及监管单位的管理需求。

ISO/IEC 5962:2021定义了用于传递与软件包相关的组件以及元数据信息的标准数据格式SPDX，包括软件包信息、文件信息和代码片段信息、依赖关系信息等软件组成成分信息，在SPDX格式规范中，未包含第三方服务信息、用于管理软件开发和构建流程的工具和系统信息等软件相关信息，而开发工具的和第三方服务提供商都是攻击者的重点攻击目标，与一些重大的软件供应链安全攻击事件紧密相关，因此将这些信息纳入软件物料清单，对于软件供应链安全风险的高效应急处置至关重要。

国内在软件供应链安全方面已经着手制定相关标准，包括《信息安全技术 软件供应链安全要求》、《信息安全技术 软件产品开源代码安全评价办法》等，前者确立了软件供应链安全目标，规定了软件供应链安全风险管理要求和供需双方的组织管理和供应活动管理安全要求，能够对软件供应链中的供需双方开展风险管理、组织管理和供应活动管理提供指导，后者给出了软件产品中的开源代码安全评价目标、评价指标体系和评价方法，适用于软件产品包含的开源代码安全评价工作。

目前国内外正式发布的标准中，并没有能够覆盖最新的软件供应链攻击场景、满足系统运营者以及监管单位管理需求的软件物料清单格式的标准，本标准的制定将填补我国在软件物料清单格式方面相关标准的空白，完善我信息技术领域的标准规范体系。

**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**

目前我国现有与软件供应链安全相关法律有《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》《网络安全审查办法》。网络安全审查办法要求关键信息基础设施采购的产品和服务，需要进行网络安全审查，网络安全审查需要能够识别供应中断等供应链风险。关键信息基础设施保护条例要求运营者采购安全可信的网络产品和服务，因此运营者需要建立安全可信网络产品的评价和选择策略。行业层面，金融行业发布了《关于规范金融业开源技术应用与发展的意见》，要求金融机构建立开源技术应用台账，支持金融机构加强开源技术供应链管理。

2018年，我国出台了供应链安全管理国家标准《信息安全技术 ICT 供应链 安全风险管理指南》，该标准采用风险评估的思路，从产品全生命周期的角度开 展风险分析及管理，以实现供应链的完整性、保密性、可用性和可控性安全目标。国内在软件供应链安全方面已经着手制定相关标准，包括《信息安全技术 软件供应链安全要求（报批稿）》、《信息安全技术 软件产品开源代码安全评价办法（报批稿）》等，前者确立了软件供应链安全目标，规定了软件供应链安全风险管理要求和供需双方的组织管理和供应活动管理安全要求，能够对软件供应链中的供需双方开展风险管理、组织管理和供应活动管理提供指导，后者给出了软件产品中的开源代码安全评价目标、评价指标体系和评价方法，适用于软件产品包含的开源代码安全评价工作。综上所述，本标准与现行法律、法规以及国家标准不存在冲突与矛盾。

**七、重大分歧意见的处理经过和依据**

暂无。

**八、涉及专利的有关说明**

不涉及。

**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**

涉及影响国家安全的软件系统应依据本标准建立软件物料清单，明确清单内容范围、生成方式、生成频率、生成深度、更新校验机制等，明确生成的软件物料清单的交付方式包括交付流程、交付方式以及交付过程的安全保障措施，明确软件物料清单在组织内部的实际使用场景，包括软件资产管理、软件漏洞管理、安全事件响应等。应建设软件物料清单管理工具平台，通过技术手段实现软件物料清单的统一管理。

**十、其他应当说明的事项**

无。

《网络安全技术 软件物料清单数据格式》标准编制组

2024年4月26日