原文链接：<https://www.linuxfoundation.org/blog/blog/what-is-an-sbom>

原文文本放在最后

翻译：

什么是 SBOM？  
Linux基金会 | 2021.6.15

国家电信和信息管理局最近要求提供广泛的反馈，以定义最低限度的软件材料清单。它由一个简单的问题（“什么是软件材料清单？”）为框架，标志着在软件安全领域迈出了极为重要的一步，也是开放标准的一个关键时刻。

根据国家电信和信息管理局的软件材料清单常见问题解答，"软件材料清单是一个完整、正式结构化的列表，列出了构建（即编译和链接）特定软件所需的组件、库和模块，以及它们之间的供应链关系。这些组件可以是开源的，也可以是专有的；可以是免费的，也可以是付费的；可以是广泛可用的，也可以是有限访问的。" 未来几十年，能够在团队和公司之间顺畅共享的软件材料清单，将是关键行业和数字基础设施软件管理的核心部分。

国际标准化组织针对开源许可合规性的国际标准（ISO/IEC 5230:2020—信息技术—OpenChain规范）要求对提供的软件进行材料清单管理的过程。这与NTIA提高软件透明度的目标相一致，并展示了全球行业如何应对这一领域的挑战。例如，对于所有提供的软件组件都包含软件材料清单已经成为最佳实践，甚至不仅仅局限于开源软件。

十多年前，开源社区就已经意识到并开始着手解决软件材料清单“成分清单”这一需求。如今，业界的事实标准，也是最广泛使用的方法，叫做软件包数据交换。国家电信和信息管理局提议的最低限度软件材料清单定义中的所有要素，今天都可以通过软件包数据交换来实现，并且还可以涵盖更广泛的使用场景。

软件包数据交换在过去十年里自然发展，以适应软件行业的需求，涵盖了许可合规性、安全性等问题。这个社区由来自数百家公司的人组成，软件包数据交换标准本身是目前市场上最健壮、最成熟、最广泛采用的软件材料清单。

完整的软件包数据交换规范只是整个情况的一部分。像SPDX Lite这样的可选组件，由先锋电子、索尼、日立、瑞萨和富士通等公司开发，为小型供应商提供了一个集中的软件材料清单子集。软件包数据交换背后的社区方法使得实际使用场景能够在出现时得到及时解决。

2020年，软件包数据交换通过与联合开发基金会合作，向国际标准化组织提交了PAS转换过程，交给第一联合技术委员会。目前，软件包数据交换处于转换过程的批准阶段，并可在国际标准化组织官网上查看，ISO/IEC PRF 5962。

Linux基金会为国家通信与信息管理局准备了一份提交文件，突出了在软件包数据交换和OpenChain社区中，实际部署和使用软件材料清单所获得的知识和经验。这些经验包括隔离特定操作的实用性，如追踪时间戳和将数据许可证包括在元数据中。得到了全球技术行业各方的支持，软件包数据交换和OpenChain规范正在不断发展，来支持所有利益相关者。

**行业评论：**

索尼团队采用多种方法管理开源合规性和治理……一个例子是使用基于SPDX Lite的OSS管理模板，这是SPDX标准的一个精简子集。团队需要能够快速审查软件的类型、版本和需求，使用清晰的标准是这个过程中的关键部分。

—Tamai Hisashi，索尼集团公司高级副总裁，软件战略委员会代表

“英特尔一直是软件包数据交换规范开发的早期参与者，并在内部和外部将软件包数据交换以及其他方法，广泛应用于多个开源软件的使用案例。”

—Melissa Evers，英特尔架构、图形、软件副总裁/软件业务战略总经理

斯堪尼亚公司标准4589刚刚向我们的供应商发布，定义了我们在供应商交付涉及开源软件时的期望。那么我们在与供应商的开源关系中，要求他们做什么呢？

1）供应商符合 ISO/IEC 5230：2020（OpenChain）。如果供应商符合此规范，我们确信他们拥有专业的开源管理计划。

2）如果在为斯卡尼亚开发解决方案的过程中，供应商对开源组件进行了修改，我们希望看到这些修改被贡献到开源项目中。

3）提供ISO/IEC DIS 5962（SPDX）格式的物料清单，以及有义务直接提供源代码的情况下，我们不需要主动请求它。

—Jonas Öberg，开源官—斯卡尼亚（大众集团）

软件包数据交换格式极大地促进了整个供应链中软件组件数据的共享。在过去的八年里，Wind River 一直使用软件包数据交换格式向其客户提供软件物料清单。客户通常会请求自定义格式的软件物料清单数据。软件包数据交换的标准化使我们能够以更低的成本提供更高质量的软件物料清单。

—Mark Gisi，Wind River 开源项目办公室主任兼OpenChain规范主席

Synopsys的Black Duck团队自软件包数据交换项目启动以来就一直参与其中，我有幸协调该项目领导团队的活动超过十年。此外，来自众多公司的代表们为开发一种标准化方式来描述和传达软件包内容的重要工作做出了贡献。

—Phil Odence, Synopsys的Black Duck 团队的审计总经理

随着人们对软件物料清单有助于解决的供应链风险类型的兴趣迅速增加，软件包数据交换获得了更广泛的关注和紧迫性。FossID（现在是Snyk的一部分）从一开始就将软件包数据交换用作软件组件分析和开源许可证审计的一部分。Snyk也在加大参与力度，通过构建工具来测试SPDX v3.0草案中的漏洞分析功能，也已经为扩展软件包数据交换的使用场景做出了贡献。

—Gareth Rushgrove，Snyk产品副总裁

# 原文：

# What is an SBOM?

###### THE LINUX FOUNDATION | 15 JUNE 2021

The National Telecommunications and Information Administration (NTIA) recently asked for wide-ranging feedback to define a minimum Software Bill of Materials (SBOM). It was framed with a single, simple question (“What is an SBOM?”), and constituted an incredibly important step towards software security and a significant moment for open standards.

From NTIA’s SBOM FAQ  “A Software Bill of Materials (SBOM) is a complete, formally structured list of components, libraries, and modules that are required to build (i.e. compile and link) a given piece of software and the supply chain relationships between them. These components can be open source or proprietary, free or paid, and widely available or restricted access.”  SBOMs that can be shared without friction between teams and companies are a core part of software management for critical industries and digital infrastructure in the coming decades.

The ISO International Standard for open source license compliance ([ISO/IEC 5230:2020 – Information technology — OpenChain Specification](https://www.iso.org/standard/81039.html)) requires a process for managing a bill of materials for supplied software. This aligns with the NTIA goals for increased software transparency and illustrates how the global industry is addressing challenges in this space. For example, it has become a best practice to include an SBOM for all components in supplied software, rather than isolating these materials to open source.

The open source community identified the need for and began to address the challenge of SBOM “list of ingredients” over a decade ago. The de-facto industry standard, and most widely used approach today, is called Software Package Data Exchange ([SPDX](https://spdx.dev/)). All of the elements in the NTIA proposed minimum SBOM definition can be addressed by SPDX today, as well as broader use-cases.

SPDX evolved organically over the last decade to suit the software industry, covering issues like license compliance, security, and more. The community consists of hundreds of people from hundreds of companies, and the standard itself is the most robust, mature, and adopted SBOM in the market today.

The full SPDX specification is only one part of the picture. Optional components such as SPDX Lite, developed by Pioneer, Sony, Hitachi, Renesas, and Fujitsu, among others, provide a focused SBOM subset for smaller supplier use. The nature of the community approach behind SPDX allows practical use-cases to be addressed as they arose.

In 2020, SPDX was submitted to ISO via the PAS Transposition process of Joint Technical Committee 1 (JTC1) in collaboration with the Joint Development Foundation. It is currently in the approval phase of the transposition process and can be reviewed on the ISO website as [ISO/IEC PRF 5962](https://www.iso.org/standard/81870.html).

The Linux Foundation has prepared a submission for NTIA highlighting knowledge and experience gained from practical deployment and usage of SBOM in the SPDX and OpenChain communities. These include isolating the utility of specific actions such as tracking timestamps and including data licenses in metadata. With the backing of many parties across the worldwide technology industry, the SPDX and OpenChain specifications are constantly evolving to support all stakeholders.

## Industry Comments

The Sony team uses various approaches to managing open source compliance and governance… An example is using an OSS management template sheet based on SPDX Lite, a compact subset of the SPDX standard. Teams need to be able to review the type, version, and requirements of software quickly, and using a clear standard is a key part of this process.

—**Hisashi Tamai, SVP, Sony Group Corporation, Representative of the Software Strategy Committee**

“Intel has been an early participant in the development of the SPDX specification and utilizes SPDX, as well as other approaches, both internally and externally for a number of open source software use-cases.”

—**Melissa Evers, Vice President – Intel Architecture, Graphics, Software / General Manager – Software Business Strategy**

Scania corporate standard 4589 (STD 4589) was just made available to our suppliers and defines the expectations we have when Open Source is part of a delivery to Scania. So what is it we ask for in a relationship with our suppliers when it comes to Open Source?

1) That suppliers conform to ISO/IEC 5230:2020 (OpenChain). If a supplier conforms to this specification, we feel confident that they have a professional management program for Open Source.

2) If in the process of developing a solution for Scania, a supplier makes modifications to Open Source components, we would like to see those modifications contributed to the Open Source project.

3) Supply a Bill of materials in ISO/IEC DIS 5962 (SPDX) format, plus the source code where there’s an obligation to offer the source code directly, so we don’t need to ask for it.

—**Jonas Öberg, Open Source Officer – Scania (Volkswagen Group)**

The SPDX format greatly facilitates the sharing of software component data across the supply chain. Wind River has provided a Software Bill of Materials (SBOM) to its customers using the SPDX format for the past eight years. Often customers will request SBOM data in a custom format. Standardizing on SPDX has enabled us to deliver a higher quality SBOM at a lower cost.

—**Mark Gisi, Wind River Open Source Program Office Director and OpenChain Specification Chair**

The Black Duck team from Synopsys has been involved with SPDX since its inception, and I had the pleasure of coordinating the activities of the project’s leadership for more than a decade. In addition, representatives from scores of companies have contributed to the important work of developing a standard way of describing and communicating the content of a software package.

—**Phil Odence, General Manager, Black Duck Audits, Synopsys**

With the rapidly increasing interest in the types of supply chain risk that a Software Bill of Materials helps address, SPDX is gaining broader attention and urgency. FossID (now part of Snyk) has been using SPDX from the start as part of both software component analysis and for open source license audits. Snyk is stepping up its involvement too, already contributing to efforts to expand the use cases for SPDX by building tools to test out the draft work on vulnerability profiles in SPDX v3.0.

—**Gareth Rushgrove, Vice President of Products, Snyk**