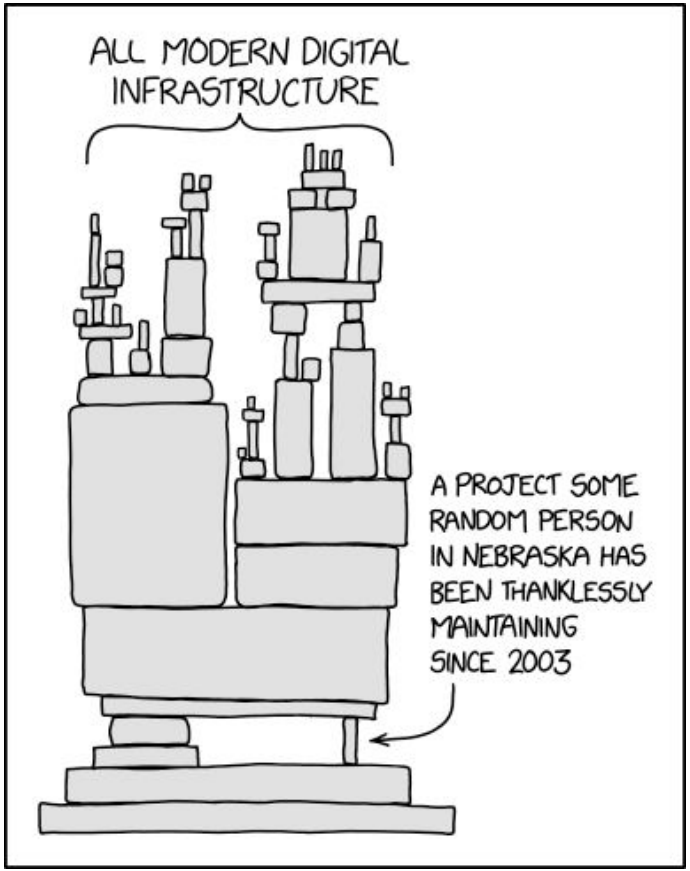
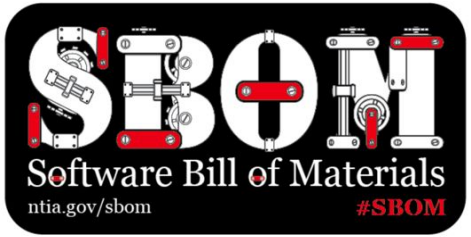
Software Bill of Materials Overview

Kate Stewart
@_kate_stewart

Most companies are **not** able to **accurately summarize** the software is running on their **systems**.



Software Bill of Materials (**SBOM**)



An SBOM is a formal record containing the details and supply chain relationships of various components used in building software.

These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-restricted.

Source: NTIA's SBOM FAQ


6 WAFFLES
AUTHENTIC
Belgian Waffles
ORIGINAL
NET WT 14.8 oz (420 g)
OAKRUN FARM
EST
BAKERY

Nutrition Facts

6 servings per container

Serving size 1 waffle (70g)

Calories per serving 310

Amount/serving	% Daily Value*	Amount/serving	% Daily Value*
Total Fat 16g	21%	**Total Carbohydrate** 37g	13%
Saturated Fat 8g	40%	Dietary Fiber 1g	4%
Trans Fat 0g		Total Sugars 17g	
Cholesterol 20mg	7%	Includes 17g Added Sugars	34%
Sodium 320mg	14%	**Protein** 4g	

Vitamin D 0mcg 0% • Calcium 16mg 2% • Iron 1mg 6% • Potassium 102mg 2%

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

INGREDIENTS: WHEAT FLOUR, VEGETABLE OIL BLEND (PALM, COCONUT AND RAPESEED OILS, WATER, MONO- AND DIGLYCERIDES), SUGAR, WATER, EGGS, INVERT SUGAR, YEAST, SOY FLOUR, SALT, NATURAL FLAVOR, SOY LECITHIN, FRUCTOSE, DEXTROSE.

CONTAINS: EGGS, SOY, WHEAT.

MADE IN A FACILITY THAT ALSO PROCESSES: MILK.

DISTRIBUTED BY:
ARYZTA LLC • SAN LEANDRO CA 94577 USA • 1-855-4-ARYZTA • WWW.OAKRUN.COM

PRODUCT OF BELGIUM

OAKRUN FARM EST 1979 BAKERY

Nutrition Facts

6 servings per container

Serving size 1 waffle (70g)

Calories per serving 310

Amount/serving	% Daily Value*	Amount/serving	% Daily Value*
Total Fat 16g	**21%**	**Total Carbohydrate** 37g	**13%**
Saturated Fat 8g	**40%**	Dietary Fiber 1g	**4%**
Trans Fat 0g		Total Sugars 17g	
Cholesterol 20mg	**7%**	Includes 17g Added Sugars	**34%**
Sodium 320mg	**14%**	**Protein** 4g	

Vitamin D 0mcg 0% • Calcium 16mg 2% • Iron 1mg 6% • Potassium 102mg 2%

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

INGREDIENTS: WHEAT FLOUR, VEGETABLE OIL BLEND (PALM, COCONUT AND RAPESEED OILS, WATER, MONO- AND DIGLYCERIDES), SUGAR, WATER, EGGS, INVERT SUGAR, YEAST, SOY FLOUR, SALT, NATURAL FLAVOR, SOY LECITHIN, FRUCTOSE, DEXTROSE.

[redacted]: EGGS, SOY, WHEAT.

MADE IN A FACILITY THAT ALSO PROCESSES [redacted]

DISTRIBUTED BY:
ARYZTA LLC • SAN LEANDRO CA 94577 USA • 1-855-4-ARYZTA • WWW.OAKRUN.COM

PRODUCT OF BELGIUM

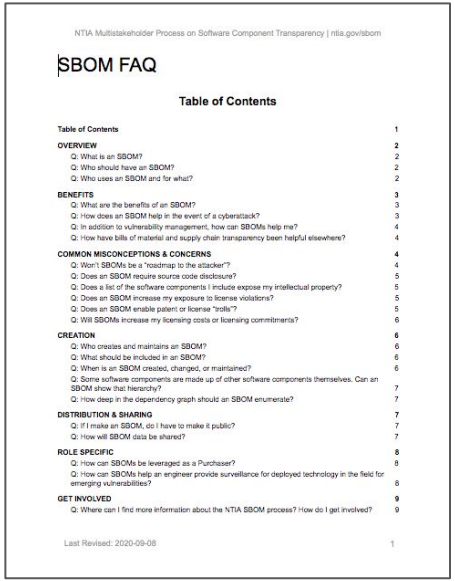
OAKRUN FARM EST 1979 BAKERY

Who should use an SBOM?

Any organization concerned about better supporting their software products internally, supporting their customers, and positively differentiating themselves in the marketplace should consider creating SBOMs and providing them to support their customers.

An SBOM is commonly required as part of any product's BOM so necessary information is available:

- **Contractual** - negotiated terms, implementation strategies
- **Legal** - compliance with licensing and regulatory obligations
- **Technical** - identification of software or component dependencies and supply chain risk, vulnerability, **safety analysis** and asset management



NTIA Multistakeholder Process on Software Component Transparency | ntia.gov/sbom

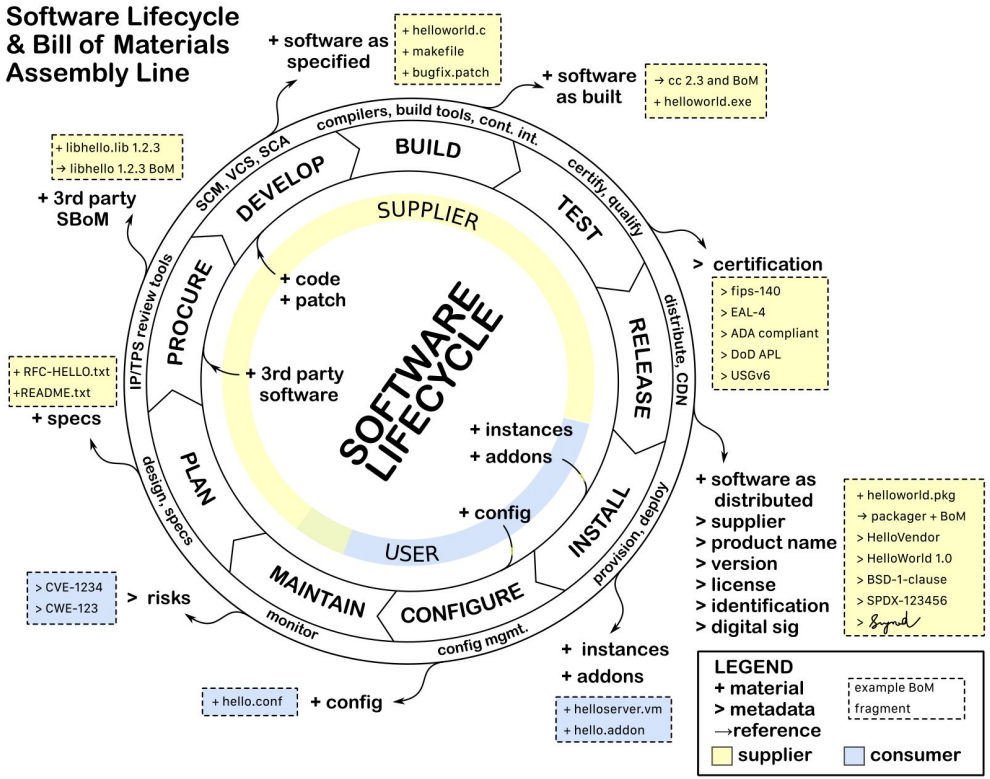
SBOM FAQ

Table of Contents

Last Revised: 2020-09-08 1

Source: [NTIA SBOM working group]

When should an SBOM be used?



Source: NTIA's [Survey of Existing SBOM Formats and Standards]

OPENCHAIN

OPENCHAIN Specification 2.0

3.0 Open Source Content Review and Approval

3.1 Bill of Materials

A process exists for creating and managing a bill of materials that includes each Open Source component (and its Identified Licenses) from which the Supplied Software is comprised.

Verification Material(s):

- ☐ 3.1.1 A documented procedure for identifying, tracking, reviewing, approving, and archiving information about the collection of Open Source components from which the Supplied Software is comprised.
- ☐ 3.1.2 Open Source component records for the Supplied Software that demonstrates the documented procedure was properly followed.

Rationale:

To ensure a process exists for creating and managing an Open Source component bill of materials used to construct the Supplied Software. A bill of materials is needed to support the systematic review and approval of each component's license terms to understand the obligations and restrictions as it applies to the distribution of the Supplied Software.

and is carried forward into OpenChain 2.1 which is now ISO/IEC 5230:2020

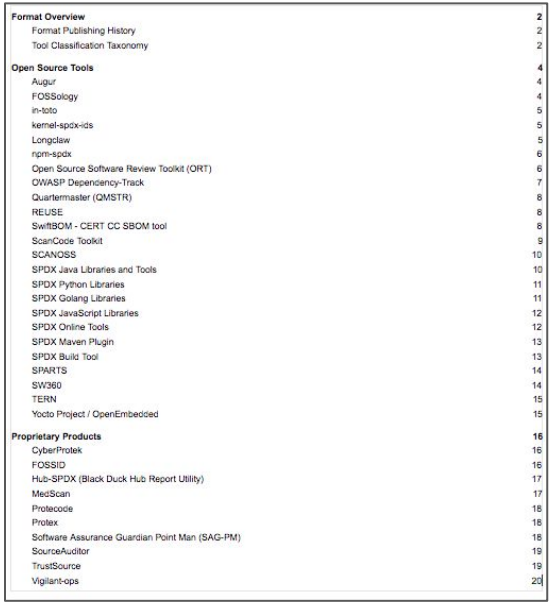
What should a minimum viable SBOM contain?

NTIA SBOM Baseline	SPDX	CycloneDX	SWID
Supplier Name	(3.5) PackageSupplier:	publisher	<Entity> @role (softwareCreator/publisher), @name
Component Name	(3.1) PackageName:	name	<softwareIdentity> @name
Unique Identifier	(3.2) SPDXID:	bom/serialNumber and component/bom-ref	<softwareIdentity> @tagID
Version String	(3.3) PackageVersion:	version	<softwareIdentity> @version
Component Hash	(3.10) PackageChecksum:	hash	<Payload>/../<File> @[hash-algorithm]:hash
Relationship	(7.1) Relationship: CONTAINS	(Nested assembly/subassembly and/or dependency graphs)	<Link> @rel, @href
Author Name	(2.8) Creator:	bom-descriptor:metadata/manufacture/contact	<Entity> @role (tagCreator), @name

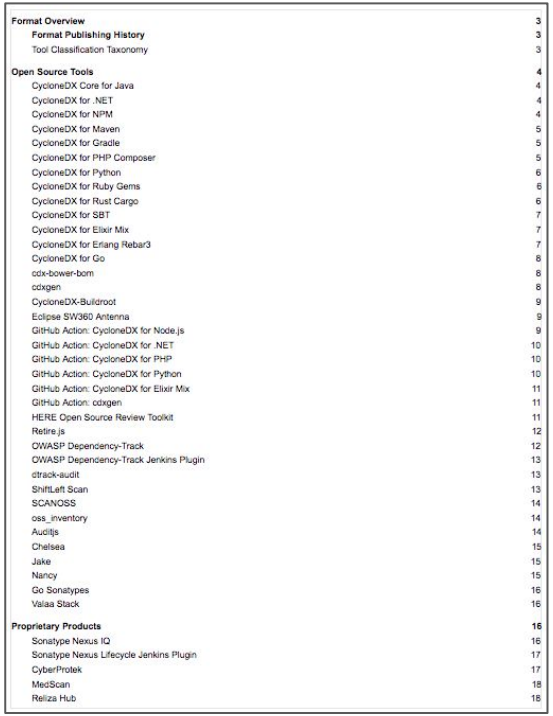
Source: NTIA's **Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)**

Tool Support for Different SBOM Formats

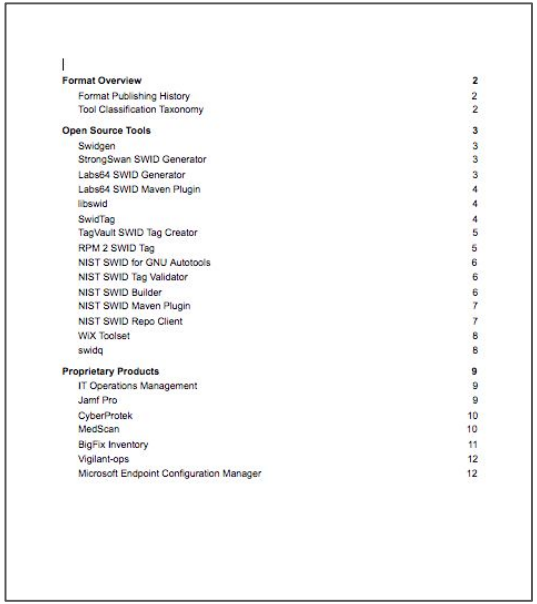
http://tiny.cc/SPDX



http://tiny.cc/CycloneDX



http://tiny.cc/SWID



Taxonomy used for Classifying SBOM Tools

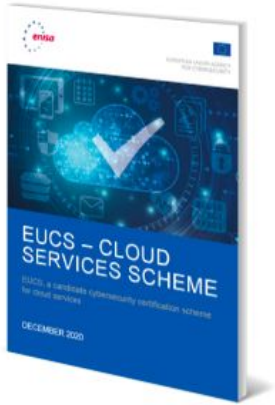
Category	Type	Description
Produce	Build	Document is automatically created as part of building an artifact and contains information about the build.
	Manual	A person will manually fill in the information
	Audit Tool	A source code analysis or audit tool will generate the document by inspection of the artifact and any associated sources.
Consume	View	Be able to understand the contents in human readable form (picture, figures, tables, text.). Use to support decision making & business processes.
	Diff	Be able to compare two documents of a given formation and clearly see the differences. For instance, comparing between two versions of a piece of software.
	Analyze	Be able to import a document into your system
Transform	Translate	Change from one file type to another file type while preserving the same information.
	Merge	Multiple sources of documents can be merged together for analysis and audit purposes
	Tool integration	Support use in other tools by APIs, libraries.

Why are you hearing more about them now?

- Supply chain security issues increasingly visible - Solarwinds, etc.
- Seeing as expectation from government & regulatory agencies:
  - in US: FDA, NERC
  - in Europe: ENISA Cybersecurity for Cloud Services

Ref	Description	Ass. Level
DEV-02.1	The CSP shall maintain a list of dependencies to hardware and software products used in the development of its cloud service	Basic
DEV-02.2	The CSP shall document and implement policies for the use of third-party and open source software	Substantial
DEV-02.3	The CSP makes its list of dependencies available to customers upon request	Substantial

Guidance elements	
DEV-02.1	For its software components, the list of dependencies is often called Software Board of Materials (SBoM). In the context of [EUCSA], Article 51(d) requires the identification and documentation of known dependencies. Dependencies should include all software modules, libraries or APIs used, as well as development tools.



Download
PDF document, 3.31 MB

Benefits from Adopting SBOMs

- Identifying both security and license **compliance requirements**
- Quantifying and managing **licenses**
- Identifying and avoiding known **vulnerabilities**
- Enabling **quantification of the risks** inherent in a software package
- **Managing mitigations** for vulnerabilities (including patching and compensating controls for new vulnerabilities)
- **Lower operating costs** due to improved efficiencies and reduced unplanned and unscheduled work.

These benefits can be seen by those who develop software, those who select or purchase software, and those who operate software, across every sector.

Source: NTIA's SBOM FAQ