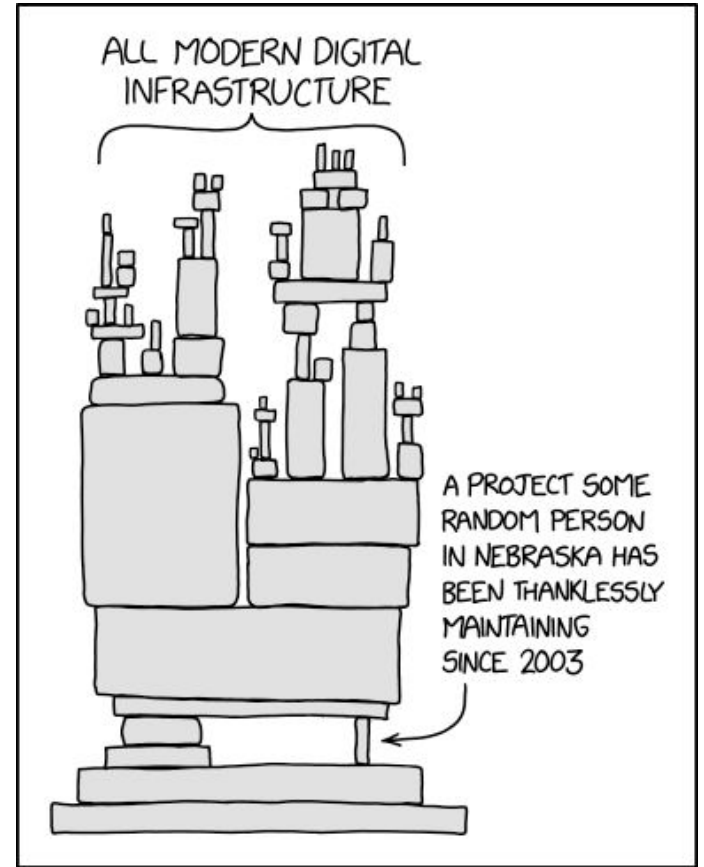


Software Bill of Materials Overview

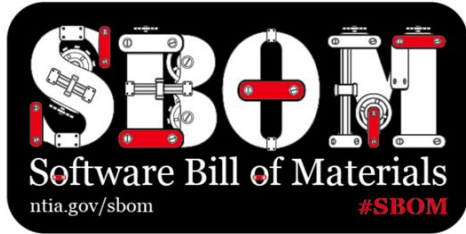
Kate Stewart
@_kate_stewart

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



Source: <https://xkcd.com/2347/> This work is licensed under a [Creative Commons Attribution-NonCommercial 2.5 License](https://creativecommons.org/licenses/by-nc/2.5/).

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](#)





Nutrition Facts

6 servings
per container

Serving size
1 waffle (70g)

Calories
per serving 310

Amount/serving

Total Fat 16g

Saturated Fat 8g

Trans Fat 0g

Cholesterol 20mg

Sodium 320mg

% Daily Value*

21%

40%

7%

14%

Amount/serving

Total Carbohydrate 37g

Dietary Fiber 1g

Total Sugars 17g

Includes 17g Added Sugars

Protein 4g

% Daily Value*

13%

4%

34%

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





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



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 | nta.gov/bom

SBOM FAQ

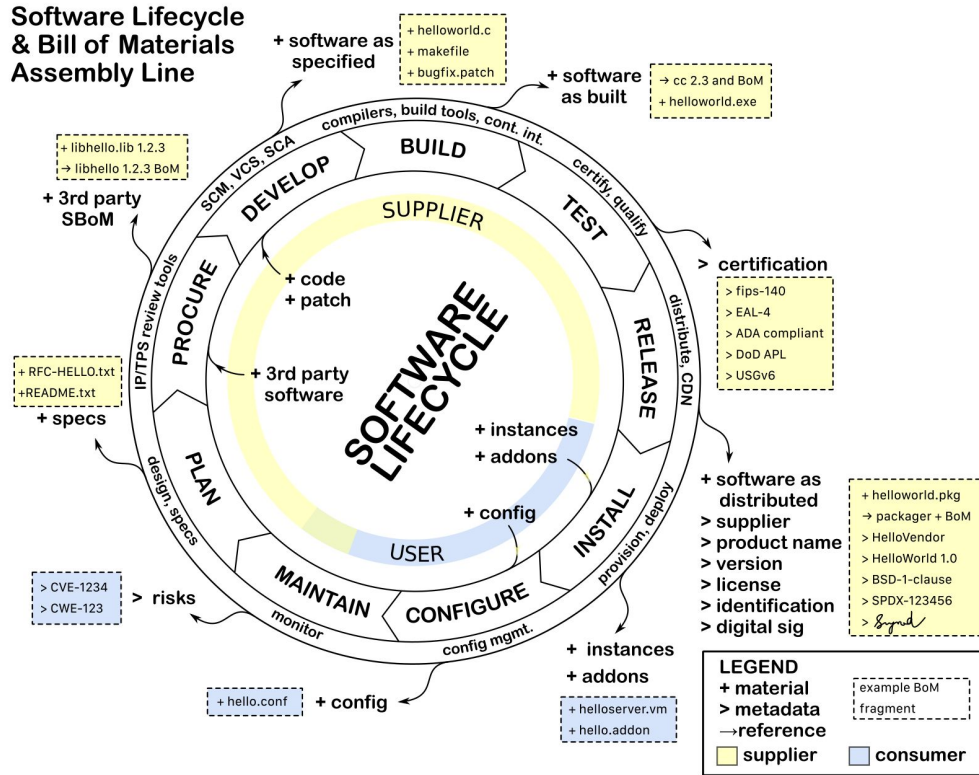
Table of Contents

Table of Contents	1
OVERVIEW	2
Q: What is an SBOM?	2
Q: Who should have an SBOM?	2
Q: Who uses an SBOM and for what?	2
BENEFITS	3
Q: What are the benefits of an SBOM?	3
Q: How does an SBOM help in the event of a cyberattack?	3
Q: In addition to vulnerability management, how can SBOMs help me?	4
Q: How have bills of material and supply chain transparency been helpful elsewhere?	4
COMMON MISCONCEPTIONS & CONCERNS	4
Q: Won't SBOMs be a "roadmap to the attacker"?	4
Q: Does an SBOM require source code disclosure?	5
Q: Does a list of the software components I include expose my intellectual property?	5
Q: Does an SBOM increase my exposure to license violators?	5
Q: Does an SBOM enable patent or license "tricks"?	5
Q: Will SBOMs increase my licensing costs or licensing commitments?	6
CREATION	6
Q: Who creates and maintains an SBOM?	6
Q: What should be included in an SBOM?	6
Q: When is an SBOM created, changed, or maintained?	6
Q: Some software components are made up of other software components themselves. Can an SBOM show that hierarchy?	7
Q: How deep in the dependency graph should an SBOM enumerate?	7
DISTRIBUTION & SHARING	7
Q: If I make an SBOM, do I have to make it public?	7
Q: How will SBOM data be shared?	7
ROLE SPECIFIC	8
Q: How can SBOMs be leveraged as a Purchaser?	8
Q: How can SBOMs help an engineer provide surveillance for deployed technology in the field for emerging vulnerabilities?	8
GET INVOLVED	9
Q: Where can I find more information about the NTIA SBOM process? How do I get involved?	9

Last Revised: 2020-09-08 1

Source: [NTIA SBOM working group](#)

When should an SBOM be used?



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>

Format Overview	2
Format Publishing History	2
Tool Classification Taxonomy	2
Open Source Tools	4
Augur	4
FOSSology	4
in-toto	5
kernal-spdx-ids	5
Longlaw	5
npm-spdx	6
Open Source Software Review Toolkit (ORT)	6
OWASP Dependency-Track	7
Quartermaster (QMSTR)	8
REUSE	8
SwiftSBOM - CERT CC SBOM tool	8
ScanCode Toolkit	9
SCANGSS	10
SPDX Java Libraries and Tools	10
SPDX Python Libraries	11
SPDX Golang Libraries	11
SPDX JavaScript Libraries	12
SPDX Online Tools	12
SPDX Maven Plugin	13
SPDX Build Tool	13
SPARTS	14
SW360	14
TERN	15
Yocto Project / OpenEmbedded	15
Proprietary Products	16
CyberProtek	16
FOSSID	16
Hub-SPDX (Black Duck Hub Report Utility)	17
MedScan	17
Protecode	18
Protex	18
Software Assurance Guardian Point Man (SAG-PM)	18
SourceAuditor	19
TrustSource	19
Vigilant-ops	20

<http://tiny.cc/CycloneDX>

Format Overview	3
Format Publishing History	3
Tool Classification Taxonomy	3
Open Source Tools	4
CycloneDX Core for Java	4
CycloneDX for .NET	4
CycloneDX for NPM	4
CycloneDX for Maven	5
CycloneDX for Gradle	5
CycloneDX for PHP Composer	5
CycloneDX for Python	6
CycloneDX for Ruby Gems	6
CycloneDX for Rust Cargo	6
CycloneDX for SBT	7
CycloneDX for Elixir Mix	7
CycloneDX for Erlang Rebar3	7
CycloneDX for Go	8
cde-bower-bom	8
cdxgen	8
CycloneDX-Buildroot	9
Eclipse SW360 Antenna	9
GitHub Action: CycloneDX for Node.js	9
GitHub Action: CycloneDX for .NET	9
GitHub Action: CycloneDX for PHP	10
GitHub Action: CycloneDX for Python	10
GitHub Action: CycloneDX for Elixir Mix	11
GitHub Action: cdxgen	11
HERE Open Source Review Toolkit	11
Retire.js	12
OWASP Dependency-Track	12
OWASP Dependency-Track Jenkins Plugin	13
stackvault	13
SHILLER Scan	13
SCANGSS	14
oss_inventory	14
Auditfs	14
Chelsea	15
Jake	15
Nancy	15
Go Sonatypes	16
Valias Stack	16
Proprietary Products	16
Sonatype Nexus IQ	16
Sonatype Nexus Lifecycle Jenkins Plugin	17
CyberProtek	17
MedScan	18
Reliza Hub	18

<http://tiny.cc/SWID>

Format Overview	2
Format Publishing History	2
Tool Classification Taxonomy	2
Open Source Tools	3
Swidgen	3
StrongSwan SWID Generator	3
Labels4 SWID Generator	3
Labels4 SWID Maven Plugin	4
libswid	4
SwidTag	4
TagVault SWID Tag Creator	5
RPM 2 SWID Tag	5
NIST SWID for GNU Autotools	6
NIST SWID Tag Validator	6
NIST SWID Builder	6
NIST SWID Maven Plugin	7
NIST SWID Repo Client	7
WX Toolset	8
swidq	8
Proprietary Products	9
IT Operations Management	9
Jamf Pro	9
CyberProtek	10
MedScan	10
BigFix Inventory	11
Vigilant-ops	12
Microsoft Endpoint Configuration Manager	12

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



[Download](#)
PDF document, 3.31 MB

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.

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.