

SBOM Field Table Mapping

Version 2.0

1 March 2024

This document provides a mapping of the National Telecommunications and Information Administration (NTIA) Minimum Elements for a Software Bill of Materials (SBOM) to the formats required by NIAP Policy #30. This document is based on SPDX v2.3 and CycloneDX v1.4 but more recent versions of the formats should be used if required to appropriately document the Elements, e.g., Component Data Type.

NTIA Element	Description	SPDX (v2.3)	CycloneDX (v1.4)
Component Name	Designation assigned to a unit of software defined by the original supplier	PackageName	name
Component Version	Identifier used by the supplier to specify a change in software from a previously identified version	PackageVersion	version
Unique Identifier	Other identifier used to identify a component, or serve as a look-up key for relevant databases	SPDXID	bom-ref swid
Component Supplier	The name of an entity that creates, defines, and identifies, components.	PackageSupplier	supplier publisher
Dependency Relationship	Characterizing the relationship that an upstream component "X" is included in software "Y"	Relationship	dependsOn
SBOM Author	The name of the entity that creates the SBOM data for this component	Creator	authors
SBOM timestamp	Record of date and time of the SBOM creation	Created	timestamp
SBOM Hash*	Unique value to prove the integrity of the SBOM	FileChecksum	signature
Component Hash*	Unique identification value of a specific package that correlates to the component data	PackageChecksum	hash
Component Data Type**	Provides information about the primary purpose of the identified component. This is intrinsic to how the package is being used rather than the content of the package.	PrimaryPackagePurpose	Type***

*Accepted algorithms must comply with NIST SP 800-186 and FIPS 186-5.

** Component Data Type is not an NTIA Element but is specified in CycloneDX and SPDX

***For software components, classify as application if no more specific appropriate classification is available or cannot be determined for the component

Additional Information

Component Data Types

Note: Some products may require component types from more recent versions of the specified formats. In these cases, the most recent versions of CycloneDX and SPDX should be used.

Definition	CycloneDX Component Type	SPDX Component Type
	application	APPLICATION
	framework	FRAMEWORK
	library	LIBRARY
image which can be used by a container runtime application	container	CONTAINER
	operating-system	OPERATING SYSTEM
refers to a chipset, processor, or electronic board	device	DEVICE
provides low level control over a device's hardware	firmware	FIRMWARE
single file which can be independently distributed (configuration file, statically linked binary, Kubernetes deployment, etc)	file	FILE
refers to an archived collection of files (.tar, .zip, etc)		ARCHIVE
collection of source files		SOURCE
used to install software on disk		INSTALL
if the package doesn't fit into the above component types		OTHER