SBOM Options and Decision Points

"We are all in a supply chain – most of us are in the middle."

Purpose

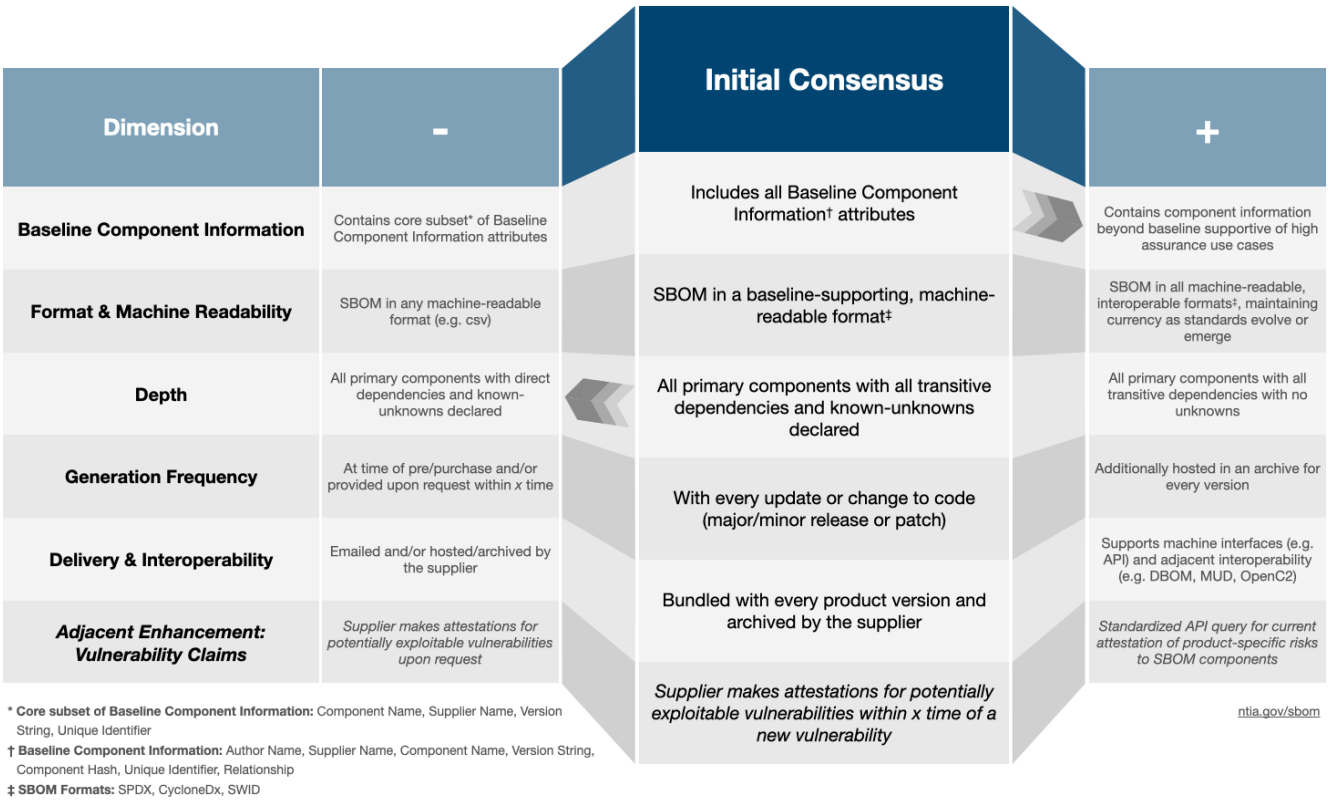
The purpose of this document is twofold with regard to Software Bill of Materials (SBOM). First, to frame the dimensions for what is possible with modern development practices. Second, to support more consistent and effective articulation of needs between requesters and suppliers of SBOMs. Subsequent documents elaborate on each perspective.

Introduction

As a companion to "SBOM at a Glance", this document highlights six of the key dimensions and decision points that emerged from the NTIA multistakeholder process for SBOM. For each of these SBOM dimensions, the graphic below presents three things:

- The initial consensus for what is possible today with modern development processes,
- Enhancements (+) for emerging and high assurance use cases, and
- Fallbacks (-) to accommodate industry adoption time and legacy processes/technologies

Depicted fallback and enhancement examples are independent and exist on a continuum.



SBOM Options and Decision Points

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within *x* time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	*Supplier makes attestations for potentially exploitable vulnerabilities upon request*	*Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability*	*Standardized API query for current attestation of product-specific risks to SBOM components*

* **Core subset of Baseline Component Information:** Component Name, Supplier Name, Version String, Unique Identifier
† **Baseline Component Information:** Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship
‡ **SBOM Formats:** SPDX, CycloneDx, SWID

Last revised: 2021-04-27