

# SBOM Use Case

SCITT Use Case Discussion

September 12, 2022

# Types of SBOM's

- SBOM are used for various purposes
  - License Management
  - Dependency Tracking
  - Risk Assessment
  - Vulnerability Monitoring
- SBOM content is “tuned” to serve its intended purpose
- This Use Case represents an SBOM that consumers require for Risk Management and Vulnerability Monitoring

# Consumer SBOM Requirements

- Listing of components that **will be installed in a customer ecosystem** including on-premise and cloud infrastructure
- MUST satisfy NTIA minimum requirements
- [Serves as an attestation](#) by a vendor claiming the complete list of components included in a software PRODUCT
- SBOM is just one of several “evidence artifacts” needed for Executive Order 14028 following [NIST SP 800-161 recommendations](#) and [Other NIST guidance](#)
- Ideally, include link to NIST SBOM Vulnerability Disclosure Report (SBOM VDR) see [SPDX Version 2.3 K.1.9](#) for details
- Following [NTIA Framing guidelines](#) second edition (2021), the “Primary Component” (first one listed in SBOM) represents the “Product Level”

# NTIA Guidelines

A note about terminology in this document: *Components* are units of software defined by suppliers or authors. *Attributes* are information about components and SBOM entries, primarily designed to identify components. An *SBOM entry* identifies a component and its associated attributes. An *SBOM* is a collection of one or more *SBOM entries*.

Software that might commonly be called a “product” is treated as a type of component, often considered to be the primary component and subject of the SBOM.

More terms are defined in [Section 4](#).

REF: page 8 of NTIA Framing Document

# NTIA Minimum Elements

<b>Data Field</b>	<b>Description</b>
<b>Supplier Name</b>	The name of an entity that creates, defines, and identifies components.
<b>Component Name</b>	Designation assigned to a unit of software defined by the original supplier.
<b>Version of the Component</b>	Identifier used by the supplier to specify a change in software from a previously identified version.
<b>Other Unique Identifiers</b>	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
<b>Dependency Relationship</b>	Characterizing the relationship that an upstream component X is included in software Y.
<b>Author of SBOM Data</b>	The name of the entity that creates the SBOM data for this component.
<b>Timestamp</b>	Record of the date and time of the SBOM data assembly.

# CISA ICT\_SCRM Task Force

- <https://www.cisa.gov/ict-scrm-task-force>
- This use case is under consideration by the Small and Medium Business work group for publication this year
- Two SBOM examples are available online:
  - [SPDX Version 2.3](#) (with link to NIST SBOM VDR)
  - [CycloneDX Version 1.2](#)

# SBOM Discovery and Distribution Today

- Software Vendor provides URL to SBOM ([REA uses an open-source VRF](#) to identify all required NIST SP 800-161 evidence data and NIST attestations for a consumer to download)
- SBOM is typically located on a Customer Portal, under access control
- Consumers may request a particular SBOM representation and format, i.e. SPDX V 2.3 in JSON format
- Vendors may produce only a single SBOM type and format, i.e. CycloneDX in XML format
- Ideally SBOM's are digitally signed and Vendor provides information to verify legitimate signatures (X.509 Thumbprint) for specific software packages, identified by a SHA-256 hash value
- Combination of SHA-256 hash and X.509 Thumbprint are used to verify “trust declarations” for a software product in a Registry (i.e. SAG-CTR™ in REA's scenario)

# SBOM Use Case Review for SCITT

- [https://hackmd.io/QuqKhy\\_bQ1qG9yyyBuEABg?view](https://hackmd.io/QuqKhy_bQ1qG9yyyBuEABg?view)