NTIA Framing - Naming-Focused Use Cases

Actors

- Author – the author of an SBOM. It may be the Supplier of the Primary Component or another SBOM Stakeholder
- SBOM Consumer – an entity that consumes SBOMs. Examples include a Healthcare Delivery Organization that procures medical devices, or a Medical Device Manufacturer that develops medical devices and includes third-party components.
- SBOM Stakeholder – a Supplier or SBOM Consumer
- Supplier – an entity that creates SBOMs for the components they development. A supplier may also consume SBOMs for included components.

Artifacts

- Baseline Elements – the set of SBOM baseline elements defined by the Framing Group:
    - Author Name
    - Supplier Name
    - Component Name
    - Version String
    - Component Hash
    - Unique Identifier
    - Relationship
- Component – a software element used by a Supplier. In some cases, a Component is also a Primary Component
- Primary Component – a software element developed by a Supplier that is described by the SBOM
- SBOM – a document that identifies the software Components that make up the Bill of Materials for a Primary Component. The SBOM also contains the identifying information for the Primary Component.

Summary-Level Use Case: An SBOM is used to provide Software Transparency

A summary-level use case that is executed over an extended period of time.

User-Goal Use Cases	Assumptions	Steps	Example/Notes
Use Case 1: A Supplier Creates an SBOM for a Primary Component	• Supplier is source of truth for the Baseline Elements and any other information associated with the Primary Component • Supplier provides Baseline Elements in their SBOM	1. Supplier establishes their Supplier Name for the Primary Component following industry guidance 2. Supplier follows best practices for establishing the Component Name and Version String 3. Supplier identifies the first-level Components used by the Primary Component 4. Supplier obtains an SBOM for each included Component 5. The Supplier creates an SBOM in an industry recommended format a. Supplier keeps track of this information during the lifecycle process b. Supplier will include as many of the Baseline Elements as possible as well as any additional information they deem useful or necessary c. The Supplier uses the Component SBOM to obtain the included Component's Baseline Elements (see Use Case 3)	ACME creates the ACME infusion pump and ACME creates the SBOM for the infusion pump that contains (at least) its first level components (Bob's browser, etc.). The SBOM will clearly identify the ACME infusion Pump, which is the Primary Component. A Supplier registry may be used to establish the Supplier Name. Tooling, specifications, etc. may be used to identify the Components.

User-Goal Use Cases	Assumptions	Steps	Example/Notes
Use Case 2: An SBOM Stakeholder Creates an SBOM	• The Supplier of the Component has not created an SBOM • The SBOM Stakeholder is now the Author • The SBOM Stakeholder will make a best-effort approach to establishing the baseline information • The SBOM Stakeholder will follow the SBOM Component Naming Best Practices • Based on the SBOM content, the SBOM Consumer will be able to determine that the SBOM was not created by the Supplier of the Component	1. The SBOM Stakeholder follows best practices for naming 2. The SBOM Stakeholder makes a best-effort approach to identify the Components 3. The SBOM Stakeholder will include as many of the Baseline Elements as possible as well as any additional information they deem useful or necessary 4. The SBOM Stakeholder creates an SBOM in an industry recommended format 5. The SBOM Stakeholder will list themselves as the Author so it is clear that the SBOM information is not from the Supplier	Mustard Hospital finds an old ACME infusion pump purchased 10 years ago, it does not have an SBOM and nor does ACME so Mustard leverages a tool or third party to create an SBOM for them. If (1) a supplier wanted to provide a notice of unfixed vulnerabilities for components not directly included or (2) a supplier wanted to provide a notice of non-exploitability of vulnerabilities of components not directly included THEN they might want to create “best effort" included SBOMs to make it clear which included components were being referenced. This would be especially important in cases where there were multiple instances of an included component in a product but where some but not all had patches applied. The Author may use tooling or other means to identify the Components.

User-Goal Use Cases	Assumptions	Steps	Example/Notes
Use Case 3: A Supplier Includes the Baseline Elements for an Included Component in the SBOM	• The SBOM should be obtained from the Supplier of the included Component • Baseline Elements from the SBOM should be used to identify the included Component • If the Component SBOM is not available, a best-effort approach should be used to establish the Baseline Elements (see Use Case 2) • A Supplier may include the optional Component Hash. • If the Supplier creates an instance of the component, then the Supplier should generate the hash (e.g. a build of OpenSSL v1.1.1) • Otherwise, the Component Hash from the SBOM should be used if available	1. A Supplier includes a Component in their Primary Component 2. The Supplier obtains the SBOM for the Component 3. The Supplier obtains the Baseline Elements for the included Component from the Component SBOM they obtained 4. The Supplier adds the Component to the SBOM for the Primary Component and identifies the Component in the SBOM by using the Baseline Elements	ACME wants to include a DOORS Operating System in its new infusion pump so ACME obtains the SBOM from DOORS
Use Case 4: A Supplier Distributes an SBOM	• Industry best practices should be followed for distributing the SBOM.	1. Supplier will provide this information to SBOM Consumer in a way they have established and communicated	This use case will be further expanded in the future.

User-Goal Use Cases	Assumptions	Steps	Example/Notes
Use Case 5: An SBOM Consumer Uses a SBOM	• The SBOM Consumer has obtained an SBOM for a Component • The Supplier has included the Baseline Elements in the SBOM that identify the Primary Component and the included Components	1. A SBOM Consumer obtains an SBOM for a Primary Component 2. The SBOM Consumer uses the SBOM to identify the included Components 3. The SBOM Consumer determines that a vulnerability has been reported against an included Component 4. The SBOM Consumer contacts the Supplier and requests information about the vulnerability 5. The Supplier provides details on the impact of the vulnerability (e.g. no impact) and actions the SBOM Consumer should take (e.g. no action required, patch available)	Mustard Hospital gets an SBOM from ACME for an infusion pump. New vulnerability, KNOCK KNOCK, is reported and is related to DOORS operating system. Mustard looks at ACME's SBOM and sees it uses the DOORS operating system. A car manufacturer has a software problem and issues a recall to update the software. The car manufacturer is ultimately responsible to notify customer and get patch applied through the dealer. Multiple actions may be taken by the SBOM Consumer when using an SBOM, such as checking a Software License, etc. This is just one example.