NTIA Software Component Transparency Guidance Document

Note to reader: this guidance document is intended to reflect the Software Transparency initiative and help guide our work. This document is offered as a draft and is intended to foster communication and alignment within and between the working groups. All members are encouraged to read, feedback, and propose changes that ensures a fully representative and accurate document. Specific language recommendations are useful.

I. Mission Statement

Develop and execute an approach for how manufacturers and vendors can communicate useful and actionable information about the third-party software components that comprise modern software and IoT devices, and how this data can be used by enterprises to foster better security decisions and practices.

The goal of this initiative is to foster a market offering greater transparency to organizations, who can then integrate this data into their risk management approach.

(source: NTIA Software Transparency website)

II. Scope

The scope of this initiative will include the definition of the structure of an sBOM, how it can be shared, and how it can be used to help foster better security decisions and practices. To make the sBOM useful, this initiative will also need to outline the applicable use cases to ensure that the output is useful for all stakeholders.

All industries utilizing software should be considered in scope of this initiative, including automotive, financial, healthcare, and “traditional” IT.

Related Dependencies and Supporting Activities:

- Methodology for mapping vulnerabilities to components
- Stand-up of unified sharing mechanism for sBOMs
- Approach for documenting relationship between components for any given sBOM
- License management
- Lists of known vulnerabilities, exploitability, or patch level

III. Goals

The overall goal of this initiative is to outline of the idea of software transparency and the problems it seeks to solve, including how to share SBOM data. This is intended to help reduce cybersecurity risk. It will be approached primarily by sharing information about

software components with the necessary stakeholders so that users can do better risk management, specifically vulnerability management and impact assessments. With this, the user can prioritize vulnerability responses and management, including adjusting the risk assessment and taking actions in addition to patching.

A standardized model for software component information that is structured for sharing across multiple industry sectors
The information required should be set at a minimum needed for the purposes identified to minimize burden to vendors and users.

The goals of this initiative include:

High Level Goals

1. Ensure process is community-driven, consensus-led, and risk-based (ALL)
2. Define/gain consensus on one or a constrained number of (initial) use cases. I'm going to strongly recommend "Vulnerability Management" is one required use case. Risk Assessment and Acquisition/Procurement could be others. (I've also hear asset management and vendor management). I'd almost make this the first goal but I'm OK with community/consensus being first. I've listened into some of the other WG calls and everybody is struggling with use cases. (Framing, or possibly all WGs)
3. Define the list of stakeholders: sBOM providers and sBOM consumers (Framing)
4. Meet common needs across sectors, e.g. healthcare, automotive, traditional IT
5. Identify list of users of sBOMs (Framing, Use Cases)
6. Identify purpose of the sBOM (Framing)

Terminology and Definitions

1. Define sBOM (requires agreement on intended use/use cases first!) (Framing)
2. Decide if sBOM is the right term or if it is something else (Framing)
    a. sBOM, SBOM, sBoM, CBOM?
3. Define useful terminology (Framing)
        a. Define component, package, product

Designing the sBOM

1. Identify SBoM requirements (Framing, others?)

2. Define sBOM structure, including naming conventions (S&F)
3. Ensure sBOM is human-readable, machine-readable and collatable (S&F)
4. Outline the level of granularity in sBOM, i.e. to what level does the sBOM need to go (S&F) –
    a. need a good definition of what is a product, what is a component and what is a package.
5. Ensure level of detail in sBOM is lightweight enough to be feasible yet still provide enough detail (S&F)

Sharing the sBOM

1. Propose methodology for how sBOM information will be shared to ensure that it is updatable and accessible (Framing)
2. Define frequency of sBOM updates (Framing)

Using the sBOM

1. Define Use Cases for how sBOMs will be used both currently and in future (Use Case) - including supporting the out of scope items
2. Detail barriers to success (Use Case or Framing?)
3. Define “Meta Use Cases or Functional Uses” – defining general uses of sBOMs and the needed functionality (Framing)
4. Outline how sBOM may be shared (Framing)
5. Provide implementation guides (Framing)
6. Detail a proof of concept from a real-world scenario (Healthcare POC)
7. Provide guidance to providers and users of sBOMs, including how to make and use (Framing)

IV. Big Open Questions

1. Big open questions go here? We need to raise and eventually define them to create the sandbox?
2. See slides too

V. Expected Initial Deliverables

1. Guidance document for NTIA Software Component Transparency initiative (this document)
2. List of users of sBOM
3. List and description of use cases
4. Structure of sBOM (list of elements required)
5. Useful Terminology and Definitions
6. Map of Use Cases to Case Studies
7. Purpose of the sBOM
8. Limitations of an sBOM (what the sBOM cannot provide)

Framing Deliverables for Feb F2F

1. Guidance Document, initial version outlining first phase mission, scope, goals
2. Initial list of Functional Uses/Meta Use Cases
3. Initial Structure of Base sBOM example

VI. sBOM example

SW Component	***Developer/ Manufacturer Name***	***Major Version***					***Comments***
Protocol Buffers (C#)	Google	Proto3					
Windows Embedded 8.1 Industry Pro 64-bit	Microsoft	N/A					
Microsoft SQL Server 2012 Express (Service Pack 3)	Microsoft	11.0.6020.0					
OpenSSL	OpenSSL	0.9.8a					

VII. Phased Deliverables

VIII. Planning for Phases