SBOM Myths vs. Facts

The NTIA Multistakeholder Process on Software Component Transparency[1] seeks to provide industry-agnostic guidance and resources to support adoption and implementation of Software Bill of Materials (SBOM).[2]

As the practice of SBOM expands beyond trailblazing industries (e.g., Financial Services and Healthcare) and becomes more widely adopted, the resulting network effect will amplify the initial and inherent benefits that SBOMs provide. With increased awareness comes increased opportunity for misunderstanding. This document is intended to help the reader to understand and dispel common, often sincere myths and misconceptions about SBOM. This list is not intended to be comprehensive. For more common questions and concerns, see the SBOM FAQ.[3]

The Myths	The Facts
Myth: SBOMs are a roadmap to the attacker	Attackers can leverage the information contained in SBOMs. However, the defensive benefits of transparency far outweigh this common concern as SBOMs serve as a "roadmap for the defender". All information is dual-edged, but insufficient software transparency affords attackers asymmetrical advantages. ● Attackers don't need SBOMs. Mass, indiscriminate attacks like WannaCry serve to remind us that foreknowledge is not a prerequisite to cause harm. ● Attackers and their tools can more easily identify software components. Conversely, it is often quite challenging, disruptive, inefficient, and even unlawful for defenders to determine the same. ● Attackers of any single product can already find human-readable target components – licensing requirements have been increasingly requiring disclosure for decades. SBOMs seek to level the playing field for defenders by providing additional transparency – at enterprise scale – with standard, machine-readable decision support.
Myth: An SBOM alone provides no useful or actionable information	The baseline component information supports a number of use cases for those who produce, choose, and operate software, as outlined in NTIA's "Roles and Benefits" document.[4] For example, during an active attack, an SBOM allows an enterprise to answer, "Am I affected?" and "Where am I affected?" in minutes or hours, instead of days or weeks. Additionally, the baseline component information enables vital transparency and auditability, allowing for further expansion and enrichment in additional use cases. The Executive Order on Improving the Nation's Cybersecurity (No. 14028)[5] also expects significant value for federal agencies.
Myth: An SBOM needs to be made public	An SBOM does not need to be made public. The act of making an SBOM is separate from sharing it with those who can use this data constructively. The author may advertise and share the SBOM at their discretion. In other cases, sector-specific regulations or legal requirements may require more or less access to the SBOM. The Executive Order on Improving the Nation's Cybersecurity (No. 14028) is also clear that making an SBOM publicly available is a choice, not a requirement. Section 4 (e) (vii) states "providing a purchaser a Software Bill of Materials (SBOM) for each product directly **or** by publishing it on a public website."[6]

Myth: SBOMs will expose my intellectual property/trade secrets	SBOMs are a summary of included software components and do not expose intellectual property (IP). Patents and algorithms are not included. There are several things to consider with regard to SBOM contents and IP: ● There is a difference between a list of ingredients and a recipe. ● The IP of third-party open-source components belongs to their respective authors or copyright holders. ● It is increasingly common for component licensing terms to require disclosure. ● Code is not included in an SBOM, just component references. ● Contracts, legal agreements, or other requirements may prohibit the disclosure of certain components. In this case, the SBOM should indicate the presence of a unique "known unknown" component. Independent of the content of the SBOM, the confidentiality and distribution of the SBOM is up to the producer, and need not necessarily be public. (See also: "Myth: An SBOM needs to be made public")
Myth: No processes exist to support scalable production and use of SBOMs	William Gibson said, "The future is already here – it's just not evenly distributed." Software composition analysis tools have been used internally in some sectors for more than a decade. However, the practice of sharing across organizational boundaries is new. A growing list of commercial and open-source tools[7,8,9] is emerging as a result of a confluence of industry activities, including the NTIA multistakeholder process on Software Component Transparency,[10] Executive Order on Improving the Nation's Cybersecurity (No. 14028),[11] multiple industry Proofs of Concept,[12,13,14] and three translatable SBOM formats.[15,16,17] Processes and integrations are also co-evolving as a result of increased adoption across sectors. Some sectors are already further along (5+ years) in their journey and, through the proofs of concept, are supporting SBOM adoption in other industries. The machine-readability of SBOMs further enables scalability. The combination of all these developments and innovations supports many options for implementations at scale. For historical context and comparable journeys, other foundational cybersecurity infrastructure, such as CVE and MITRE ATT&CK, also started with limited people, processes, and technology. Past investments in their potential now benefit cybersecurity and all who depend upon it. Investments in SBOM are expected to have similar long-ranging benefits.

References

[1] NTIA Multistakeholder Process on Software Component Transparency https://www.ntia.gov/SoftwareTransparency.

[2] NTIA Software Bill of Materials https://www.ntia.gov/SBOM.

[3] NTIA SBOM FAQ https://www.ntia.doc.gov/files/ntia/publications/sbom_faq_-_20201116.pdf.

[4] Roles and Benefits for SBOM Across the Supply Chain https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf.

[5] Executive Order on Improving the Nation's Cybersecurity, No. 14028 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[6] Executive Order on Improving the Nation's Cybersecurity, No. 14028 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[7] SPDX Tools List https://tiny.cc/SPDX (Google login required).

[8] CycloneDX Tools List https://tiny.cc/CycloneDX (Google login required).

[9] SWID Tools List https://tiny.cc/SWID (Google login required).

[10] NTIA Multistakeholder Process on Software Component Transparency https://www.ntia.gov/SoftwareTransparency.

[11] Executive Order on Improving the Nation's Cybersecurity, No. 14028 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[12] Healthcare Proof of Concept Report https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf.

[13] Energy Sector SBOM Proof of Concept https://inl.gov/sbom-poc/.

[14] Automotive ISAC Summit – SBOM Proof of Concept https://automotiveisac.com/auto-isac-summit-2021/.

[15] SPDX Spec https://spdx.github.io/spdx-spec/.

[16] CycloneDX Spec https://cyclonedx.org/docs/.

[17] SWID Spec https://www.iso.org/standard/65666.html.