Response to the National Telecommunications and Information Administration call for Software Bill of Materials Elements and Considerations

Author: Brian Fox (bfox@sonatype.com)
Title: CTO and Cofounder, Sonatype Inc.

As the long-time stewards of Maven Central and key members of the open source software community, Sonatype applauds the National Telecommunications and Information Administration (NTIA) and its effort to define and publish the minimum elements for a Software Bill of Materials (SBOM).

Through this comment, Sonatype recommends two key requirements be added to enable practical, scalable, and interoperable use of SBOMs in support of The Executive Order on Improving the Nation's Cybersecurity.

The first recommendation is to mandate machine readability, rather than merely recommend it. The EO only required that SBOMS be made available by being "published directly" or "on a public website". Further, NTIA's published Notice (RIN 0660–XC051) recommends, but does not require, that SBOMs be machine readable ("**should** be machine-readable and **should** allow ''for greater benefits through automation and tool integration.'').

Since nearly all software is composed of reusable components, a completed application's SBOM will necessarily be constructed by exposing the SBOMs of each underlying dependency all the way down the stack. Given the pace of modern software development, it is not feasible to manually share and consume SBOMs. Therefore, mandating that SBOMs support machine readability is the only scalable solution.

The second recommendation is to mandate SBOM standards that fundamentally offer interoperability. The interoperability challenge is simple; while licenses and vulnerabilities have well defined id and numbering schemes (e.g. CVE numbers), the identity of the software being described does not. There are many ecosystems that provide common components for reuse, such as Apache Maven, NuGet, npm, rpm, each with its own naming convention. A standard identification scheme that can leverage the innate ecosystem naming convention while being extensible to support new ecosystems, and use cases, will ensure interoperability by specifying the components being annotated. The package-url spec[1] is one such specification that is already supported as a secondary identifier by at least two of the proposed SBOM standards, CycloneDX and SPDX. Requiring all SBOM standards to support an interoperability identifier standard like purl, and further requiring SBOMs to **populate this field** is critical to ensure automation and usability across projects and standards.

[1] https://github.com/package-url/purl-spec