Source: Pierre Metivier (https://flic.kr/p/rdHr) CC BY-NC / Desaturated from the original

CISA Hosted
SBOM-a-Rama
Feb 29, 2024

SBOM Tooling & Implementation Work Stream

Tooling and Implementation Work Stream

Co-chairs: Melissa Rhodes & Kate Stewart

Meeting since August 25, 2022

- Thursday at 1500 EDT
- Contact SBOM@cisa.dhs.gov to be added to mailing list and meeting invite

Discussion of SBOM tooling implementation pain points and propose strategies to improve interoperability

Melissa Rhodes

Medtronic

SBOM Program Manager

melissa.m.rhodes@medtronic.com

Kate Stewart

Linux Foundation

VP of Dependable Embedded Systems

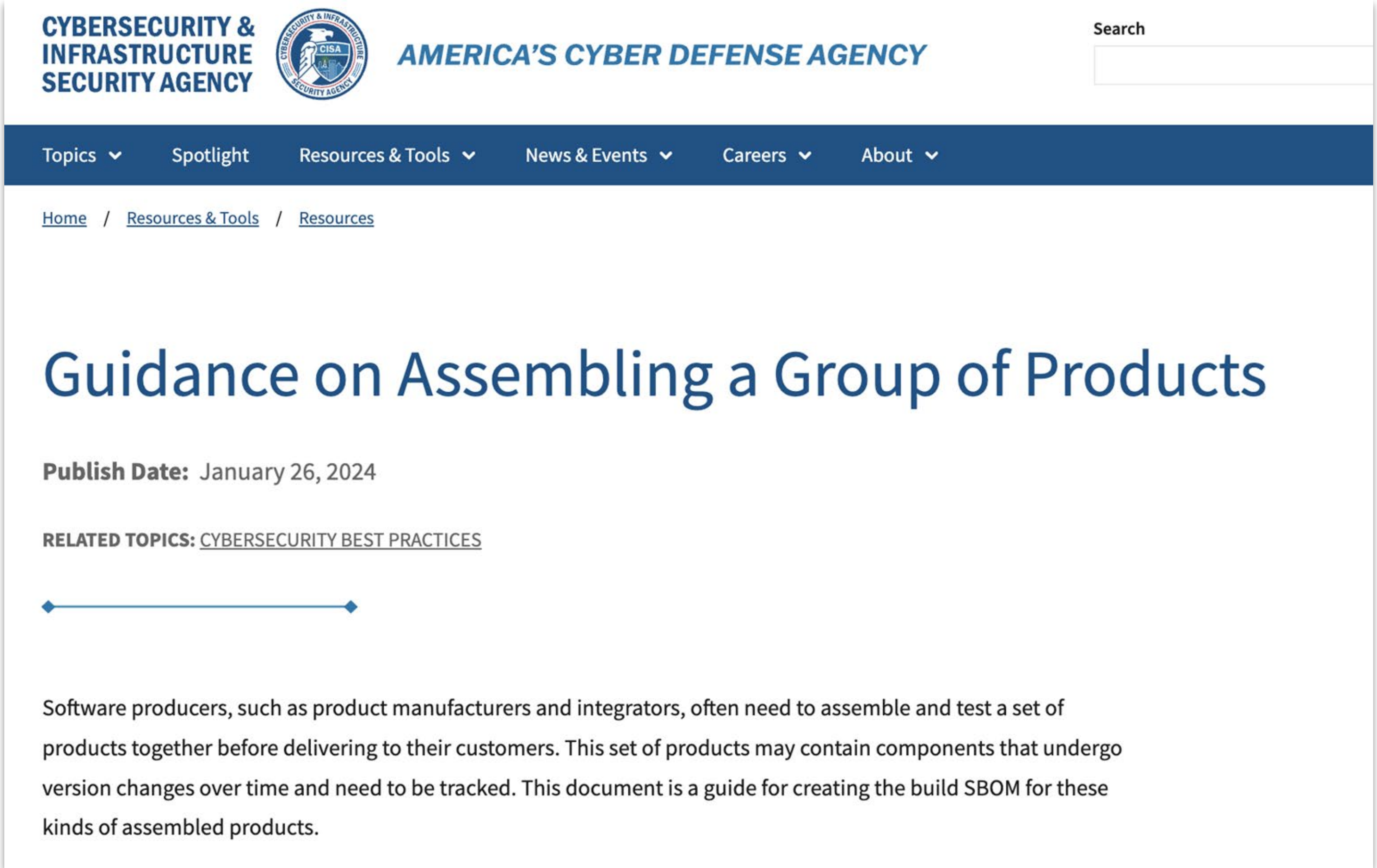
stewart@linux.com

Outline

- History (last SBOM-a-Rama to now)
  - SBOMs for Product Lines
  - Evolution of Pragmatic Guidance to filling in SBOM minimum elements
  - Evolution of Tooling Taxonomy
- SBOM Field Definitions - building up pragmatic guidance
  - Format adherence (syntax)
  - What is filled → (semantics)
  - “Red areas” for where problems”
  - Pragmatic Practices - for field contents.
- Tooling Taxonomy
  - Historical Efforts
  - Current Work
- Next Steps
  - Publish of pragmatic guidance for minimum fields
  - Evolve Tooling Taxonomy and build concensus
  - Plugfests? Extending minimum to match what’s in use?

History: AKA 2023/6/14 → 2024/2/29 SBOM-a-rama

- Publish SBOM Product Lines
- Started working on Tooling Taxonomy
- Working Pragmatic practices for filling in SBOM minimum elements


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
Home / Resources & Tools / Resources

Guidance on Assembling a Group of Products

Publish Date: January 26, 2024

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

Software producers, such as product manufacturers and integrators, often need to assemble and test a set of products together before delivering to their customers. This set of products may contain components that undergo version changes over time and need to be tracked. This document is a guide for creating the build SBOM for these kinds of assembled products.

Source: https://www.cisa.gov/resources-tools/resources/guidance-assembling-group-products

Product Line BOM’s need to be managed during evolution

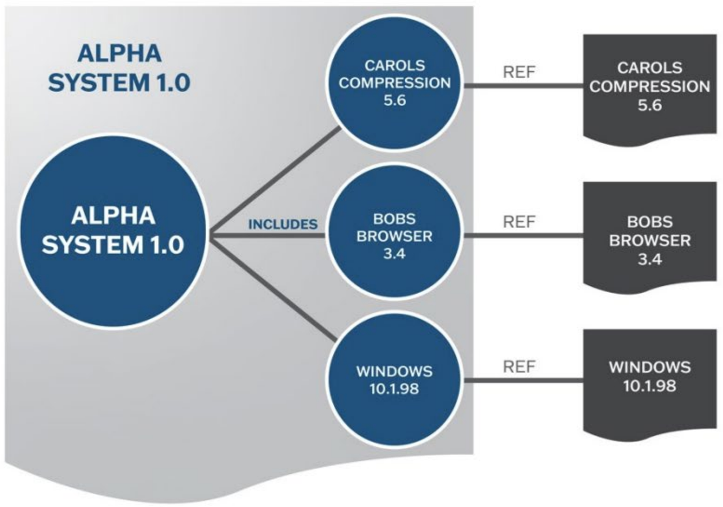


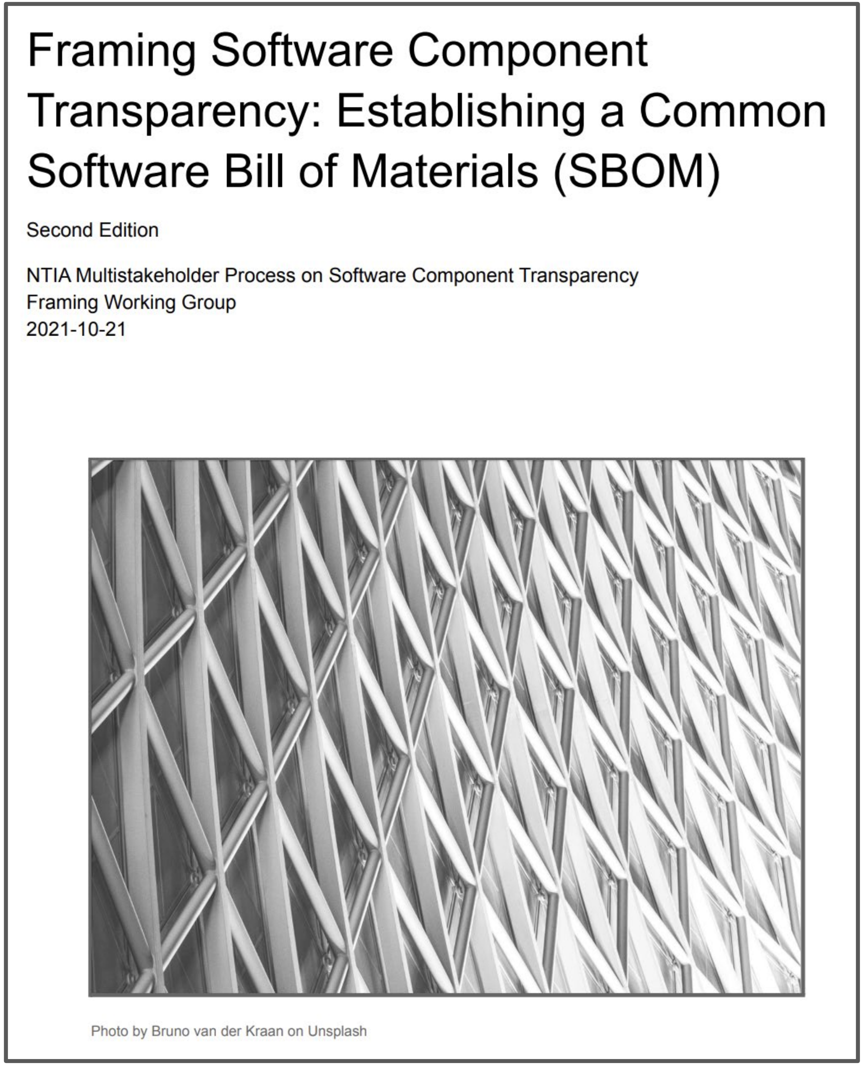
Figure 1: Sample graphical representation of a PLB-SBOM for “Alpha System 1.0”

Source: https://www.cisa.gov/sites/default/files/2024-01/Assembling-a-Group-of-Products_508c_0.pdf

What is “Quality data” for SBOM Field Descriptions?

Started with the stakeholder-drafted “Framing” document from NTIA (2021)

https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf



Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)

Second Edition

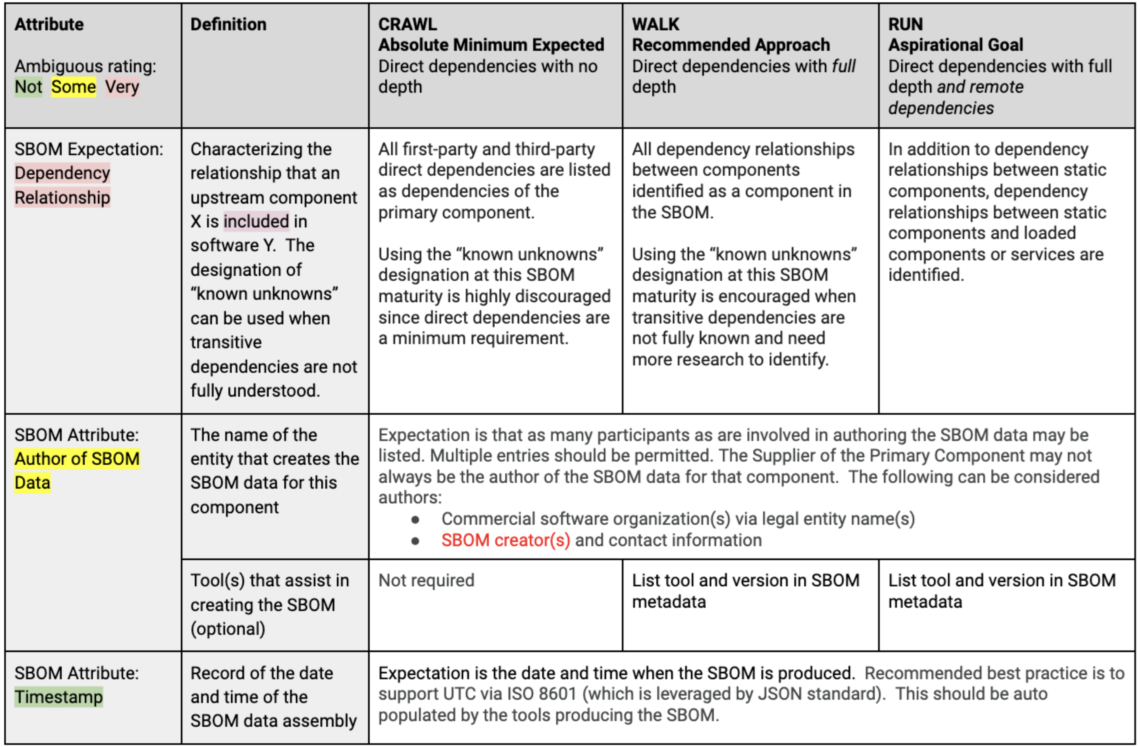
NTIA Multistakeholder Process on Software Component Transparency
Framing Working Group
2021-10-21

Photo by Bruno van der Kraan on Unsplash

WIP: Common Understanding of SBOM Elements

Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y
Author of SBOM Data	The name of the entity that creates the SBOM data for this component
Timestamp	Record of the date and time of the SBOM data assembly
Root of Dependencies	A piece of software can be represented as a hierarchical tree, made up of components that can, in turn, have subcomponents, and so on.
Level of Dependencies	At a minimum, all top-level dependencies must be listed with enough detail to seek out the transitive dependencies recursively.
Known Unknowns	For instances in which the full dependency graph is not enumerated in the SBOM, the SBOM author must explicitly identify “known unknowns.”
Hash of the Component.	A cryptographic hash would provide a foundational element to assist in this mapping, as well as helping in instances of renaming and whitelisting.

Draft of Pragmatic Expectations - Work in Progress



Attribute Ambiguous rating: Not Some Very	Definition	CRAWL **Absolute Minimum Expected** Direct dependencies with no depth	WALK **Recommended Approach** Direct dependencies with *full* depth	RUN **Aspirational Goal** Direct dependencies with full depth *and remote dependencies*
SBOM Expectation: Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y. The designation of “known unknowns” can be used when transitive dependencies are not fully understood.	All first-party and third-party direct dependencies are listed as dependencies of the primary component. Using the “known unknowns” designation at this SBOM maturity is highly discouraged since direct dependencies are a minimum requirement.	All dependency relationships between components identified as a component in the SBOM. Using the “known unknowns” designation at this SBOM maturity is encouraged when transitive dependencies are not fully known and need more research to identify.	In addition to dependency relationships between static components, dependency relationships between static components and loaded components or services are identified.
SBOM Attribute: Author of SBOM Data	The name of the entity that creates the SBOM data for this component	Expectation is that as many participants as are involved in authoring the SBOM data may be listed. Multiple entries should be permitted. The Supplier of the Primary Component may not always be the author of the SBOM data for that component. The following can be considered authors: ● Commercial software organization(s) via legal entity name(s) ● SBOM creator(s) and contact information		
	Tool(s) that assist in creating the SBOM (optional)	Not required	List tool and version in SBOM metadata	List tool and version in SBOM metadata
SBOM Attribute: Timestamp	Record of the date and time of the SBOM data assembly	Expectation is the date and time when the SBOM is produced. Recommended best practice is to support UTC via ISO 8601 (which is leveraged by JSON standard). This should be auto populated by the tools producing the SBOM.		

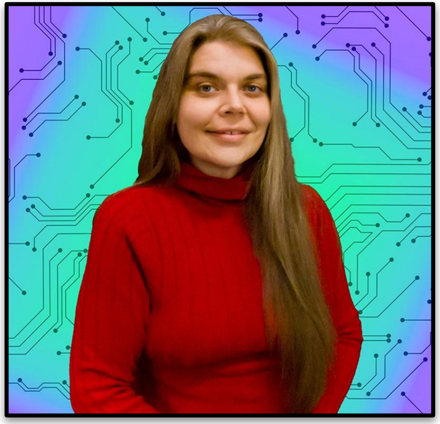
Segmented advice into maturity of producer:

- Crawl
- Walk
- Run

model employed.

Tooling Taxonomy Evolution

Meetings led by Lynn Westfall



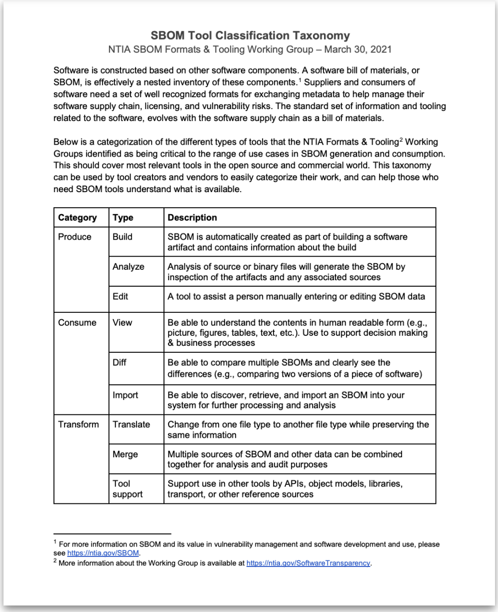
Lynn Westfall (Virtual)

The Modem Lisa

SBOM, ITAM & IT Procurement Consultant
lynn@themodemlisa.com

Similarly to work in 2021 on SBOM Tool Classification Taxonomy, this effort was picked up from the Formats & Tooling group.

Outcomes from this criteria gathering and defining effort may end up in use as part of a collaboration with the OpenSSF SBOM Everywhere SIG volunteer effort to create a dedicated SBOM Landscape, primarily focused on tooling



SBOM Tool Classification Taxonomy
NTIA SBOM Formats & Tooling Working Group – March 30, 2021

Software is constructed based on other software components. A software bill of materials, or SBOM, is effectively a nested inventory of these components.[1] Suppliers and consumers of software need a set of well recognized formats for exchanging metadata to help manage their software supply chain, licensing, and vulnerability risks. The standard set of information and tooling related to the software, evolves with the software supply chain as a bill of materials.

Below is a categorization of the different types of tools that the NTIA Formats & Tooling[2] Working Groups identified as being critical to the range of use cases in SBOM generation and consumption. This should cover most relevant tools in the open source and commercial world. This taxonomy can be used by tool creators and vendors to easily categorize their work, and can help those who need SBOM tools understand what is available.

Category	Type	Description
Produce	Build	SBOM is automatically created as part of building a software artifact and contains information about the build
	Analyze	Analysis of source or binary files will generate the SBOM by inspection of the artifacts and any associated sources
	Edit	A tool to assist a person manually entering or editing SBOM data
Consume	View	Be able to understand the contents in human readable form (e.g., picture, figures, tables, text, etc.). Use to support decision making & business processes
	Diff	Be able to compare multiple SBOMs and clearly see the differences (e.g., comparing two versions of a piece of software)
	Import	Be able to discover, retrieve, and import an SBOM into your system for further processing and analysis
Transform	Translate	Change from one file type to another file type while preserving the same information
	Merge	Multiple sources of SBOM and other data can be combined together for analysis and audit purposes
	Tool support	Support use in other tools by APIs, object models, libraries, transport, or other reference sources

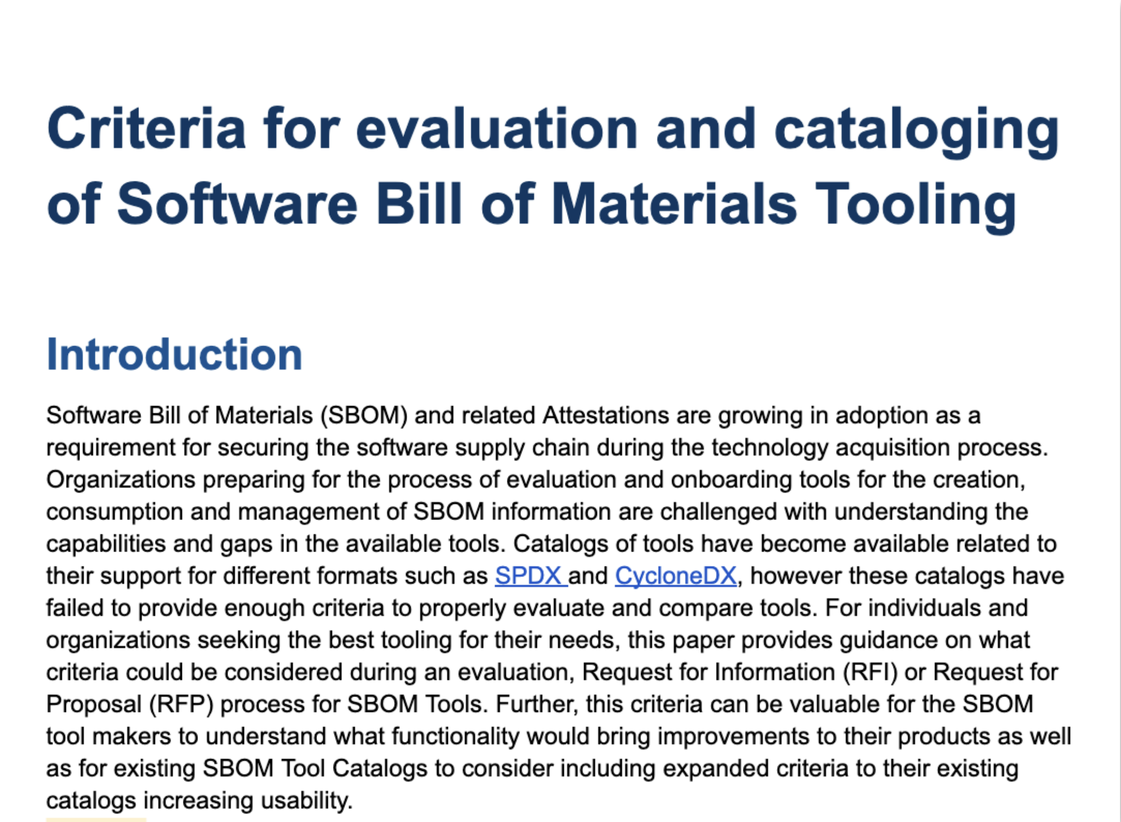
[1] For more information on SBOM and its value in vulnerability management and software development and use, please see https://ntia.gov/SBOM.

[2] More information about the Working Group is available at https://ntia.gov/SoftwareTransparency.

Source:
https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy-2021mar30.pdf

Work in Progress

Much criteria has been identified, defined and organized into a white paper which will include a worksheet of criteria for ease of future review.



Criteria for evaluation and cataloging of Software Bill of Materials Tooling

Introduction

Software Bill of Materials (SBOM) and related Attestations are growing in adoption as a requirement for securing the software supply chain during the technology acquisition process. Organizations preparing for the process of evaluation and onboarding tools for the creation, consumption and management of SBOM information are challenged with understanding the capabilities and gaps in the available tools. Catalogs of tools have become available related to their support for different formats such as SPDX and CycloneDX, however these catalogs have failed to provide enough criteria to properly evaluate and compare tools. For individuals and organizations seeking the best tooling for their needs, this paper provides guidance on what criteria could be considered during an evaluation, Request for Information (RFI) or Request for Proposal (RFP) process for SBOM Tools. Further, this criteria can be valuable for the SBOM tool makers to understand what functionality would bring improvements to their products as well as for existing SBOM Tool Catalogs to consider including expanded criteria to their existing catalogs increasing usability.

Draft Document at:
https://docs.google.com/document/d/1TKPIjT7Rfc38F0OMuXIlPqFRoH7wj2H8x3w13Pgy8V4/edit#heading=h.3kcprhiiv0b8

Next Steps

Continued work on defining and organizing tooling criteria would greatly benefit from additional participation. Feel free to comment on the document directly.

Finish Pragmatic advice document for filling in fields and publishing SBOMs.

Review if pain points highlighted from last poll is still accurate.

- If so, start working on next priority
- If not, determine topics to add, and redo poll to determine point to focus.

Questions?

Want to help?

- Weekly meeting on Thursday at 3pm ET for Pragmatic Expectations
- Weekly meeting on Wednesday at 1pm ET for Criteria
- Please join our mailing list https://groups.google.com/g/cisa-sbom-tooling

Contact SBOM@cisa.dhs.gov if you need help to be added to mailing list and to be added to the meeting invite if you want to join in the live discussion.