INL/MIS-22-70383-Revision-0

Software Bill of Materials (SBOM) Sharing Lifecycle Report Presentation

April 2023

Jeremiah Trent Stoddard, Tyler Williams, Michael Adam Cutshaw

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-22-70383-Revision-0

Software Bill of Materials (SBOM) Sharing Lifecycle Report Presentation

Jeremiah Trent Stoddard, Tyler Williams, Michael Adam Cutshaw

April 2023

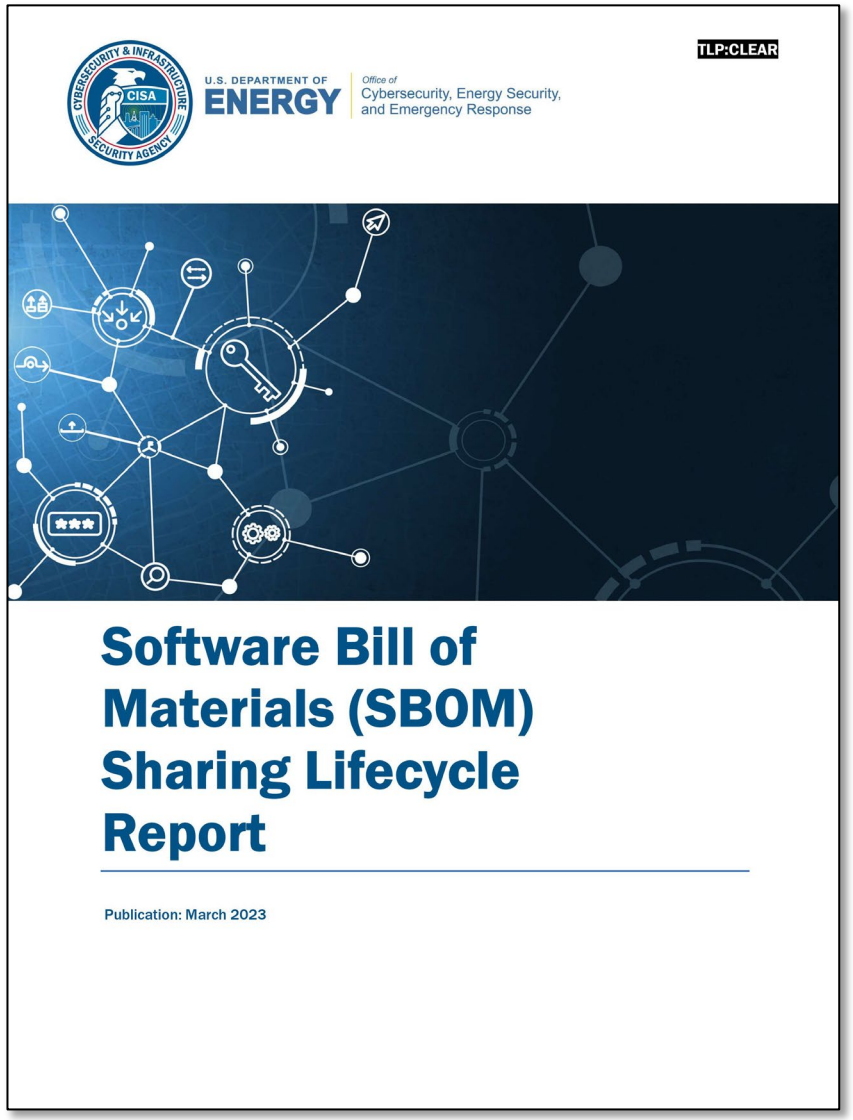
Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Software Bill of Materials (SBOM) Sharing Lifecycle Report

A CISA and DOE CESER collaboration



SBOM Sharing Lifecycle Report Overview

DOE Cybersecurity, Energy Security, and Emergency Response (CESER) and the Cybersecurity & Infrastructure Security Agency (CISA) co-sponsored the SBOM Sharing Lifecycle Report

Authors, contributors, and reviewers came from Idaho National Laboratory, Pacific Northwest National Laboratory, CISA, and CESER.

Purpose of the Report:

- Enumerate and describe the different parties and phases of the SBOM sharing lifecycle
- Assist readers in choosing suitable SBOM sharing solutions

SBOM Sharing Lifecycle: NTIA Conceptual SBOM Exchange

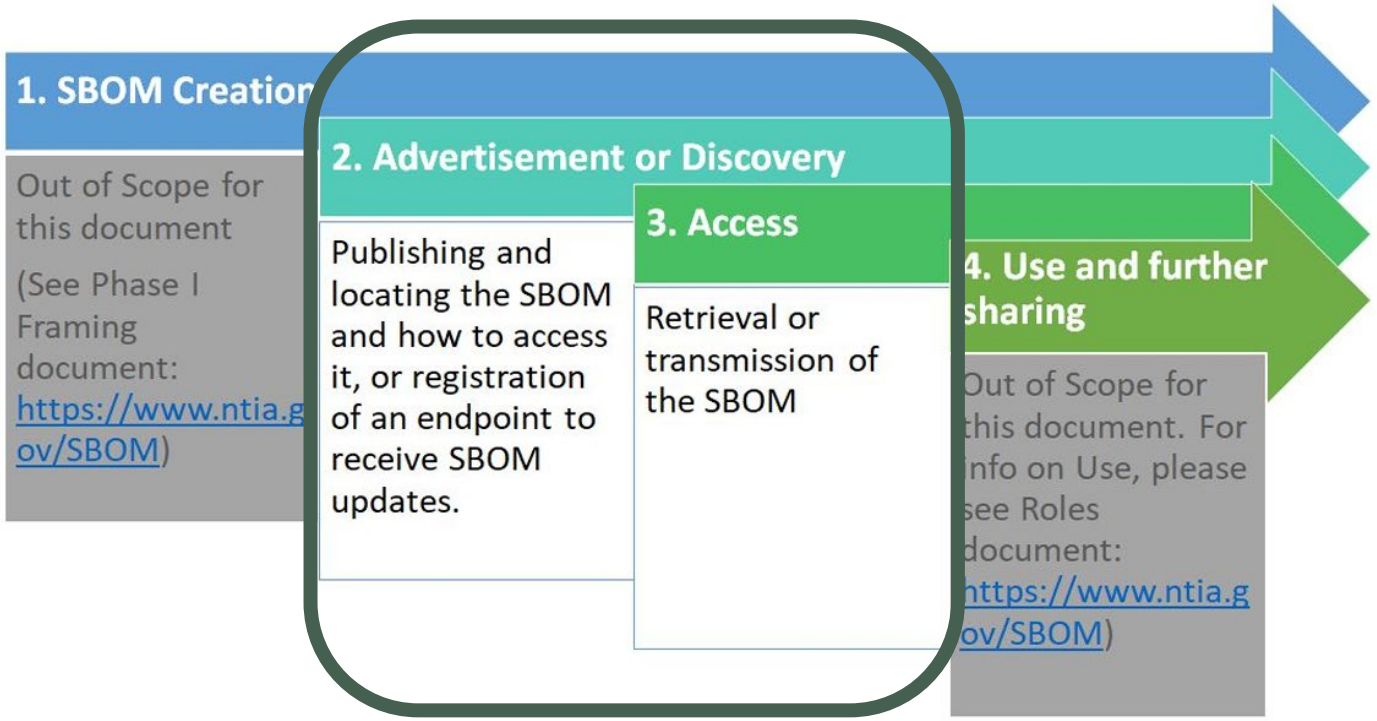


Figure 1: Conceptual SBOM exchange

Source: NTIA Multistakeholder Process "*Sharing and Exchanging SBOMs*" document

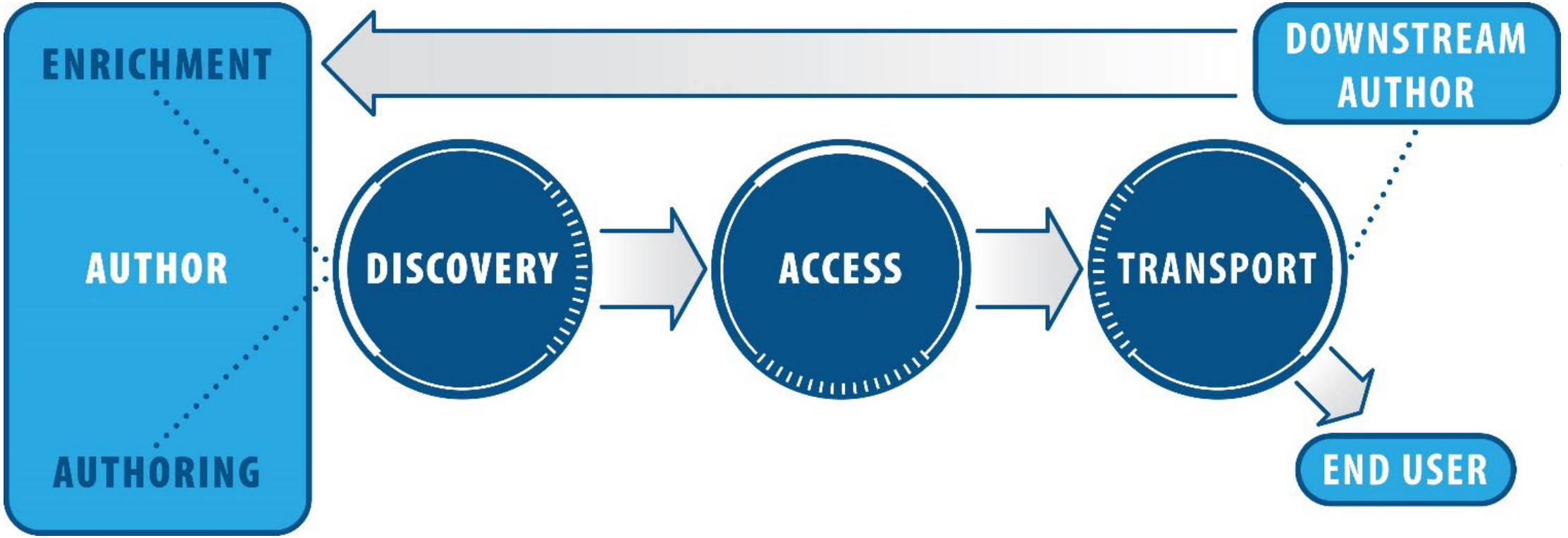
SBOM Sharing Lifecycle Phases

SBOM Sharing Lifecycle Report Definitions

Term	Definition
Author	Creates an SBOM.
Consumer	Receives the transferred SBOM. This could include roles such as: third parties, authors, integrators, and end users.
Provider	Possesses an SBOM.
Discovery	Mechanism used by the consumer to know the SBOM exists and how to access it.
Access	Access control mechanisms used by the author or provider to regulate who can view or use an SBOM. **NTIA definition: Transfer of the SBOM using the method derived from discovery.**
Transport	The mechanism provided by the author or provider to transfer an SBOM. Also, the action of the consumer receiving an SBOM.
Enrichment	Activities that leverage an SBOM to create a new product, which may include the antecedent SBOM. This may be done by an author, consumer, provider, or other third party.
Sophistication	The relative amount of time, resources, subject-matter expertise, effort, and access to tooling needed to implement a phase of the SBOM sharing lifecycle. Sophistication can be either Low, Medium, or High.

Adjusted Definition

New Definitions



SBOM Sharing Lifecycle Phases

Lifecycle Phase	Sophistication - Low	Sophistication - Medium	Sophistication - High

Discovery	• Consumer initiated
	• Limited or non-existent guidance given by Provider
		• SBOM placed in software source code
		  – Point in time (Singular version)
		  – Manufacturer Usage Description (MUD)
		• Known central repository
		• Website
			• Automated propagation of available SBOMs
			• Continuous updates to relevant parties
			• Publish/Subscribe pattern
			• Distributed ledger

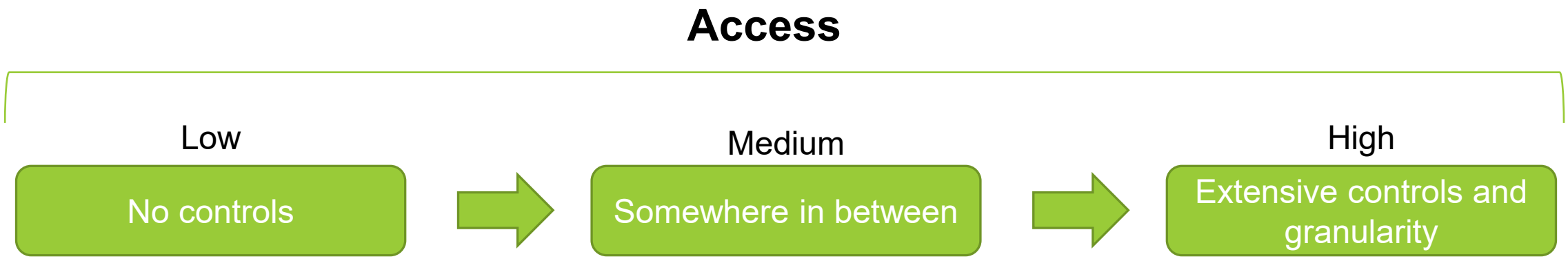
Access	• No controls in place • Manual controls • Case-by-case	• Authentication required • Limited access control granularity • Private/broadcast/public channels, roles • Private chains/consensus algorithm	• Delegated authentication and access controls • Full access control granularity
Transport	• Human-initiated process • Point-to-point • Verbal transmission	• Inconsistent, varied method or documentation • Ad hoc automation	• Documented • Repeatability • Automated access • Well known protocols (e.g., REST/RESTful/ SOAP API) • Distributed ledger synchronization

SBOM Sharing Lifecycle Sophistication Examples

Sophistication Trends

As sophistication increases:

- Automation increases
- Interoperability increases
- Timeliness increases
- Features increase
- Initial provider effort increases
- Consumer effort decreases



SBOM Sharing Survey

The purpose of the survey was to understand the current state of SBOM sharing among stakeholders

39 organizations were contacted, and 21 responses were provided

- Respondents were initially contacted via email and then given an opportunity for a video teleconferencing session to answer questions with appropriate follow-up

Transport responses were categorized into one of the three methods identified in the NTIA's "Sharing and Exchanging SBOMs" document

- Respondents not using all NTIA SBOM sharing methods

In the aggregate, SBOM stakeholders may be currently hesitant to adopt more advanced SBOM sharing methods due to an unwillingness to dedicate resources to an area within software supply chain risk management that is still maturing

SBOM Sharing Lifecycle Report Conclusions

The path to widespread sharing of SBOMs involves increasing capabilities that focus on automation and interoperability within the SBOM sharing lifecycle phases

The SBOM sharing ecosystem would benefit from a variety of sharing solutions created by parties seeking to meet stakeholder's unique circumstances

Future work may include:

- Finding ways to lower costs associated with higher sophistication solutions
- Exploring the concept of SBOM enrichment to understand the different activities and products that may constitute enrichment
- Considering a broader SBOM survey to better understand the SBOM user base and the desirable features users need with an eye toward maturing the exchange framework and providing users with recommended features

Please email Jeremiah Stoddard (Jeremiah.Stoddard@inl.gov), Michael Cutshaw (Michael.Cutshaw@inl.gov), or Tyler Williams (Tyler.Williams@pnnl.gov) if you have any questions or comments about the SBOM Sharing Lifecycle Report (Link).

Your feedback is appreciated