Energy Sector SBOM POC

EXPLORING THE APPLICATION OF SOFTWARE BILLS OF MATERIALS IN THE ENERGY SECTOR

JUNE 21, 2023

Agenda

- Welcome!
- Recap of SBOM POC efforts to date
- Venues for SBOM Engagement
- Continued building body of knowledge
- Q: How do you use BOMs in your environments?
- Discuss Priorities and Unique Requirements for the Energy Sector

DOE CESER sponsored SBOM Research

- CESER monthly SBOM POC meetings, 3rd Weds @ Noon Eastern
- CESER SBOM Website: https://sbom.inl.gov/
- CyTRICS has unique requirements and its own SBOM Schema
- CESER Sponsored Programs: Energy Cyber Sense and CyTRICS

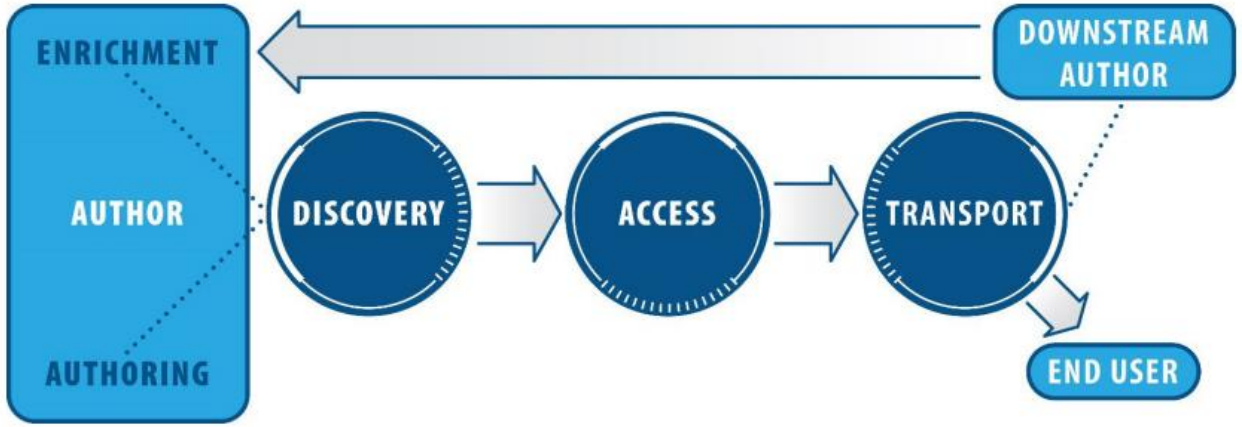
DOE CESER and DHS CISA sponsored SBOM Research

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

- Completed research and delivered a paper on “Software Bill of Materials (SBOM) Sharing Lifecycle Report”
  - https://www.osti.gov/biblio/1969133

Abstract

As Software Bill of Materials (SBOM) adoption efforts mature, SBOM sharing continues to occur, but no single solution or set of solutions have become ubiquitous. The purpose of this report is to enumerate and describe the different parties and phases of the SBOM sharing lifecycle and assist readers in choosing suitable SBOM sharing solutions based on the amount of time, resources, subject-matter expertise, effort, and access to tooling that is available to the reader to implement a phase of the SBOM sharing lifecycle. The SBOM sharing lifecycle consists of the Discovery, Access, and Transport of an SBOM and this report details these individual phases and how an SBOM goes from author to the consumer. This report also details how potential enrichment activities may be performed on an SBOM to create a new product before or after it has been shared. The concept of a sophistication classification for SBOM sharing solutions is concurrently introduced with a focus on the inclusion



Venues for SBOM (and other BOMs) Engagement

Other venues for SBOM Engagement

- CISA SBOM Workstreams, SBOM-a-Rama, and more. https://www.cisa.gov/sbom
- Department of Defense
- Standards development: active CycloneDX® and SPDX® communities
  - CycloneDX® – Open Worldwide Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.
  - SPDX® – open-source project hosted by the Linux Foundation
- Examples of Global support for SBOM research
  - EU Cyber Resilience Act
  - UK seeking to expand existing regulation
  - Japan Cybersecurity Strategy: Ministry of Economy, Trade and Industry
  - Germany

CISA SBOM Workstreams ?

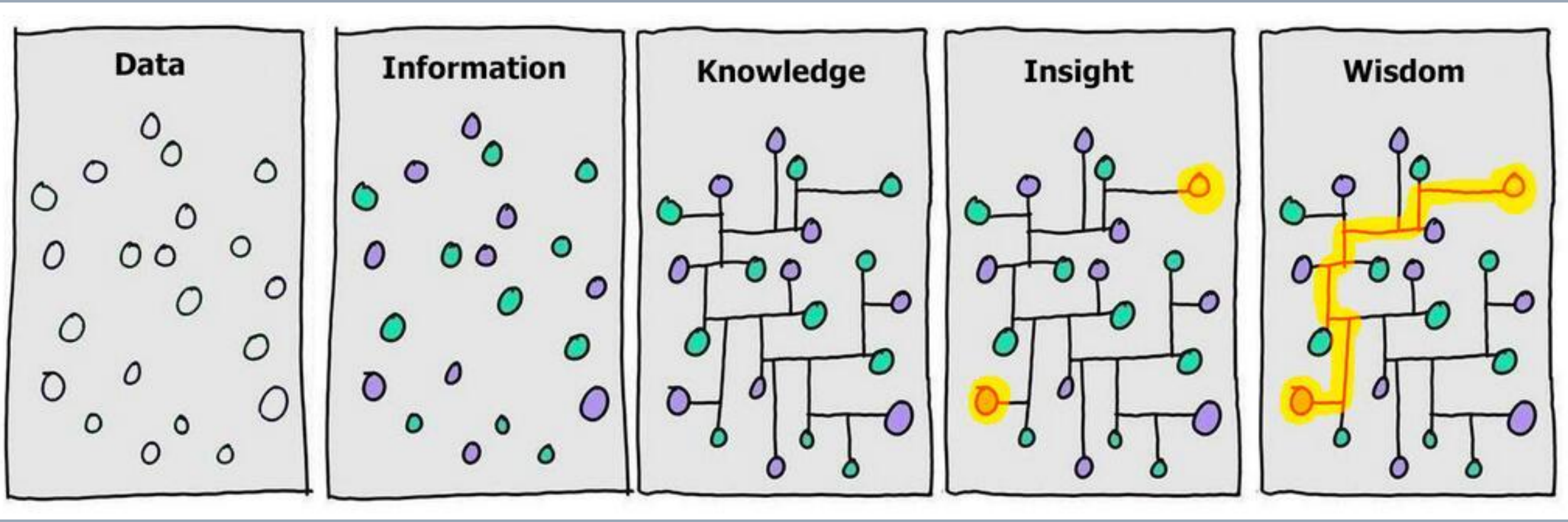
- Vulnerability Exploitability eXchange (VEX)
  Meeting Day/Time: Monday 10 AM ET – 11 AM ET (weekly)
  The VEX workstream defines and refines the Vulnerability Exploitability eXchange (VEX) model, which allows attestations on whether a product is affected or not affected by a given vulnerability, and characterizes VEX use cases and operations.

- Sharing & Exchanging
  Meeting Day/Time: Monday 12 PM ET – 1 PM ET (weekly)
  The Sharing and Exchanging workstream will focus on the topic of moving SBOMs, and related metadata, across the software supply chain. The community will have discussions centered around understanding how to enable discovery and access, while underscoring the importance of solution interoperability.

- On-Ramps & Adoption
  Meeting Day/Time: Tuesday 12 PM ET – 1 PM ET (weekly)
  The On-Ramps and Adoption workstream will focus on promoting education and awareness to help lower the costs and complexities of adoption, allowing newer or less mature organizations to provide, request, and use SBOMs to secure and understand their organization's risk. The workstream may also define use cases for SBOM, as well as coordinate efforts across all new and existing SBOM-related workstreams to assist in marketing as well as help to avoid substantive overlap.

- Cloud & Online Applications
  Meeting Day/Time: Wednesday 3 PM ET – 4 PM ET (bi-weekly)
  The Cloud and Online Applications workstream will focus on integrating current understanding around SBOM into the context of online applications and modern infrastructure. Most of the existing discussion around SBOM, particularly around SBOM use cases, has focused on on-premise software. Cloud and Software-as-a-Service (SaaS)-based software comprises a large and growing segment of the software ecosystem. It will be important to integrate the current understanding of SBOM with emergent advances in cloud-native technologies to tell better stories about SBOM use cases for cloud and understand how this will be handled across organizational boundaries.

- Tooling & Implementation
  Meeting Day/Time: Thursday 3 PM ET – 4 PM ET (weekly)
  The Tooling and Implementation workstream will focus on opportunities and challenges for automating the SBOM ecosystem. This ecosystem will be driven by a range of accessible and constructive tools and enabling applications, both open source and proprietary. This work will potentially enhance existing SBOM data with further implementation details, encourage interoperability across tools and uses, and foster the advancement and efficiency of the tooling marketplace.



https://twitter.com/kenburbary/status/714576446446940160/photo/1

Continued building body of knowledge for others learning about SBOMs

Other Meetings

Proof of Concept Kickoff, Apr. 26, 2021 - https://youtu.be/HRG92cvQi5o

SBOM-POC Charter, May 19, 2021 - https://youtu.be/KFQeiT9FUvU

MURAL Synthesis Work, June 2, 2021 - https://inl.gov/wp-content/uploads/2021/07/SBOM-POC-Mural-Synthesis-Release.pdf

Brainstorming, June 16, 2021 - https://youtu.be/y-KRFQg2wDo

Healthcare POC Lessons Learned, June 30, 2021 - https://youtu.be/DihY41_G47k

Use Cases for SBOM, July 14, 2021 - https://youtu.be/l61esNfj2xk

Use Cases for SBOM, Aug. 25, 2021 - https://youtu.be/xZW_ghskEmg

Use Cases for SBOM, Sept. 8, 2021 - https://youtu.be/dvfzLdmOcoI

Cooking Classes

Cooking Class on Making an SBOM, Sept. 22, 2021 - https://youtu.be/Tk4v1IrSNSA

Cooking Class on Open Source, Oct. 6, 2021 - https://youtu.be/5D0P84ayGpg

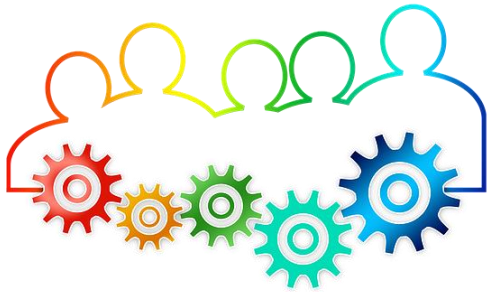
Cooking Class on VEX, Oct 20, 2021 - https://youtu.be/KjMHxeHYgIQ

Cooking Class on Preparing to Use SBOM's, Nov. 3, 2021 - https://youtu.be/Tqkdb3XvR08

Cooking Class on Exploring Information in an SBOM, Nov 17, 2021 - https://youtu.be/Qkx7PezvwGM

2022 Continued the momentum

- Updated SBOM website to make it easy to filter topic areas
- Continued SBOM education and awareness
- Collaboration with Energy and other industry partners, S4 SBOM conference, VEX, All Hazards Analysis, SBOM In Nuclear, draft report out on SBOM Sharing Lifecycle, Building an SBOM from Binaries, SBOM Transports, Venues for SBOM discussion
- https://www.youtube.com/playlist?list=PLX2nBoWRisnU3IdO_lXo41ZVaN2rvcUbx



Owner/Operators, Q: How are you using BOMs in your environment today?

1. How are you using BOMs in your environment today?
2. Are there any success stories that you can share?
3. What is your organization's vision for BOMs?
4. Challenges and opportunities when it comes to BOMs?

Defining next steps

- What should we focus on next?
- What are the top priorities?

#	Description	Addressed by
118	Demo/Walkthrough of Full SBOM lifecycle	
10	Develop standard contract clauses	
67	SBOMS for legacy components	
122	General SBOM whitepaper	SBOM at a Glance: https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf How-To Guide for SBOM Generation: howto_guide_for_sbom_generation_v1.pdf (ntia.gov) SBOM Suppliers Playbook: https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf Software Consumers Playbook: https://www.ntia.gov/files/ntia/publications/software_consumers_sbom_acquisition_management_and_use_-_final.pdf
1	Create SBOMs from open-source product	Cooking Class on Open Source, Oct. 6, 2021 - https://youtu.be/5D0P84ayGpg
54	SBOM confidentiality	Healthcare POC Lessons Learned, June 30, 2021 - https://youtu.be/DihY41_G47k
2	Develop SBOM taxonomy	JuiceBox Demo, Nov. 17, 2021 Minimum Elements for SBOM - https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

#	Description	Addressed by
25	How to create SBOMs when no source code is available	
40	Address the gap that open source & Commercial are part of a single product	
62	Using SBOMs for vulnerability management	Cooking Class on VEX, Oct 20, 2021 - https://youtu.be/KjMHxeHYgIQ Vex Overview - https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf
105	How to maintain an SBOM	Cooking Class on Preparing to Use SBOM's, Nov. 3, 2021 - https://youtu.be/Tqkdb3XvR08
106	Minimum attributes of the SBOM	Healthcare POC Lessons Learned, June 30, 2021 - https://youtu.be/DihY41_G47k Cooking Class on Making an SBOM, Sept. 22, 2021 - https://youtu.be/Tk4v1IrSNSA Cooking Class on Exploring Information in an SBOM, Nov 17, 2021 -

	Description
	Demo/Walkthrough of Full SBOM lifecycle
	Develop standard contract clauses + procedures, tools, engagement practices
	SBOMS for legacy components
✓	General SBOM whitepaper
✓	Create SBOMs from open-source product
✓	SBOM confidentiality
✓	Develop SBOM taxonomy
	How to create SBOMs when no source code is available
	Address the gap that open source & Commercial are part of a single product
✓	Using SBOMs for vulnerability management
✓	How to maintain an SBOM
✓	Minimum attributes of the SBOM
	Regulatory Landscape Overview (BRIEF) + DOE Guidance

	Description	New Priority Level
	Demo/Walkthrough of Full SBOM lifecycle	3
	Develop standard contract clauses	2
	SBOMS for legacy components	
✓	General SBOM whitepaper	
✓	Create SBOMs from open-source product	
✓	SBOM confidentiality	
✓	Develop SBOM taxonomy	
	How to create SBOMs when no source code is available	
	Address the gap that open source & Commercial are part of a single product	
✓	Using SBOMs for vulnerability management	
✓	How to maintain an SBOM	
✓	Minimum attributes of the SBOM	
	Regulatory Landscape Overview (BRIEF) + DOE Guidance	1

#	Description	New Priority Level	Responsible Adults
	Demo/Walkthrough of Full SBOM lifecycle	3	
	Develop standard contract clauses	2	
	SBOMS for legacy components		
✓	General SBOM whitepaper		
✓	Create SBOMs from open-source product		
✓	SBOM confidentiality		
✓	Develop SBOM taxonomy		
	How to create SBOMs when no source code is available		
	Address the gap that open source & Commercial are part of a single product		
✓	Using SBOMs for vulnerability management		
✓	How to maintain an SBOM		
✓	Minimum attributes of the SBOM		
	Regulatory Landscape Overview (BRIEF) + DOE Guidance	1	J Smith PNNL, T Whitney Fortress, C Crossley SE

Thank you!

Appendix

Additional backup slides for reference

Brainstorming: How are you using BOMs?

Produce Software	Choose Software	Operate Software	Ecosystem, Network Effects
Reduce unplanned, unscheduled work	Identify potentially vulnerable components	Organization can quickly evaluate whether it is using the component	Accelerated Vulnerability Management
Reduce code bloat	A more targeted security analysis	Drive independent mitigations	Amplified “Herd Immunity”
Adequately understand dependencies within broader complex projects	Verify the sourcing	Make more informed risk-based decisions	Selecting for Better Suppliers
Know and comply with the license obligations	Compliance with policies	Alerts about potential end-of-life	Weathering Suppliers going away
Monitor components for vulnerabilities	Aware of end-of-life components	Better support compliance and reporting requirements	
End-of-life (EOL)	Verify some claims	Reduce costs through a more streamlined and efficient administration	
Make code easier to review	Understand the software’s integration		
A blacklist of banned components	Pre-purchase and pre-installation planning		
Provide an SBOM to a customer	Market signal		