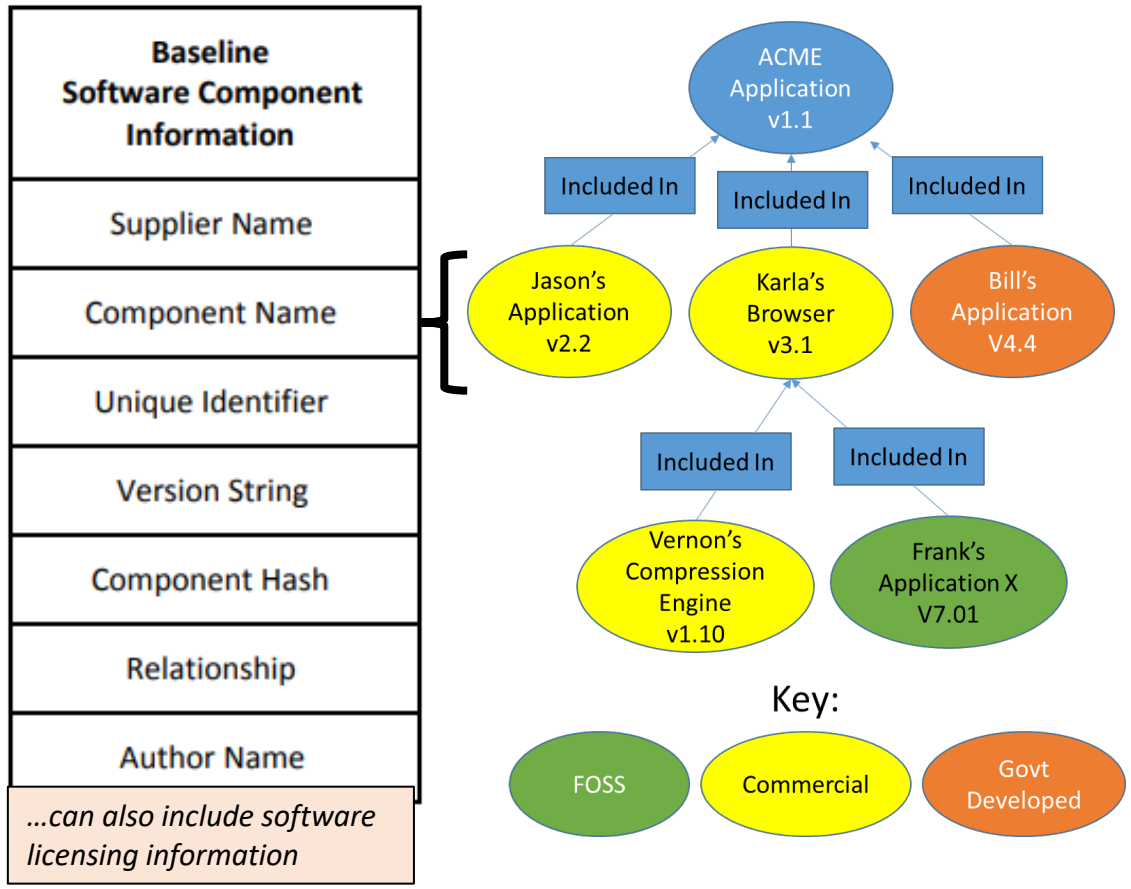
Cybersecurity in the Product Support Strategy: SBOM

Dr Jason Hamilton
Jason.Hamilton@dau.edu

20 November 2023

What is a Software Bill of Materials (SBOM)

- A formal record *containing details and supply chain relationships* of the various components used in building a software package
- Effectively a *nested inventory*; a list of ingredients that comprise the completed software solution.
- Identifies and lists the software components, information about those components, and the relationships between them.



https://ntia.gov/sites/default/files/publications/sbom_overview_20200818_0.pdf

What are the Benefits of using an SBOM?

- Identifying and avoiding known vulnerabilities
- Quantifying and managing licenses for commercial software
- Identifying both security and license compliance requirements
- Enabling risk identification and analysis inherent to a software package
- Managing vulnerability mitigation
- Lowers operating costs due to improved efficiency and reduced unplanned/unscheduled work.

SBOM enables efficient software asset management by increasing software transparency

Software BOM template					
ID	Sub ID		Name	Version	*Metadata fields as needed*
1			Acme Application	1.1	*(basic examples below)*
	1		Jason's Application	2.2	(C) Licensing incl unlimited users, renewal 1 Jan 2024
	2		Karla's Browser	3.1	(C) Govt use only, 1000 seats, renewal 1 July 2023
		1	Vernon's compression engine	1.10	(C) Govt use only, 1000 seats, renewal 1 July 2023
		2	Frank's Application X	7.01	FOSS, (addl metadata?)
	3		Bill's Application	4.4	5Ws about SW Dev approach, POC

Notional manual SW BOM (automated preferred)

https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

How can an SBOM help in the event of a cyber attack?

When flaws/vulnerabilities are discovered, SBOMs *help to quickly identify affected software, assess its usage, and analyze the associated risk*.

- This helps suppliers more rapidly produce patches or other remediations
- Helps consumers apply remediations independently of the supplier;
- *Allows rapid identification of software that is not affected.*

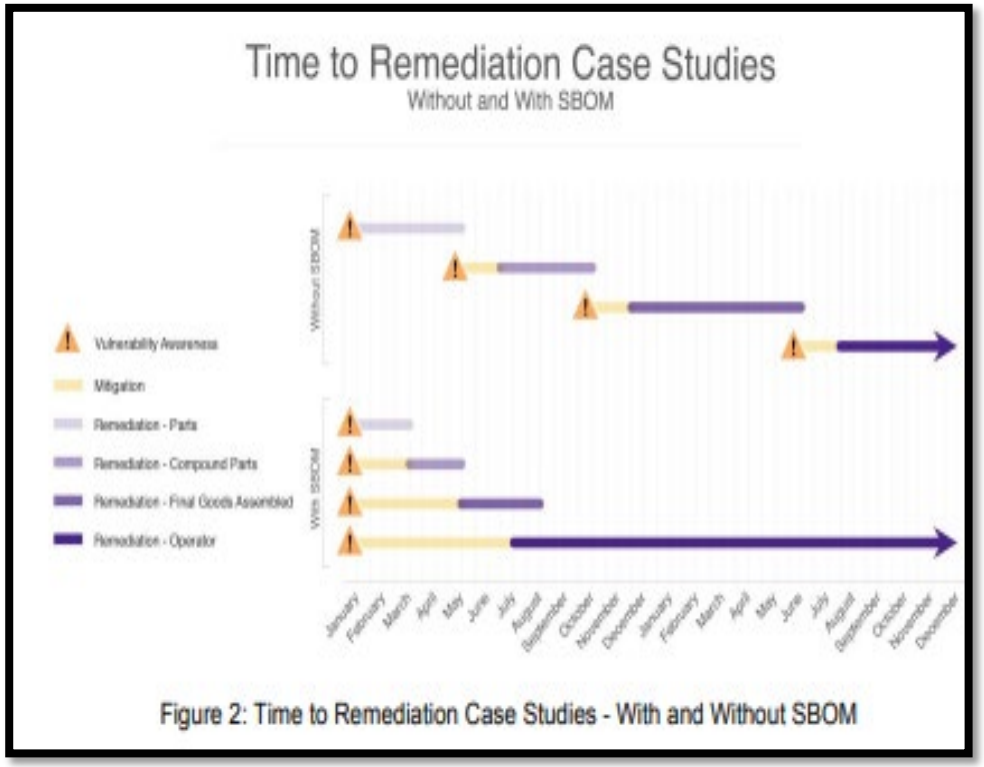


Figure 2: Time to Remediation Case Studies - With and Without SBOM

https://ntia.gov/sites/default/files/publications/sbom_faq_-_20201116_0.pdf

SBOM Resources

xBOM Working Group

SOFTWARE BILL OF MATERIALS | National Telecommunications and Information Administration (ntia.gov)

- Contains links to many of the subjects discussed in this session

What is Software Bill of Materials (SBOM)? – YouTube

- Helpful video by Mr. Nic Chaillan, former Chief Software Officer for USAF/USSF

https://blog.usu.com/en-us/8-best-practices-for-successful-software-license-management

- Great resource for Software lifecycle management

ASSIST-QuickSearch Document Details (dla.mil)

- BOM for Logistics and Supply Chain Risk Management DID information and format

https://jfrog.com/knowledge-base/best-practices-for-software-bill-of-materials-sbom-management/

- Best practices related to SBOM management

Executive Order 14028: Improving the Nation's Cybersecurity | GSA

Backup Slides