



# Software Bill of Materials Progress towards Transparency in the SW Supply Chain

Allan Friedman, PhD  
Director of Cybersecurity Initiatives,  
National Telecommunications and Information Administration,  
US Department of Commerce  
[afriedman@ntia.gov](mailto:afriedman@ntia.gov)      @allanfriedman

# Paying Attention vs. Checking email

Tracking and communicating third party components in software and IoT with a “**software bill of materials**” can

- Improve and communicate secure development practices
- Help enterprise customers protect themselves
- Foster better markets for secure products

The US Department of Commerce has convened an open and consensus-driven **multistakeholder process** to develop a shared vision around SBOM and software transparency

Stakeholders have drafted documents reviewing the *what*, the *why*, and the *how*.







**Mudge** @dotMudge · 27 Aug 2016

If you have a 2013 **Mercedes** S-class you have libtiff, netcat, and libpcap, pre-installed.





# Analogies

SOYBEAN OIL, PALM OIL, PARTIALLY HYDROGENATED  
L, PARTIALLY HYDROGENATED COTTONSEED OIL, AND  
OIL WITH TBHQ AND CITRIC ACID ADDED TO P  
HIGH FRUCTOSE CORN SYRUP, CONTAINS TWO  
FOOD STARCH – MODIFIED, SKIM MILK, LEAV  
PYROPHOSPHATE, MONOCALCIUM PHOSPHAT  
YCERIDES, SALT, SORBIC ACID (TO PRESERVE  
ARTIFICIAL FLAVORS, PROPYLENE GLYCOL MON  
UR. SOY LECITHIN. XANTHAN GUM. AGAR. NUTM

We understand the role of a list of ingredients.

# Analogies

 <b>SAFETY DATA SHEET</b>							
<b>1. Identification</b> <b>Product Identifier:</b> Poly 74-20 Liquid Rubber Part B Poly 74-24 Liquid Rubber Part B Poly 74-29 Liquid Rubber Part B Poly 74-29 White Liquid Rubber Part B Poly 74-30 Liquid Rubber Part B Poly 74-30 Clear Liquid Rubber Part B Poly 74-30 HT Liquid Rubber Part B Poly 74-31 Liquid Rubber Part B Poly 74-41 Liquid Rubber Part B Poly 74-45 Liquid Rubber Part B <b>Product Code(s):</b> 74-20B, 74-24B, 74-29B, 74-29WHITE, 74-30B, 74-30CLEAR, 74-30HTB, 74-31B, 74-41B, 74-45B <b>Use:</b> Component for Polyurethane Mold Rubber. For Industrial Professional use only. <b>Manufacturer:</b> Polytek Development Corp. 55 Hilson St., Exton, PA 19341 USA Phone Number: +1 610-559-8620 (9 a.m. to 5 p.m. EST) Emergency Phone: CHEMTREC 800-424-9300 or +1 703-527-3887 E-mail: <a href="mailto:info@polytek.com">info@polytek.com</a>							
<b>2. Hazards Identification</b> <b>GHS Classification:</b> Specific Target Organ Toxicity - Exposed Exposure Category 2 <b>Label Element:</b> Warning!  Contains Diethyltoluenediamine <b>Hazard Phrases:</b> H373 May cause damage to organs through prolonged or repeated exposure. <b>Precautionary Phrases:</b> P260 Do not breathe vapors. P314 Get medical advice if you feel unwell. P501 Dispose of contents and container to licensed, permitted incinerator, or other thermal destruction device in accordance with local and national regulations. <b>Supplemental Information:</b> None known. This is one part of a two-part system. Read and understand the hazard information on Part A before using.							
<b>3. Composition/Information on Ingredients</b> <table border="1"> <thead> <tr> <th>Chemical Name</th> <th>CAS #</th> <th>%</th> </tr> </thead> <tbody> <tr> <td>Diethyltoluenediamine</td> <td>68479-99-1</td> <td>1-3%</td> </tr> </tbody> </table>		Chemical Name	CAS #	%	Diethyltoluenediamine	68479-99-1	1-3%
Chemical Name	CAS #	%					
Diethyltoluenediamine	68479-99-1	1-3%					
<b>4. First-Aid Measures</b> <b>Eye Contact:</b> Flush thoroughly with water, holding the eyelids open to be sure the material is washed out. Get medical attention if irritation persists. <b>Skin Contact:</b> Remove contaminated clothing. Wash contact area thoroughly with soap and water. Get medical attention if irritation persists. <b>Inhalation:</b> Remove person to fresh air. Get medical attention if symptoms persist. <b>Ingestion:</b> Do not induce vomiting unless directed to do so by medical personnel. Get medical attention.							
<b>5. Most Important Symptoms/Effects:</b> May cause mild eye and skin irritation. May be harmful if swallowed. <b>Indication of Immediate Medical Attention/Special Treatment:</b> Immediate medical attention is not required.							
<b>6. Fire-Fighting Measures</b> <b>Extinguishing Media:</b> Use water fog, foam, carbon dioxide or dry chemical. Do not use solid water stream. Solid stream of water into hot product may cause violent steam generation or eruption. <b>Specific Hazards:</b> Not classified as flammable or combustible. Product will burn under fire conditions. <b>Special Protective Equipment &amp; Precautions for Fire-Fighters:</b> Wear positive pressure, self-contained breathing apparatus and full-body protective clothing. Cool fire-exposed containers with water.							
<b>6. Accidental Release Measures</b> <b>Personal Precautions, Protective Equipment and Emergency Procedures:</b> Remove all ignition sources. Clear non-emergency personnel from the area. Wear appropriate protective clothing to prevent eye and skin contact and avoid breathing vapors. Caution - spill area may be slippery. <b>Methods and Materials for Containment and Cleanup:</b> Cover with an inert absorbent material and collect into an appropriate container for disposal. Avoid releases to the environment. Report spills and releases as required to appropriate authorities.							
<b>7. Handling and Storage</b> <b>Safe Handling:</b> Use with adequate ventilation. Avoid contact with the eyes, skin and clothing. Wash thoroughly after handling. Do not eat, drink or smoke in the work area. Keep container closed when not in use. <b>Safe Storage:</b> Store indoors at temperatures below 120°F (49°C). Store in original containers. Avoid getting moisture into containers. Keep containers tightly closed.							
<b>8. Exposure Controls/Personal Protection</b> <b>Occupational Exposure Limits:</b> None Established <b>Ventilation:</b> Use with adequate general or local exhaust ventilation to minimize exposure levels. <b>Respiratory Protection:</b> If needed, an approved respirator with organic vapor cartridges may be used. Respirator selection and use should be based on contaminant type, form and concentration. For higher exposures or in an emergency, use a supplied-air respirator. <b>Skin Protection:</b> Wear impervious gloves, such as nitrile rubber or neoprene rubber. <b>Eye Protection:</b> Wear chemical safety goggles. <b>Other Protective Measures:</b> Wear impervious clothing to prevent skin contact and contamination of personal clothing. An eye wash facility and washing facility should be available in the work area. Follow applicable regulations and good Industrial Hygiene practices.							
<b>9. Physical and Chemical Properties</b> <b>Appearance:</b> Liquid of varied colors <b>Odor:</b> Slightly pungent <b>Odor Threshold:</b> No data available <b>pH:</b> Not applicable <b>Melting Point:</b> No data available <b>Boiling Point:</b> No data available <b>Flash Point:</b> > 350°F (>177°C) <b>Evaporation Rate:</b> No data available <b>Upper/Lower Flammability Limits:</b> No data available <b>Vapor Pressure:</b> <0.01 mm Hg @ 25°C <b>Vapor Density:</b> No data available							
Data Prepared/Revised: Dec. 4, 2013; Supersedes: April 3, 2013 <small>© 2013 Polytek Development Corp.</small>							

Updated Polytek® Safety Data Sheet [Page 1 Only]





In the manufacturing world, we track parts and components used in assembly to understand the manufacturing and maintenance process.

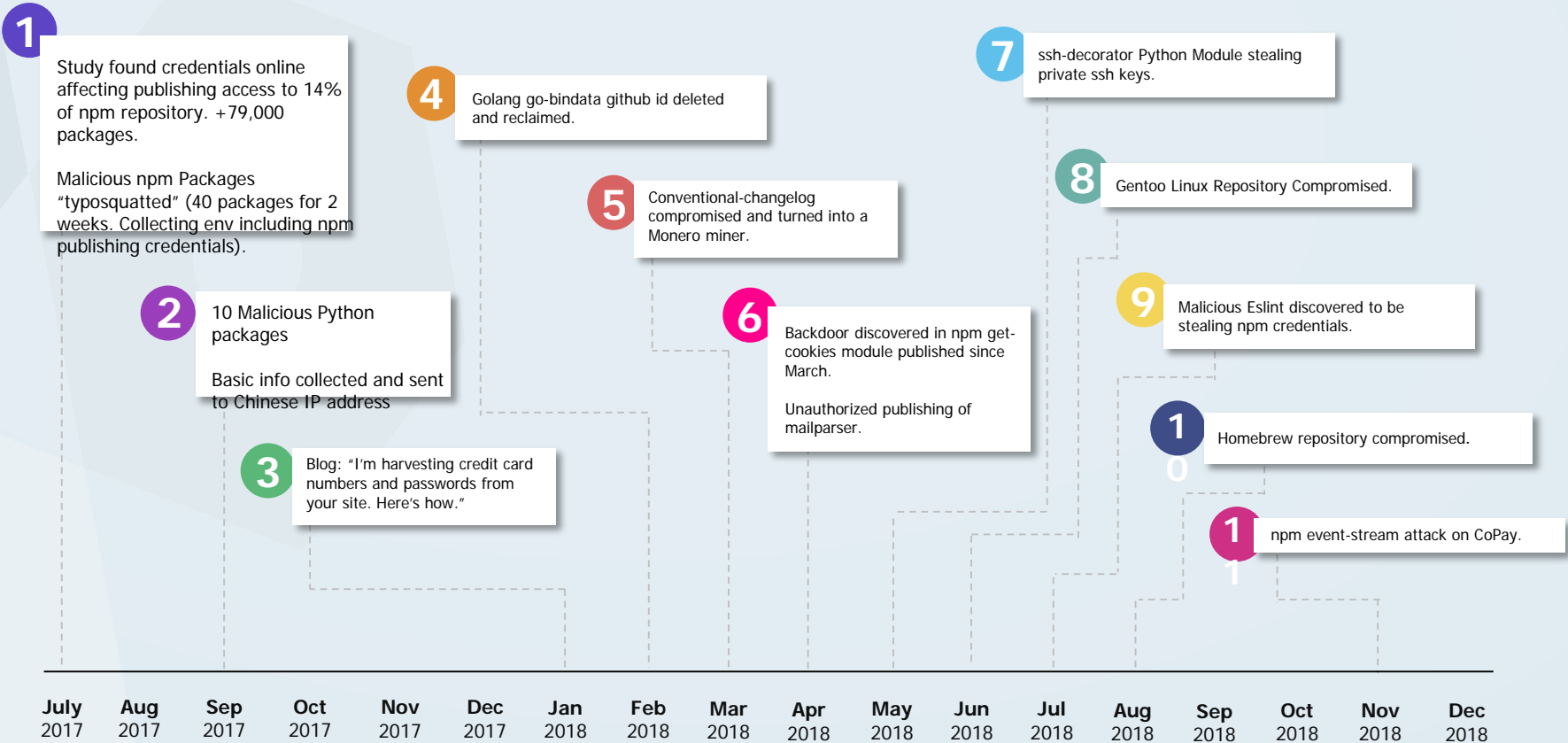


# Analogies



# No longer just an “emerging” risk

## Software Supply Chain Attacks



# 300+ Backdoored Github Libraries



# 300+ Backdoored Github Libraries



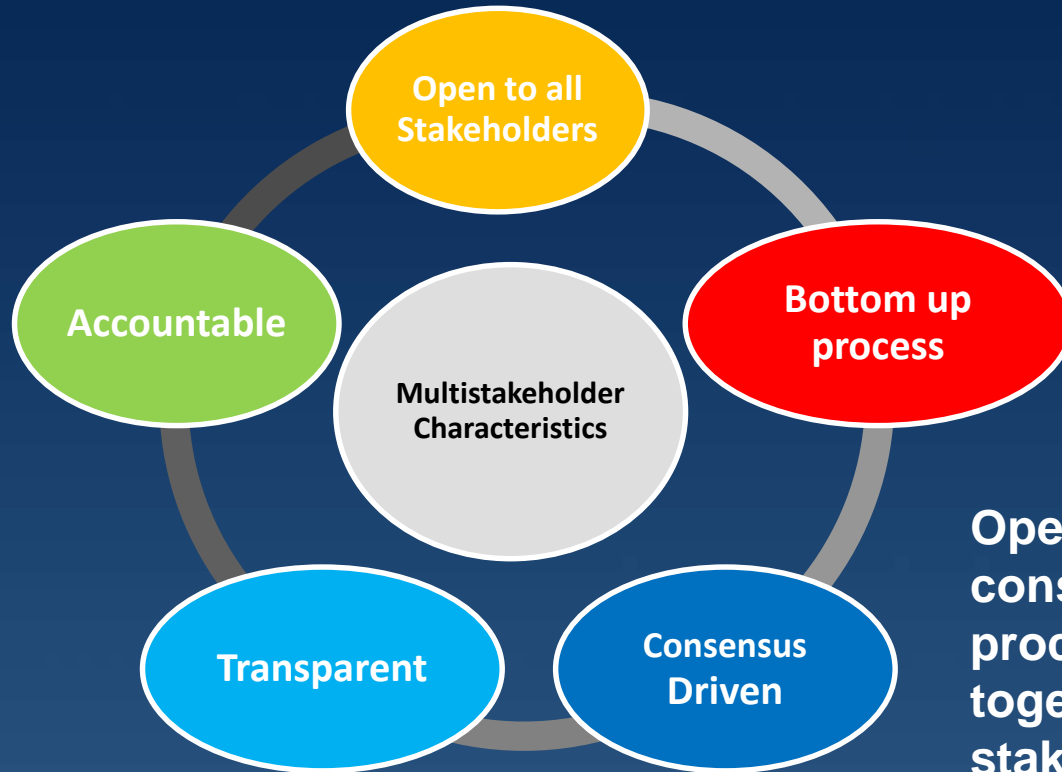
# Why don't we do this today?



# Enter: Your Friends, the Feds

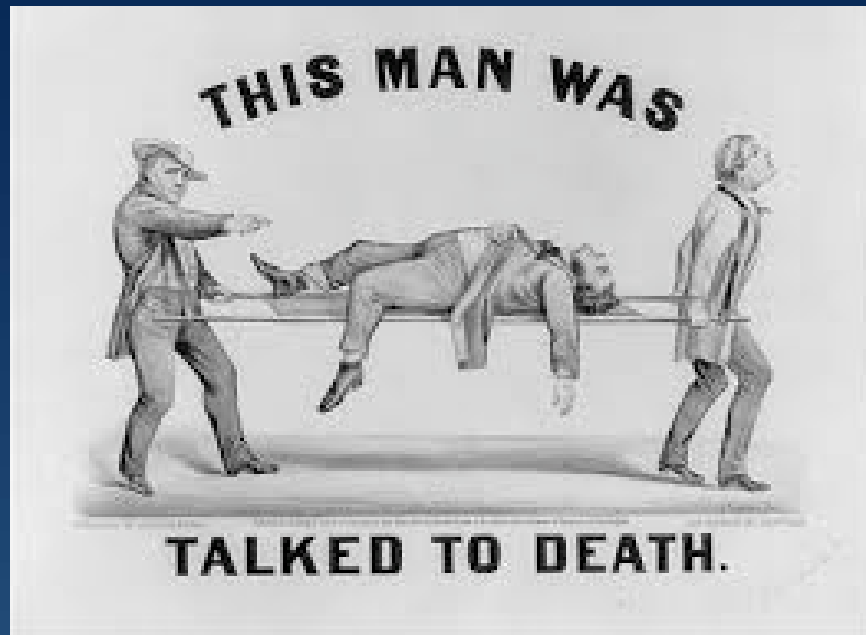


# The Multistakeholder Model



Open, transparent, consensus based processes that bring together diverse stakeholders can catalyze real progress across the ecosystem.







# The problem to be solved



# The problem to be solved

*Modern software systems involve increasingly complex and dynamic supply chains.*

# The problem to be solved

*Modern software systems involve increasingly complex and dynamic supply chains.*

*Lack of systemic transparency into the composition and functionality of these systems contributes substantially to cybersecurity risk as well as the costs of development, procurement, and maintenance.*

# The problem to be solved

*Modern software systems involve increasingly complex and dynamic supply chains.*

*Lack of systemic transparency into the composition and functionality of these systems contributes substantially to cybersecurity risk as well as the costs of development, procurement, and maintenance.*

*In our increasingly interconnected world, risk and cost impact not only individuals and organizations directly but also collective goods like public safety and national security.*

# How a transparency solution can help

- Enhancing the identification of vulnerable systems and the root cause of incidents

# How a transparency solution can help

- Enhancing the identification of vulnerable systems and the root cause of incidents
- Identifying suspicious or counterfeit software components

# How a transparency solution can help

- Enhancing the identification of vulnerable systems and the root cause of incidents
- Identifying suspicious or counterfeit software components
- Reducing unplanned and unproductive work

# How a transparency solution can help

- Enhancing the identification of vulnerable systems and the root cause of incidents
- Identifying suspicious or counterfeit software components
- Reducing unplanned and unproductive work
- Supporting more informed market differentiation and component selection

# How a transparency solution can help

- Enhancing the identification of vulnerable systems and the root cause of incidents
- Identifying suspicious or counterfeit software components
- Reducing unplanned and unproductive work
- Supporting more informed market differentiation and component selection
- Reducing duplication of effort by standardizing formats across multiple sectors

- Harmonization
- Amplification & routinization
- Extensions & innovation



**GOALS**

# Making progress

- Clear appreciation across sectors on the potential value of transparency
  - The broad scope of the problem
  - Machine-readability of the solution
  - Focus on a minimum viable solution with extensions.



# What is an SBOM?



# The “minimum viable” SBOM

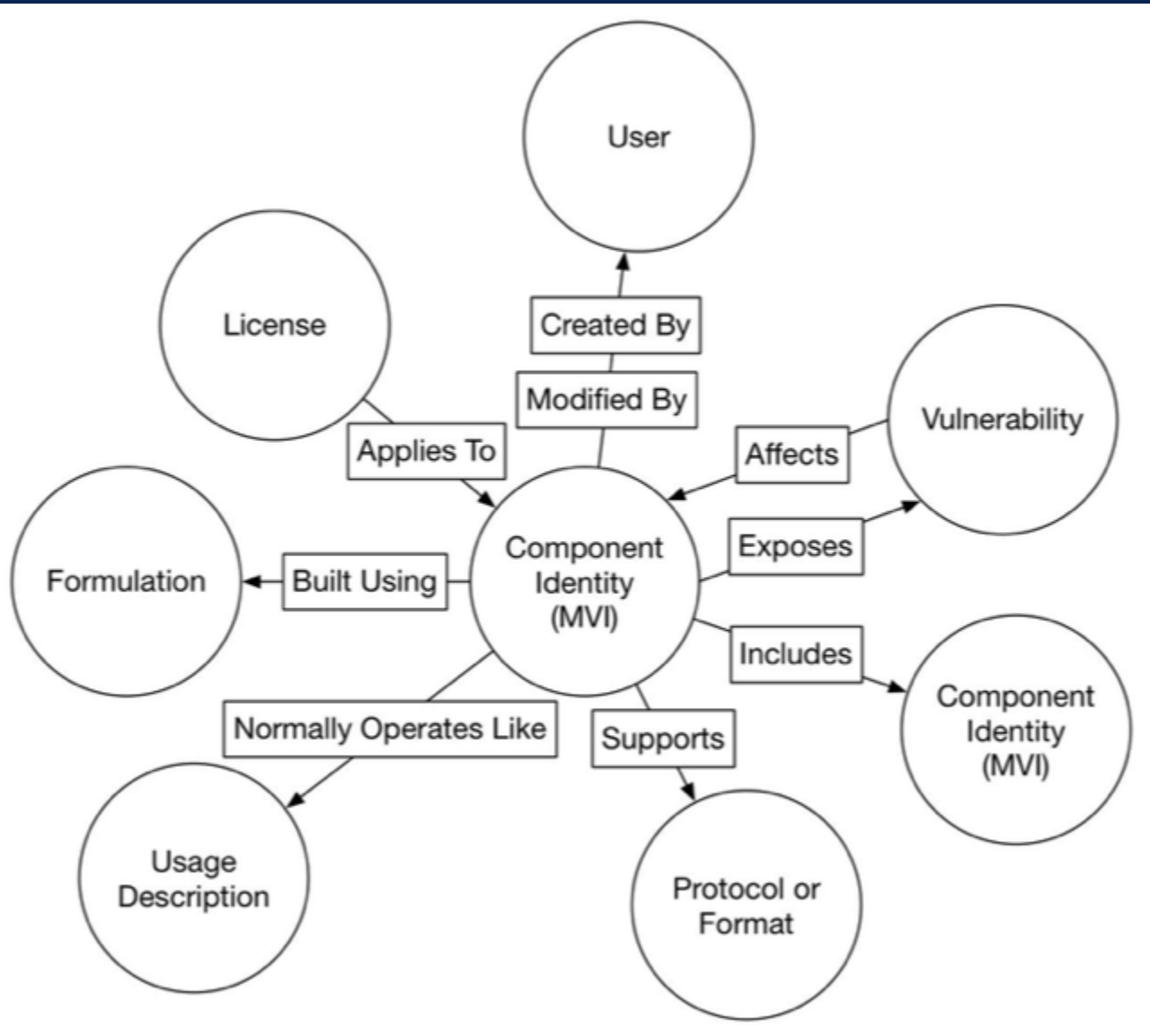
- Identity of Component
  - (Sufficient uniqueness)
- Relationship between components
- Extensions



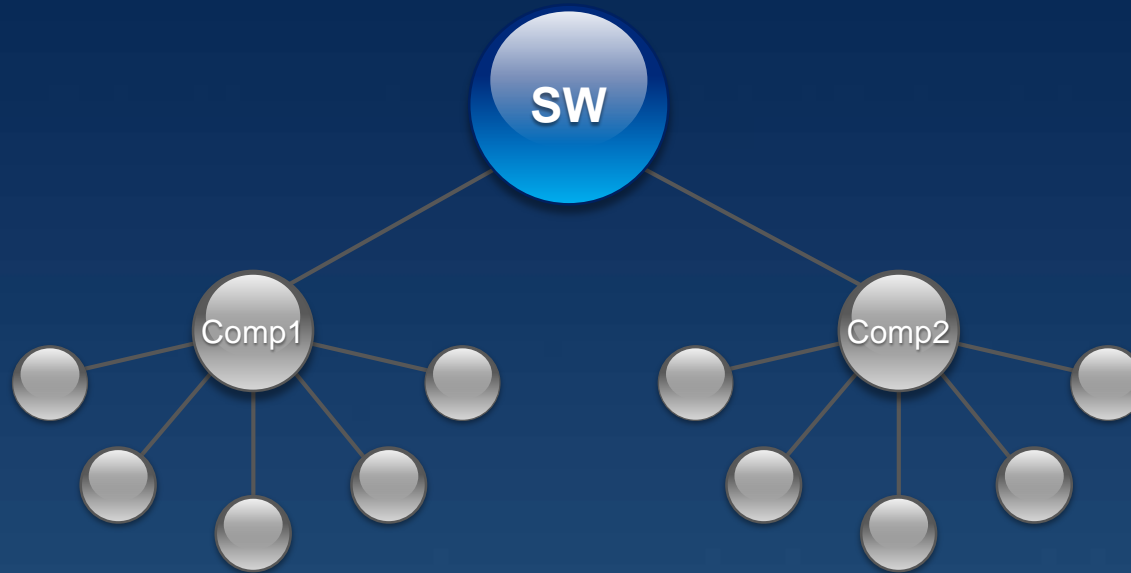
# Naming is Hard



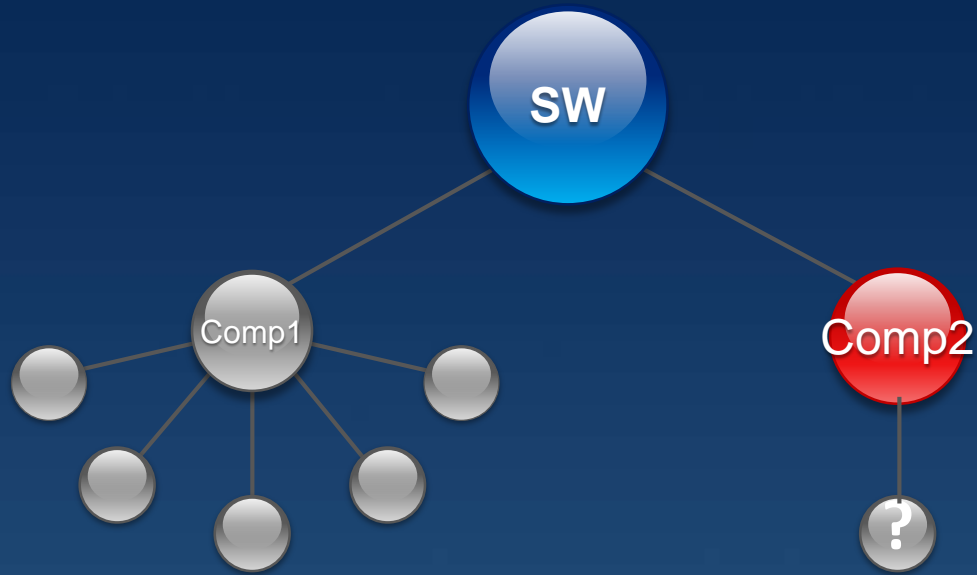
# Feature Support



# SBOM as a graph

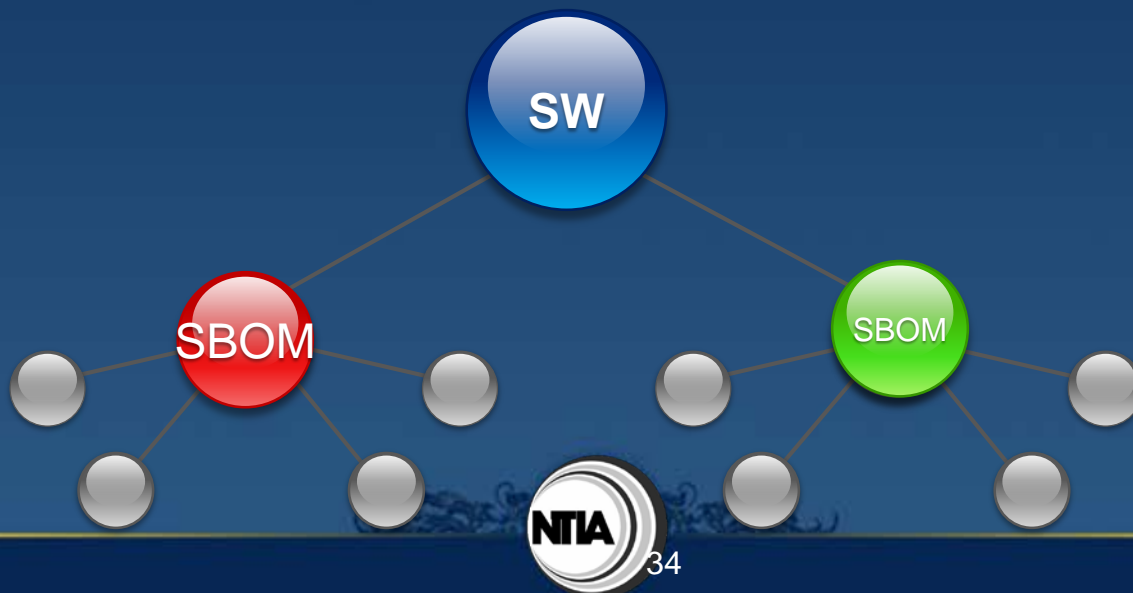


# Being Clear about Opacity



# Data about data

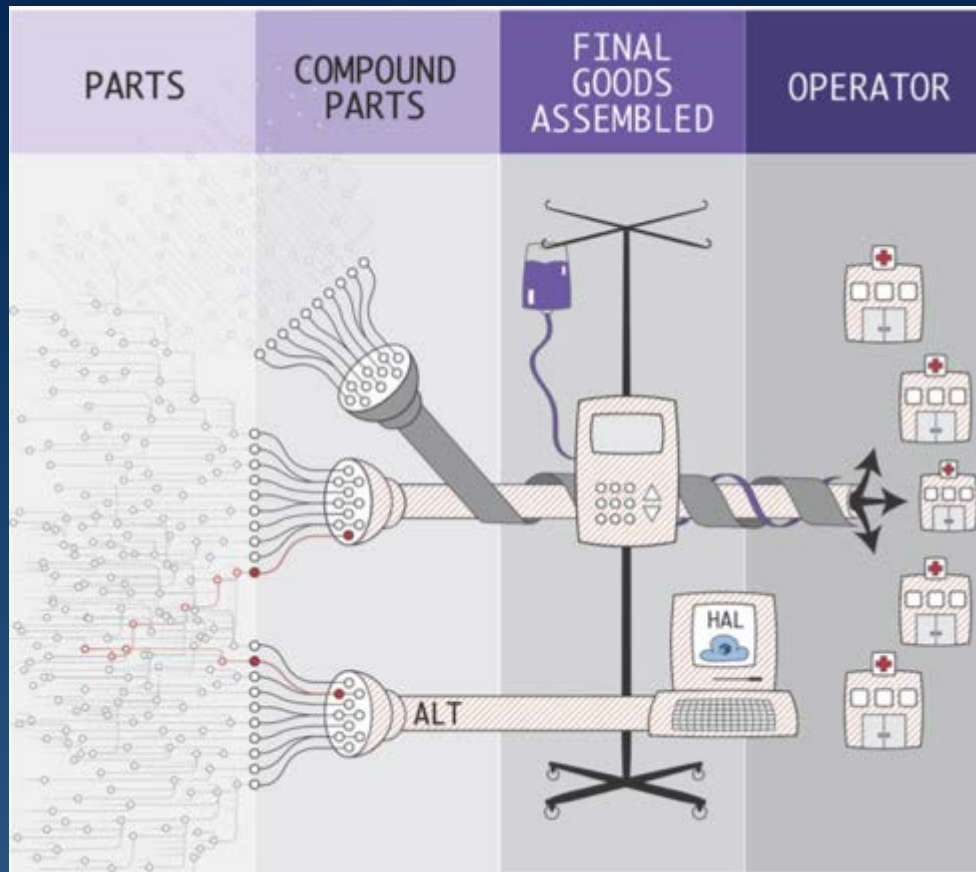
- I built this set of SBOM data
- VS
- This is SBOM data from someone else.



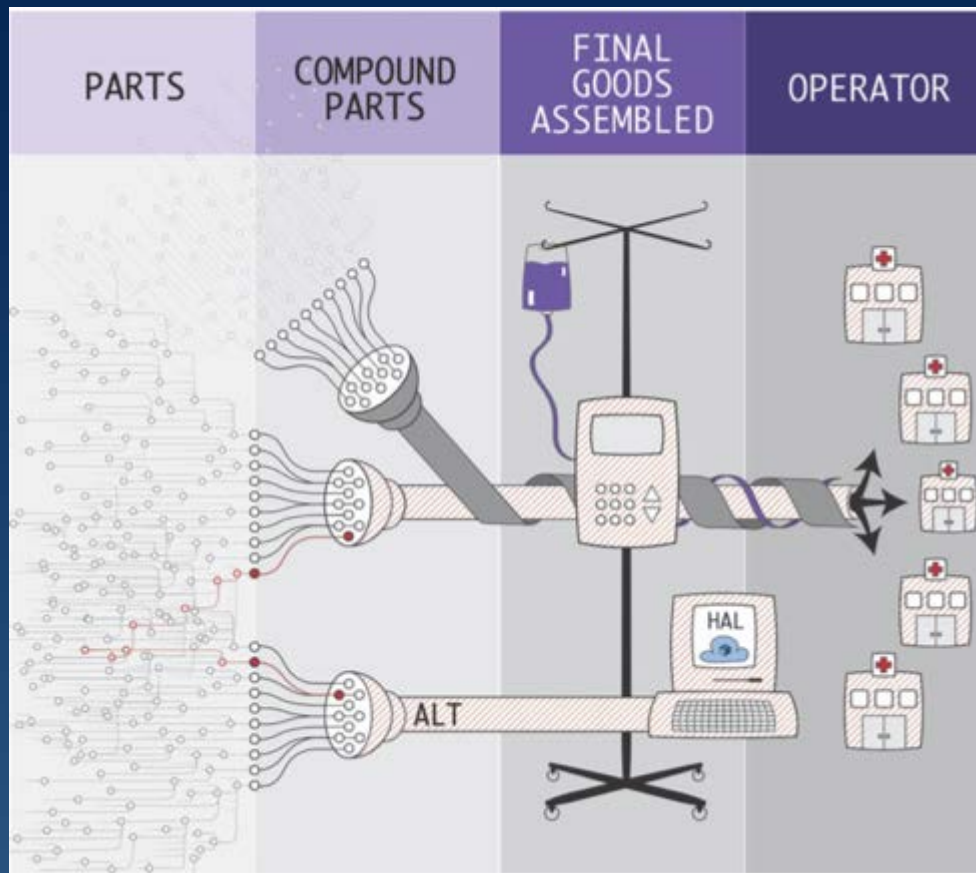
# Why should we use an SBOM?



# A supply chain perspective



# A supply chain perspective



- Supplier selection
- Supply selection
- Supply vigilance

# Capturing Stories

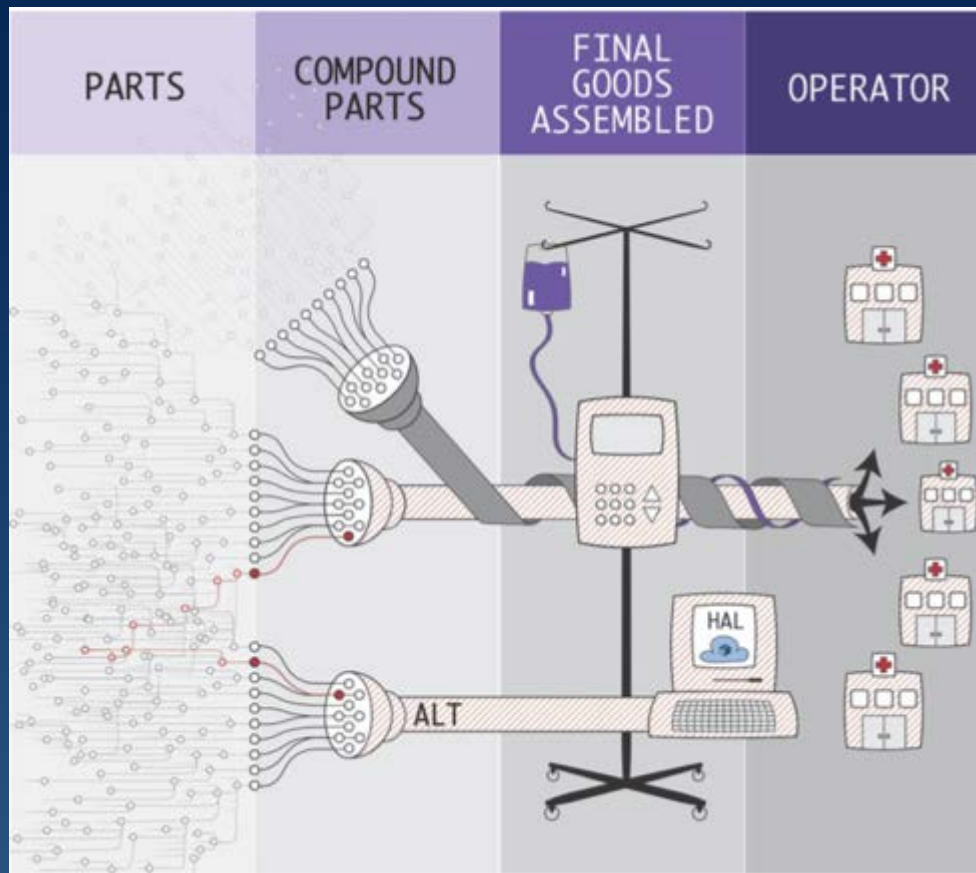
Each of these offers unique perspectives on the current and potential value of transparency.

We would love to have your perspective!

PARTS			COMPOUND PARTS			FINAL GOODS ASSEMBLED			OPERATOR		
S1	S2	S3	S1	S2	S3	S1	S2	S3	S1	S2	S3
			<small>Chris Rossini</small> RedHat			ENTERPRISE					
						<small>Chris Gates</small> Velentium			<small>Mike Powers</small> Christiana Health		
									<small>Scott Yu</small> BoA		
			<small>Justi Corran</small> PTC			INDUSTRIAL					
									<small>Bob Martin</small> DoD		
						\$OTHER					



# A supply chain perspective

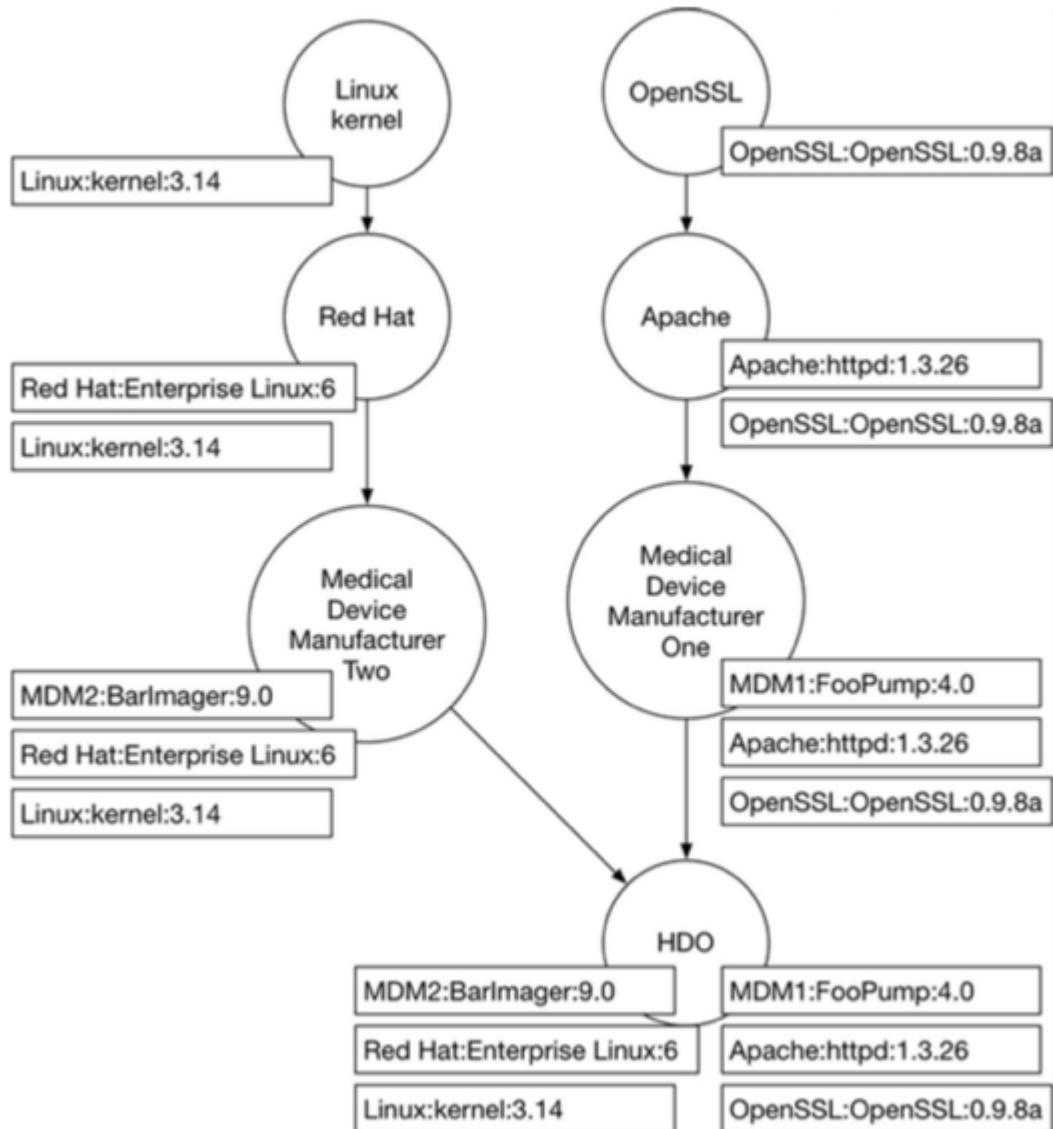


- Writer/Maker
- Acquirer/Purchaser
- Operator/Maintainer

# How do we SBOM?



# Recall...



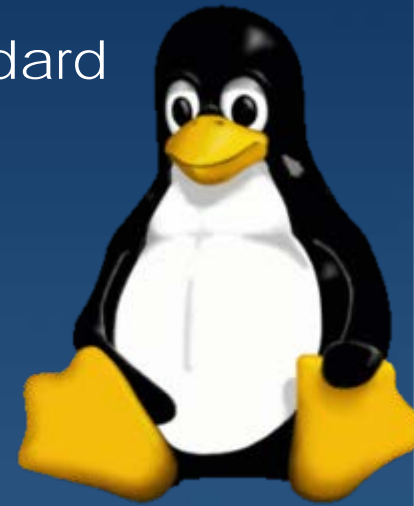
# Not a Standards Development process



**FORTUNATELY, WE HAVE SOME EXISTING TOOLS THAT WE CAN USE FOR SBOM DATA**

# Software Package Data Exchange (SPDX)

SPDX® is an open standard for communicating software bill of material information (including components, licenses, copyrights, and security references). The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The grass-roots effort includes representatives from more than 20 organizations—software, systems and tool vendors, foundations and systems integrators—all committed to creating a standard for software package data exchange formats.



# SPDX Example

```
# Document Header
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
SPDXID: SBOMDOCUMENT
DocumentName: SBOM-Proof-of-concept
DocumentNamespace: http://example.com
Created: 2018-12-18Y22:11:34Z
CreatorComment: <text> This document was
created as a proof-of-concept </text>
```

## # Packages

```
PackageName:alsa-conf
SPDXID: yocto/alsa-conf@1.1.0
PackageVersion: 1.1.0
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
```

```
PackageName:alsa-conf-base
SPDXID: yocto/alsa-conf-base@1.1.0
PackageVersion: 1.1.0
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
```

```
PackageName:alsa-lib
SPDXID: yocto/alsa-lib@1.1.0
PackageVersion: 1.1.0
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
```

```
Relationship: yocto/libasound2@1.1.0 PACKAGE_OF yocto/alsa-lib@
Relationship: yocto/libc6@2.23.0 PACKAGE_OF yocto/alsa-lib@1.1.
```

...

<https://github.com/spdx/spdx-spec>



# Software Identification (SWID)

SWID tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015.



# SWID tag example

```
<SoftwareIdentity name="alsa-conf" tagId="yocto/alsa-conf@1.1.0" version="1.1.0"/>
<SoftwareIdentity name="alsa-conf-base" tagId="yocto/alsa-conf-base@1.1.0"
version="1.1.0"/>
<SoftwareIdentity name="alsa-lib" tagId="yocto/alsa-lib2@1.1.0" version="1.1.0">
  <Link href="swid:yocto/libasound2@1.1.0" rel="requires"/>
  <Link href="swid:yocto/libc6@2.23.0" rel="requires"/>
</SoftwareIdentity>
...
```

# Translation between formats



**WE HAVE IDENTIFIED THE COMMON ELEMENTS.  
A 'BILINGUAL' ECOSYSTEM DOES NOT OFFER TOO MANY CHALLENGES**

Rather than pick a winner, we will build out guidance to support both formats with effective interoperability.


# Related efforts in the ecosystem



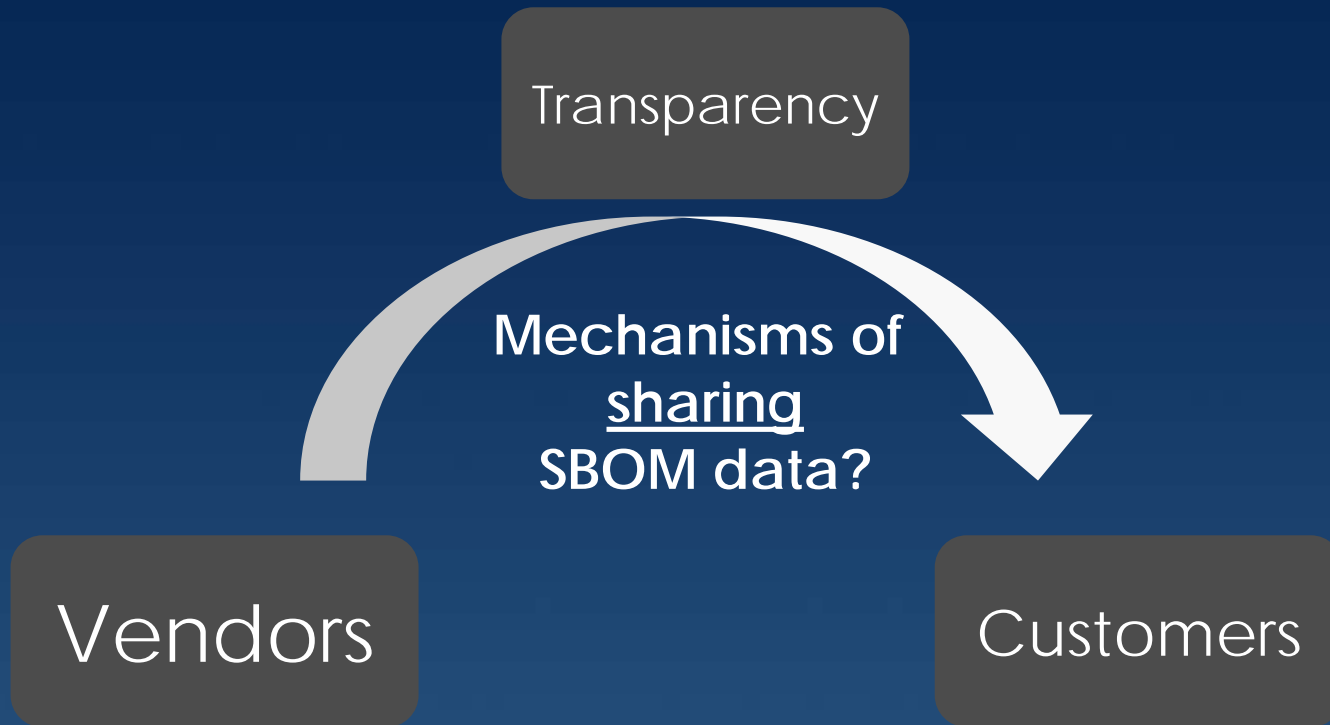
- Software Heritage Index
- Package URL (Purl)
- OpenChain
- CPE



Open questions to figure out *together*

A wide-angle, high-angle photograph of a massive industrial warehouse. The floor is filled with long, parallel rows of pallets, each heavily loaded with cardboard boxes. The boxes are organized into neat, repeating patterns that stretch far into the distance. The warehouse has a high ceiling with a complex network of steel beams and pipes. On the right side, there are elevated walkways with metal railings. In the background, more stacks of boxes and some industrial equipment are visible. A white rectangular text box is superimposed over the upper-middle portion of the image, containing the text "Obstacles to obtaining SBOM data?".

Obstacles to obtaining SBOM data?



# **Vulnerability vs. Exploitability**



# Next steps

- Drafts of “minimum viable” by late June for feedback.
- After “minimum viable”
  - Extensions of data for use cases
  - Tooling
  - Awareness and Adoption



# To recap...

- Tracking third party components can help understand and address a wide range of risks across the entire ecosystem
- An ongoing, open process convened by NTIA is bringing together experts to address:
  - What a Software Bill of Materials is
  - Why it can help across the supply chain
  - How we can implement it
- Next steps will focus on tooling and extensions
- Get involved in the NTIA process!
  - Contact [afriedman@ntia.gov](mailto:afriedman@ntia.gov)
  - @allanfriedman



Thank You!

*afriedman@ntia.doc.gov*

