RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-R02

Software Bill of Materials: Progress toward Transparency of Third-Party Code

Allan Friedman, PhD

Director of Cybersecurity Initiatives
National Telecommunications & Information Administration
US Department of Commerce
@allanfriedman

Should I pay attention or look at my phone?

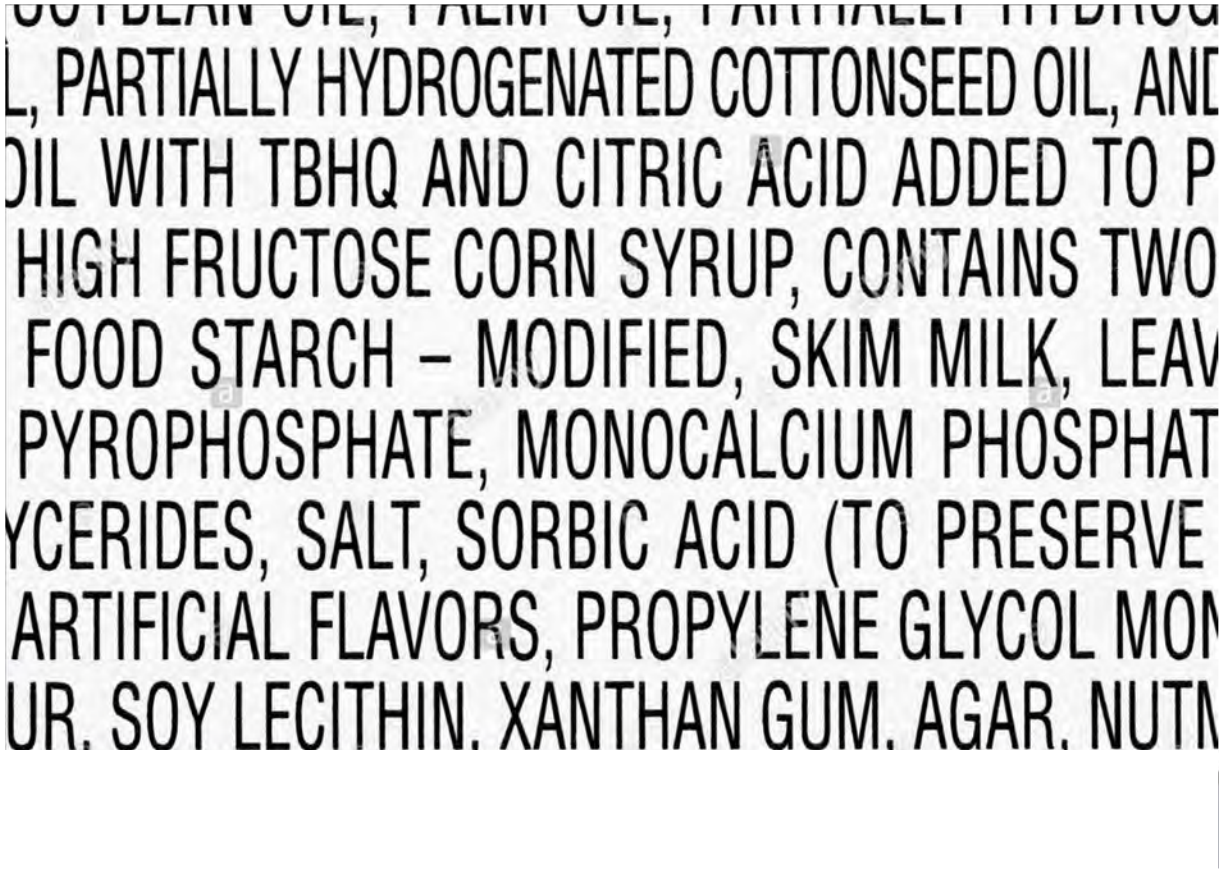
- *Focusing* on transparency in the software supply chain
- *Understanding* the NTIA process
- *Finding* common ground on what a Software Bill of Materials is
- *Documenting* the myriad use cases
- *Identifying* existing formats to implement
- *Engaging* to make the process better

RSAConference2019

Thinking about transparency

A bit of background

Analogies



We understand the role of a list of ingredients.

Analogies

Polytek Development Corp.

SAFETY DATA SHEET

1. Identification

Product Identifier: **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

Product Code(s): 74-20B, 74-24B, 74-29B, 74-29WHITEB, 74-30B, 74-30CLEARB, 74-30HTB, 74-31B, 74-41B, 74-45B

Use: Component for Polyurethane Mold Rubber. For Industrial/Professional use only.

Manufacturer: Polytek Development Corp.
55 Hilton St., Easton, PA 18042 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: sds@polytek.com

2. Hazards Identification

GHS Classification:
Specific Target Organ Toxicity - Repeated Exposure Category 2

Label Elements: Warning!

Contains Diethyltoluenediamine

Hazard Phrases
H373 May cause damage to pancreas through prolonged or repeated exposure.

Precautionary Phrases
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.

Supplemental Information: None known.
This is one part of a two-part system. Read and understand the hazard information on Part A before using.

3. Composition/Information on Ingredients

Chemical Name	CAS #	%
Diethyltoluenediamine	68479-98-1	1-<3%

4. First-Aid Measures

Eye Contact: Rinse thoroughly with water, holding the eyelids open to be sure the material is washed out. Get medical attention if irritation persists.
Skin Contact: Remove contaminated clothing. Wash contact area thoroughly with soap and water. Get medical attention if irritation persists.
Inhalation: Remove person to fresh air. Get medical attention if symptoms persist.
Ingestion: Do not induce vomiting unless directed to do so by medical personnel. Get medical attention.
Most Important Symptoms/Effects: May cause mild eye and skin irritation. May be harmful if swallowed.
Indication of Immediate Medical Attention/Special Treatment: Immediate medical attention is not required.

5. Fire-Fighting Measures

Extinguishing Media: 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.
Specific Hazards: Not classified as flammable or combustible. Product will burn under fire conditions.
Special Protective Equipment & Precautions for Fire-Fighters: Wear positive pressure, self-contained breathing apparatus and full-body protective clothing. Cool fire-exposed containers with water.

6. Accidental Release Measures

Personal Precautions, Protective Equipment and Emergency Procedures: 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.
Methods and Materials for Containment and Cleanup: 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.

7. Handling and Storage

Safe Handling: 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.
Safe Storage: Store indoors at temperatures below 120°F (49°C). Store in original containers. Avoid getting moisture into containers. Keep containers tightly closed.

8. Exposure Controls/Personal Protection

Occupational Exposure Limits: None Established.
Ventilation: Use with adequate general or local exhaust ventilation to minimize exposure levels.
Respiratory Protection: 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.
Skin Protection: Wear impervious gloves, such as butyl rubber or nitrile rubber.
Eye Protection: Wear chemical safety goggles.
Other Protective Measures: 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 practice.

9. Physical and Chemical Properties

Appearance: Liquid of varied colors
Odor: Slightly pungent
Odor Threshold: No data available
pH: Not applicable
Melting Point: No data available
Boiling Point: No data available
Flash Point: > 350°F (>177°C)
Evaporation Rate: No data available
Upper/Lower Flammability Limits: No data available
Vapor Pressure: <0.01 mm Hg @ 25°C
Vapor Density: No data available

Date Prepared/Revised: Dec. 6, 2013; Supersedes: April 3, 2013

Analogies

No longer just an “emerging” risk

Software Supply Chain Attacks

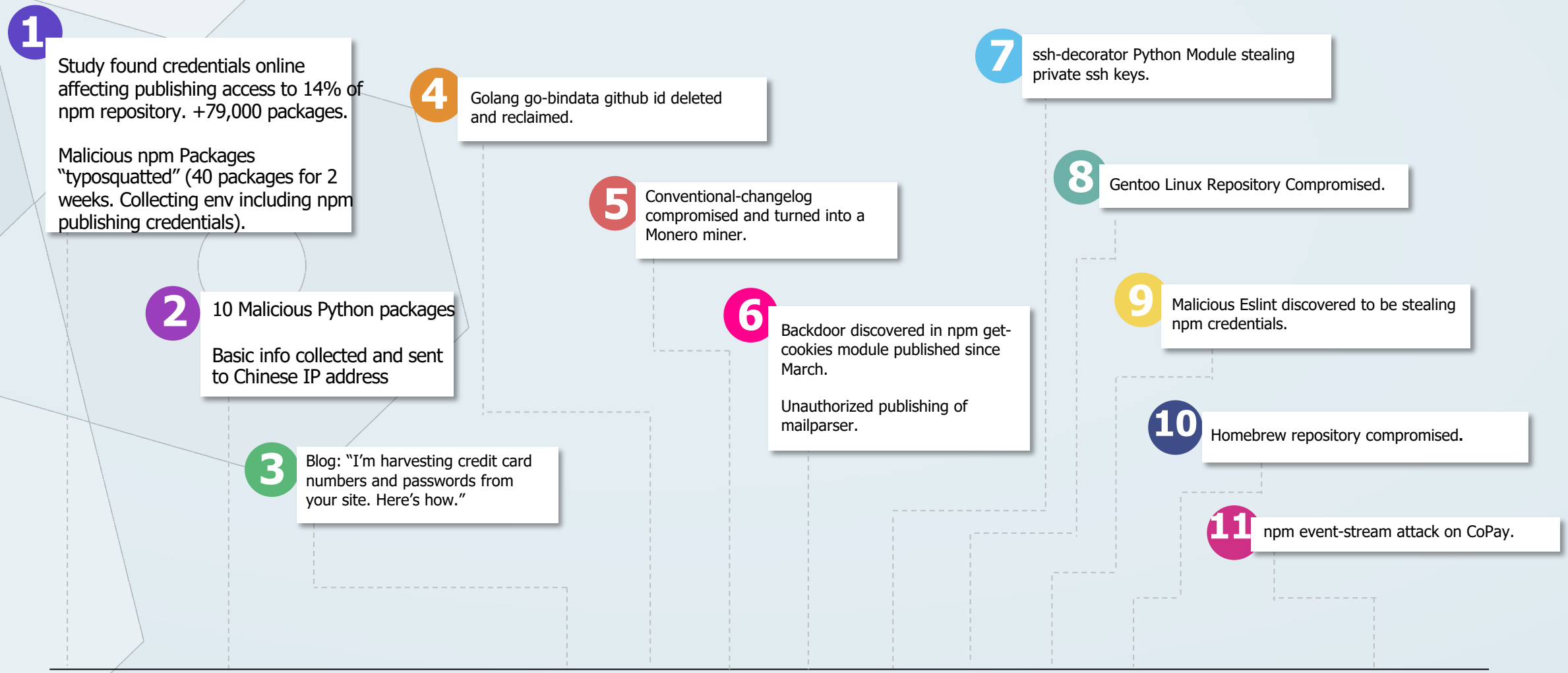


Image by Sonatype

RSAConference2019

What we're doing about it

Enter your good friends at NTIA


Peter Schrank

Bottom-Up Approach

The policy side

THE MULTISTAKEHOLDER PROCESS

The “multistakeholder process”

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

What we're not doing

- Regulation
- Source code disclosure

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

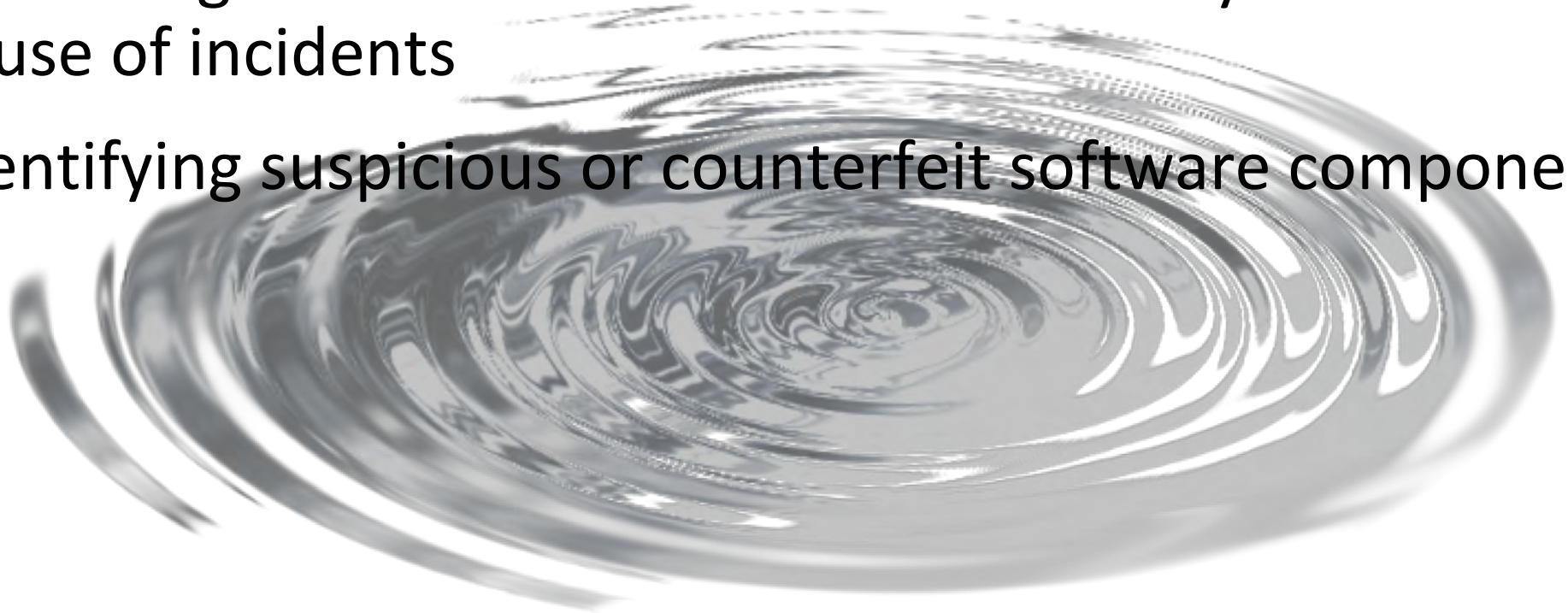
Modern software systems involve increasingly complex and dynamic supply chains.

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.

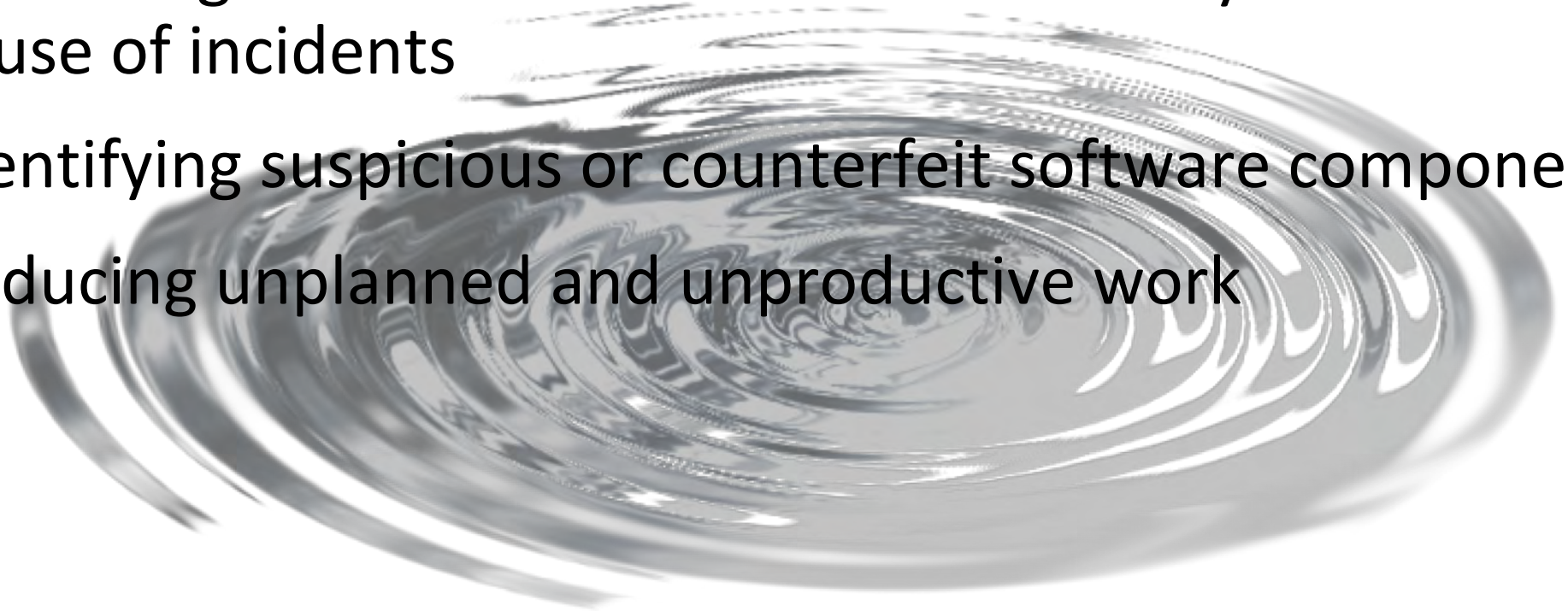
How a transparency solution can help

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

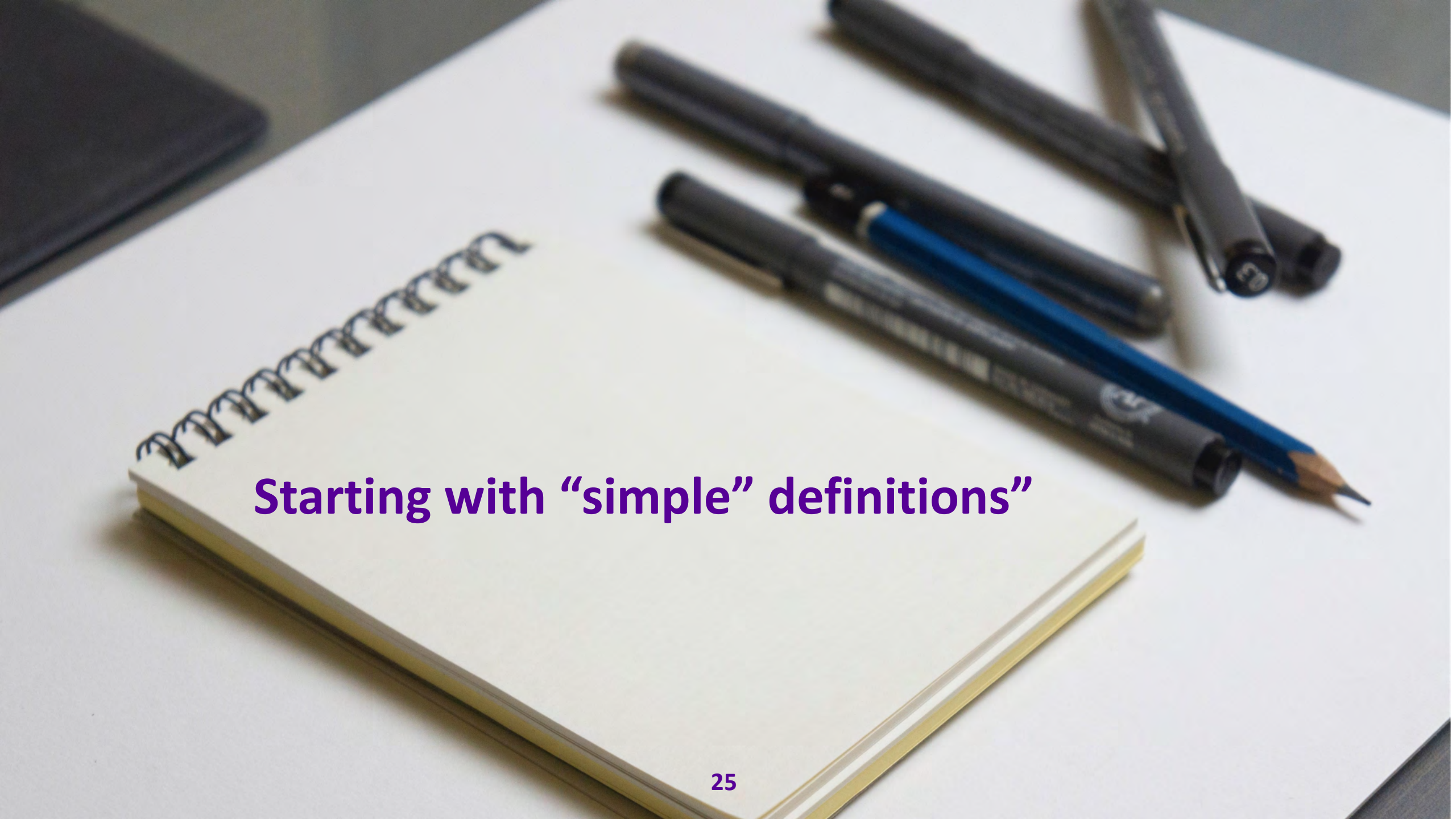
Making progress

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

RSAConference2019

WHAT IS AN SBOM?

Working to frame the problem

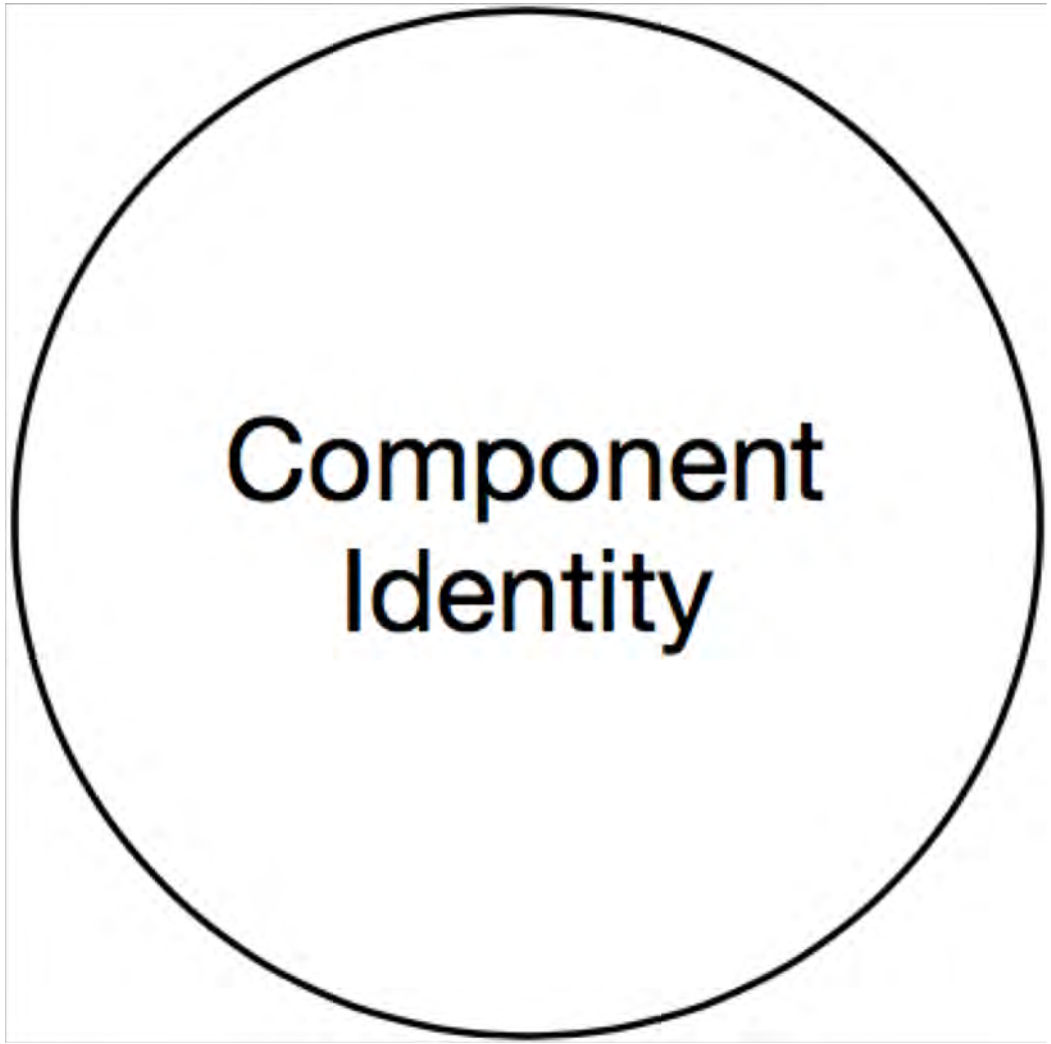


Starting with “simple” definitions”

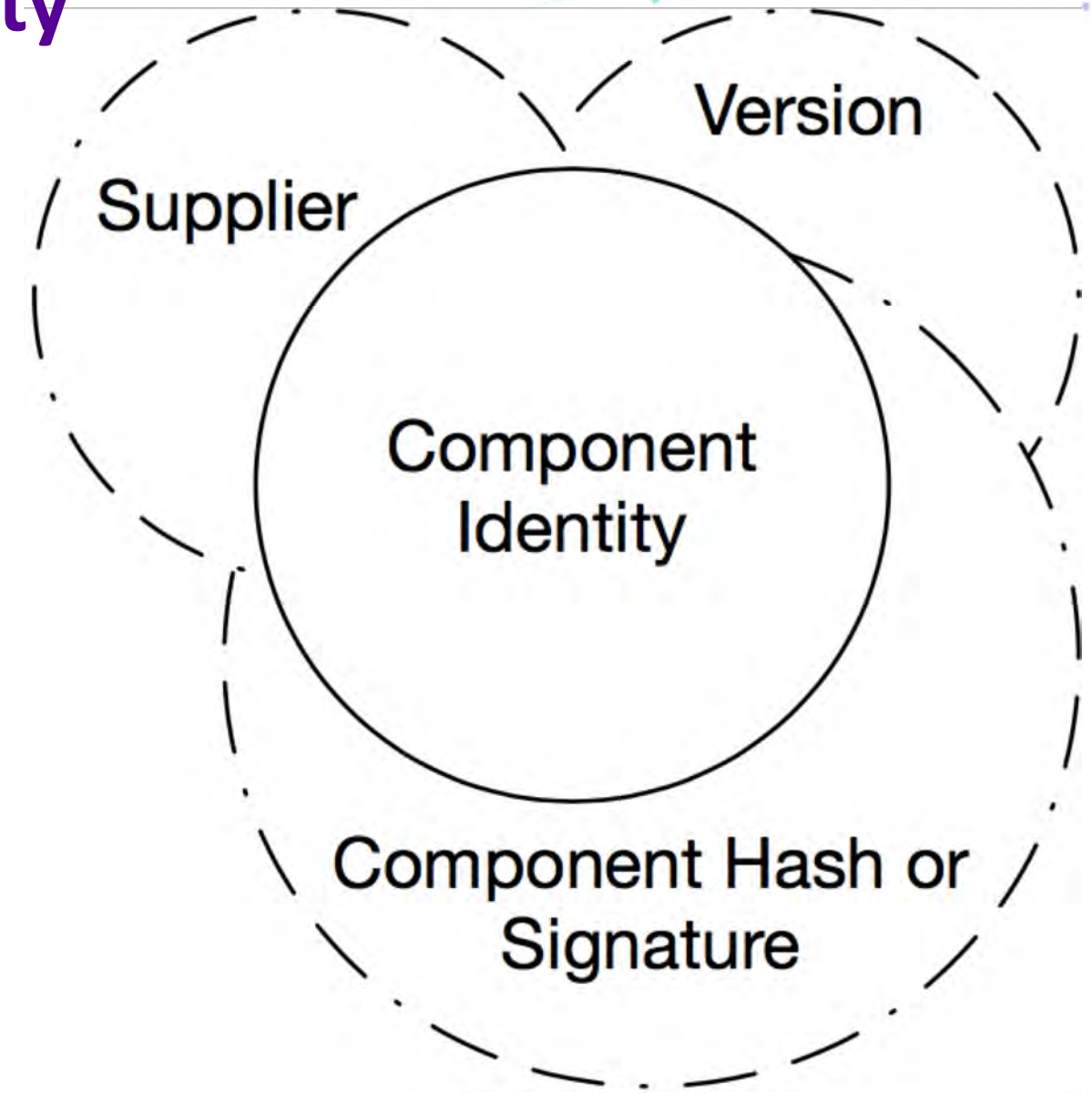
The Big Tent

A process that should reflect as many interests and use cases as possible,
while trying to rapidly identify a “minimum viable product”

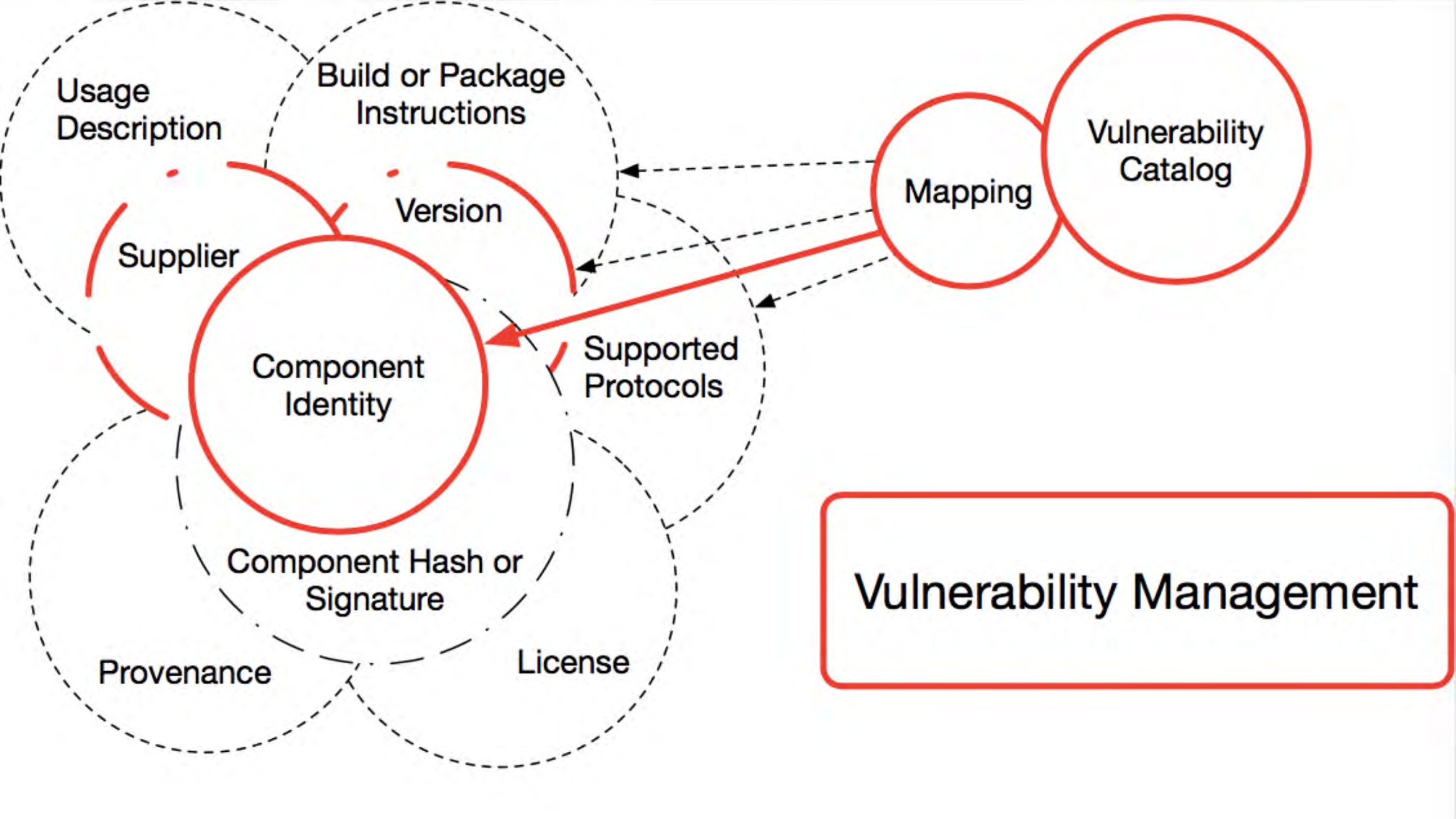
Core Identity



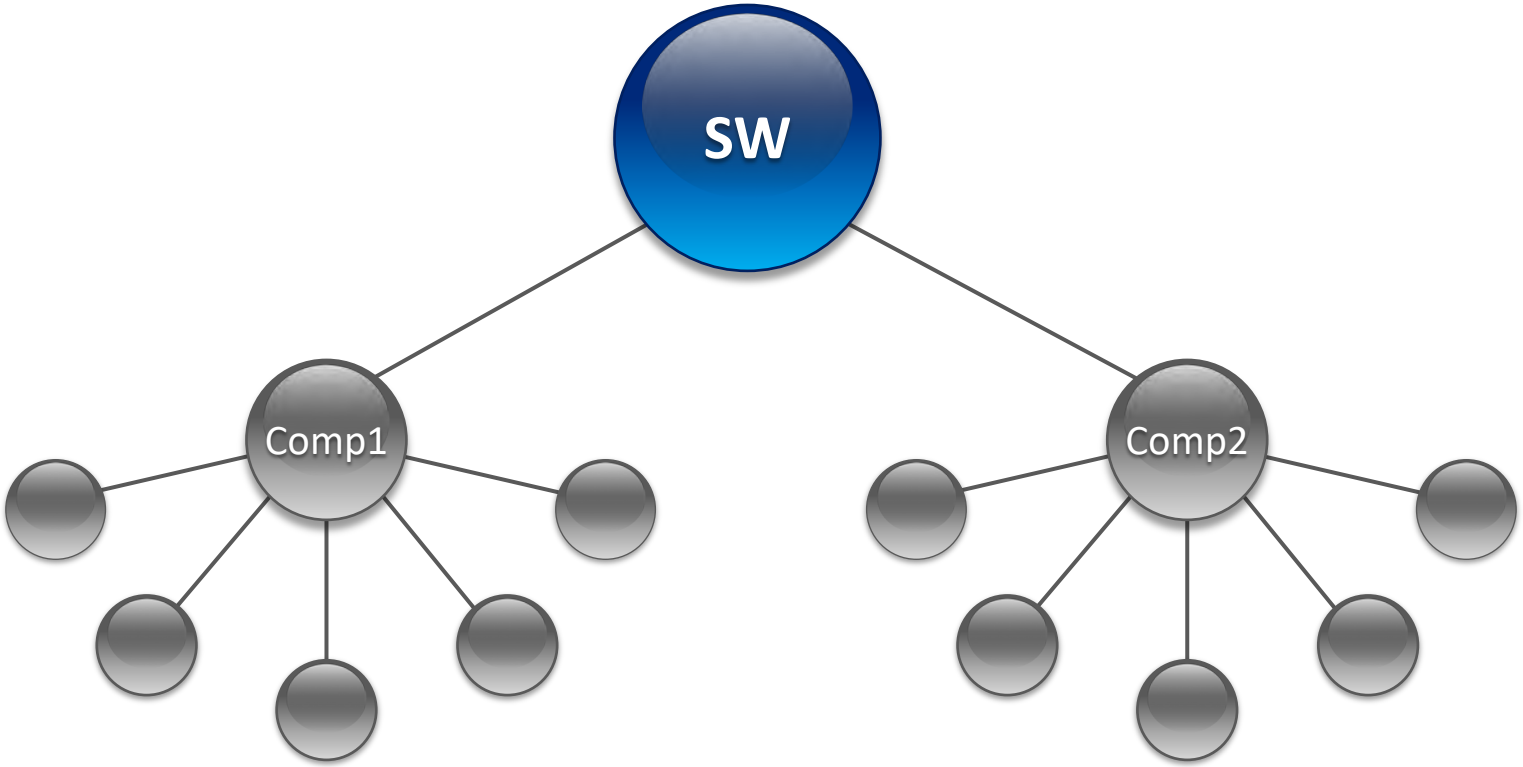
Basic Identity



The namespace challenge


Usage Description
Build or Package Instructions
Version
Supplier
Component Identity
Supported Protocols
Component Hash or Signature
Provenance
License
Mapping
Vulnerability Catalog
Vulnerability Management

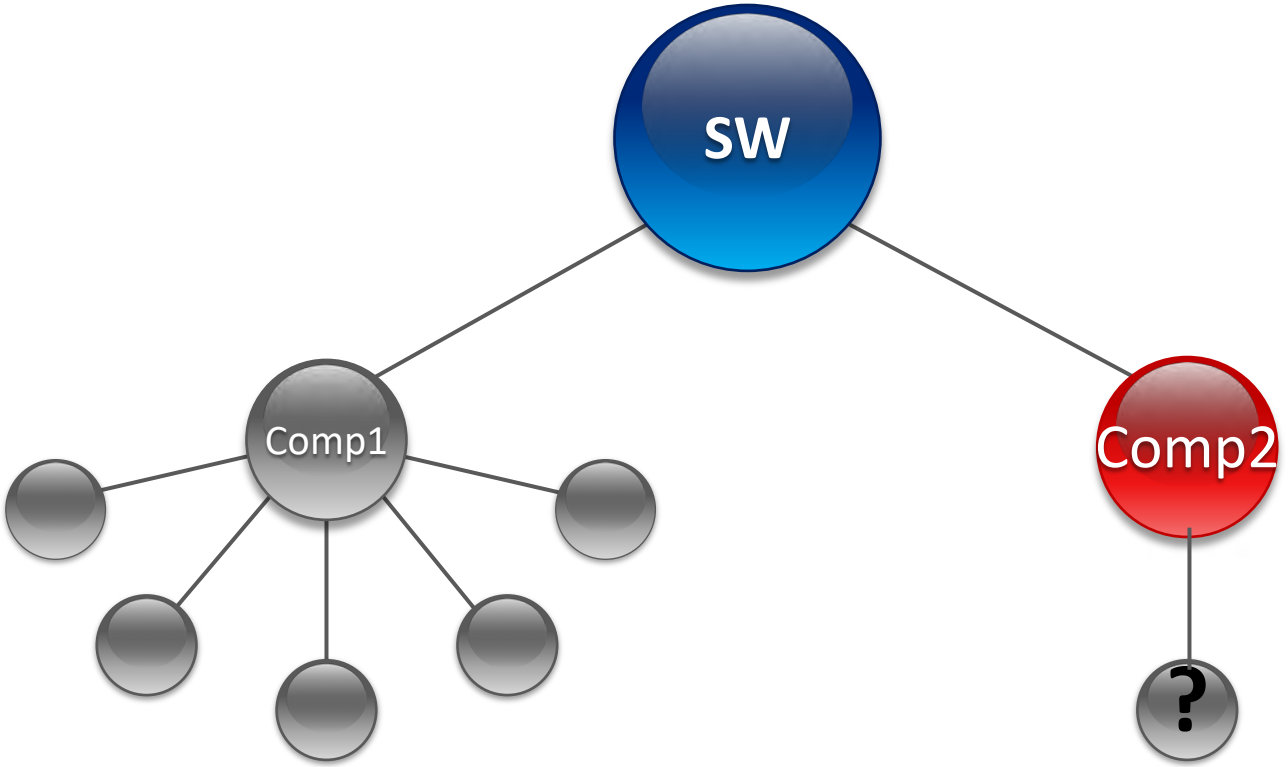
SBOM as a graph



How many levels deep?

CAPTURING ALL LEVELS VS. EACH SUPPLIER PRODUCES AN SBOM RECURSIVELY

Being Clear about Opacity

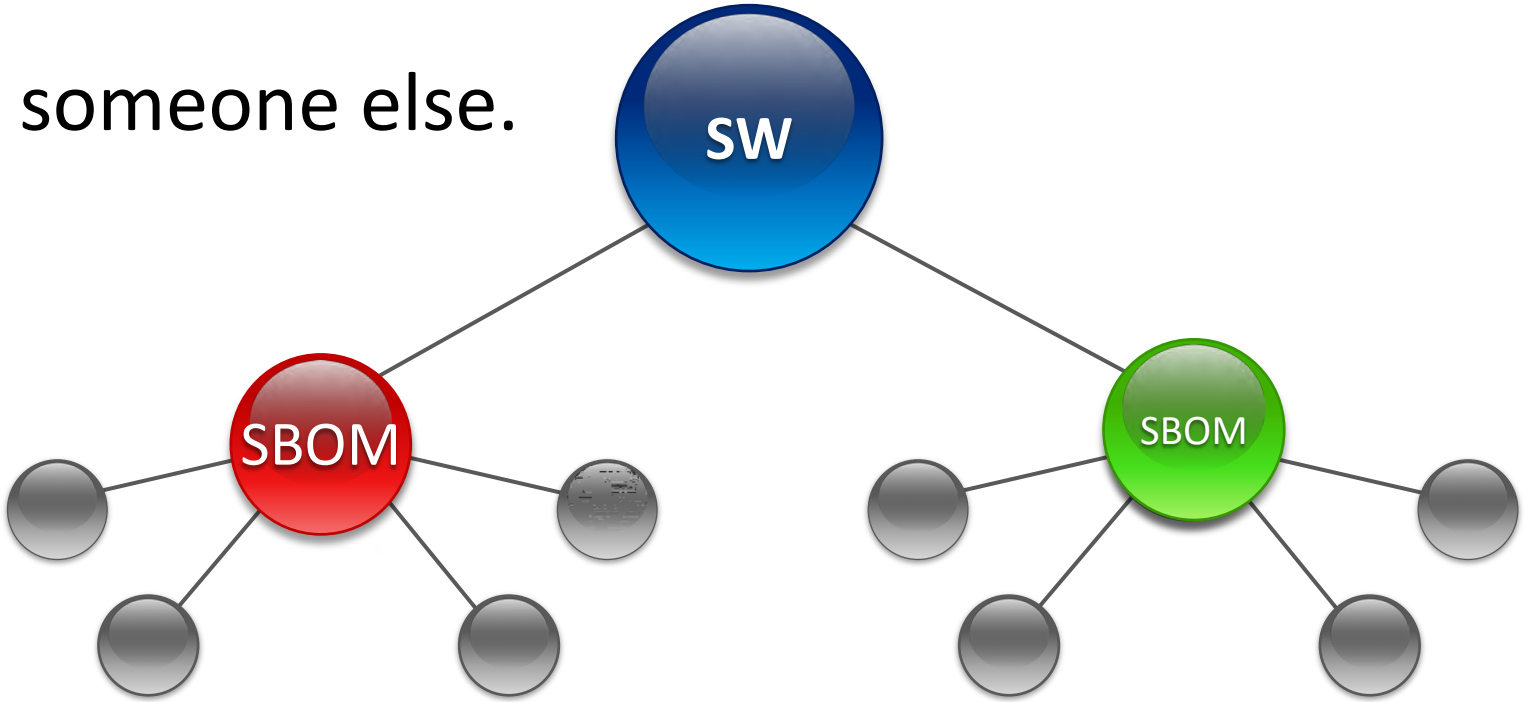


Data about data

- I built this set of SBOM data

vs

- This is SBOM data from someone else.

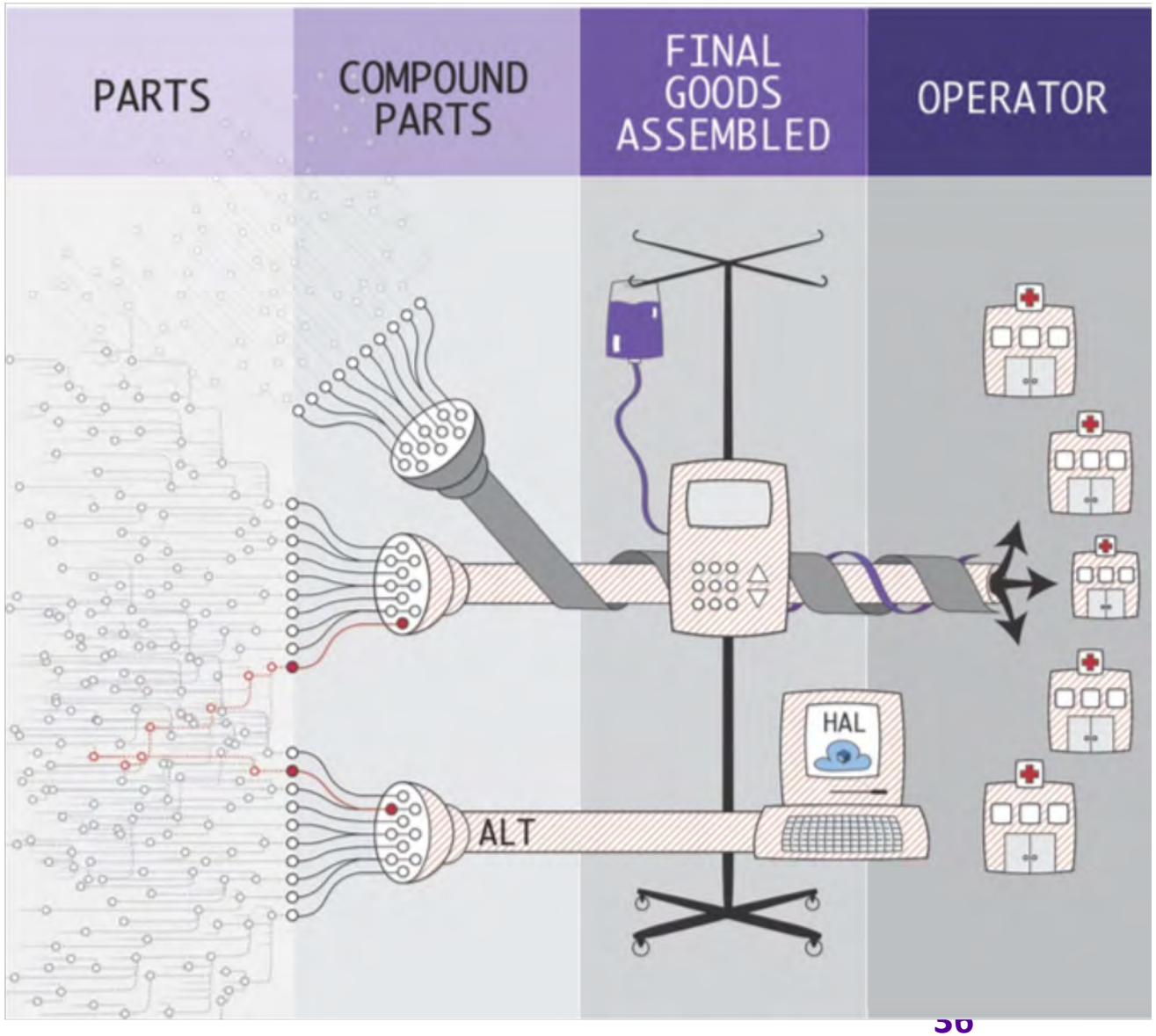


RSAConference2019

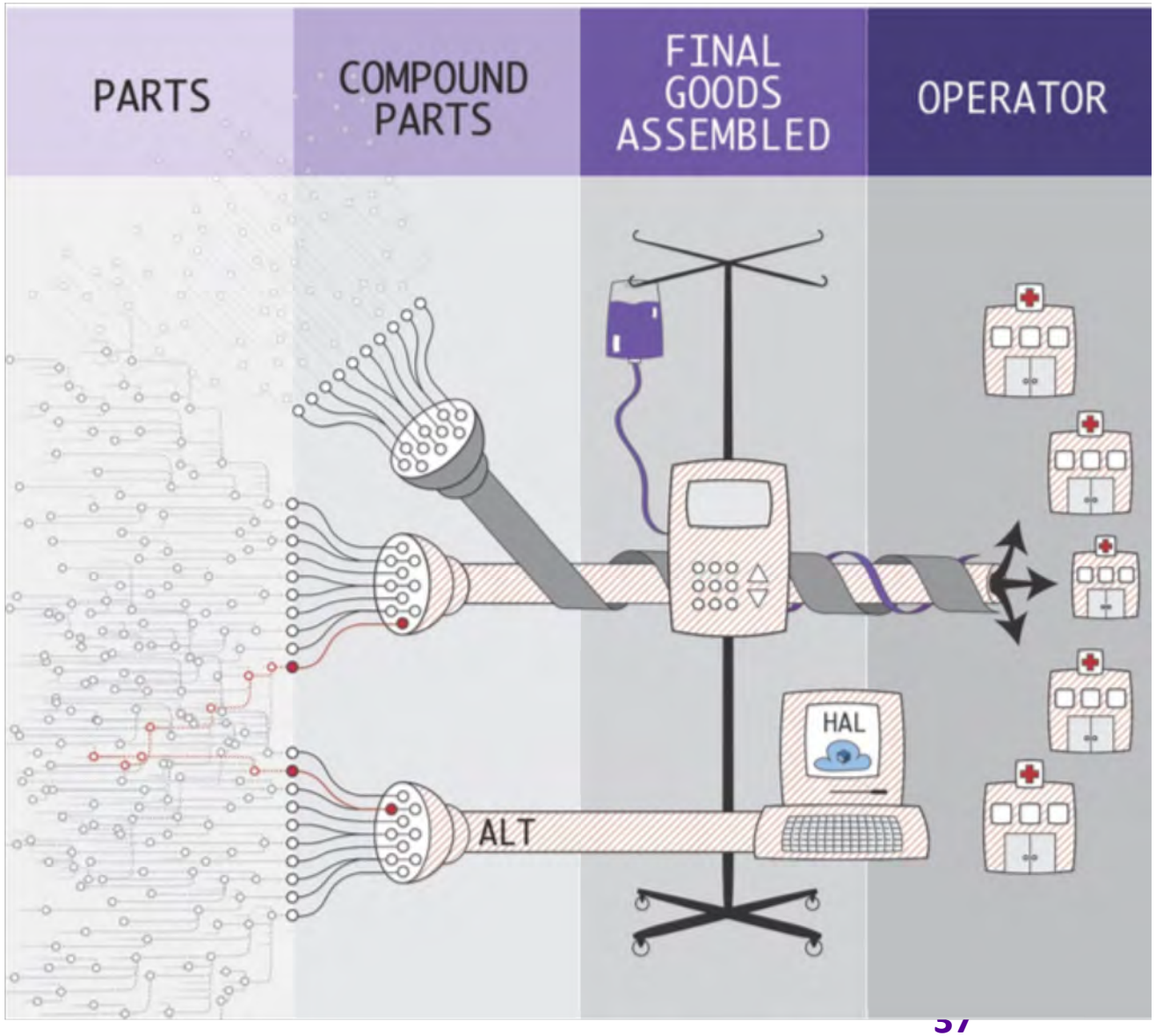
WHY SHOULD WE USE AN SBOM?

Working to understand current practices and potential use cases

A supply chain perspective



A supply chain perspective

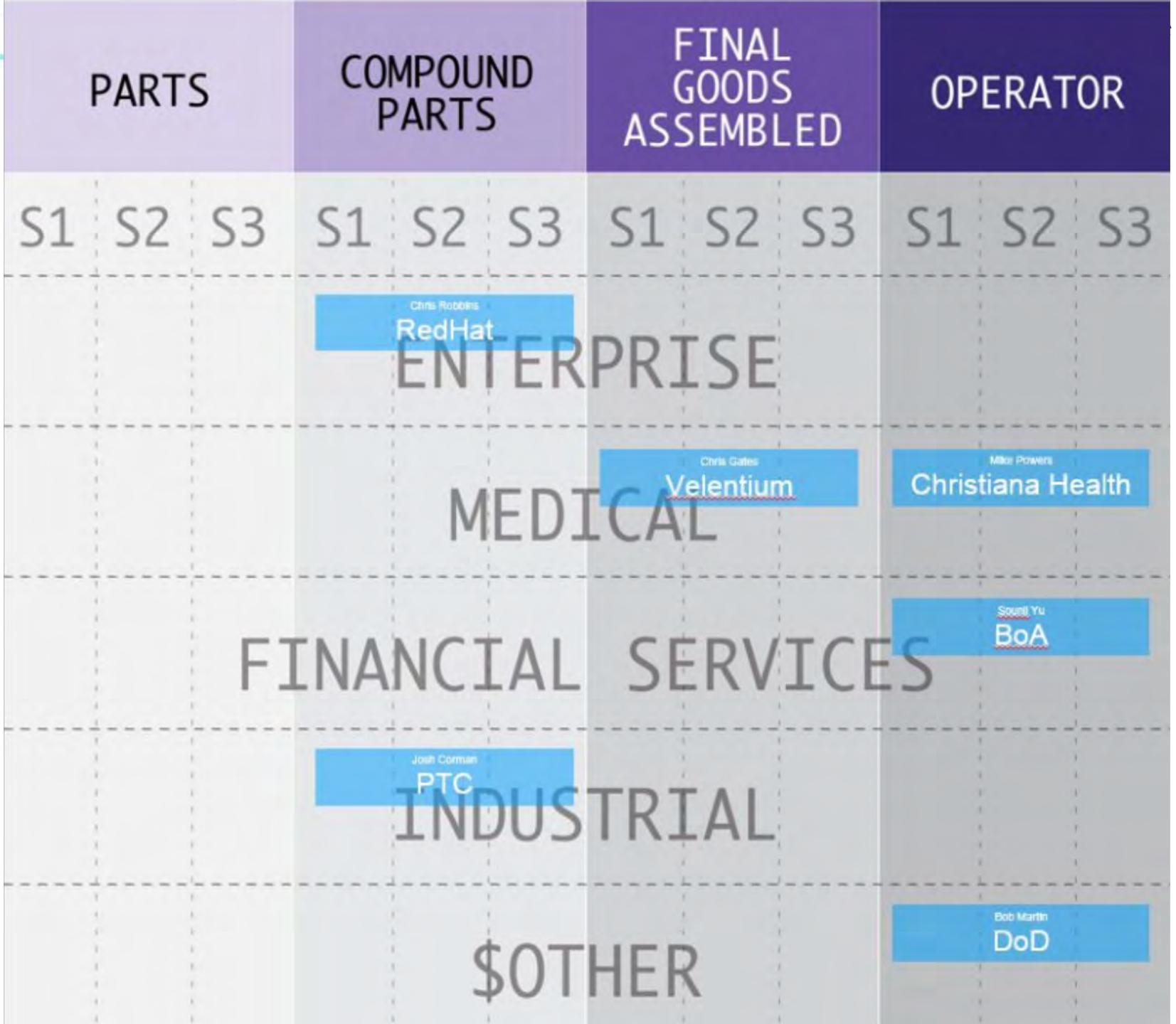


- Supplier selection
- Supply selection
- Supply vigilance

Capturing Stories

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

We would love to have your perspective!

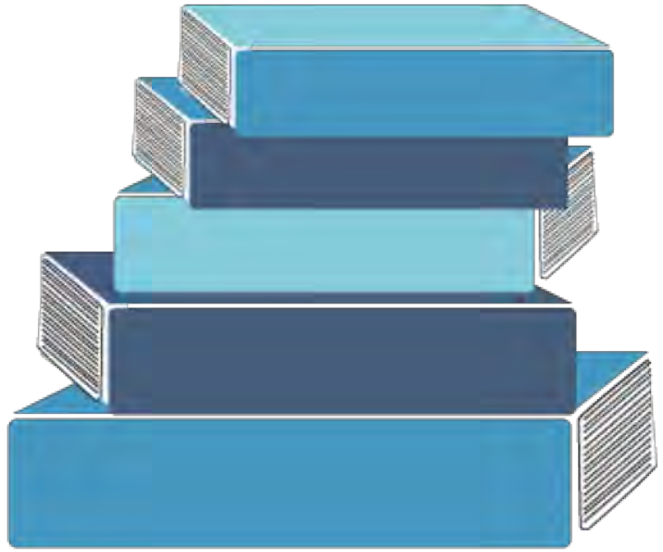


RSAConference2019

HOW DO WE SBOM

Working to understand the existing standards and formats

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.

THE LINUX FOUNDATION

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

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>
...
```

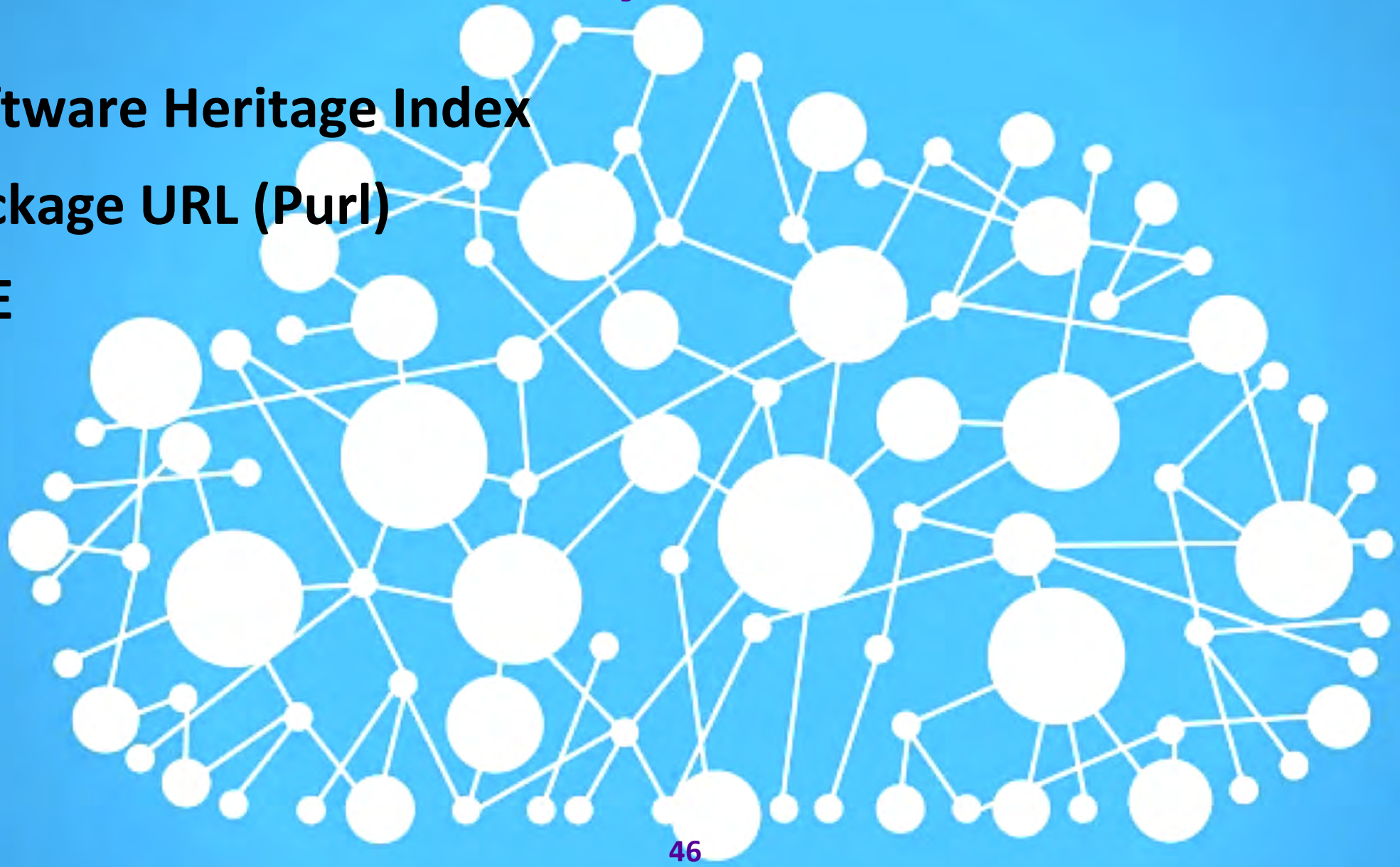
Translation between formats

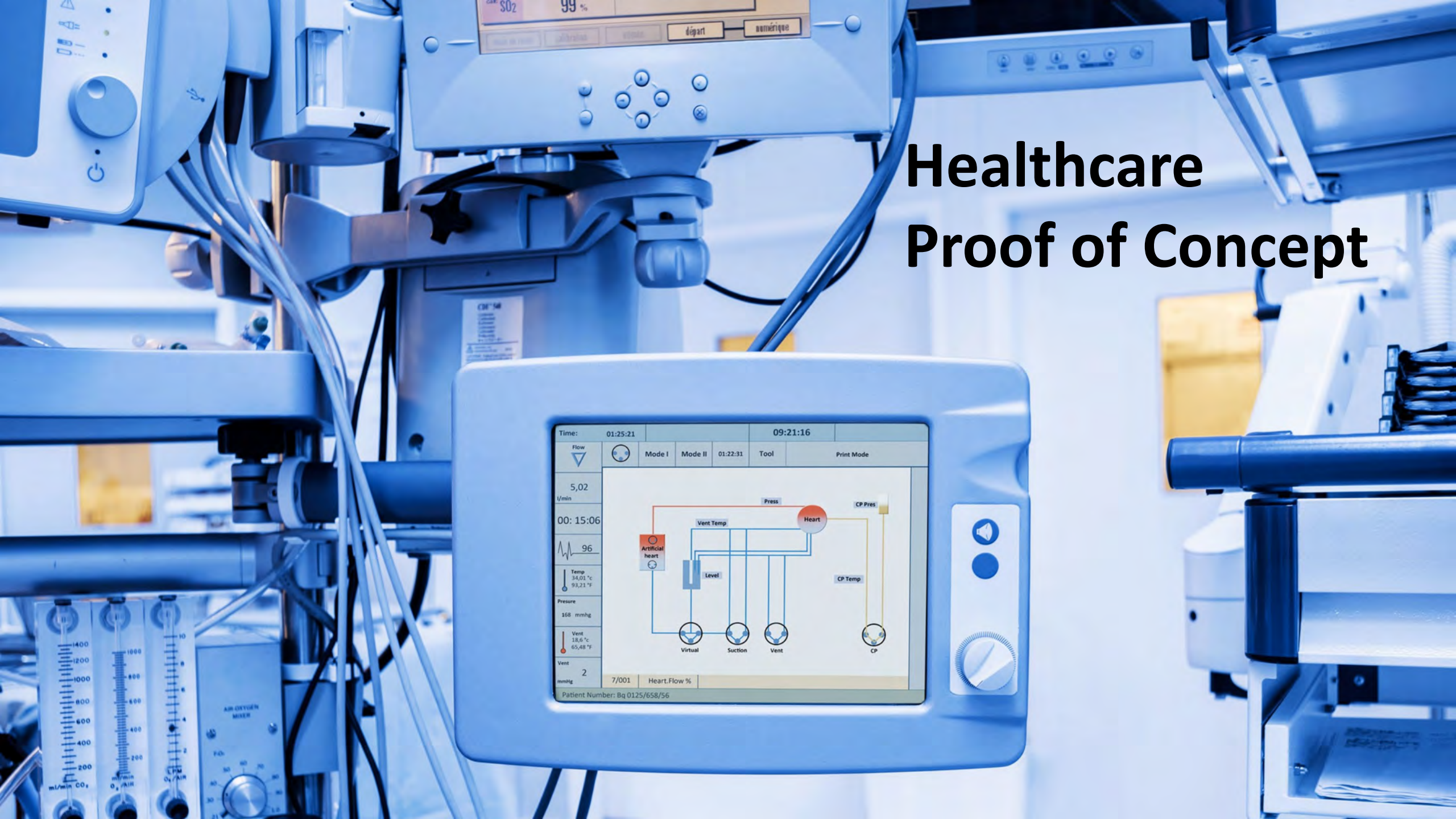
WE HAVE IDENTIFIED THE COMMON ELEMENTS.
A 'BILINGUAL' ECOSYSTEM DOES NOT OFFER TOO MANY CHALLENGES

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

Related efforts in the ecosystem

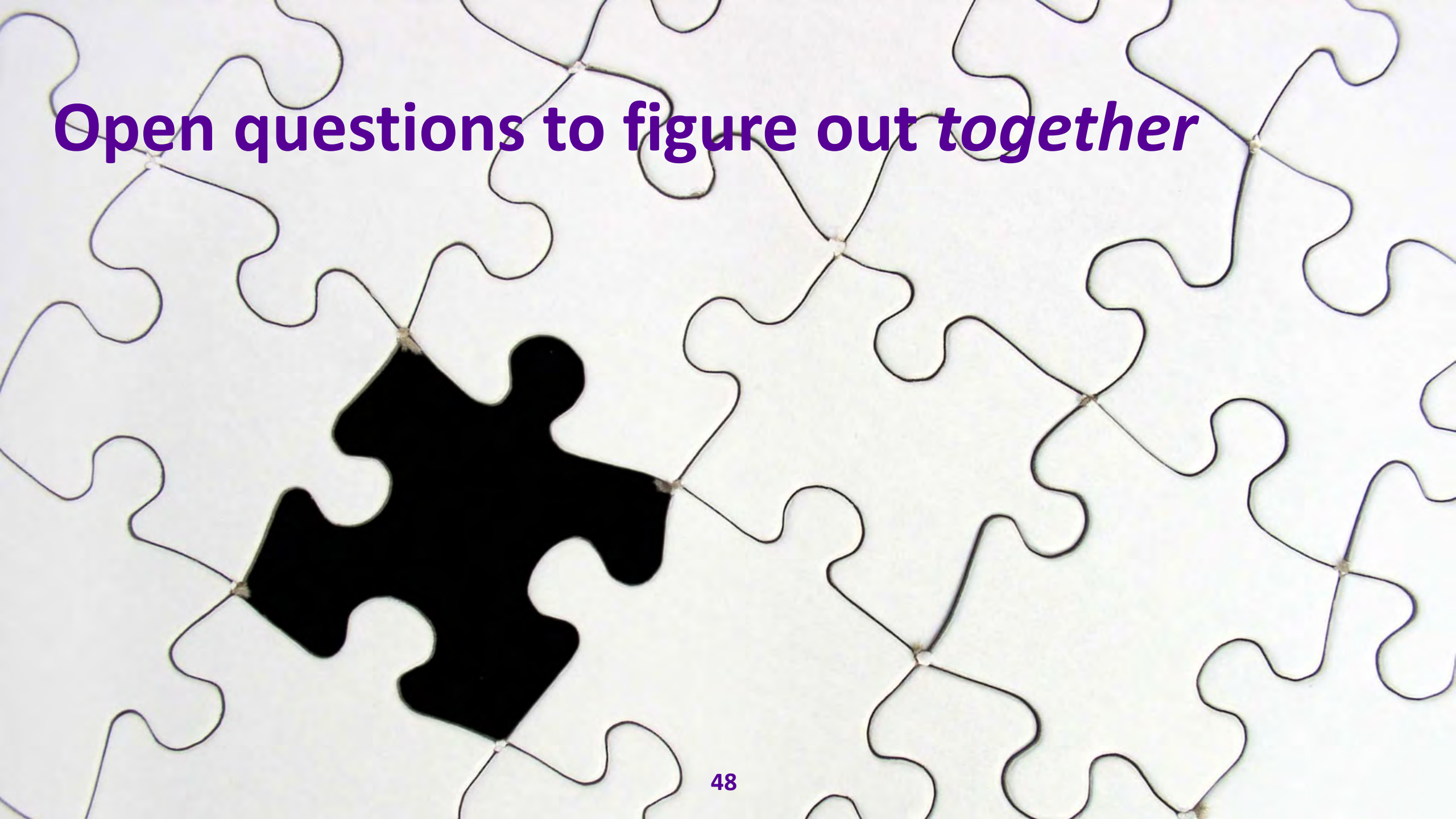
- Software Heritage Index
- Package URL (Purl)
- CPE



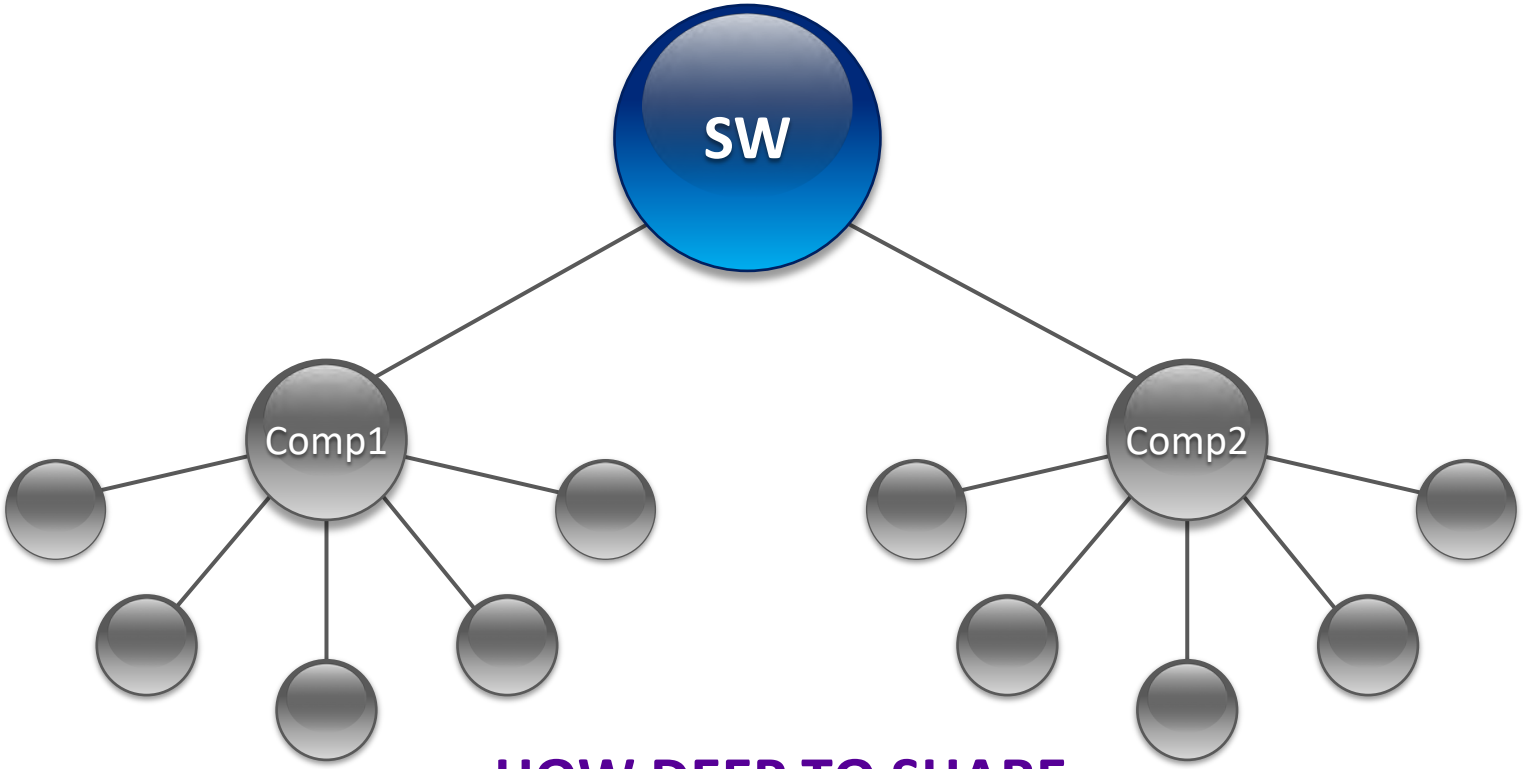


Healthcare Proof of Concept

Open questions to figure out *together*

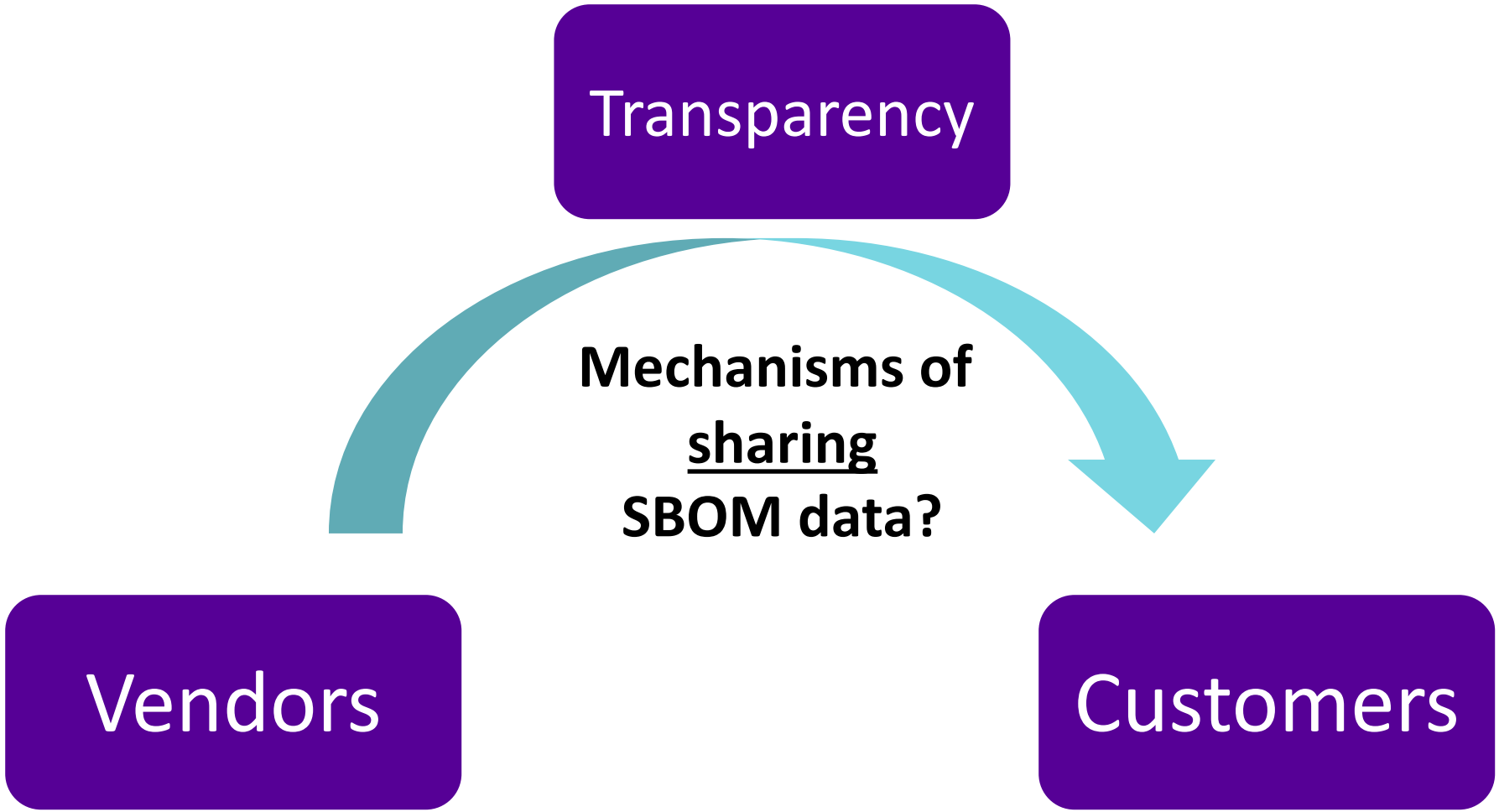


Responsibilities and Exceptions



HOW DEEP TO SHARE
SOURCING SBOM DATA
DEALING WITH INCOMPLETE DATA

Obstacles to obtaining SBOM data?


Transparency
Mechanisms of sharing SBOM data?
Vendors
Customers

Vulnerability vs. Exploitability

To recap…

- Tracking third party components can help understand and address a wide range of risks across the entire ecosystem

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:

phillipmartin.info

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

phillipmartin.info

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

phillipmartin.info

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

phillipmartin.info

Applications: what you can do

Applications: what you can do

- Think - What would this mean for you?
  - How would your organization or sector change if SBOMs were expected or supplied?

Applications: what you can do

- Think - What would this mean for you?
  - How would your organization or sector change if SBOMs were expected or supplied?
- Prepare – Start pushing for change
  - What would it take to track your 3rd party components?
  - What tooling would you need?

Applications: what you can do

- Think - What would this mean for you?
  - How would your organization or sector change if SBOMs were expected or supplied?
- Prepare – Start pushing for change
  - What would it take to track your 3rd party components?
  - What tooling would you need?
- Get involved in the NTIA process!
  - Contact afriedman@ntia.doc.gov