# Ok, SBOMs exist…

# Now what?

**Allan Friedman, PhD**

**National Telecommunications & Information Administration**
**US Department of Commerce**

**afriedman@ntia.gov** **@allanfriedman**

# Ok, SBOMs exist…

# Wait… What's an SBOM?

**Allan Friedman, PhD**

**National Telecommunications & Information Administration**
**US Department of Commerce**

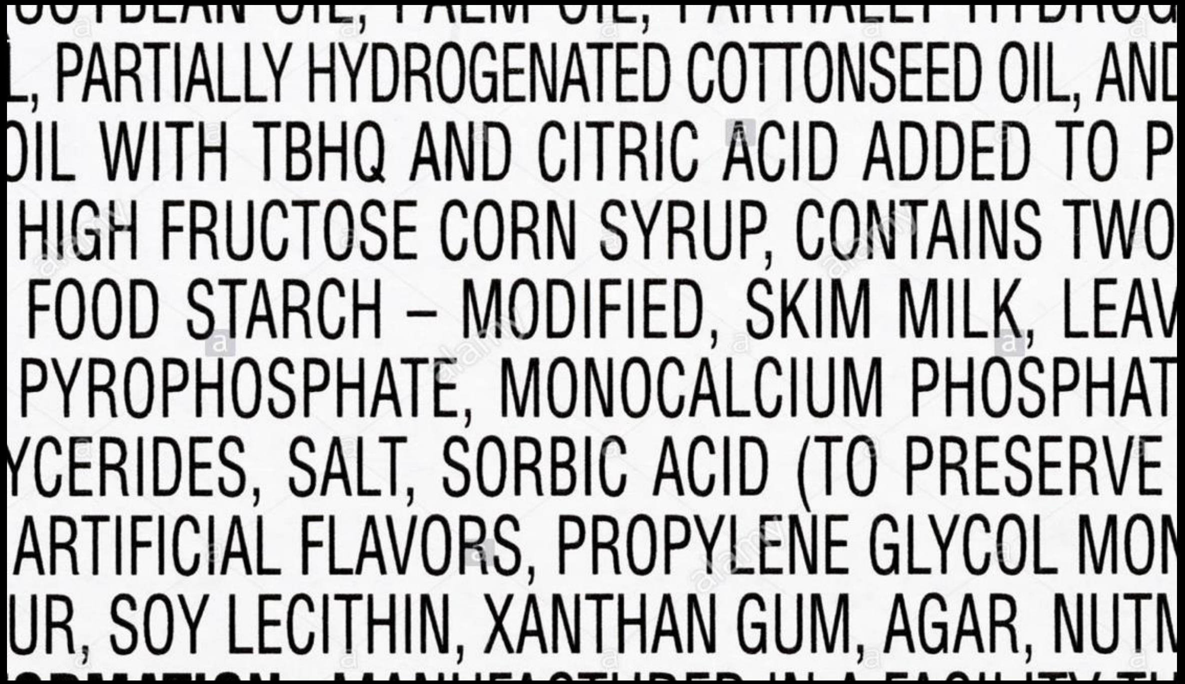
**afriedman@ntia.gov** **@allanfriedman**

How many organizations can answer:

Am I potentially affected by $vulnerabilty

# Transparency can help markets thrive

- Food ingredients and food labels
- Safety Data Sheets in the chemical industry
- Hardware Bills of Material (BOM) in industry



OYBEAN OIL, PALM OIL, PARTIALLY HYDROG

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

ORMATION: MANUFACTURED IN A FACILITY TH

Supplier

Component Name

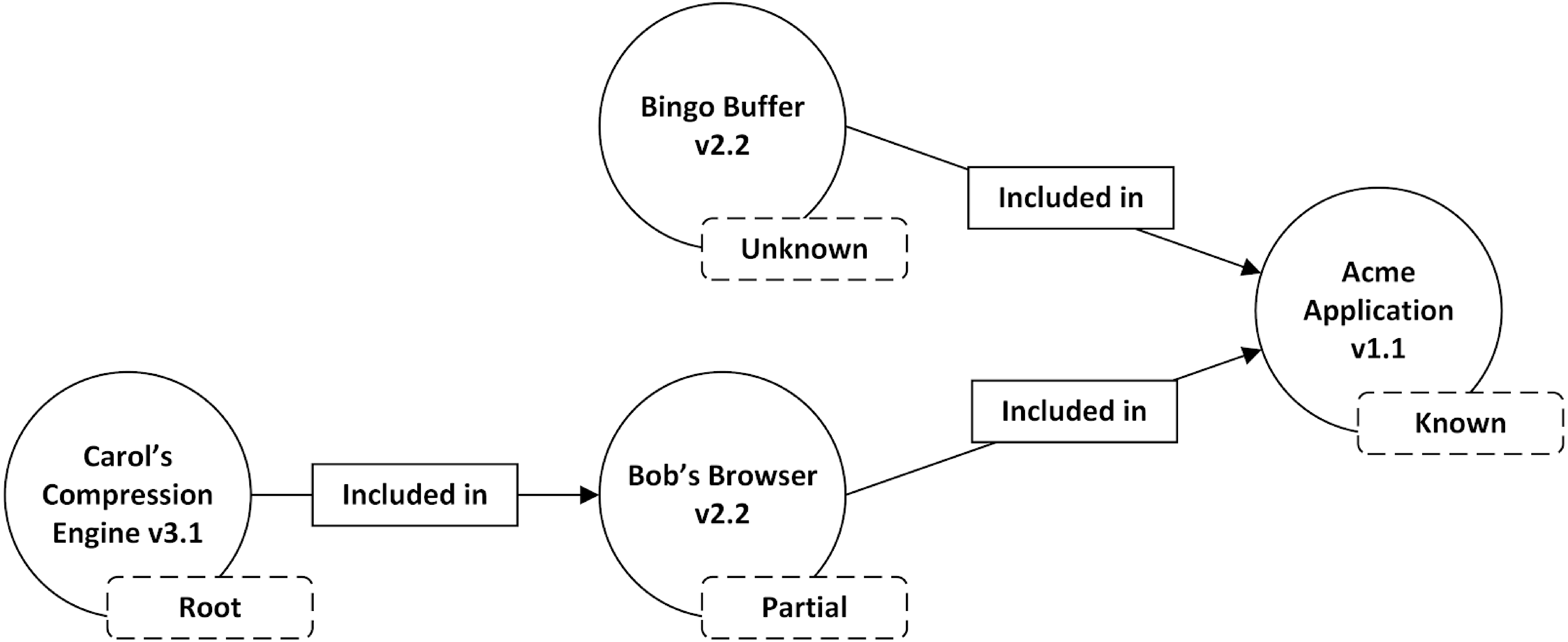
Version

Hash

A Software Component ≈ A Library

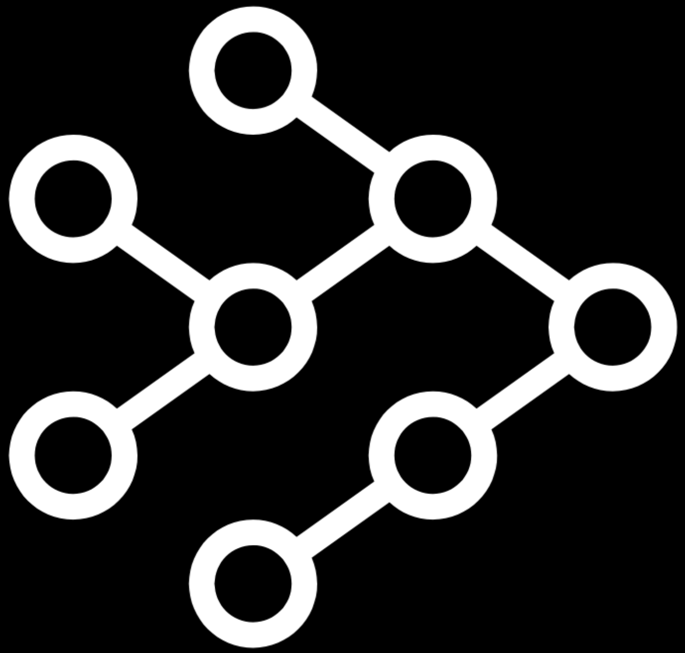
Baseline Identity: *“sufficiently uniquely identify components”*

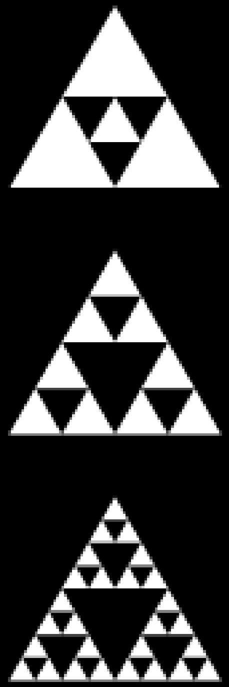
# An Example SBOM



*We want to be clear about known unknowns.*

# How many levels deep?





*Must include all top-level includes, and ideally makes a best-effort for all known components.*

# Software Supply Chain Roles / SBOM Benefits

## Produce Software

Understand component and code dependencies

Monitoring/reviewing for vulnerabilities

Awareness of component EOL, orphan, etc.

Enable black- and whitelists

Less unplanned maintenance work

Transparency for customers

## Choose Software

Identify vulnerable components

Verify sourcing

Compliance with policies

Awareness of component EOL, orphan, etc.

Show best practices by supplier

Know  and comply with licensing

## Operate Software

Easily ID vulnerabilities

Drive independent mitigations

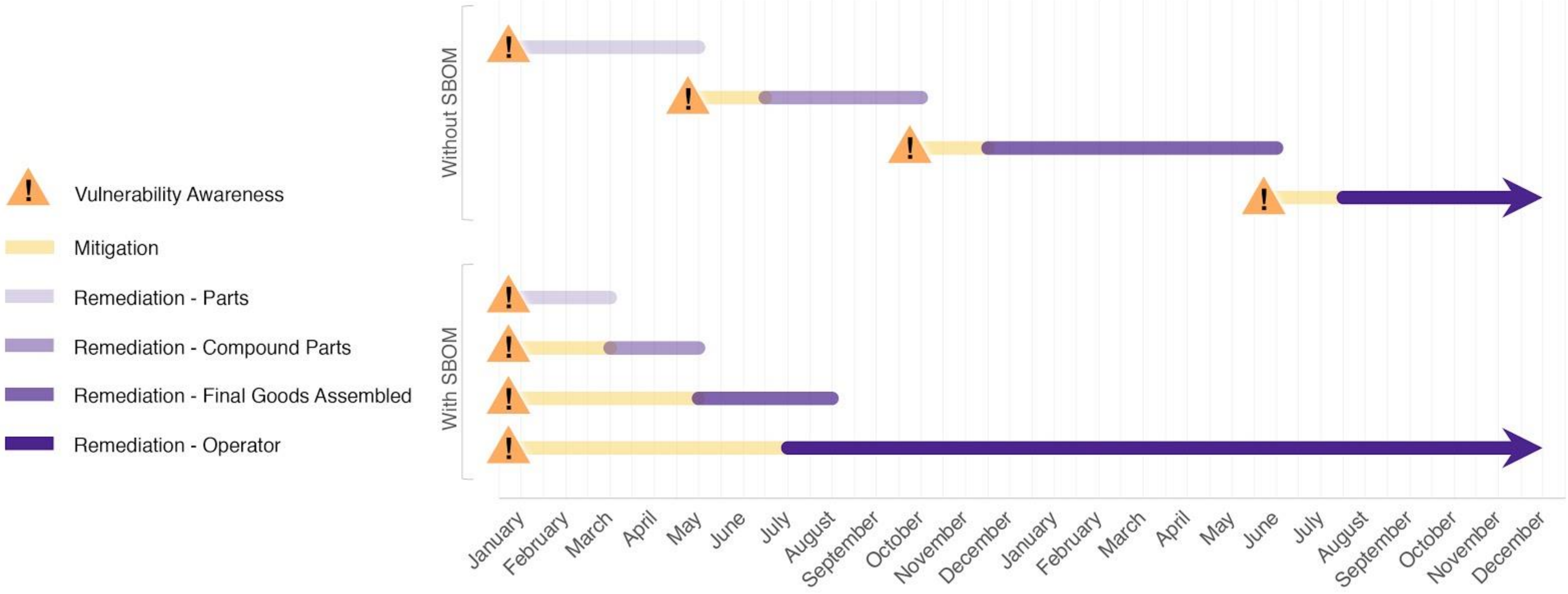
Better risk analysis - “Roadmap for the defender”

Streamline administration

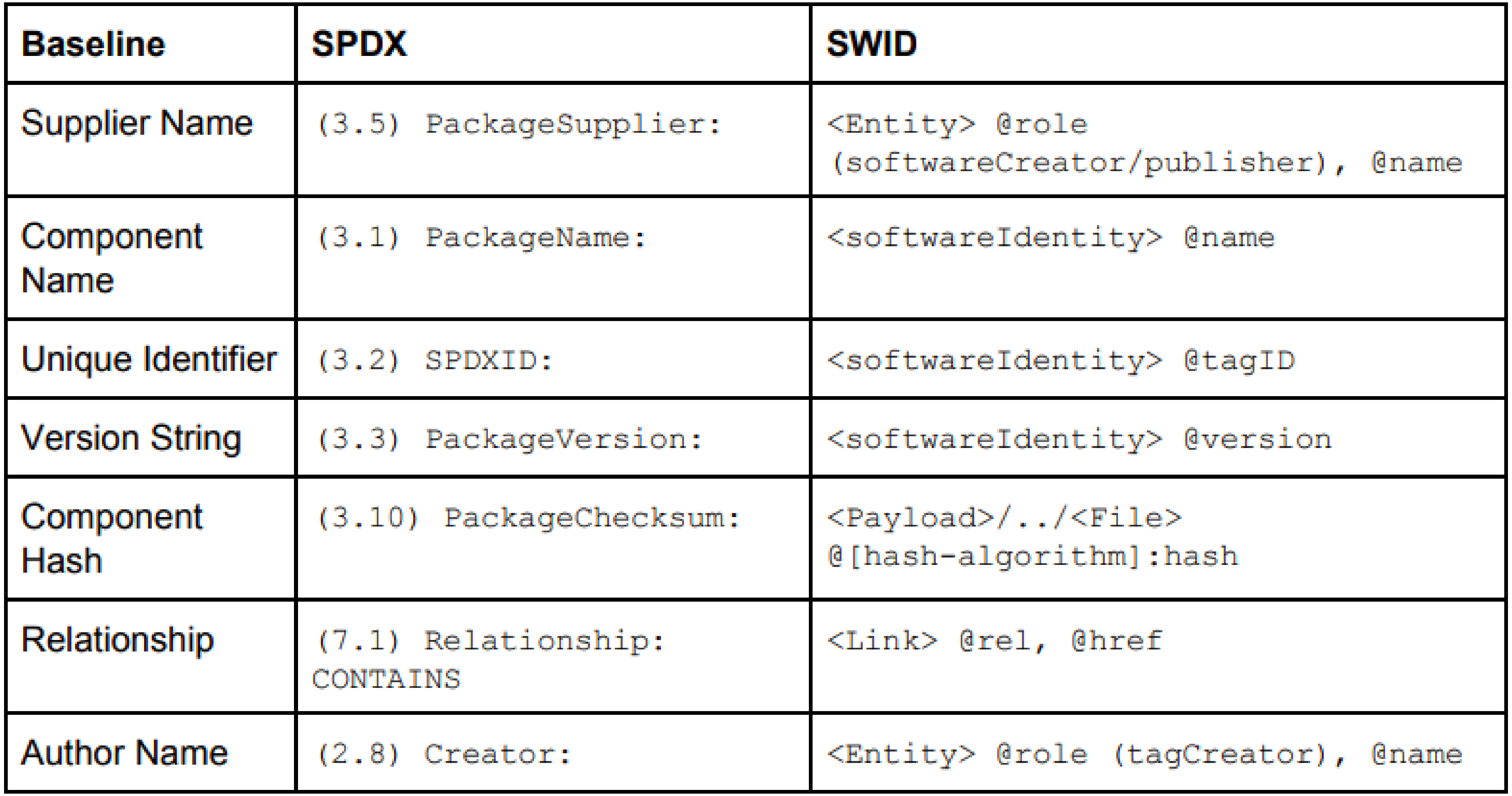
Awareness of component EOL, orphan, etc.

# Time to Remediation Case Studies

## Without and With SBOM



# Existing Standards to Convey SBOM data



| Baseline | SPDX | SWID |
|---|---|---|
| Supplier Name | `(3.5) PackageSupplier:` | `<Entity> @role (softwareCreator/publisher), @name` |
| Component Name | `(3.1) PackageName:` | `<softwareIdentity> @name` |
| Unique Identifier | `(3.2) SPDXID:` | `<softwareIdentity> @tagID` |
| Version String | `(3.3) PackageVersion:` | `<softwareIdentity> @version` |
| Component Hash | `(3.10) PackageChecksum:` | `<Payload>/../<File> @[hash-algorithm]:hash` |
| Relationship | `(7.1) Relationship: CONTAINS` | `<Link> @rel, @href` |
| Author Name | `(2.8) Creator:` | `<Entity> @role (tagCreator), @name` |

# Progress in a cross-sector industry-led process

- Clear appreciation across sectors on the potential value of transparency
- Consensus on
  - The broad scope of the problem
  - Focus on a baseline SBOM
  - “rough consensus and running code”
  - Machine-readability of the solution
- Resources: ntia.gov/SBOM

✓ What is an SBOM

✓ Why should we SBOM

✓ How do we SBOM

✓ Can we SBOM today?

# Ok, SBOMs exist…

# Now what?

Allan Friedman, NTIA

David Foose, Ovation/Emerson

Kaleem Khawaja, BP

# Next steps on SBOM– Easier and Cheaper

- Refining and extending the model
  - Mechanism for sharing SBOM data
  - High assurance: integrity, pedigree, provenance
  - Cloud & containers
- Tooling for automation
  - What tools exist today?
  - What tools do we need?
- Awareness and adoption
  - Draft contract language
  - Further demonstrations in different sectors
- *Get involved*
  - *afriedman@ntia.gov* *@allanfriedman* *ntia.gov/SBOM*