What's in my Software?
Introducing a Software Bill of Materials Specification

Robert Martin
MITRE

Allan Friedman
NTIA
US Dept of Commerce

How many organizations can answer:

Am I potentially affected by $vulnerabilty

URGENT/1

Should I pay attention or look at literally anything else on the Internet?

- Transparency helps markets across the supply chain
- Progress towards SBOM and transparency
  - The what, the why, and the how
- Introducing a new SBOM specification
- How you can get involved
  - Join this international, cross-sector community
  - SBOM – ask for it by name!

INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, "B" VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LECITHIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEAROYL LACTYLATE, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40. 518701

CONTAINS WHEAT, EGG, MILK AND SOY

212016_MP

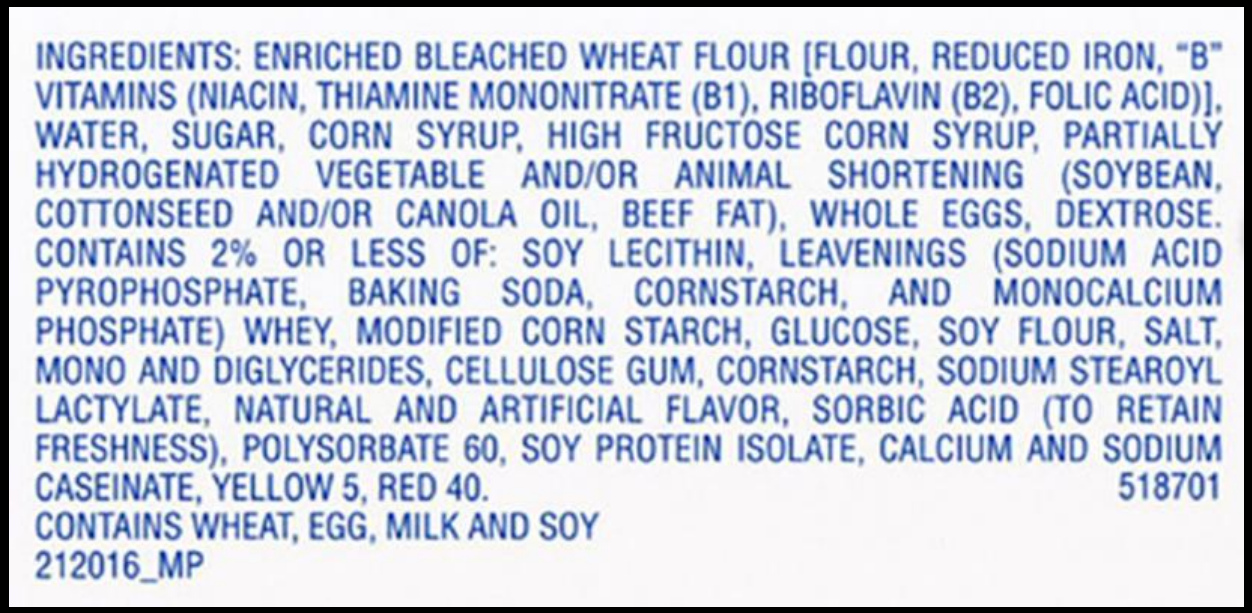
OUR [FLOUR, REDUCED IRON, "B"
1), RIBOFLAVIN (B2), FOLIC ACID)],
TOSE CORN SYRUP, PARTIALLY
MAL SHORTENING (SOYBEAN,
AT), WHOLE EGGS, DEXTROSE.
N, LEAVENINGS (SODIUM ACID
STARCH, AND MONOCALCIUM
H, GLUCOSE, SOY FLOUR, SALT,
CORNSTARCH, SODIUM STEAROYL
VOR, SORBIC ACID (TO RETAIN
FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM
CASEINATE, YELLOW 5, RED 40.
CONTAINS WHEAT, EGG, MILK AND SOY
212016_MP

518701

INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, "B" VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LECITHIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEAROYL LACTYLATE, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40. 518701
CONTAINS WHEAT, EGG, MILK AND SOY
212016_MP

URGENT/11

What is the software equivalent?



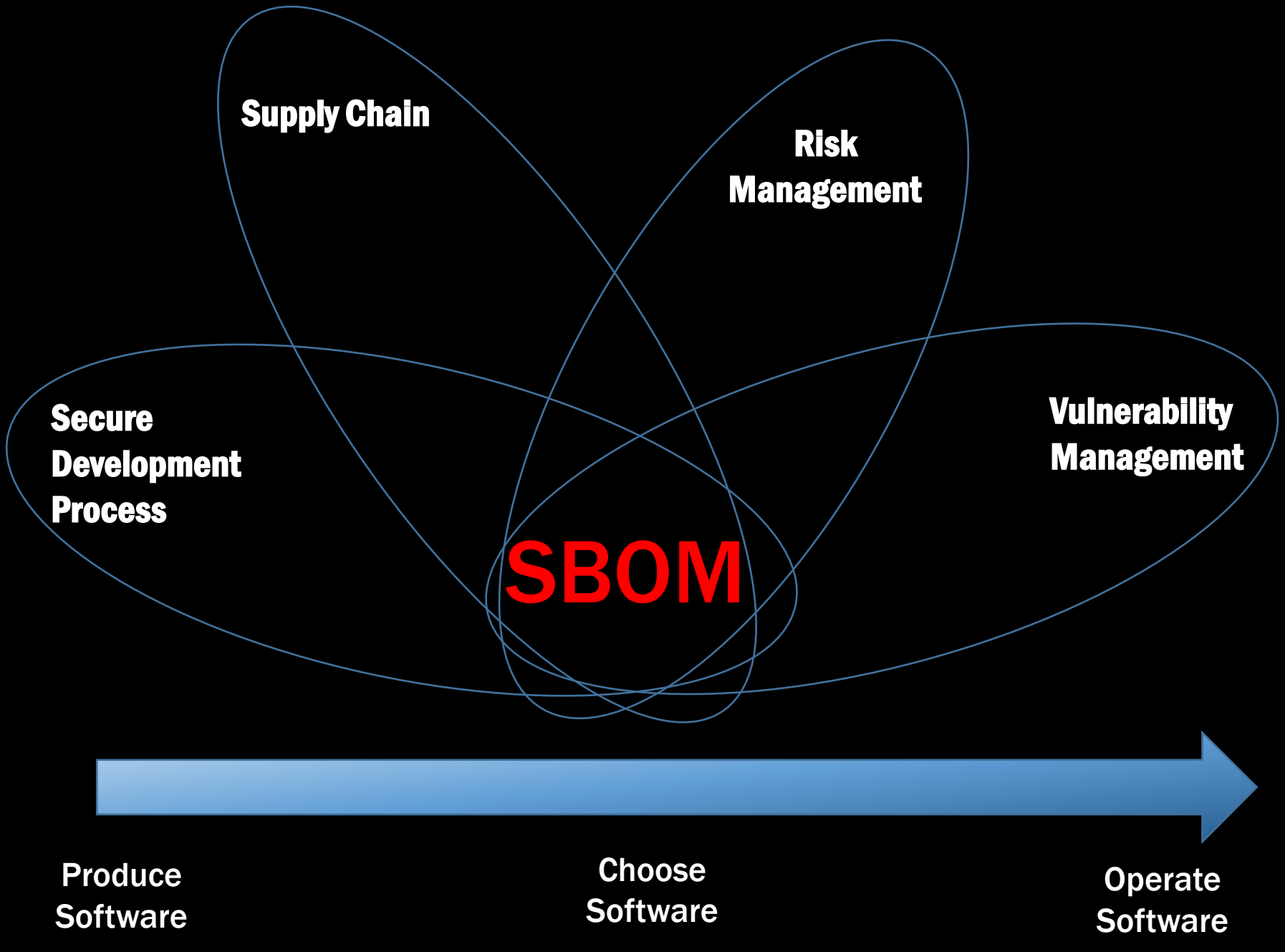
INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, "B" VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LECITHIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEAROYL LACTYLATE, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40. 518701
CONTAINS WHEAT, EGG, MILK AND SOY
212016_MP

Software Bill of Materials

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software

An SBOM is effectively a nested inventory: a list of ingredients that make up software components.

An SBOM identifies and lists software components, information about those components, and the relationships between them


Supply Chain
Risk Management
Secure Development Process
Vulnerability Management
SBOM
Produce Software
Choose Software
Operate Software

How are we going to do this?

NTIA's Process on Software Component Transparency

Cross sector

Healthcare

Energy

Auto

ICT

Finance

Government

Entire Supply chain

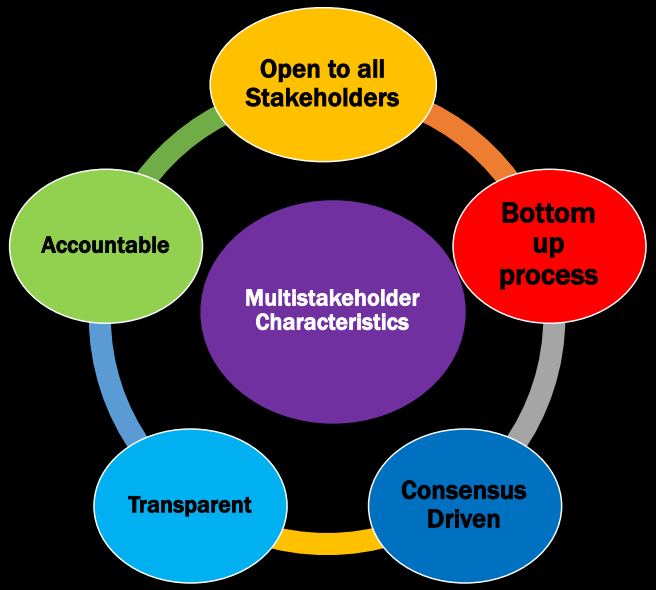
Open source

Middleware

Commercial SW

Embedded

Customers



NTIA's open, transparent, consensus-based processes bring together diverse stakeholders can catalyze real progress across the ecosystem.

What the NTIA process is not doing

- Regulation
- Source code disclosure
- Standards Development
- Solving all supply chain issues

Making progress

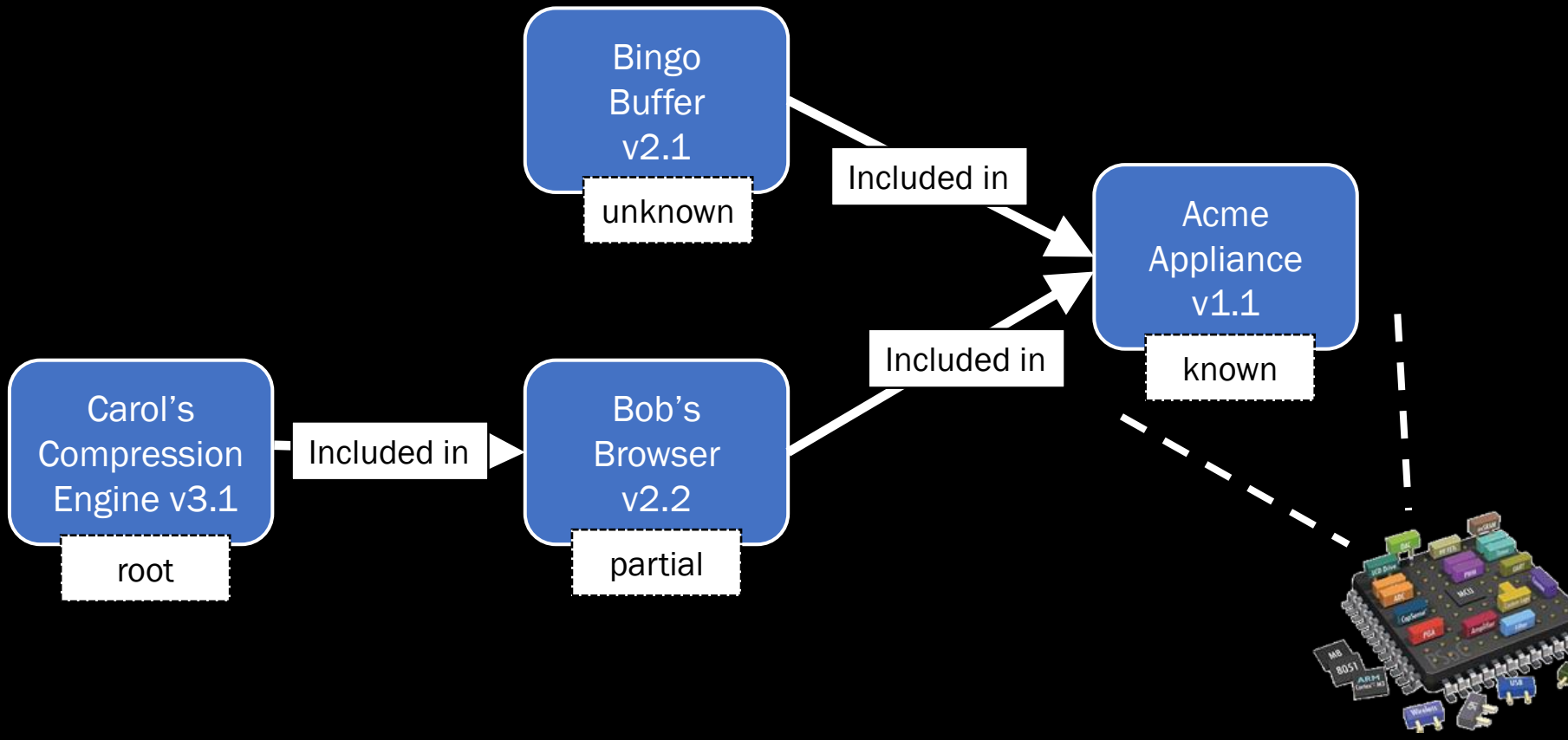
- Clear appreciation across sectors on the potential value of transparency
- Consensus on
  - The broad scope of the problem
  - Focus on a baseline SBOM
  - Machine-readability of the solution
  - Modularity and Scalability
- Resources: ntia.gov/SBOM

✓ What is an SBOM
✓ Why should we SBOM
✓ How do we SBOM
✓ Can we SBOM today?

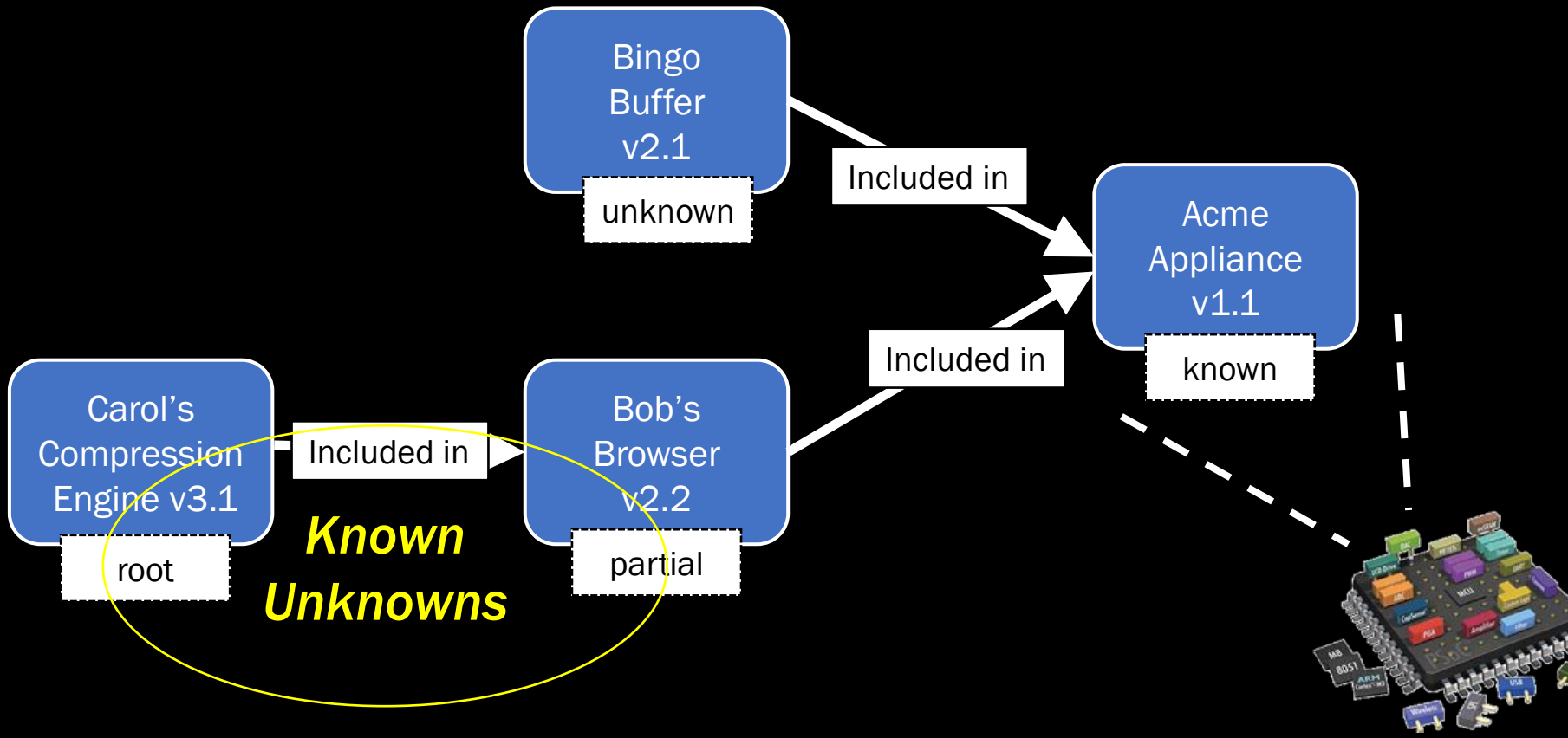
Current work: focus on deployment and SBOMs in the real world

What is an SBoM?

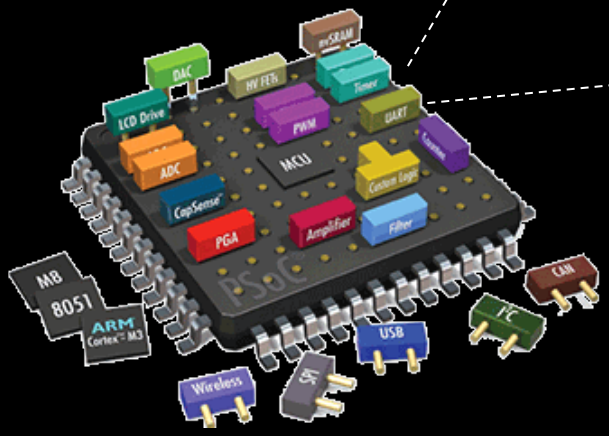
A toy example

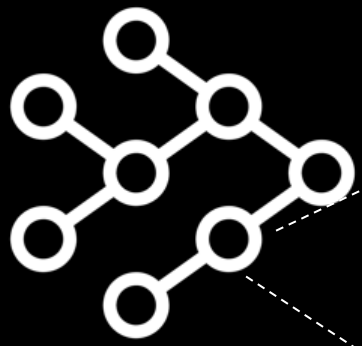


A toy example



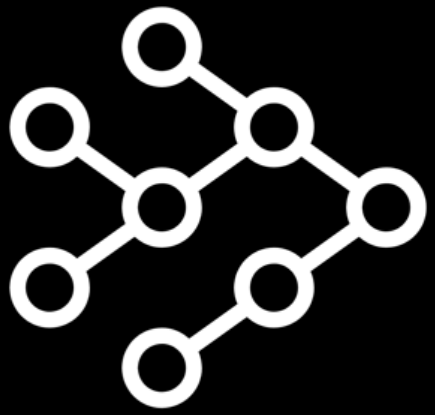
Software Components





Supplier
Component
Version
Hash

How many levels deep?



<u>Must</u> include all top-level includes.
<u>Should</u> ask for includes' SBOMs.
<u>Ideally</u> makes a best-effort for all known components.

Why should we SBoM?

SBOM Roles and Benefits

Produce Software

Understand component and code dependencies

Monitoring/reviewing for vulnerabilities

Awareness of component EOL, orphan, etc.

Enable allow- and deny-lists

Less unplanned maintenance work

Transparency for customers

Choose Software

Identify vulnerable components

Compliance with policies

Awareness of component EOL, orphan, etc.

Show best practices by supplier

Know and comply with licensing

Operate Software

Easily ID vulnerabilities

Better risk analysis - “Roadmap for the defender”

Streamline administration

Drive independent mitigations

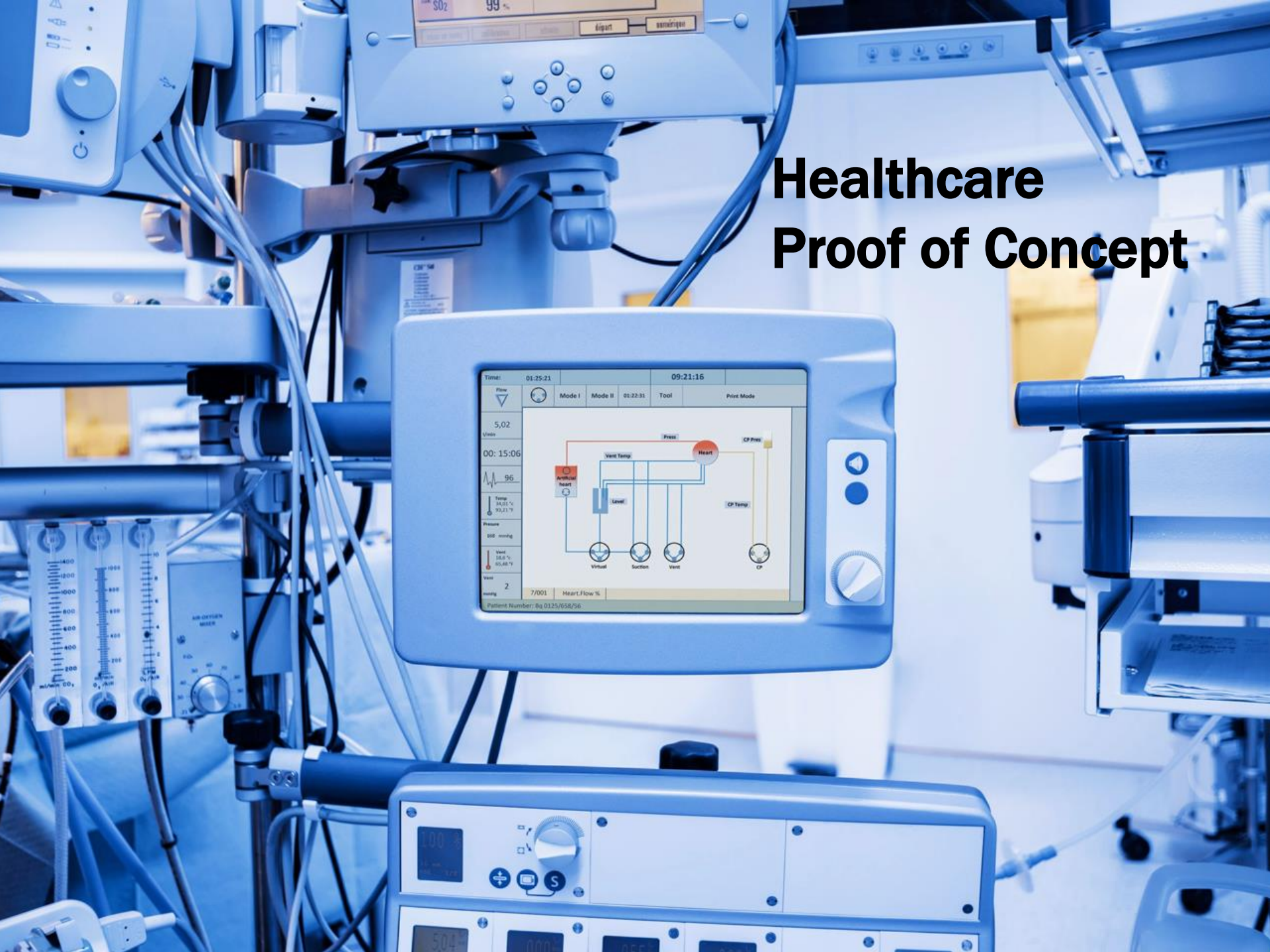
How should we SBoM?

Translation between formats

- We have identified the common elements.
- A ‘multilingual’ ecosystem does not offer too many challenges
- Rather than pick a winner, focus on guidance to support <u>all</u> relevant, active, and approved formats with effective interoperability.

Implementing core SBOM fields

Field	SPDX	SWID	CycloneDX
Supplier	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/ publisher), @name	publisher
Component	(3.1) PackageName:	<softwareIdentity> @name	name
Unique Identifier	(3.2) SPDXID:	<softwareIdentity> @tagID	bom/serialNumber and component/bom-ref
Version	(3.3) PackageVersion:	<softwareIdentity> @version	version
Component Hash	(3.10) PackageChecksum:	<Payload>/../<File> @[hash-algorithm]:hash	hash
Relationship	(7.1) Relationship: CONTAINS	<Link>@rel, @href	(Nested assembly/subassembly and/or dependency graphs)
SBOM Author	(2.8) Creator:	<Entity> @role (tagCreator), @name	bom-descriptor: metadata/manufacture/contact


Healthcare
Proof of Concept

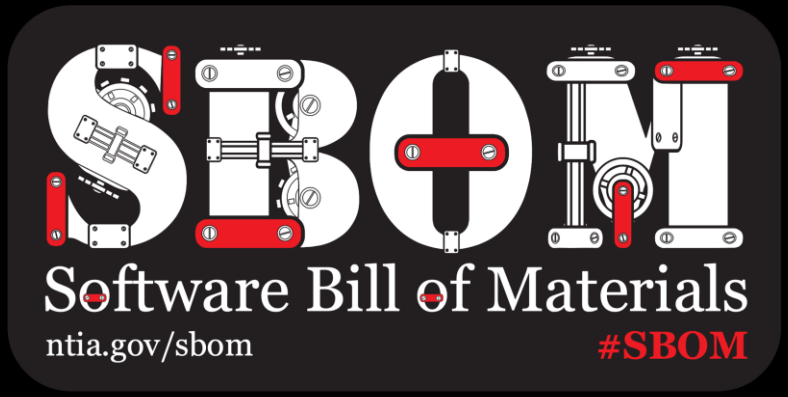
A new SBOM standard!

What's coming next from the SBOM community

- Refining and extending the SBOM approach
  - Software namespace
  - Mechanisms for sharing SBOM data
  - Vulnerability vs Exploitability
  - High assurance: integrity, pedigree, provenance
  - Cloud & containers
  - Dock with other efforts around supply chain
- Tooling for automation
  - What tools exist today?
  - What tools do we need?
- Awareness and adoption
  - Get the message to the community
  - Draft contract language
  - Further demonstrations in different sectors
- Playbooks and how-to guides

To recap...

- Tracking third party components can help understand and address a wide range of risks across the entire ecosystem
- Cross-sector supply-chain driven approach
  - What a Software Bill of Materials is
  - Why it can help across the supply chain
  - How we can implement it
- Sectors and orgs can shape their own future through Proof-of-Concept exercises
- New standards emerging for even more power and options
- Ongoing work needs your help to build and use SBOM data



Get involved in the NTIA process!

Contact: afriedman@ntia.gov
Read: ntia.gov/SBOM

Join the conversation
@allanfriedman #SBOM