

June 14, 2023

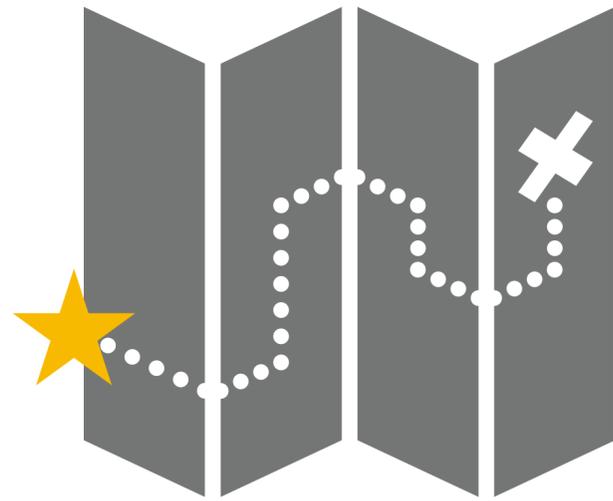
ONRAMPS & ADOPTION

Community Working Groups (CISA Phase)

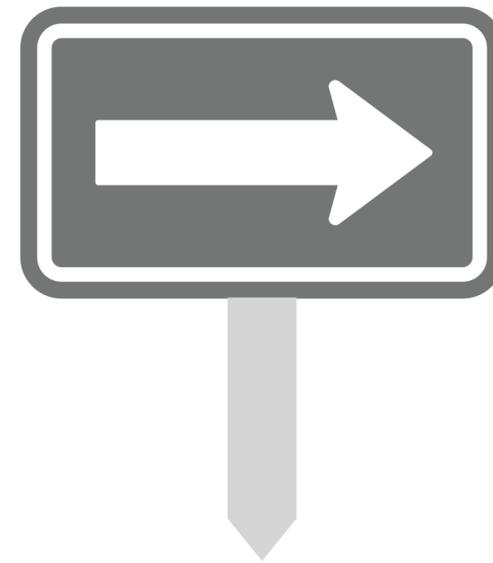
Audra Hatch, Joshua Corman



ONRAMPS & ADOPTION – MISSION / VISION / GOALS



Starting Point



Sign Posts



Identify & Bridge Gaps



EMPATHY & IMPEDANCE MISMATCH

BIDIRECTIONAL MINDFULNESS & EMPATHY





PAST

SBOM (AND BEYOND)

Ingredients

- Inventory
- Parts
- Lists
- 1..n Suppliers
- BoM (Bill of Materials)

Known Vulnerabilities

- CVEs ++
- *Potentially* exploitable
- Not “Attack Surface”

Exploitable Vulnerabilities

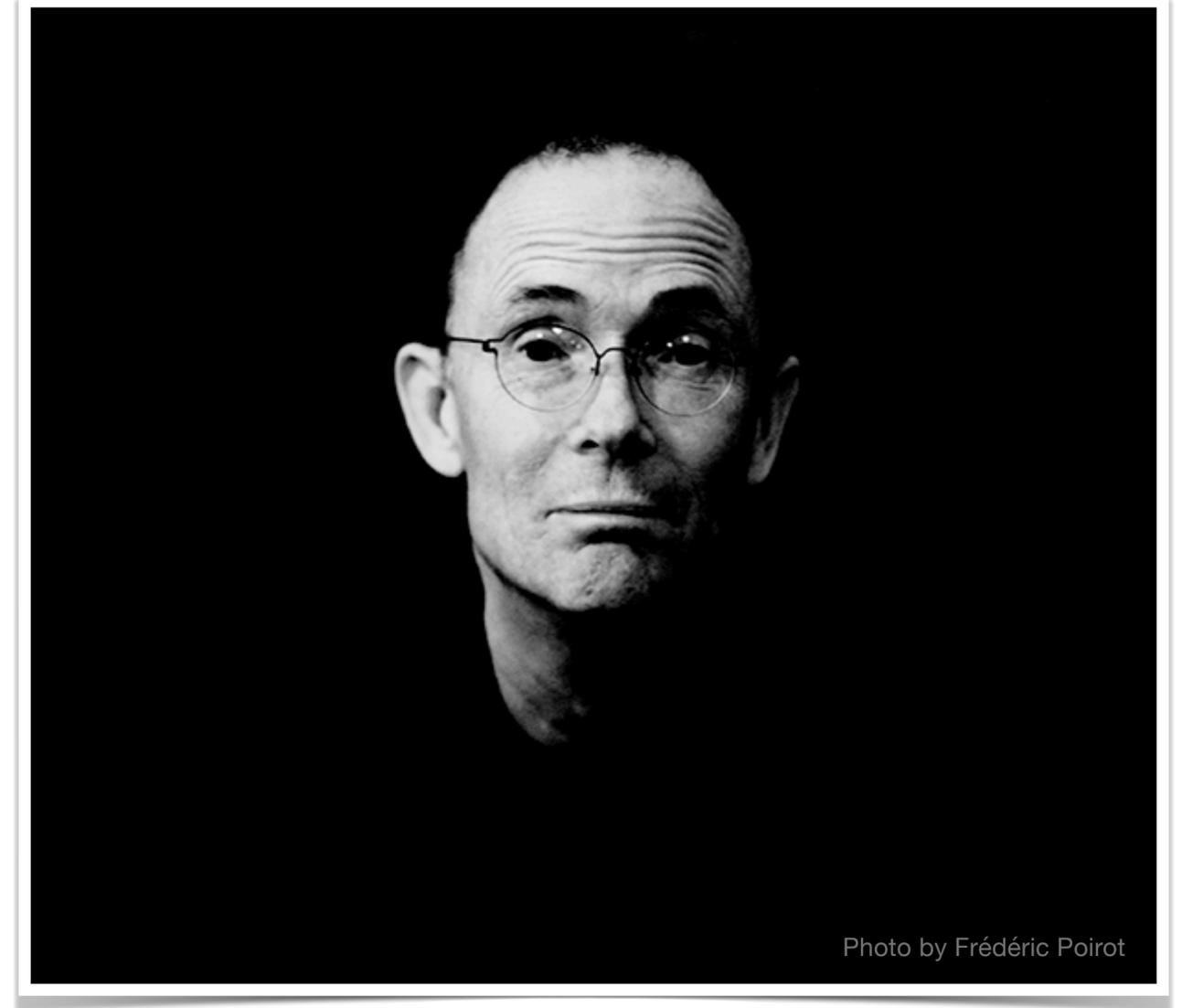
- Attack Surface
- Code Flow
- Other mitigations

- Direct Exploitation
- Chained attacks
- Deserialization

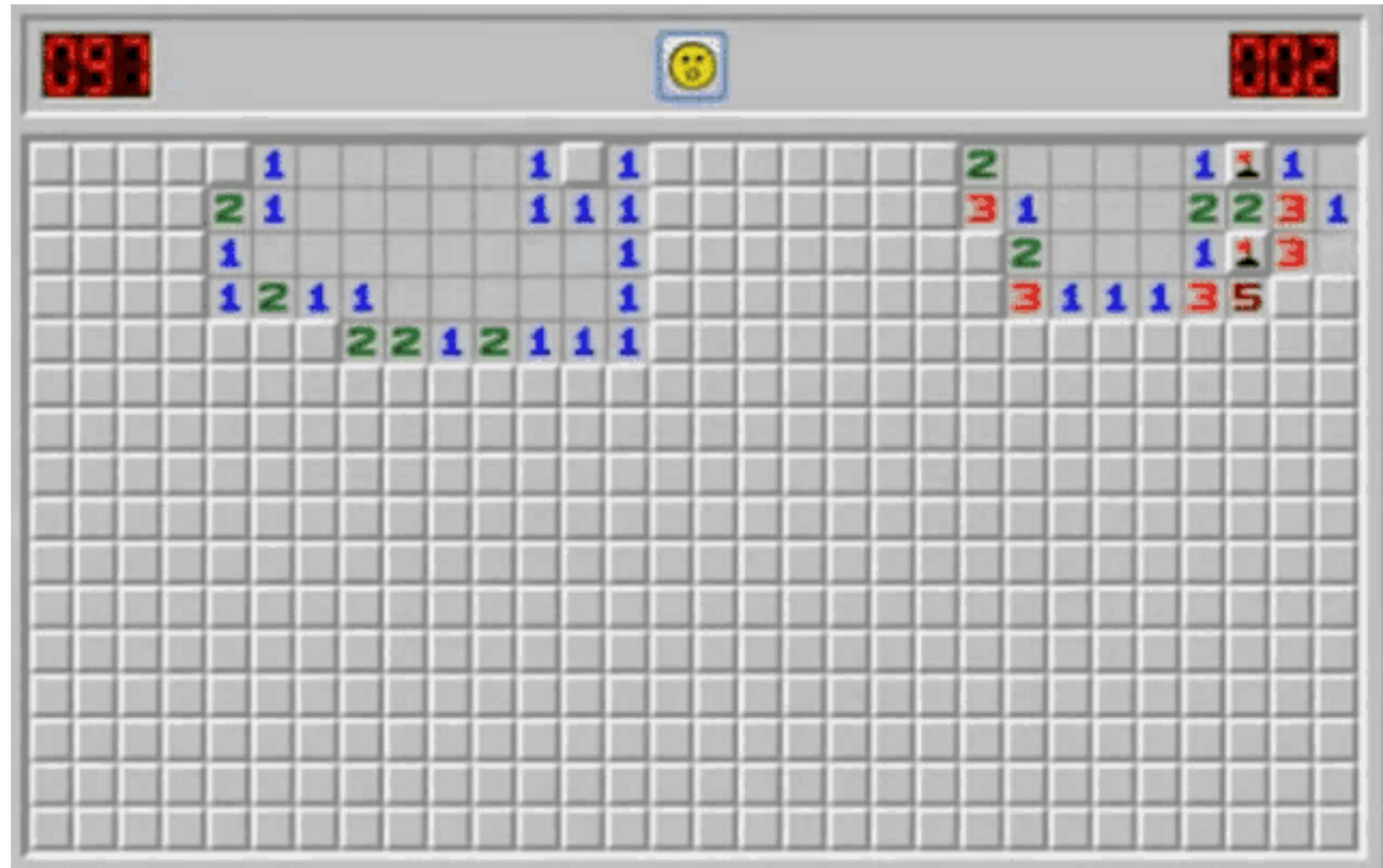
SBOM IS HERE

*“The future is already here —
it’s just not very evenly
distributed.”*

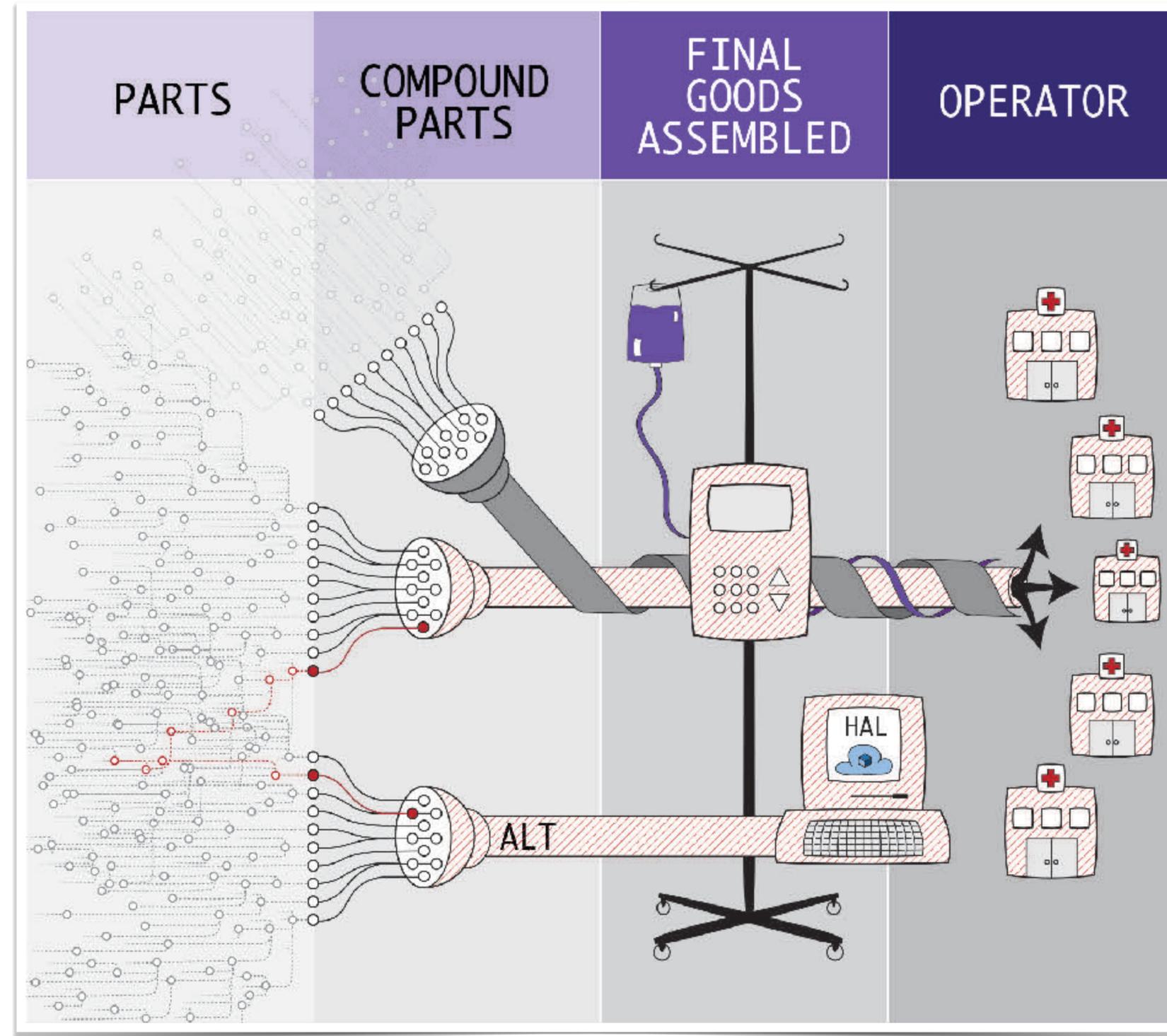
– William Gibson



BOMBS & VISIBILITY



WE'RE ALL IN A SUPPLY CHAIN – MOST OF US ARE IN THE MIDDLE







Produce

The person or organization that creates a software component or software for use by others

[write/create/assemble/package]



Produce

The person or organization that creates a software component or software for use by others

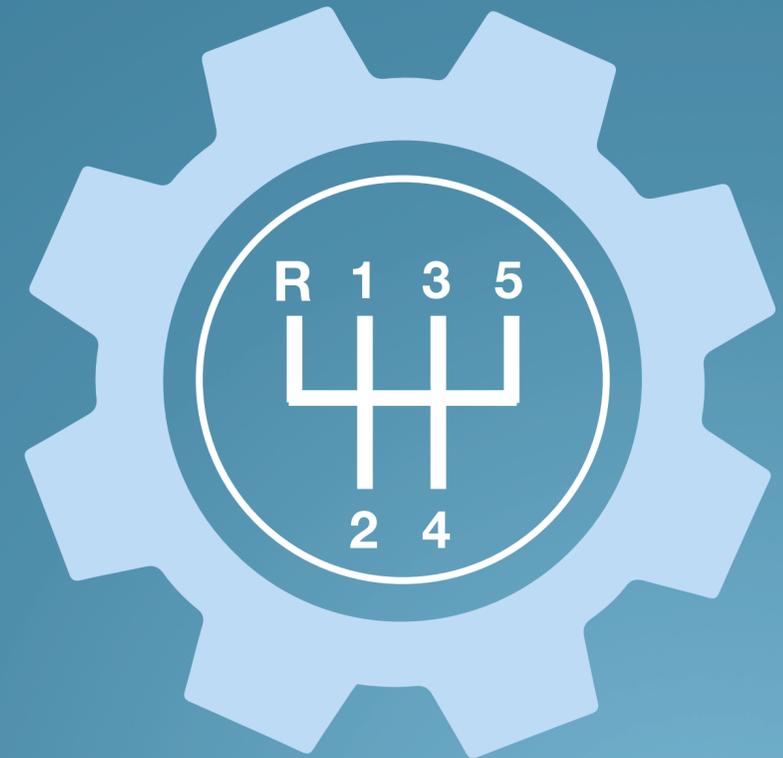
[write/create/assemble/package]



Choose

The person or organization that decides the software, products, and/or suppliers for use

[purchase/acquire/source/select/approve]





Produce

The person or organization that creates a software component or software for use by others

[write/create/assemble/package]



Choose

The person or organization that decides the software, products, and/or suppliers for use

[purchase/acquire/source/select/approve]



Operate

The person or organization that operates the software component or software

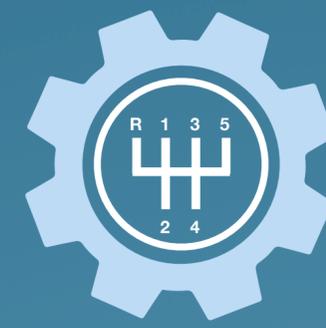
[uses/monitor/maintain/defend/respond]



Produce



Choose



Operate

Benefits



Cost



Security Risk



License Risk



Compliance Risk



High Assurance

Less unplanned, unscheduled work	A more accurate total cost of ownership	More efficient administration
Avoid known vulnerabilities	Easier due diligence	Faster identification and resolution. Know if and where specific software is affected.
Quantify and manage licenses and associated risk	Easier due diligence	More efficient, accurate response to license claims
Easier risk evaluation. Identify compliance requirements earlier in lifecycle	More accurate due diligence, catch issues earlier in lifecycle	Streamlined process
Make assertions about artifacts, sources, and processes used	Make informed, attack-resistant choices about components	Validate claims under changing and adversarial conditions

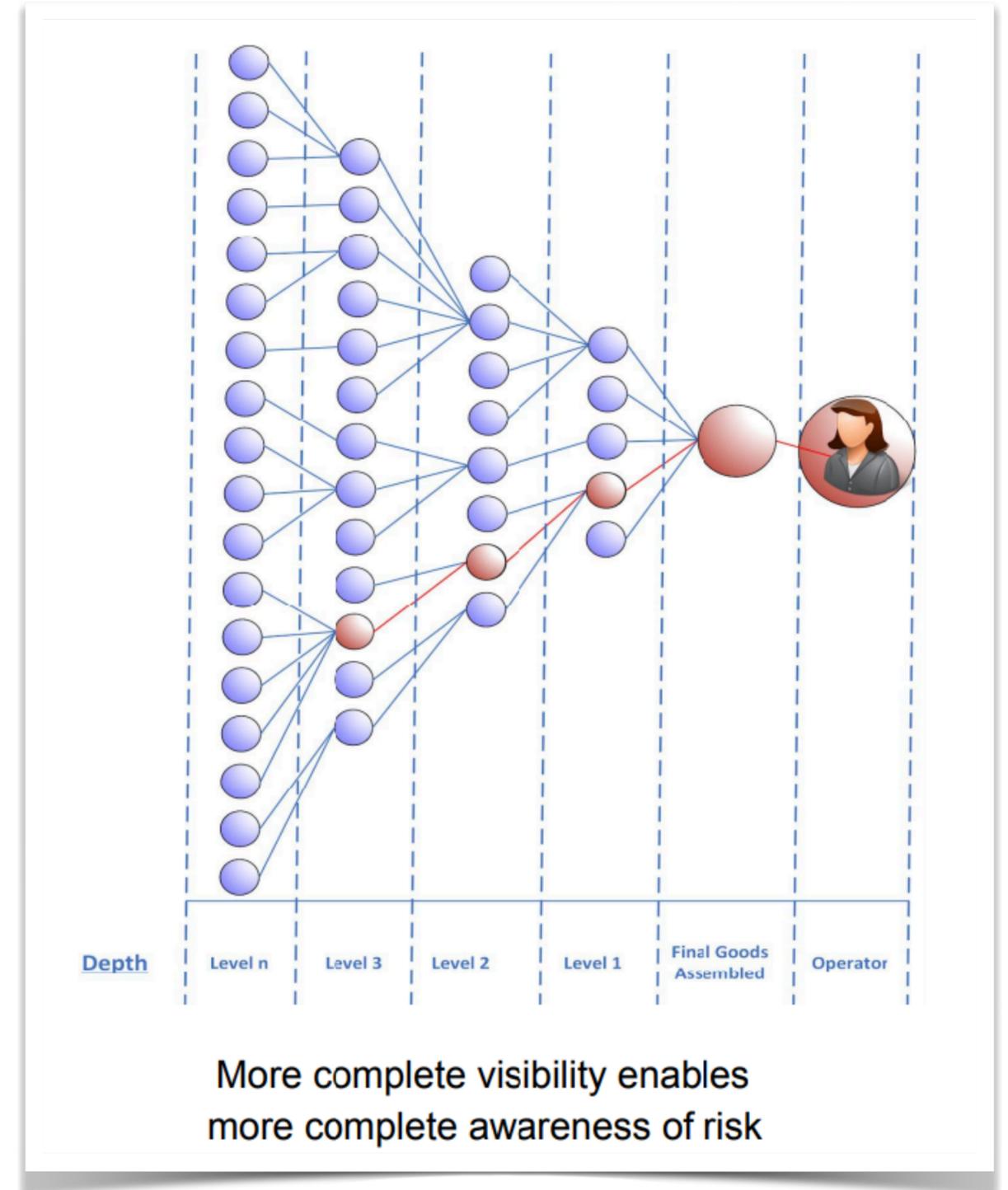
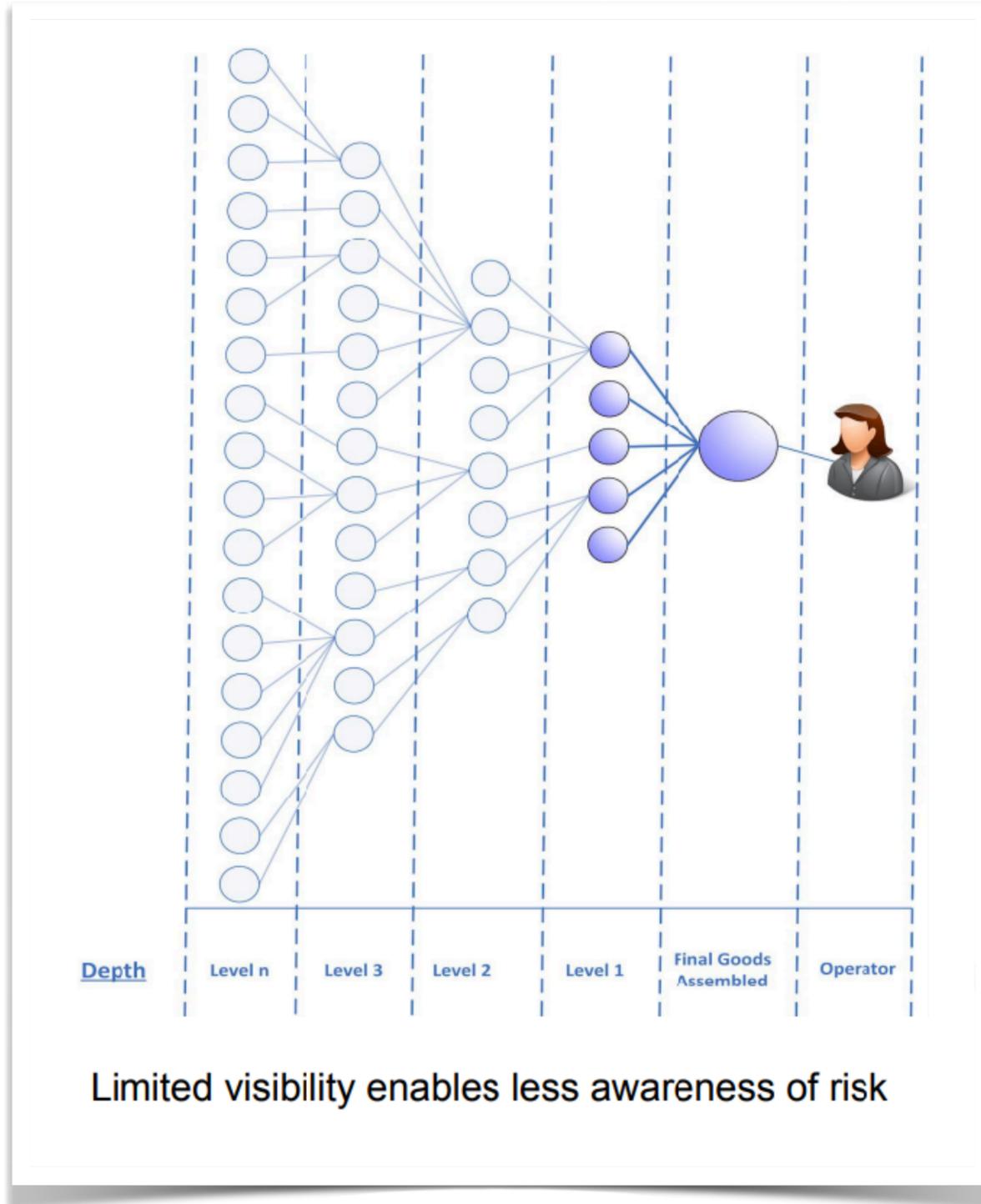
USE CASES, ROLES & BENEFITS

- Captures use cases for SBOM throughout the software supply chain
- Describes SBOM Personas and related benefits for those who:
 - Produce Software
 - Choose Software
 - Operate Software
- Also details Ecosystem, Network Effects, and Public Health Benefits of SBOMs
- Details Related Efforts (Updated and published separately on ntia.gov/sbom)
- SBOM Depth vs. Effectiveness
- High Assurance Use Cases

Roles and Benefits for SBOM Across the Supply Chain NTIA Multistakeholder Process on Software Component Transparency Use Cases and State of Practice Working Group

Introduction	2
The Software Supply Chain	4
About this document: Goals and Methodology	4
Perspective: Produce Software	5
Reduce unplanned, unscheduled work	6
Reduce code bloat	7
Adequately understand dependencies within broader complex projects	7
Know and comply with the license obligations	7
Monitor components for vulnerabilities	7
End-of-life (EOL)	8
Make code easier to review	8
A blacklist of banned components	8
Provide an SBOM to a customer	8
Perspective: Choose Software	9
Identify potentially vulnerable components	9
A more targeted security analysis	10
Verify the sourcing	10
Compliance with policies	10
Aware of end-of-life components	10
Verify some claims	10
Understand the software's integration	10
Pre-purchase and pre-installation planning	11
Market signal	11
Perspective: Operate Software	12
Organization can quickly evaluate whether it is using the component	12
Drive independent mitigations	13
Make more informed risk-based decisions	13
Alerts about potential end-of-life	13
Better support compliance and reporting requirements	13
Reduce costs through a more streamlined and efficient administration	13
Ecosystem, Network Effects, and Public Health Benefits of SBOM	14
Accelerated Vulnerability Management	15

DEPTH / LIMITATIONS



SBOM AT A GLANCE

- Intro to SBOMs, supporting literature, and the pivotal role of SBOMs for supply chain transparency
 - What is an SBOM?
 - Benefits & Use Cases
 - Baseline Component Information
 - Machine-Readable Formats & Tools
 - Sharing & Exchanging
 - Learn More
- Published on ntia.gov/sbom

SBOM at a Glance

Purpose

This document is an introduction to the practice of Software Bill of Materials (SBOM), supporting literature, and the pivotal role SBOMs play in providing much-needed transparency, enabling stakeholders to answer questions like “Am I affected?” and “Where am I affected?” when faced with a supply chain concern.

What is an SBOM?

An SBOM is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships. These inventories should be comprehensive – or should explicitly state where they could not be. SBOMs may include open source or proprietary software and can be widely available or access-restricted.¹

SBOMs should also include baseline attributes with the ability to uniquely identify individual components in a standard data format. The most efficient generation of SBOMs is as a byproduct of a modern development process. For older software, less-automated methods exist.

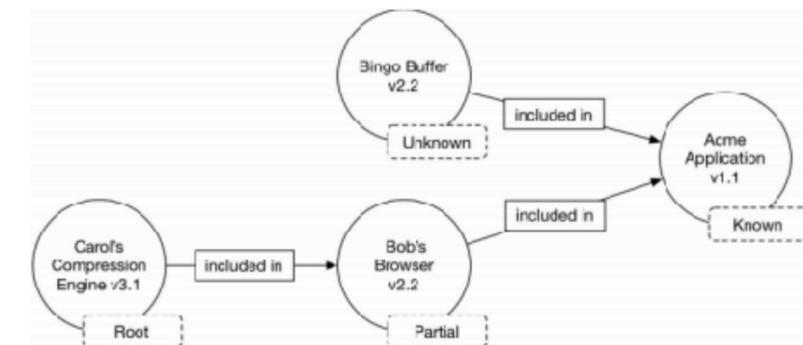


Figure: Conceptual SBOM tree with upstream relationship assertions

Benefits and Use Cases

The benefits and use cases for SBOMs² are numerous; vary across stakeholders who produce, choose, and operate software; and are amplified when combined. Benefits include reducing cost, security risk, license risk, and compliance risk. Use cases include improved software development, supply chain management, vulnerability management, asset management, procurement, and high assurance processes. An ongoing SBOM Healthcare Proof of Concept³ has exercised many of these use cases and demonstrated the value of producing, sharing, and consuming SBOMs, prompting similar proofs of concept in the Automotive and Energy industries.

SBOM FAQ

- Frequently asked questions about:
 - SBOMs
 - Benefits & Roles
 - Common Misconceptions & Concerns
 - Creation
 - Distribution & Sharing
 - Related Efforts
- Updated draft available for review and feedback
- Published on ntia.gov/sbom

SBOM FAQ

Table of Contents

Table of Contents	1
OVERVIEW	3
Q: What is an SBOM?	3
Q: Who should have an SBOM?	3
Q: Who uses an SBOM and for what?	3
BENEFITS	4
Q: What are the benefits of an SBOM?	4
Q: How does an SBOM help in the event of a cyberattack?	4
Q: In addition to vulnerability management, how can SBOMs help me?	5
Q: How have bills of material and supply chain transparency been helpful elsewhere?	5
COMMON MISCONCEPTIONS & CONCERNS	5
Q: Won't SBOMs be a "roadmap to the attacker"?	5
Q: Does an SBOM require source code disclosure?	6
Q: Does a list of the software components I include expose my intellectual property?	6
Q: Does an SBOM increase my exposure to license violations?	6
Q: Does an SBOM enable patent or license "trolls"?	6
Q: Will SBOMs increase my licensing costs or licensing commitments?	7
CREATION	7
Q: Who creates and maintains an SBOM?	7
Q: What should be included in an SBOM?	7
Q: What data formats exist for conveying SBOM data?	7
Q: Are there tools that translate between SBOM formats?	8
Q: When is an SBOM created, changed, or maintained?	8
Q: Some software components are made up of other software components themselves. Can an SBOM show that hierarchy?	8
Q: How deep in the dependency graph should an SBOM enumerate?	9
DISTRIBUTION & SHARING	9
Q: If I make an SBOM, do I have to make it public?	9
Q: How will SBOM data be shared?	9
ROLE SPECIFIC	10
Q: How can SBOMs be leveraged as a Purchaser?	10

SBOM MYTHS VS. FACTS

- Intended to help the reader to understand and dispel common, often sincere myths and misconceptions about SBOM.
- Published on ntia.gov/sbom

NTIA Multistakeholder Process on Software Component Transparency | ntia.gov/sbom

SBOM Myths vs. Facts

The NTIA Multistakeholder Process on Software Component Transparency¹ seeks to provide industry-agnostic guidance and resources to support adoption and implementation of Software Bill of Materials (SBOM).²

As the practice of SBOM expands beyond trailblazing industries (e.g., Financial Services and Healthcare) and becomes more widely adopted, the resulting network effect will amplify the initial and inherent benefits that SBOMs provide. With increased awareness comes increased opportunity for misunderstanding. This document is intended to help the reader to understand and dispel common, often sincere myths and misconceptions about SBOM. This list is not intended to be comprehensive. For more common questions and concerns, see the SBOM FAQ.³

The Myths	The Facts
Myth: SBOMs are a roadmap to the attacker	Attackers can leverage the information contained in SBOMs. However, the defensive benefits of transparency far outweigh this common concern as SBOMs serve as a "roadmap for the defender". All information is dual-edged, but insufficient software transparency affords attackers asymmetrical advantages. <ul style="list-style-type: none">• Attackers don't need SBOMs. Mass, indiscriminate attacks like WannaCry serve to remind us that foreknowledge is not a prerequisite to cause harm.• Attackers and their tools can more easily identify software components. Conversely, it is often quite challenging, disruptive, inefficient, and even unlawful for defenders to determine the same.• Attackers of any single product can already find human-readable target components – licensing requirements have been increasingly requiring disclosure for decades. SBOMs seek to level the playing field for defenders by providing additional transparency – at enterprise scale – with standard, machine-readable decision support.
Myth: An SBOM alone provides no useful or actionable information	The baseline component information supports a number of use cases for those who produce, choose, and operate software, as outlined in NTIA's "Roles and Benefits" document. ⁴ For example, during an active attack, an SBOM allows an enterprise to answer, "Am I affected?" and "Where am I affected?" in minutes or hours, instead of days or weeks. Additionally, the baseline component information enables vital transparency and auditability, allowing for further expansion and enrichment in additional use cases. The Executive Order on Improving the Nation's Cybersecurity (No. 14028) ⁵ also expects significant value for federal agencies.
Myth: An SBOM needs to be made public	An SBOM does not need to be made public. The act of making an SBOM is separate from sharing it with those who can use this data constructively. The author may advertise and share the SBOM at their discretion. In other cases, sector-specific regulations or legal requirements may require more or less access to the SBOM. The Executive Order on Improving the Nation's Cybersecurity (No. 14028) is also clear that making an SBOM publicly available is a choice, not a requirement. Section 4 (e) (vi) states "providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website." ⁶

MINIMUM ELEMENTS

NTIA Multistakeholder Process

NTIA for Executive Order

Author Name

Author of SBOM Data

Timestamp

Timestamp

Supplier Name

Supplier Name

Component Name

Component Name

Version String

Version of the Component

Component Hash

-

Unique Identifier

Other Unique Identifier(s)

Relationship

Dependency Relationship

SBOM OPTIONS & DECISION POINTS

➤ Purpose

- To frame the dimensions for what is possible with modern development practices
- To support more consistent and effective articulation of needs between requesters and suppliers of SBOMs

➤ Published on ntia.gov/sbom

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats¹, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier
 † Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship
 ‡ SBOM Formats: SPDX, CycloneDx, SWID

ntia.gov/sbom

SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM OPTIONS & DECISION POINTS

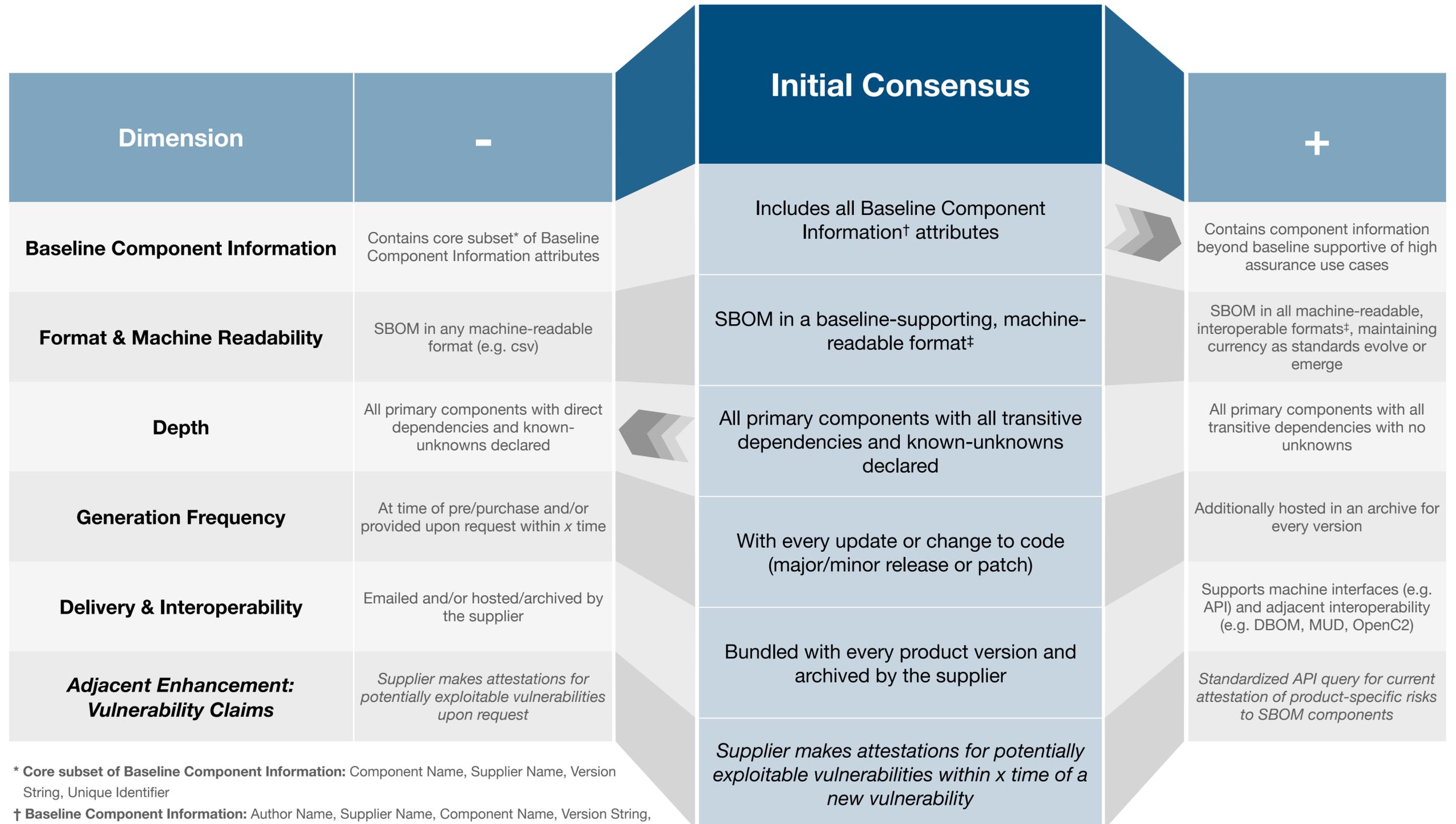
Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	<i>Supplier makes attestations for potentially exploitable vulnerabilities upon request</i>	<i>Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability</i>	<i>Standardized API query for current attestation of product-specific risks to SBOM components</i>

* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM OPTIONS & DECISION POINTS

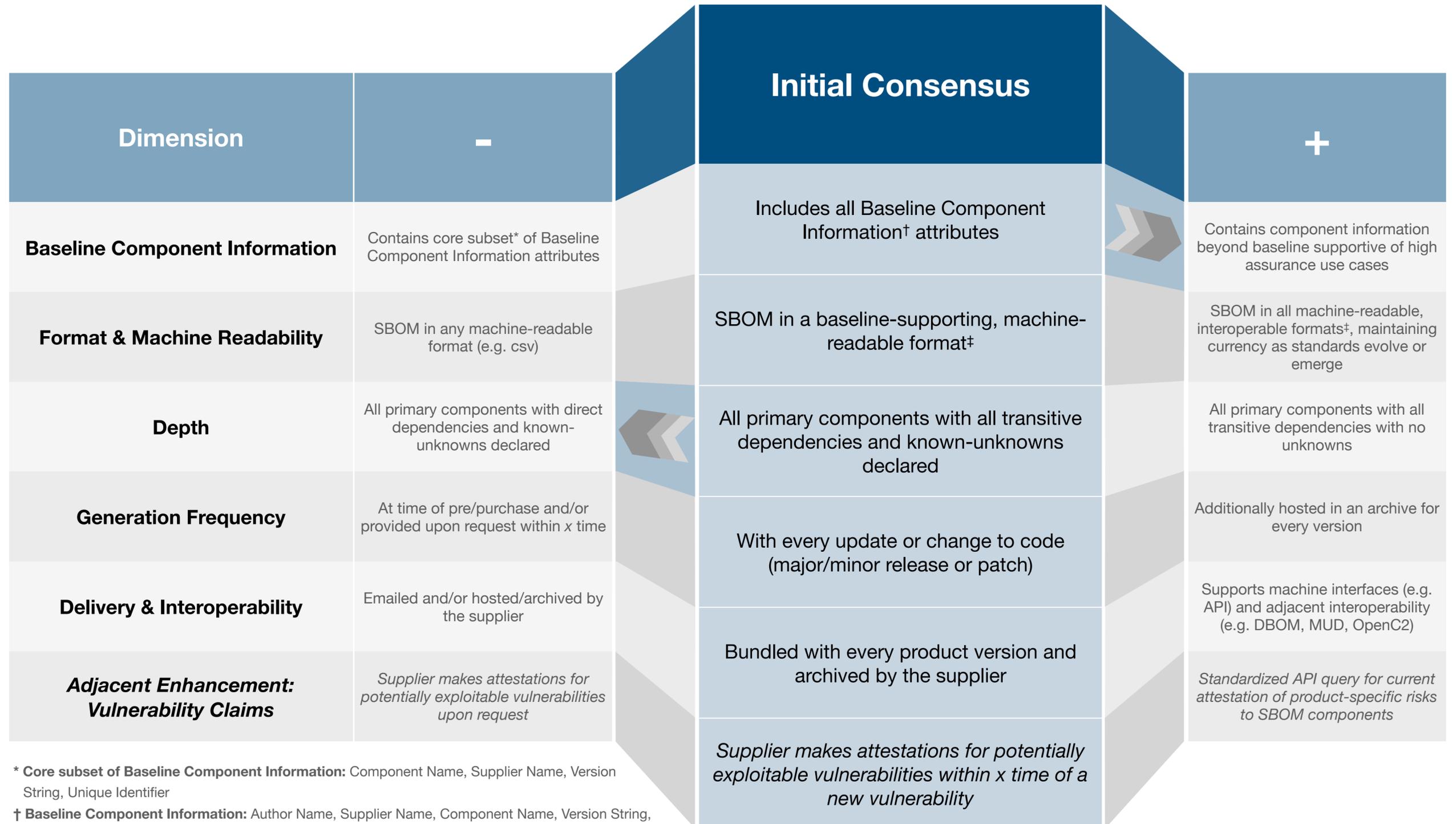


* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM OPTIONS & DECISION POINTS

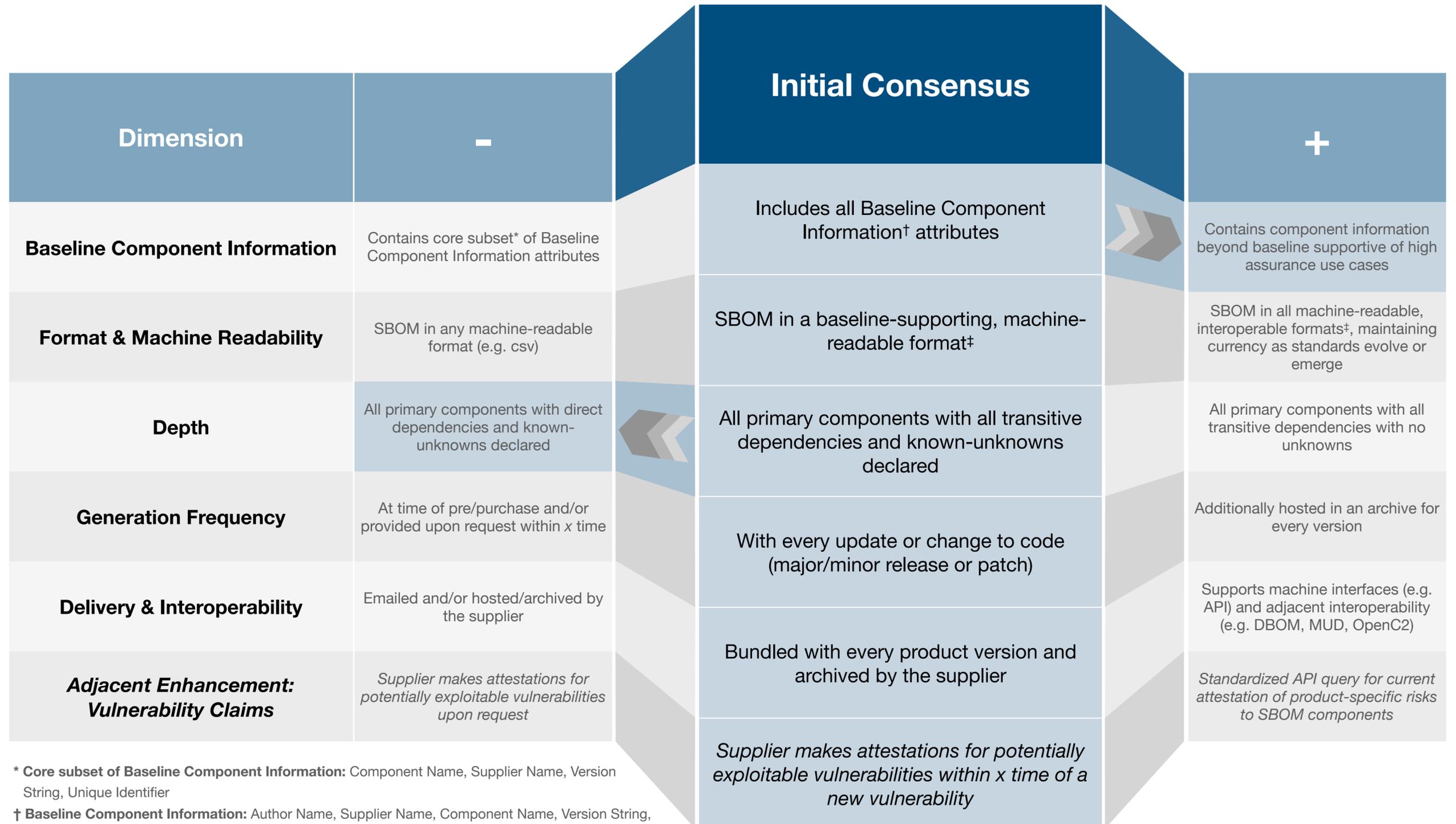


* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM OPTIONS & DECISION POINTS

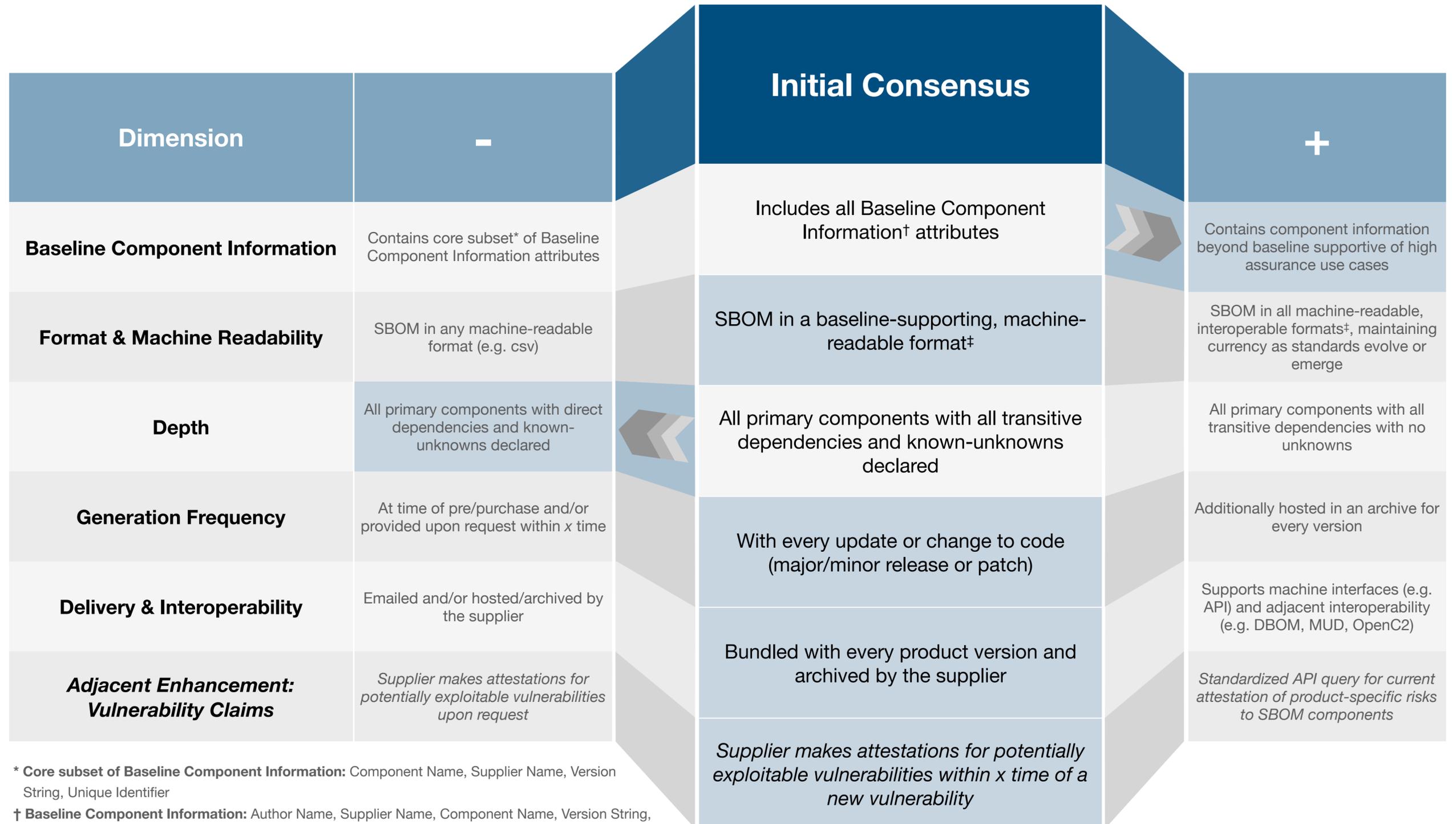


* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM OPTIONS & DECISION POINTS

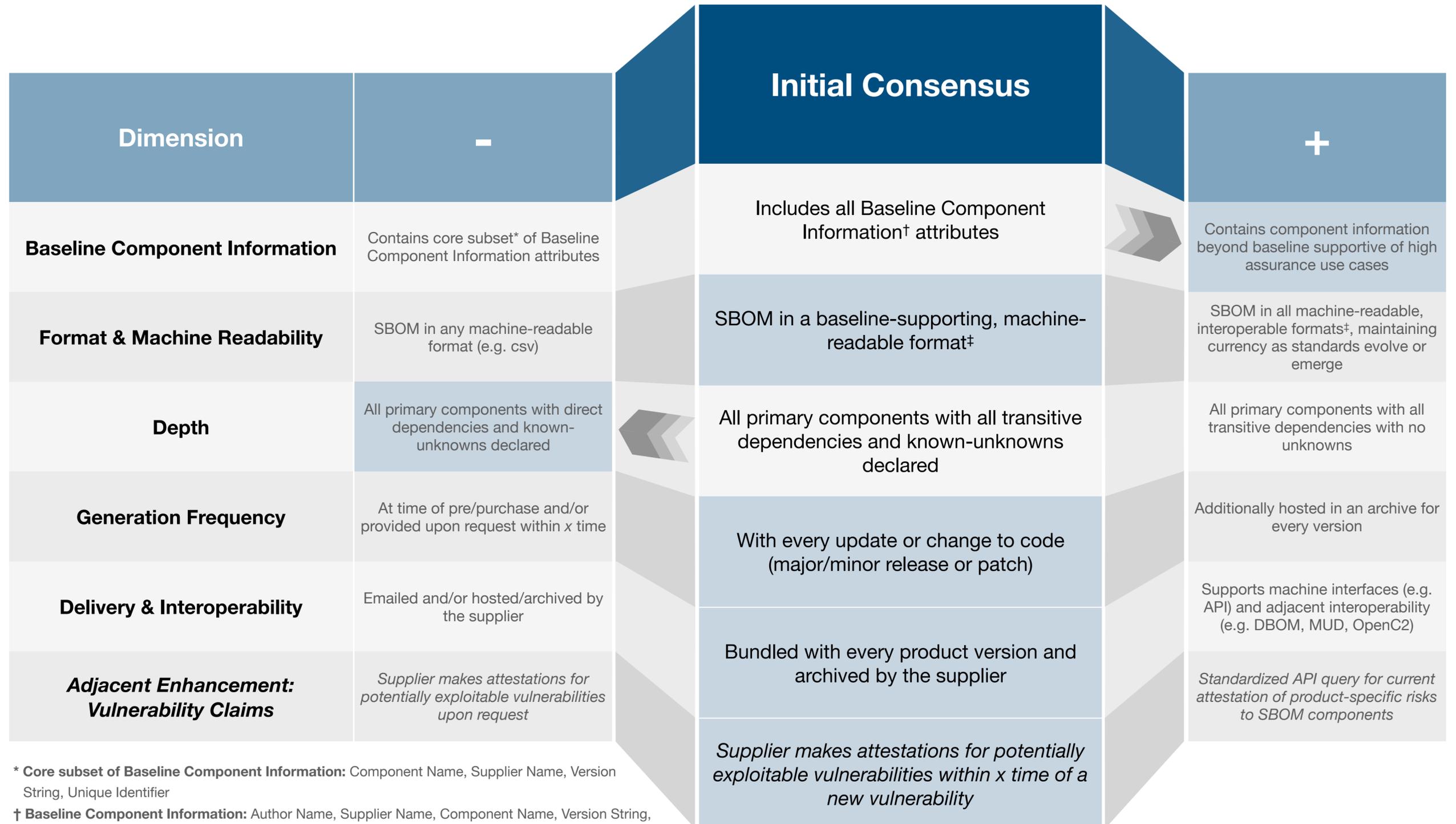


* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM OPTIONS & DECISION POINTS



* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID

SBOM-ADJACENT TOPICS

- ▶ Anomalous Software Detection
- ▶ BSA Framework
- ▶ BSIMM
- ▶ CISQ
- ▶ CVE
- ▶ CycloneDx
- ▶ DBOM
- ▶ DevSecOps
- ▶ End of Life Management
- ▶ FDA Premarket Guidance
- ▶ FS-ISAC Controls
- ▶ Hardware BOMs
- ▶ ISO Security Standards
- ▶ Joint Security Plan (JSP)
- ▶ License Management
- ▶ MDS2
- ▶ MITRE's Deliver Uncompromised
- ▶ MUD
- ▶ NERC CIP 13
- ▶ NIST SSDF
- ▶ OpenC2
- ▶ OpenChain
- ▶ OWASP Component Analysis
- ▶ OWASP SCVS
- ▶ Package URL
- ▶ Procurement
- ▶ Runtime monitoring
- ▶ SAFE Code 3rd Party Guidance
- ▶ SBOM Integrity Monitoring
- ▶ SCAP
- ▶ SCRM
- ▶ Software Dependencies
- ▶ Software Heritage
- ▶ SPDX
- ▶ Supply Chain Attack Detection
- ▶ SWID
- ▶ Vulnerability Management
- ▶ Vulnerability Prioritization
- ▶ WP.29

NTIA RESOURCES

- Additional NTIA Publications, including:
 - Explainer Videos
 - Framing SBOMs
 - Use Cases, Roles & Benefits
 - Tool Classification Taxonomy
 - Survey of Existing Formats & Standards
 - Software Supplier & Consumer Playbooks
 - How-to Guide for SBOM Generation
 - Sharing & Exchanging SBOMs
 - Software Identity
 - Overview of Vulnerability and Exploitability Exchange (VEX)
 - Healthcare Proof of Concept Reports
- Published on ntia.gov/sbom

The screenshot shows the NTIA website's page for Software Bill of Materials (SBOM). The header includes the NTIA logo, the text "National Telecommunications and Information Administration" and "United States Department of Commerce", a search bar, and a navigation menu with items like "About Us", "Key Issues", "Grants", "News", "Data Central", and "Publications". The main content area is titled "SOFTWARE BILL OF MATERIALS" and contains an introductory paragraph, followed by several sub-sections with links and brief descriptions: "Introduction to SBOM", "SBOM at a Glance (2021)", "SBOM FAQ (2021)", "SBOM Myths vs. Facts (2021)", "SBOM Explainer Videos on YouTube (2020-2021)", "Understanding SBOM", "Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) - (2021)", "SBOM Options and Decision Points (2021)", "Use Cases: Roles and Benefits for SBOM Across the Supply Chain (2019)", "SBOM Tool Classification Taxonomy (2021)", and "SBOM Implementation".

CISA RESOURCES

- ▶ Working Group Drafted:
 - ▶ Vulnerability Exploitability eXchange (VEX) Use Case Document
 - ▶ Vulnerability Exploitability eXchange (VEX) Status Justification Document
 - ▶ Minimum Requirements for Vulnerability Exploitability eXchange (VEX)
 - ▶ Types of Software Bill of Materials (SBOM)
- ▶ CISA & Partener Drafted:
 - ▶ Software Bill of Materials (SBOM) Sharing Lifecycle Report
- ▶ Published on cisa.gov/sbom

The screenshot shows the CISA website page for Software Bill of Materials (SBOM). The header includes the CISA logo and navigation menu. The main content area features a title 'Software Bill of Materials (SBOM)' and a paragraph explaining the concept. Below this, there is a call to action for an SBOM-a-Rama event. A featured content section at the bottom highlights an announcement for the event.

Software Bill of Materials (SBOM)

A "software bill of materials" (SBOM) has emerged as a key building block in software security and software supply chain risk management. A SBOM is a needed inventory, a list of ingredients that make up software components. The SBOM work has advanced since 2016 as a collaborative community effort, driven by National Telecommunications and Information Administration (NTIA) and industry efforts.

CISA will advance the SBOM work by facilitating community engagement, development, and progress, with a focus on scaling and operationalization, as well as tools, new technologies, and new use cases. This website will also be a nexus for the broader set of SBOM resources across the digital ecosystem and around the world.

An SBOM-related concept is the [Vulnerability Exploitability eXchange \(VEX\)](#). A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities.

Register to attend SBOM-a-Rama in-person or virtually, taking place on Wednesday, June 14:
[CISA SBOM-a-RAMA REGISTRATION](#)

View the agenda: [SBOM-a-Rama 2022 Agenda](#) | [CISA](#)

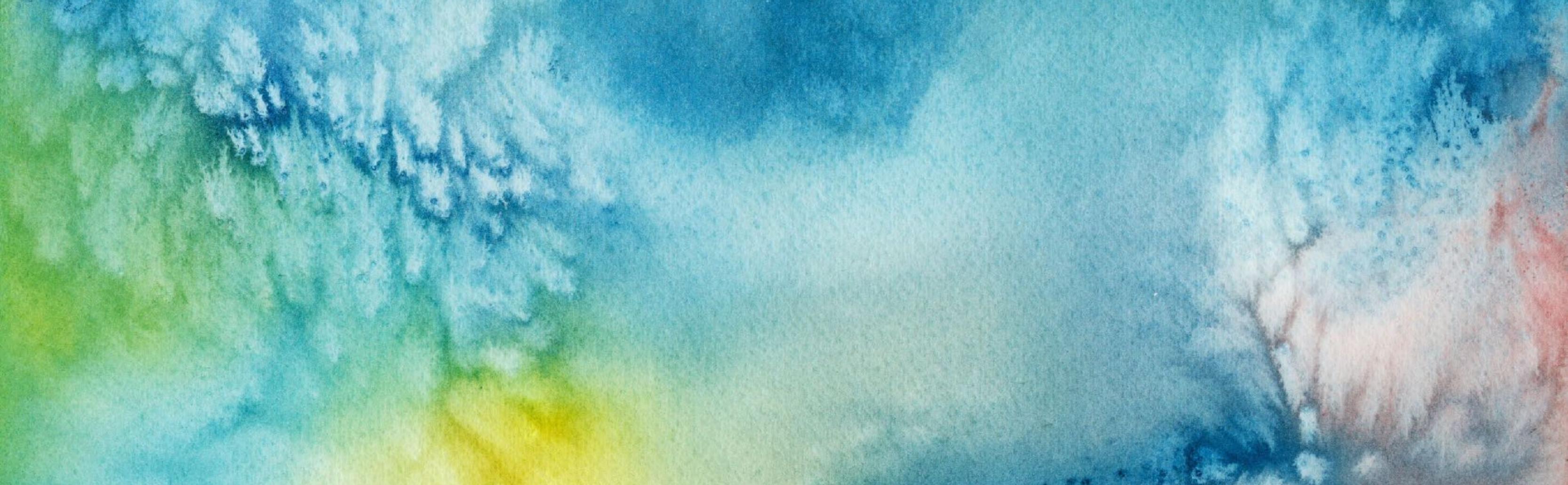
ANNOUNCEMENT

Registration is open for the SBOM-a-Rama, which will take place on Wednesday, June 14th. This hybrid event will be held virtually as well as at the USC hotel in Los Angeles, CA.

- [Learn more or register at: SBOM-a-Rama](#)
- [Download/View the Agenda](#)

Featured Content

For information about the "NTIA Co-sponsors" drafting and implementing SBOM, drafted by stakeholder, see the resources at [cisa.gov/sbom](#)



PRESENT



WHAT WE'RE WORKING ON

➤ Today's Highlights:

- News, Events, Presentations, & Resources
- Vertical-Specific Primers
- SBOM Calendar
- FAQ Draft for Review
- Crawl / Walk / Run
- Procurement / Acquisition Primer for SBOM

➤ Ongoing Efforts:

- Working Group Socratic Reviews
- FAQ
- News
- SBOM Calendar & Events
- Industry-Specific Primers
- Capturing SBOM Wants / Needs / Fears
- Related Efforts Update
- Presentations & Overviews
- Virtual Engagement Opportunities

NEWS, EVENTS, PRESENTATIONS, & RESOURCES

Presentations

- ☑ SBOM-a-rama
- ☑ Overview of SBOM Types Publication
- ☑ Overview of CISA/DOE Sharing Landscape Publication
- ☑ Overview of VEX Minimum Elements Publication
- ☑ Auto ISAC POC Update
- ☑ Log4j - Topo Presentation
- ☑ GUAC Presentation | Q&A
- ☑ United Nations: "Stronger Together: Collaboration for a Cyber-Safe World"
- ☑ ESF Supply Chain
- ☑ Sounil Presentation and Discussion
- ☑ Auto-ISAC POC Update (Presentation from 2021 Auto-ISAC Cybersecurity Summit)
- ☑ Overview of CISA Secure by Design Secure by Default Publication

NEWS, EVENTS, PRESENTATIONS, & RESOURCES

Resources

- 🕒 CISA Self Attestation Form - Request for Comments
- ✅ SLSA v1.0 Release
- ✅ FDA Refuse to Accept (RTA) Policy
- ✅ European: Cyber Resilience Act
- ✅ Secure Open Source SW Act of 2022
- ✅ FDA Pre-Market Guidance
- ✅ BOD 23-01 Asset Management & Vulnerability Mgt.
- ✅ White House OMB Memo
- ✅ NSA ODNI CISA Supply Chain Document (Sept 1)
- ✅ NDAA Language, House and Senate
- 🕒 SPDX Announces 3.0 Release Candidate with New Use Cases
- 🕒 Software Bill of Materials (SBOM) Sharing Lifecycle Report
- 🕒 Minimum Requirements for Vulnerability Exploitability eXchange (VEX)
- 🕒 Types of Software Bill of Materials (SBOM)
- 🕒 Security-by-Design and -Default
- 🕒 Japanese SBOM Guidance - Request for Comments
- 🕒 IMDRF Principles and Practices for Software Bill of Materials for Medical Device
- 🕒 IMDRF Principles and Practices for the Cybersecurity of Legacy Medical Devices
- 🕒 PATCH Act via Appropriations Bill

SBOM EVENTS CALENDAR

SBOM Events

Today ◀ ▶ June 2023 Print Week Month Agenda

Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	31	Jun 1	2	3
	TSA OT Summit 10am VEX subgroup weekly meeti 12pm SBOM Sharing Weekly Meeti	12pm Onramps & Adoption Weekly	Software and Supply Chain Assurance Event 3pm SBOM Cloud Biweekly Meetin	10:30am Cloud Stack Transparency 12pm SBOM Classic for Modern Ap 1pm SBOM Healthcare Proof of Co 3pm SBOM Tooling Weekly Meetin		
4	5	6	7	8	9	10
FIRST Conference						
	10am VEX subgroup weekly meeti 12pm SBOM Sharing Weekly Meeti	12pm Onramps & Adoption Weekly		3pm SBOM Tooling Weekly Meetin	10:30am Cloud Stack Transparency 12pm SBOM Classic for Modern Ap	
11	12	13	14	15	16	17
	10am VEX subgroup weekly meeti 12pm SBOM Sharing Weekly Meeti	Open Cybersecurity Alliance (OCA) 12pm Onramps & Adoption Weekly	SBCM-a-rama 3pm SBOM Cloud Biweekly Meetin	1pm SBOM Healthcare Proof of Co 3pm SBOM Tooling Weekly Meetin	10:30am Cloud Stack Transparency 12pm SBOM Classic for Modern Ap	
18	19	20	21	22	23	24
	10am VEX subgroup weekly meeti 12pm SBOM Sharing Weekly Meeti	12pm Onramps & Adoption Weekly		3pm SBOM Tooling Weekly Meetin	10:30am Cloud Stack Transparency 12pm SBOM Classic for Modern Ap	
25	26	27	28	29	30	Jul 1
	10am VEX subgroup weekly meeti 12pm SBOM Sharing Weekly Meeti	12pm Onramps & Adoption Weekly	3pm SBOM Cloud Biweekly Meetin	1pm SBOM Healthcare Proof of Co 3pm SBOM Tooling Weekly Meetin	10:30am Cloud Stack Transparency 12pm SBOM Classic for Modern Ap	

Events shown in time zone: Eastern Time - New York Google Calendar

SBOM EVENTS CALENDAR

- View SBOM Events Calendar: <https://bit.ly/sbom-calendar-public>
- Subscribe to SBOM Events Calendar: <https://bit.ly/sbom-calendar-subscribe>
- To submit SBOM-related events or talks for inclusion, email details and/or forward an existing calendar invitation to:
 - sbom.calendar@gmail.com
 - Include:
 - Event Title, Time, & Time Zone
 - Location & Cost, if applicable
 - Description
 - Link to registration or more information

SBOM FAQ UPDATE – DRAFT FOR REVIEW

- Contains:
 - FAQs previously vetted and approved as part of the NTIA SBOM efforts
 - Nine new questions drafted as part of the CISA working groups
- Current request for feedback is aimed toward **new or modified** questions
- Feedback on any errors, omissions, or confusion can be shared at any time for future consideration

SBOM FAQ - Draft for Review

v20230607

The current request for feedback is aimed toward new or modified questions, which are labeled as such. Feedback on any errors, omissions, or confusion can be shared at any time for future consideration.

Table of Contents

Table of Contents	1
OVERVIEW	3
Q: What is an SBOM?	3
Q: Who should have an SBOM?	3
Q: Who uses an SBOM and for what?	3
Q: Can SBOMs be generated at different points in the software lifecycle? <i>NEW</i>	4
Q: I'm still learning how to make SBOMs. Is it necessary to try to produce all the SBOM types? <i>NEW</i>	4
BENEFITS	4
Q: What are the benefits of an SBOM?	4
Q: How does an SBOM help in the event of a cyberattack?	5
Q: In addition to vulnerability management, how can SBOMs help me?	5
Q: How have bills of material and supply chain transparency been helpful elsewhere?	5
COMMON MISCONCEPTIONS & CONCERNS	6
Q: Won't SBOMs be a "roadmap to the attacker"?	6
Q: Does an SBOM require source code disclosure?	6
Q: Does a list of the software components I include expose my intellectual property?	6
Q: Does an SBOM increase my exposure to license violations?	7
Q: Does an SBOM enable patent or license "trolls"?	7
Q: Will SBOMs increase my licensing costs or licensing commitments?	7
CREATION	7
Q: Who creates and maintains an SBOM?	7
Q: What should be included in an SBOM?	7
Q: What data formats exist for conveying SBOM data?	8
Q: Are there tools that translate between SBOM formats?	8
Q: When is an SBOM created, changed, or maintained?	8
Q: Some software components are made up of other software components themselves. Can an SBOM show that hierarchy?	9
Q: How deep in the dependency graph should an SBOM enumerate?	9
DISTRIBUTION & SHARING	9
Q: If I make an SBOM, do I have to make it public?	9

Last Revised: 2023-06-07

1

SBOM FAQ UPDATE – DRAFT FOR REVIEW

- SBOM FAQ for feedback:
bit.ly/sbom-onramps-faq-june2023
- Feedback Due: June 28, 2023
- Please provide feedback via “Add a comment” on Google Document:



- Please also nominate new FAQs for future iterations.



Produce



Choose



Operate



Crawl

NTIA A&A Participants

NTIA A&A Participants

NTIA A&A Participants



Walk



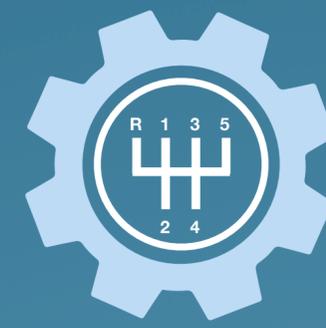
Run



Produce



Choose



Operate



Crawl

NTIA A&A Participants

CISA Participants

NTIA A&A Participants

CISA Participants

NTIA A&A Participants

CISA Participants



Walk

CISA Participants

CISA Participants



Run

CISA Participants

CISA Participants

PROCUREMENT/ACQUISITION PRIMER FOR SBOM

PERSONAS AND BENEFITS

Supply Chain Personas

- Three supply chain personas [2]:
 - Producers
 - Choosers ★
 - Operators
- Procurement and Acquisition tend to fall under "Choosers"
- It is common to represent more than one persona

Chooser Benefits

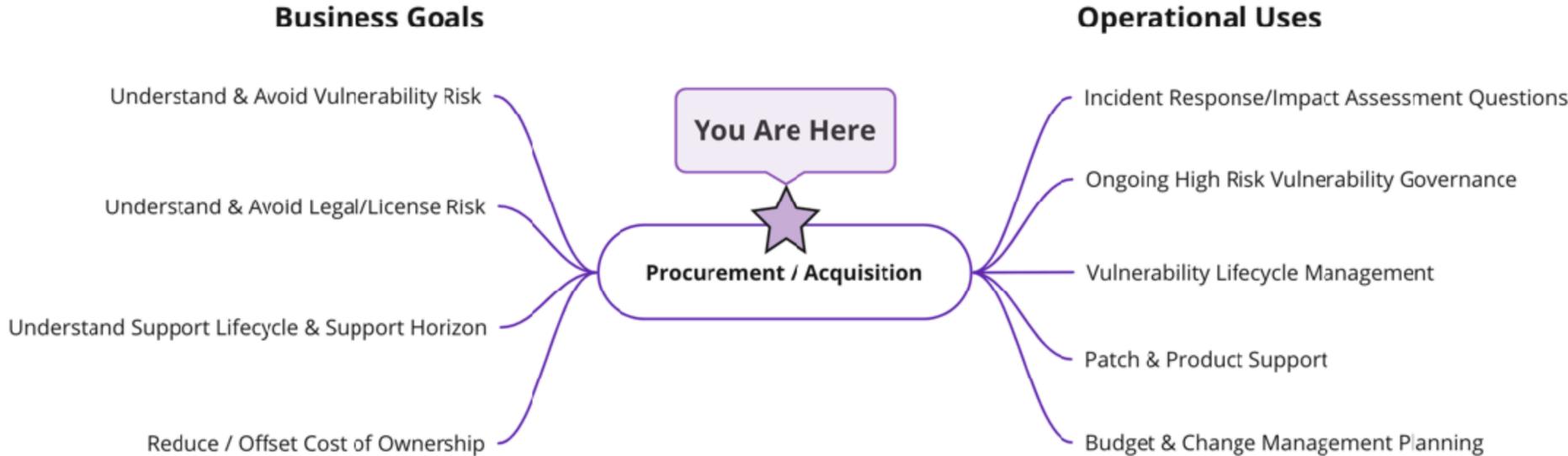
- Simplified way to support plural current and future needs of the business with less effort and less complexity
- Streamlined, consistent artifacts
- More protections via attestations and/or updates to contractual commitments
- When SBOM is missing, new negotiation and leverage points for overall procurement processes

Downstream Operator Benefits

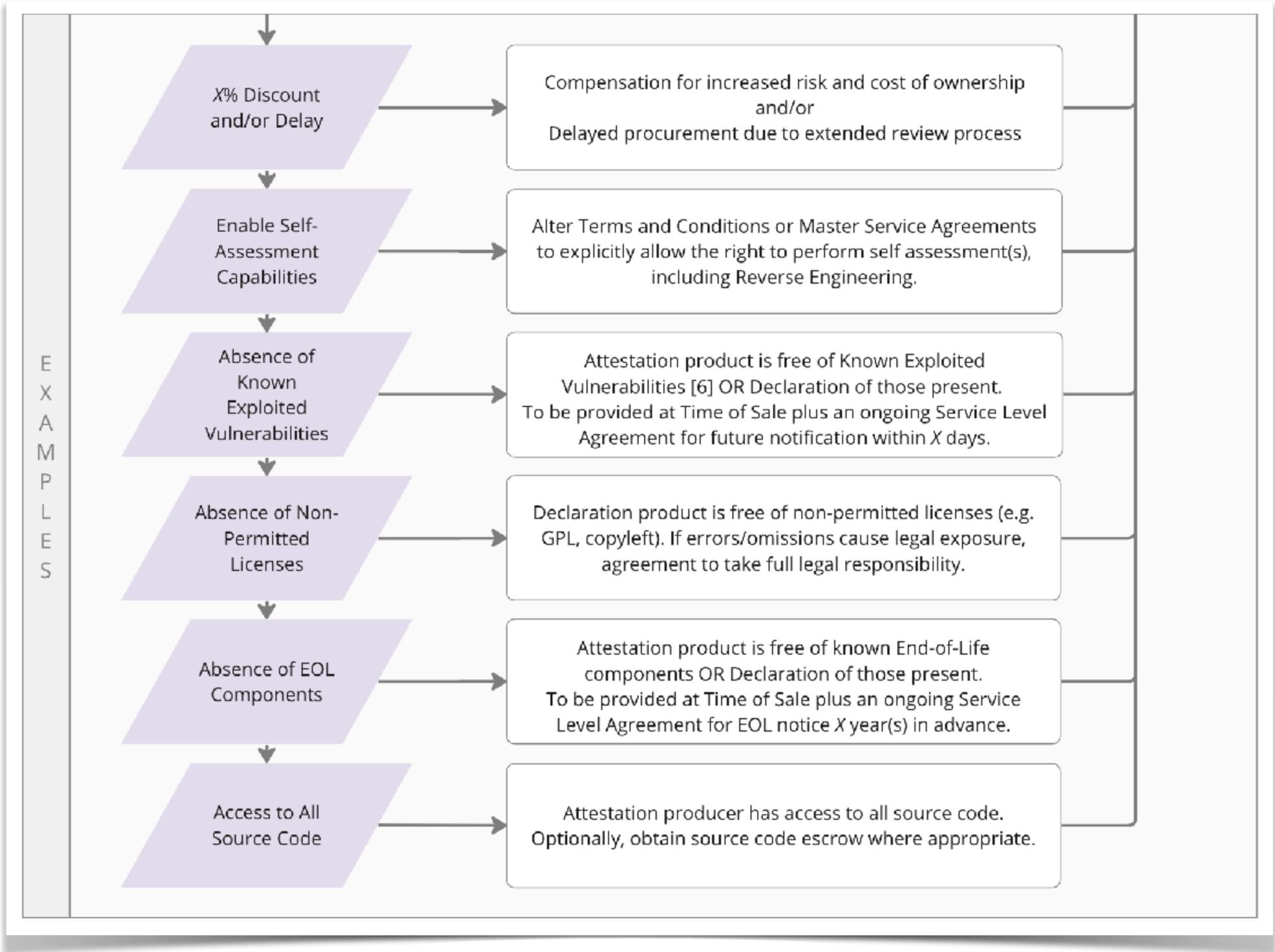
- Enables operators to perform ongoing assessment and quantification of risks inherent in software
- Manage mitigations for vulnerabilities
- Lower operating costs due to improved efficiencies
- Reduce unplanned, unscheduled work

BUSINESS GOALS & THE ROLE OF PROCUREMENT

Choosers play a brief but important role. At the intersection of business goals and business operations, procurement is advantageously positioned to obtain SBOMs for an organization. Requesting SBOMs at time of purchase and/or contract renewals yields outsized benefits: one SBOM request benefits plural stakeholders, and SBOMs enable the business to answer questions both now and in the future. Examples of business and operational use cases are provided below.



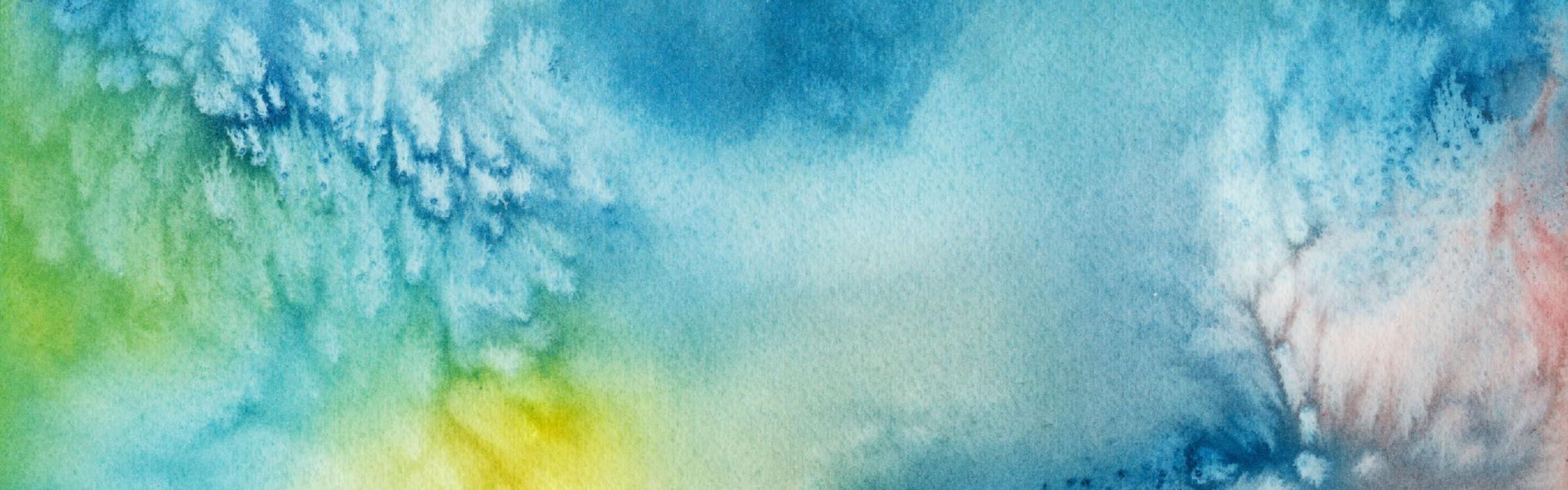
PROCUREMENT/ACQUISITION PRIMER FOR SBOM





ONGOING EFFORTS

- ▶ FAQ
- ▶ News
- ▶ SBOM Calendar & Events
- ▶ Industry-Specific Primers
- ▶ Working Group Socratic Reviews
- ▶ Capturing SBOM Wants / Needs / Fears
- ▶ Related Efforts Update
- ▶ Presentations & Overviews
- ▶ SBOM-related Resources
- ▶ Virtual Engagement Opportunities
 - ▶ Webinars, Podcasts, Conferences, Recordings, Other
 - ▶ Conference and Event Talks with Links
 - ▶ e.g. List of RSAC 2023 talks about and related to SBOM & Software Supply Chain



FUTURE

FUTURE INITIATIVES & IDEAS FOR 2023

- ▶ Workgroup Welcome Guide
- ▶ History/Timeline of SBOM
- ▶ SBOM Journeys & Testimonials
- ▶ Explainer Videos
- ▶ Stakeholder-Specific Resources for Under-Resourced
- ▶ SBOM Toy Examples/Starter Kit for Tool Testing
- ▶ “I have an SBOM. What’s next?” Materials
- ▶ Graduated Expectation Management
 - ▶ What SBOM Can/Can’t Do
 - ▶ What to Expect of SBOM Now and with Future, Iterative Improvements
 - ▶ Ensuring SBOMs meet consensus
- ▶ Related/Adjacent Effort Tracking and Improvement
- ▶ SBOMs for Firmware & Embedded Systems
- ▶ Industry/Supply-Chain Specifics

SBOM

Ingredients

- Inventory
- Parts
- Lists
- 1..n Suppliers
- BoM (Bill of Materials)

Not SBOM

Known Vulnerabilities

- CVEs ++
- *Potentially* exploitable
- Not “Attack Surface”

“VEX”

Exploitable Vulnerabilities

- Attack Surface
- Code Flow
- Other mitigations

- Direct Exploitation
- Chained attacks
- Deserialization

IMG SRC: Josh Corman NTIA.gov 2018

Excerpt from “The Opposite of Transparency” <https://youtu.be/qk2vo7ir1cl>

DevOps Enterprise Journal - log4j

Attribution

... This talk is based on an IT Revolution Forum paper

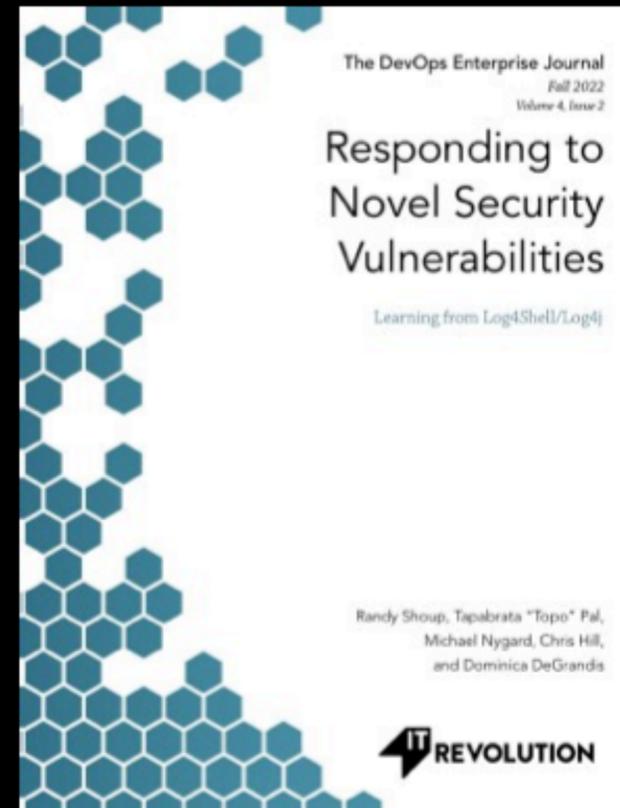
IT Revolution - DevOps Enterprise Forum - 2022

“Responding to Novel Security Vulnerabilities - Learning from Log4Shell”

By

Randy Shoup, Topo Pal, Michael Nygard, Chris Hill, Dominica DeGrandis

<https://myresources.itrevolution.com/viewer/?id=006657146>



@TopoPal

Link to Topo's Talk: https://www.linkedin.com/posts/tapabratapal_log4shell-response-patterns-learnings-from-activity-7072789564397916161-5_Fu

Excerpt from “The Opposite of Transparency” <https://youtu.be/qk2vo7ir1cl>

Symptoms (& smokescreens?) Heart of the Hydra

#RSAC

Stronger
Together



1) License violations

2) "Unfixable" issues

3) Ongoing scrutiny /
accountability

4) \$Other

www.theoi.com

Excerpt from "The Opposite of Transparency" <https://youtu.be/qk2vo7ir1cl>

Your favorite “First Principle” for Cybersecurity?



WHEEL OF FORTUNE

Security through obscurity is...

PATCH Act... ++ Law of the Land

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices Under Section 524B of the FD&C Act

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

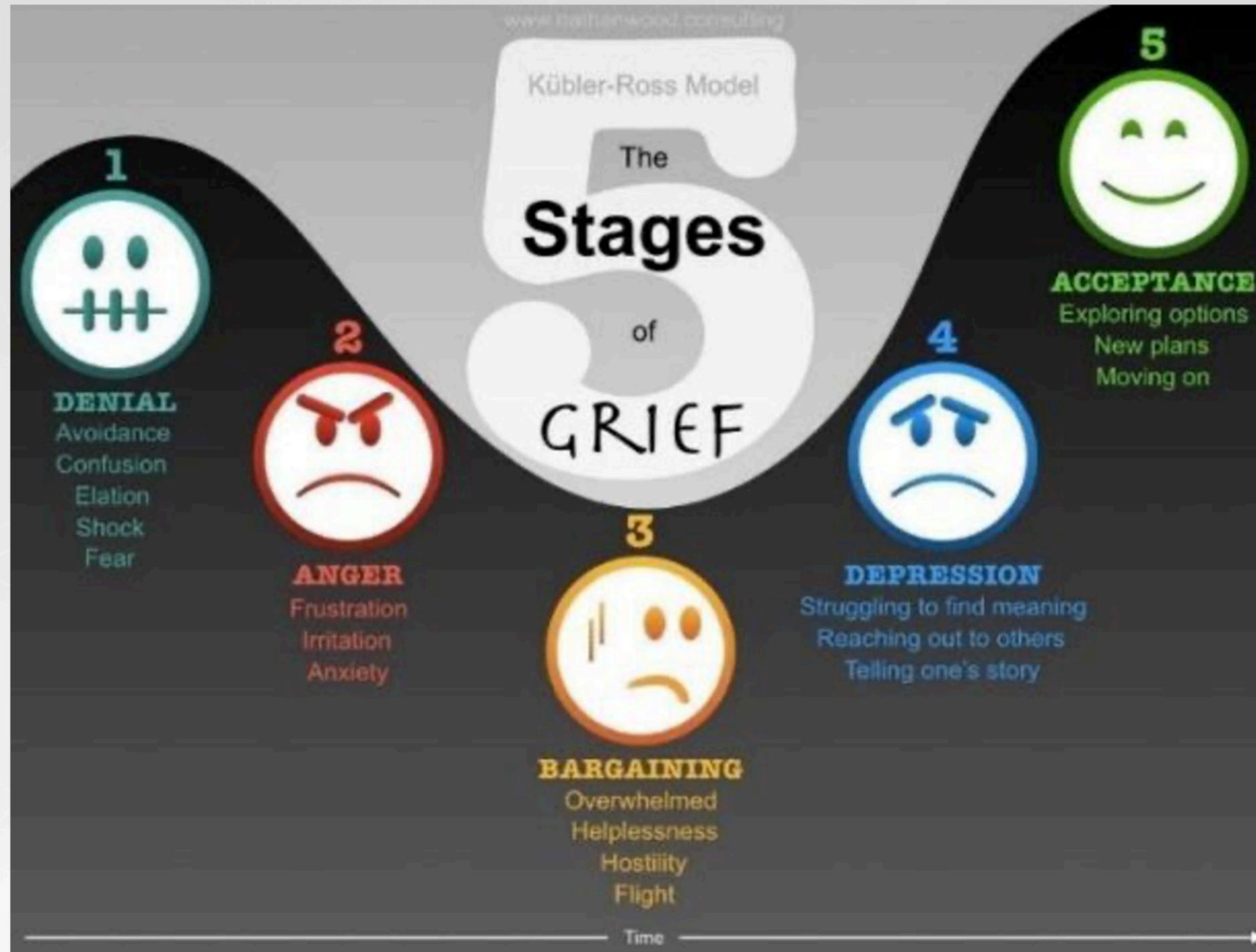
I. Introduction

On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus — "Ensuring Cybersecurity of Medical Devices" — amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices. The Omnibus states that the amendments to the FD&C Act shall take effect 90 days after the enactment of this Act on March 29, 2023. As provided by the Omnibus, the cybersecurity requirements do not apply to an application or submission submitted to the Food and Drug Administration (FDA) before March 29, 2023.

This guidance is being implemented without prior public comment because FDA has determined that prior public participation for this guidance is not feasible or appropriate (see section 701(h)(1)(C) of the FD&C Act (21 U.S.C. 371(h)(1)(C)) and 21 CFR 10.115(g)(2)). This guidance document is being implemented immediately, but it remains subject to comment in accordance with the Agency's good guidance practices.

In general, FDA's guidance documents do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word "should" in Agency guidances means that something is suggested or recommended, but not required.

I AM THE
Cavalry



How much
OPACITY...

do we add to our
TRANSPARENCY?

iamthecavalry.org

I AM THE
Cavalry

A journey? Graduated expectations over time?



Industry Landscape

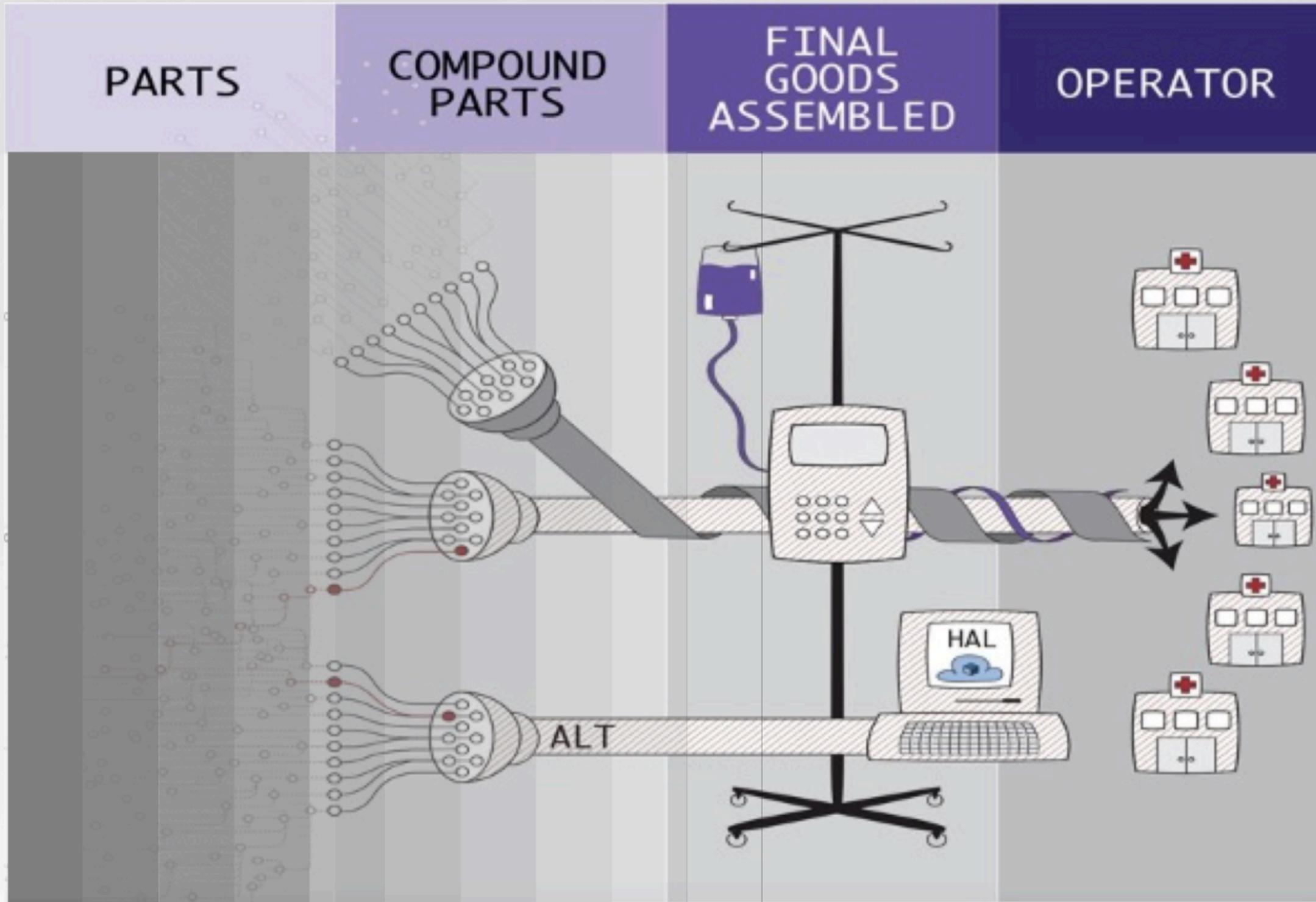
Who can't
produce
SBOMs?

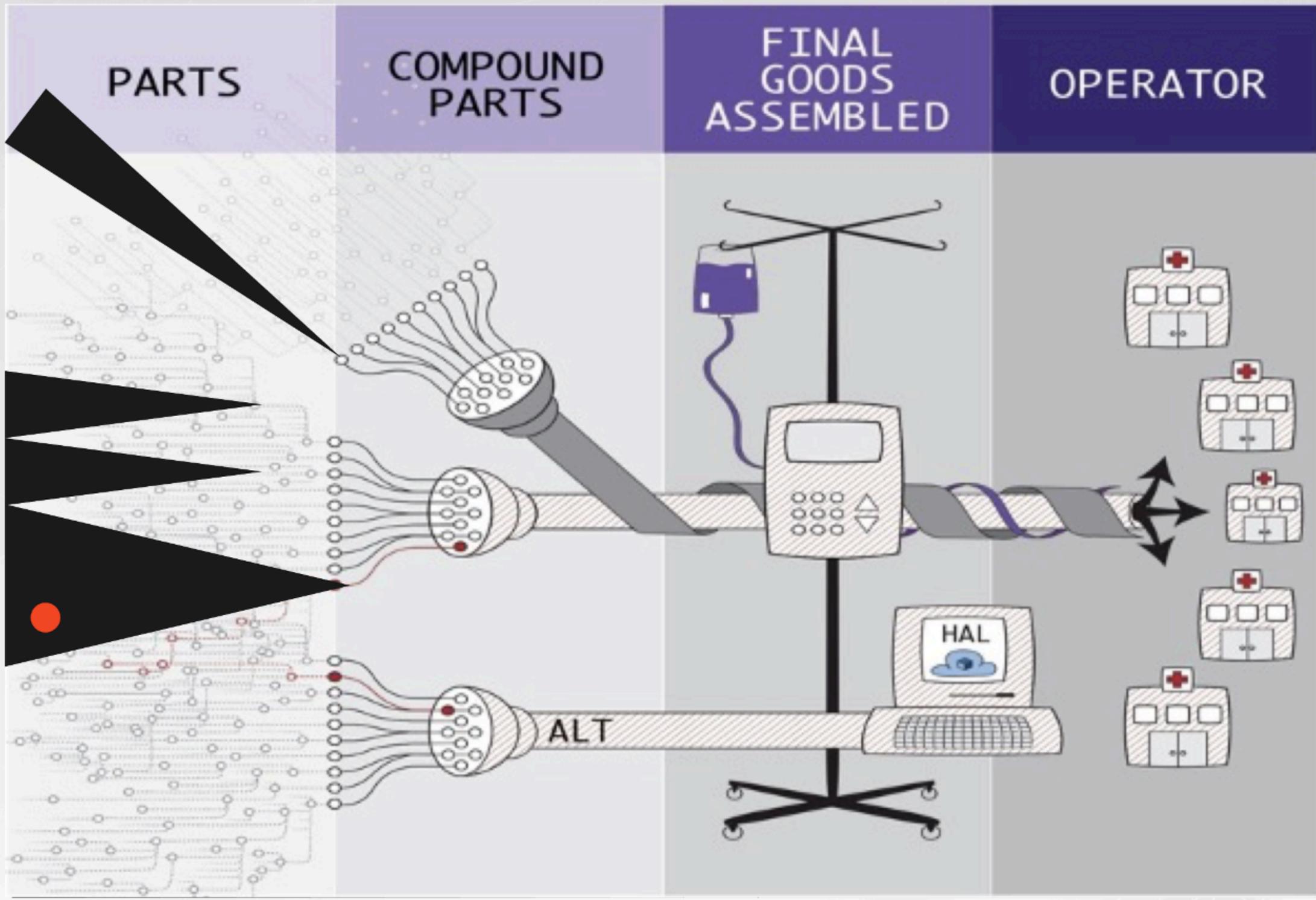
Who can
but is
unwilling to
share?

Who will share
to one degree
or another but
under NDA?

Who will
share them
publicly?

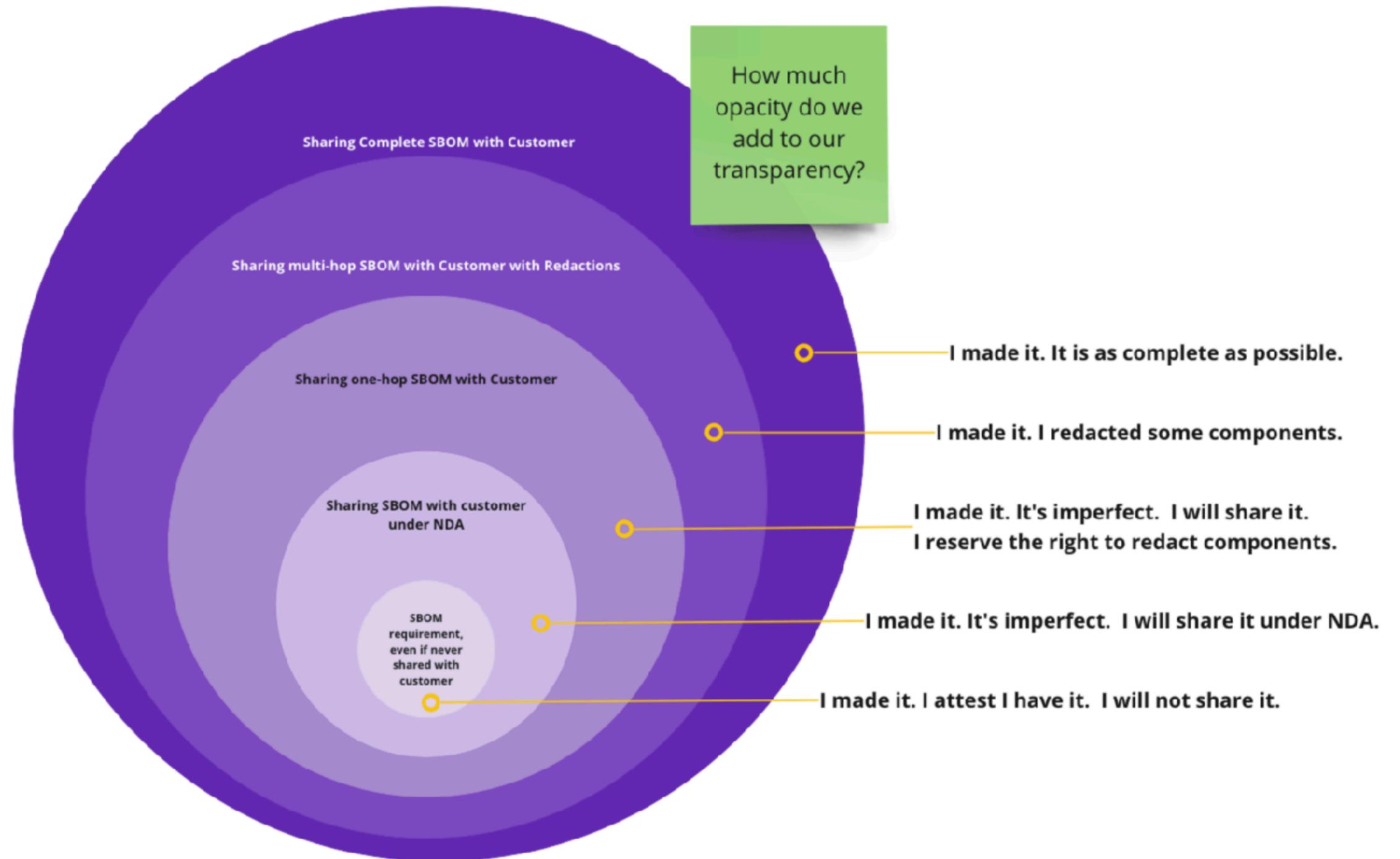






Excerpt from "The Opposite of Transparency" <https://youtu.be/qk2vo7ir1cl>

Rings of Expanding Value for SBOM



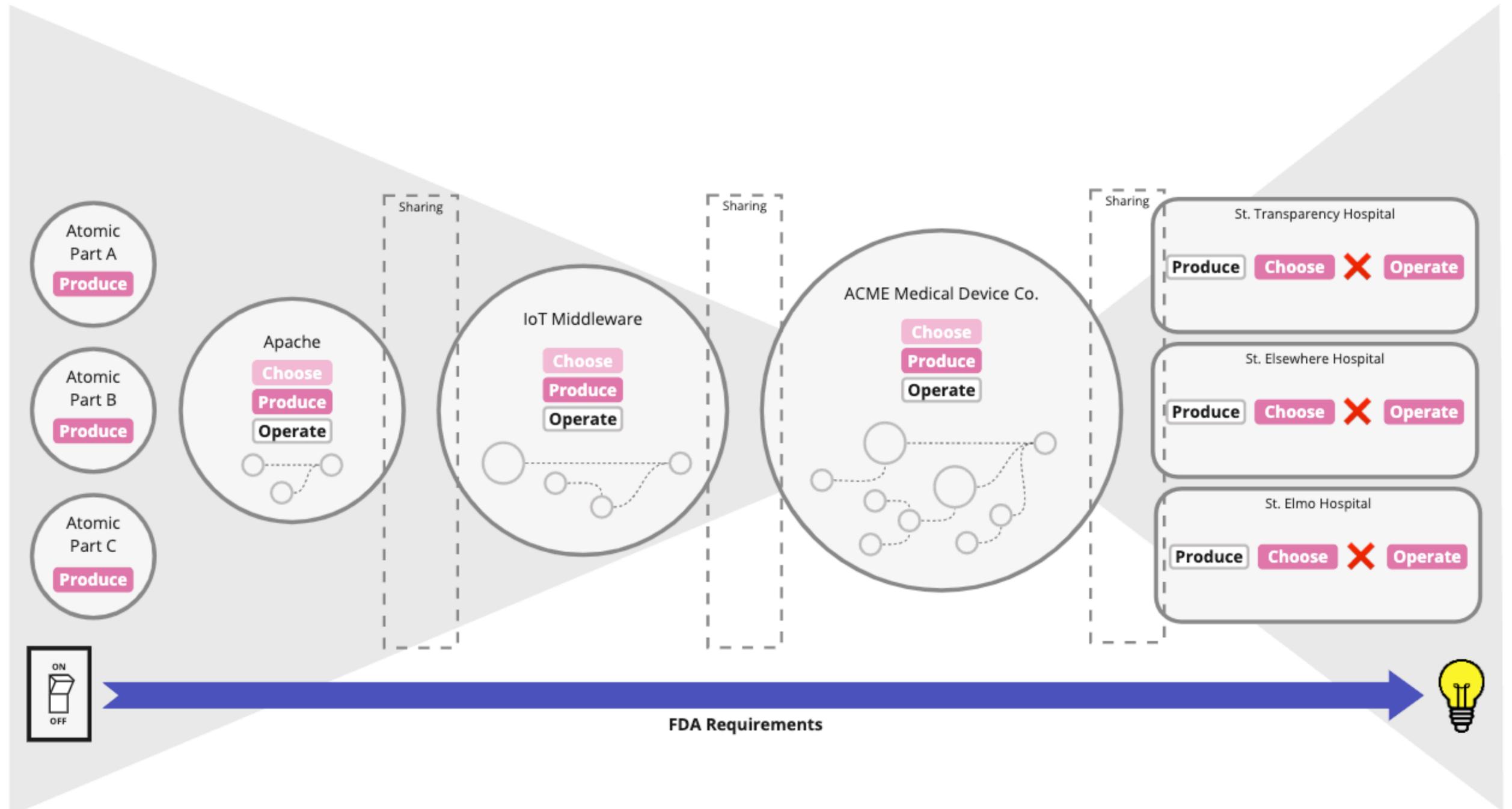
The end of CVSS?!

*KEV
EPSS
SSVC*

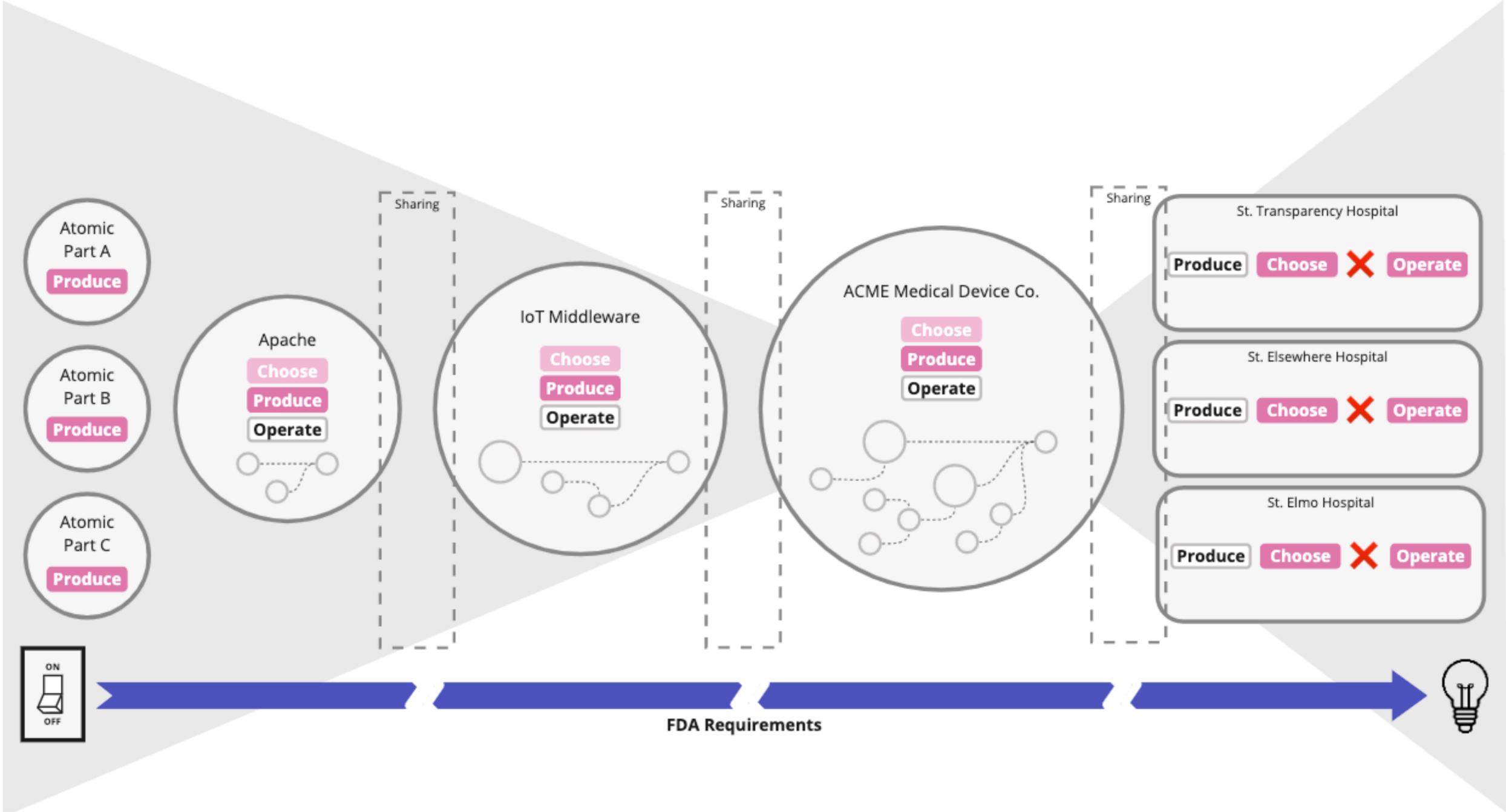
iamthecavalry.org

I AM THE
Cavalry

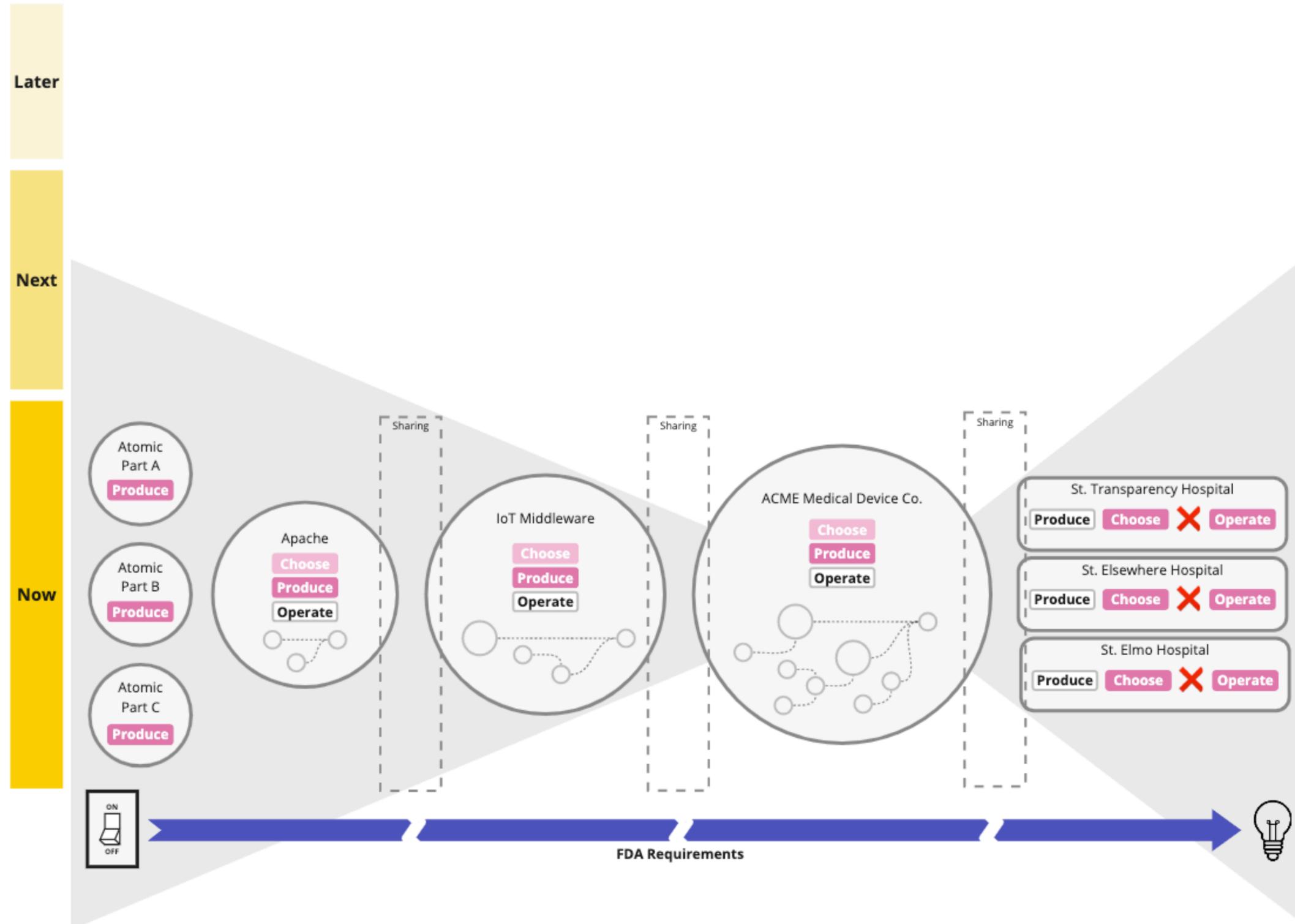
FDA USE CASE / UNIFIED FIELD THEORY



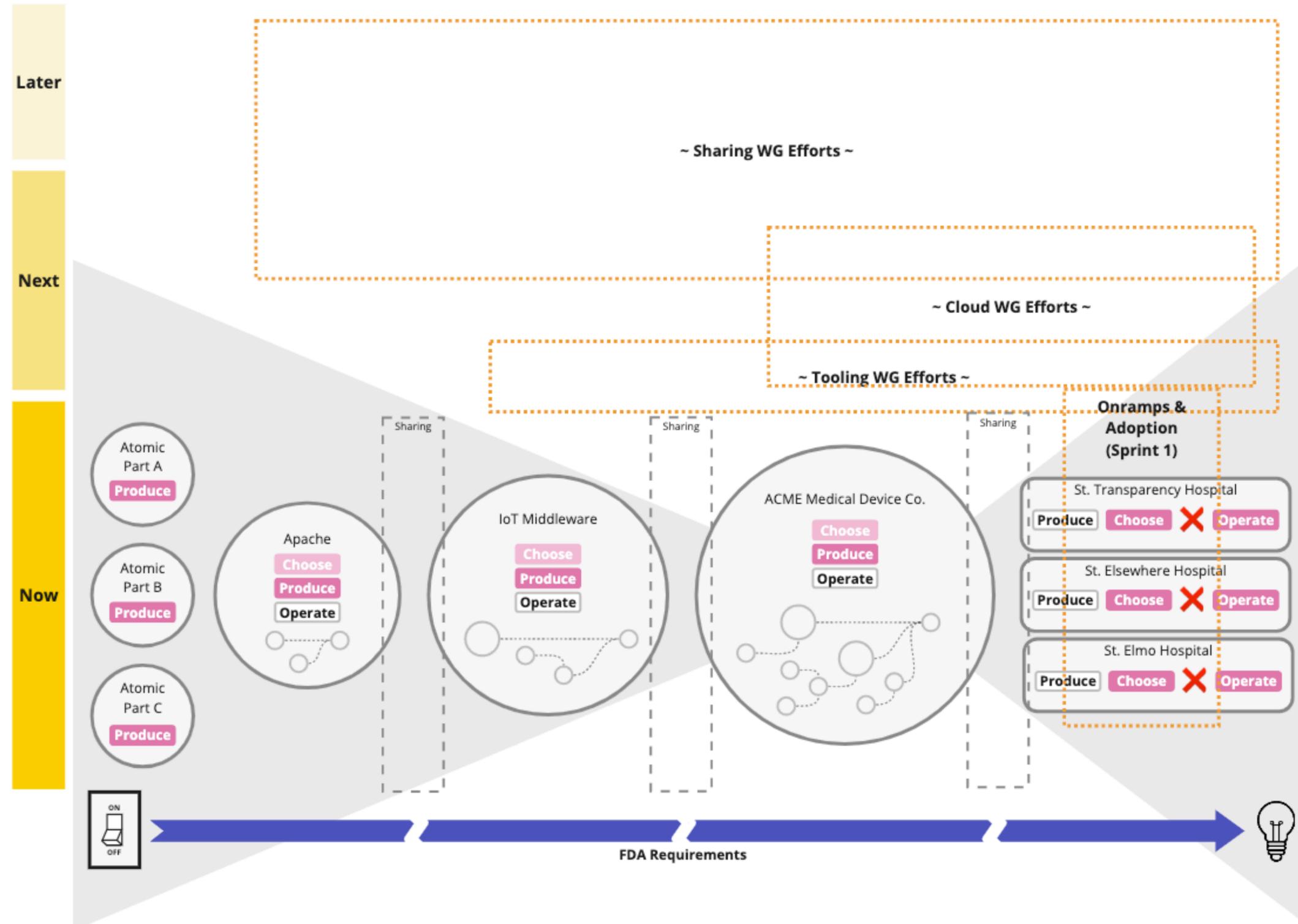
FDA USE CASE / UNIFIED FIELD THEORY



FDA USE CASE / UNIFIED FIELD THEORY



FDA USE CASE / UNIFIED FIELD THEORY



COMMUNITY ASK

- ▶ How you can help Onramps & Adoption:
 - ▶ We are seeking **new participants** and **project leads** for ongoing efforts
 - ▶ Especially Procurement/Acquisition
 - ▶ Testimonials
 - ▶ Provide feedback on the SBOM FAQ Draft for Review
 - ▶ Submit upcoming events to the SBOM Calendar
 - ▶ Introductions to creative colleagues and contributors (e.g. marketing, design, developer relations, etc.) + new industry participants
- ▶ How can Onramps & Adoption help you?
 - ▶ What other resources do you need?
 - ▶ How can we improve existing resources?
 - ▶ Do our future initiatives and priorities align with yours?



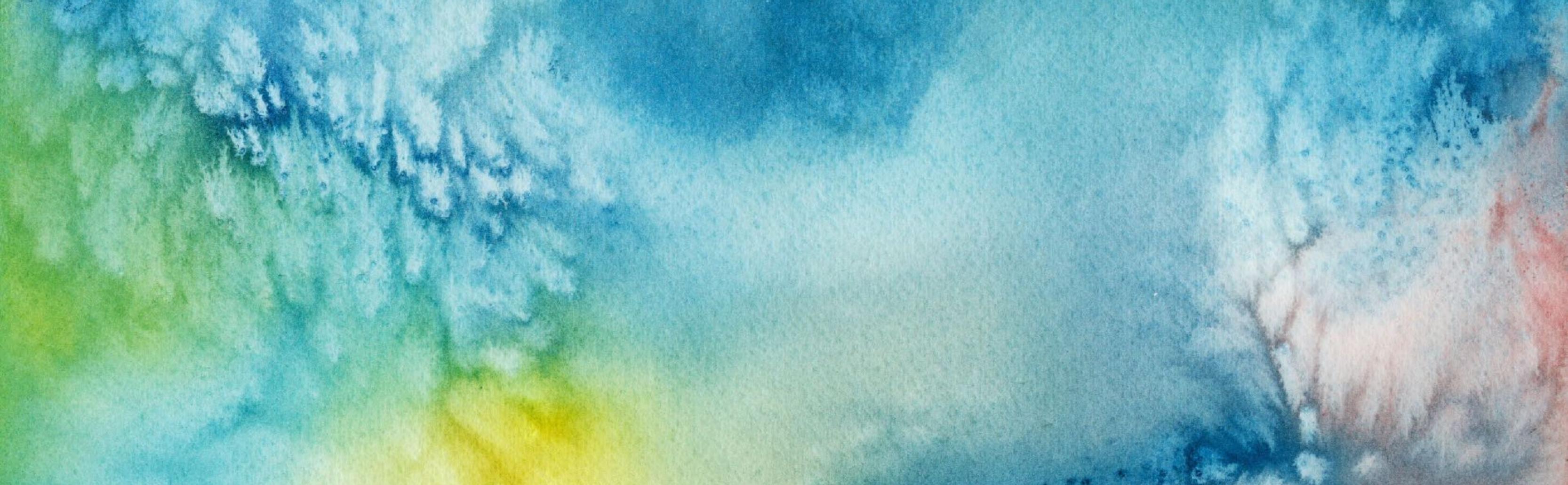
RESOURCES

- ▶ NTIA Publications
www.ntia.gov/sbom
- ▶ CISA Publications
www.cisa.gov/sbom
- ▶ FAQ
 - ▶ [Published](#)
 - ▶ [Draft for Review](#)
- ▶ SBOM Calendar
- ▶ Join our call and/or See Meeting Notes for News, Events, and Presentations

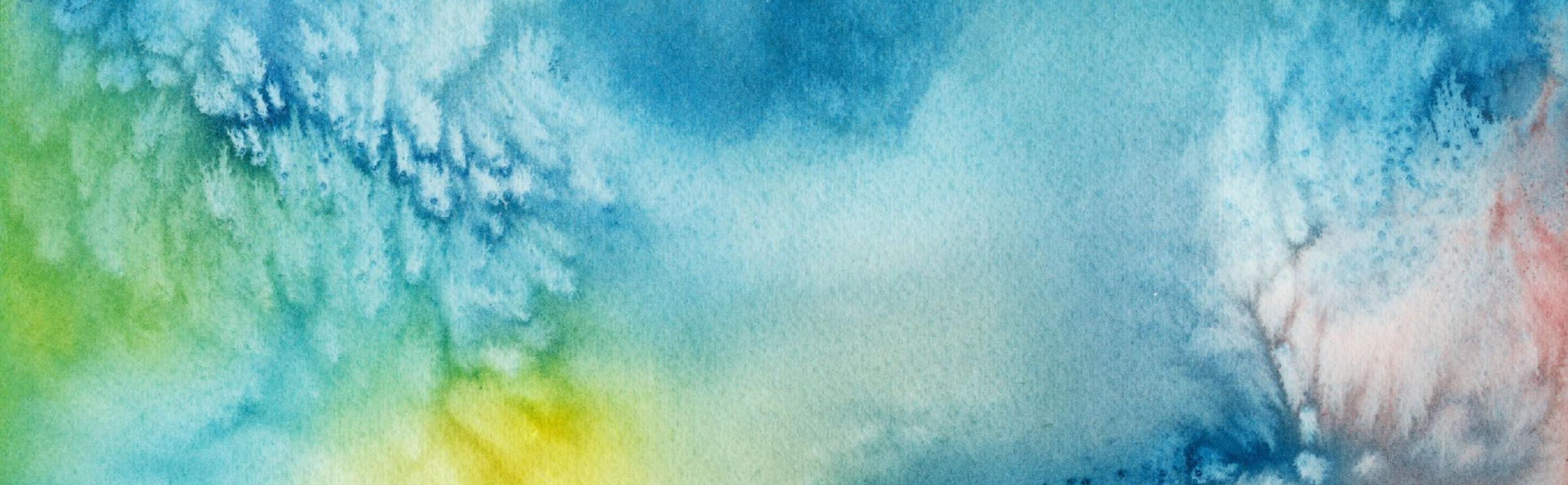


JOIN US

- Onramps & Adoption Meeting
 - Tuesdays at 12:00 PM ET
 - Join the working group:
 - Email: SBOM@cisa.dhs.gov
 - Running Meeting Notes:
 - bit.ly/sbom-onramps-meeting-notes



THANK YOU!



Q & A
