February 29, 2024

ONRAMPS & ADOPTION

Community Working Groups (CISA Phase)

Audra Hatch, Joshua Corman

ONRAMPS & ADOPTION – MISSION / VISION / GOALS

Starting Point

Sign Posts

Identify & Bridge Gaps

ONRAMPS & ADOPTION – FOCUS

General Updates

Identify Barriers

Foundational Docs

SBOM IS HERE (FOR REAL)

"The future is already here — it's just not very evenly distributed."

– William Gibson

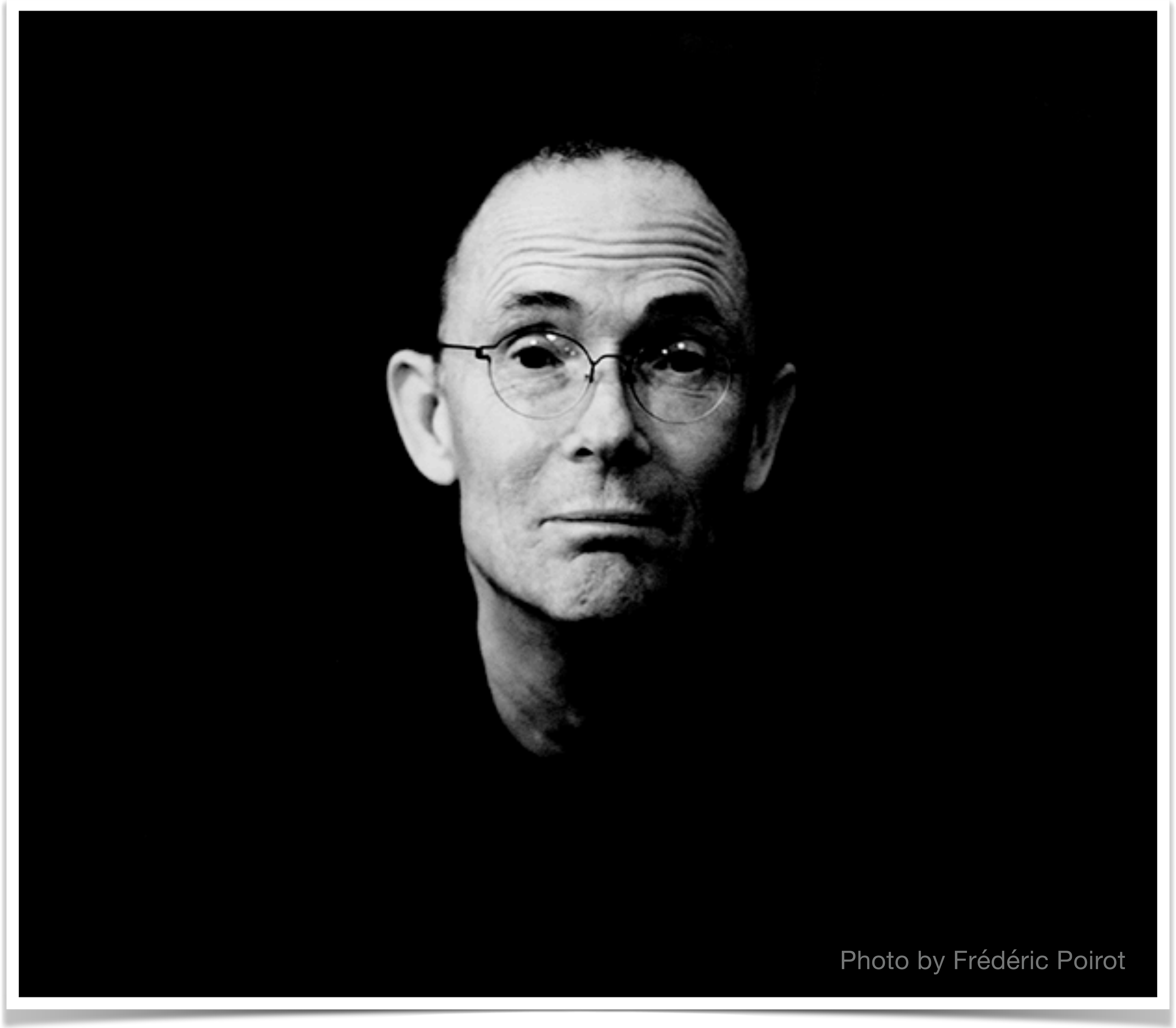
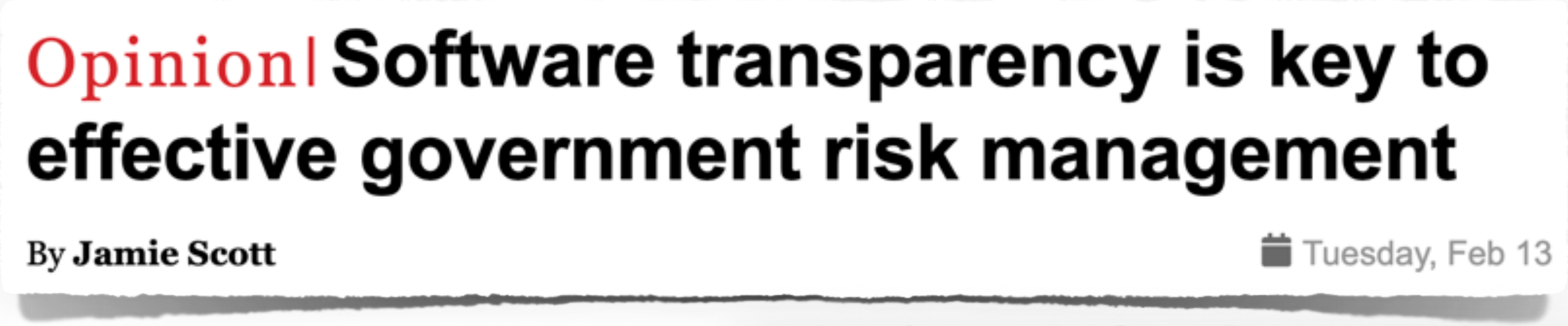


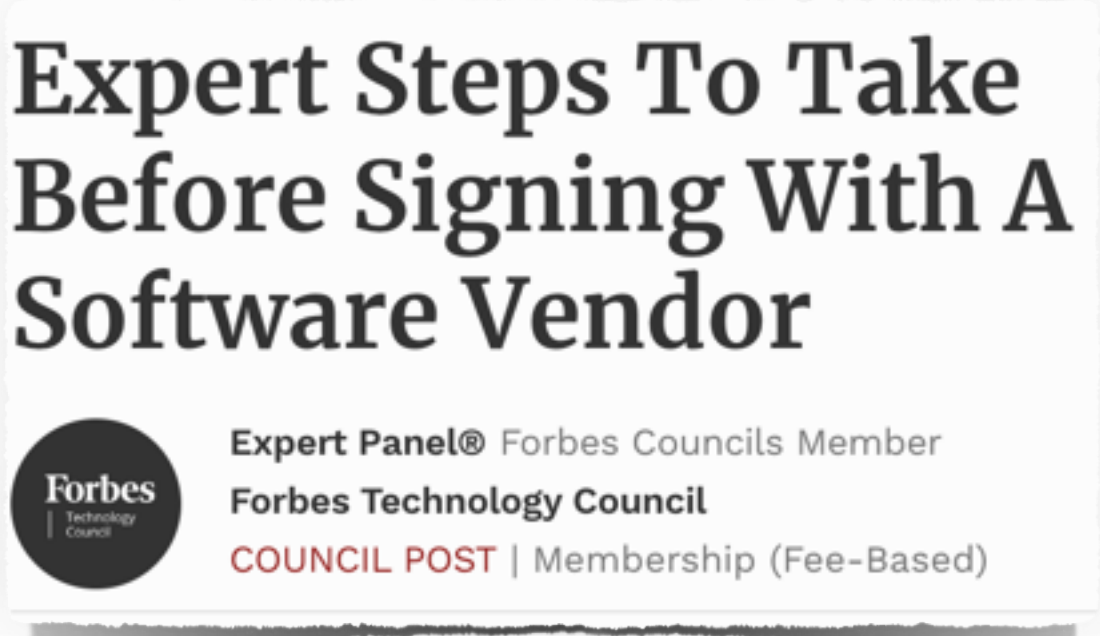
Photo by Frédéric Poirot

NEWS



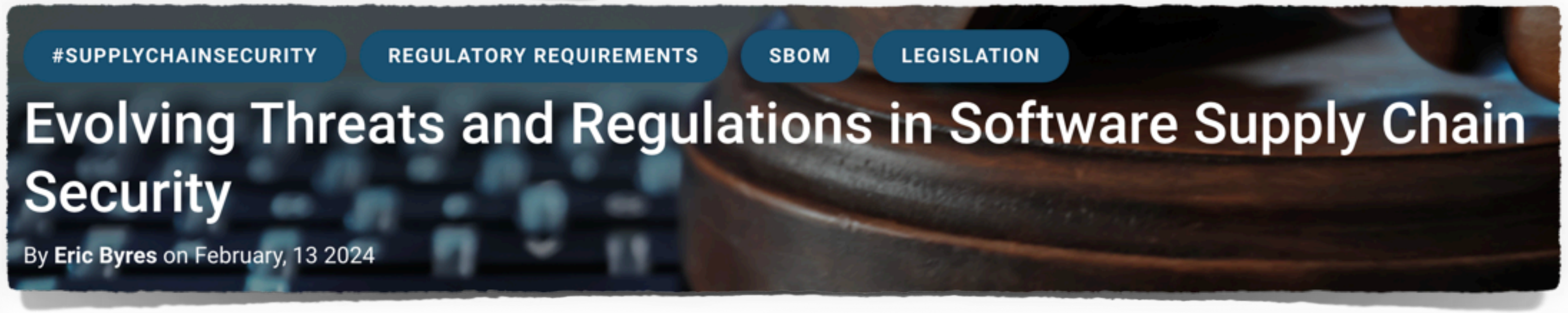
Opinion | **Software transparency is key to effective government risk management**

By **Jamie Scott** Tuesday, Feb 13



Expert Steps To Take Before Signing With A Software Vendor

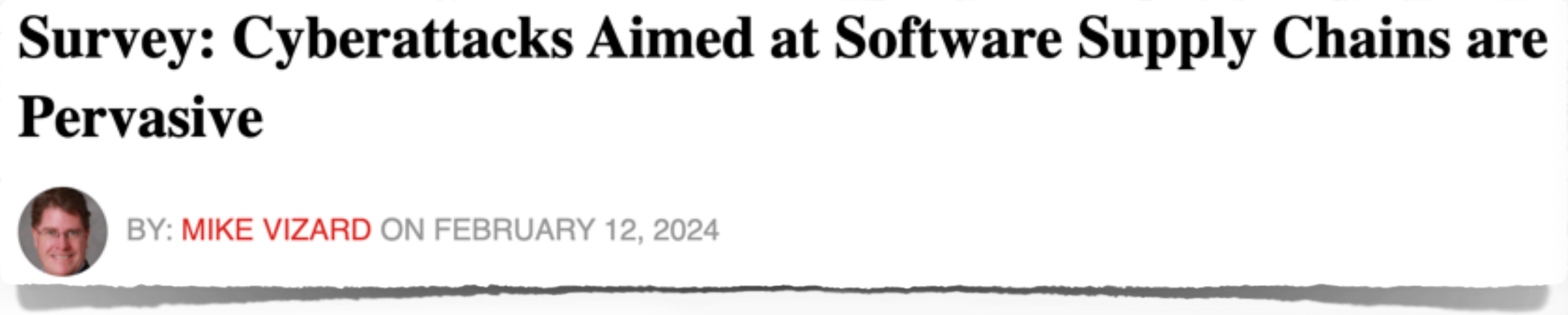
Expert Panel® Forbes Councils Member
Forbes Technology Council
COUNCIL POST | Membership (Fee-Based)



#SUPPLYCHAINSECURITY REGULATORY REQUIREMENTS SBOM LEGISLATION

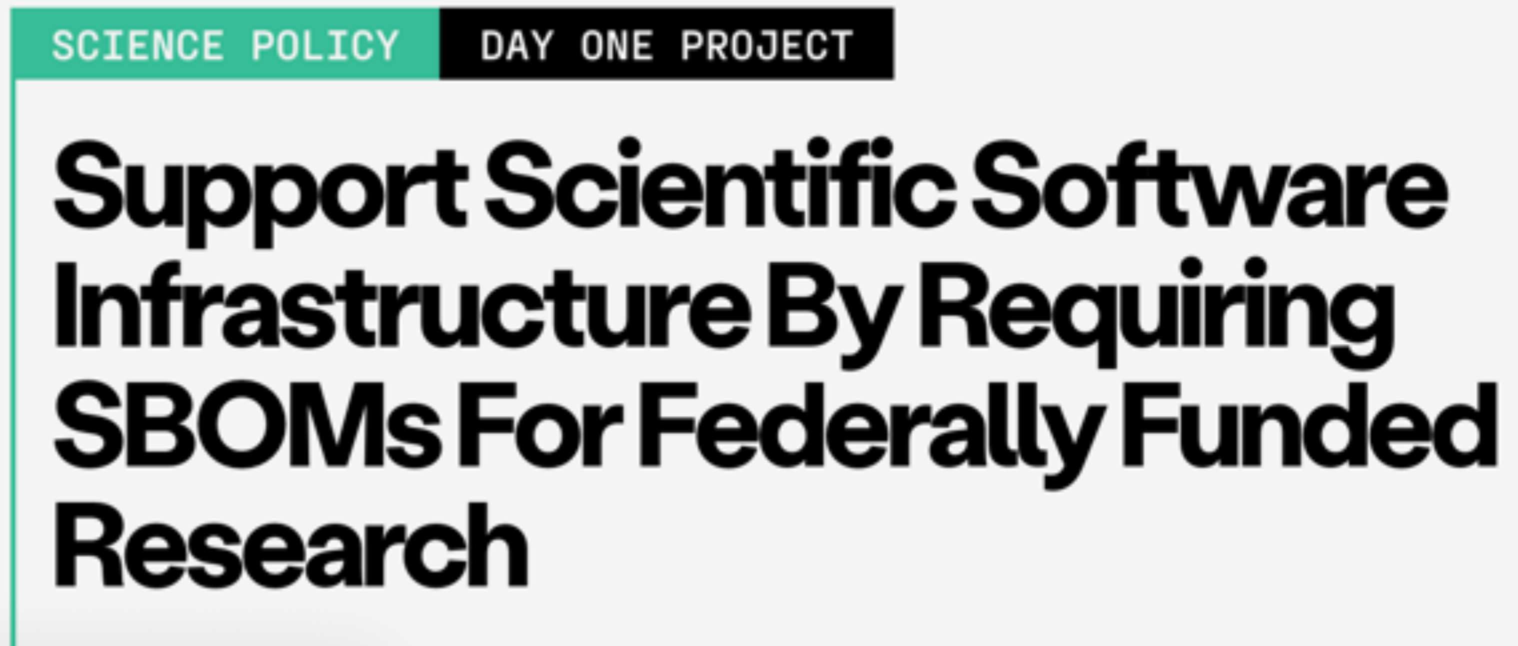
Evolving Threats and Regulations in Software Supply Chain Security

By **Eric Byres** on February, 13 2024



Survey: Cyberattacks Aimed at Software Supply Chains are Pervasive

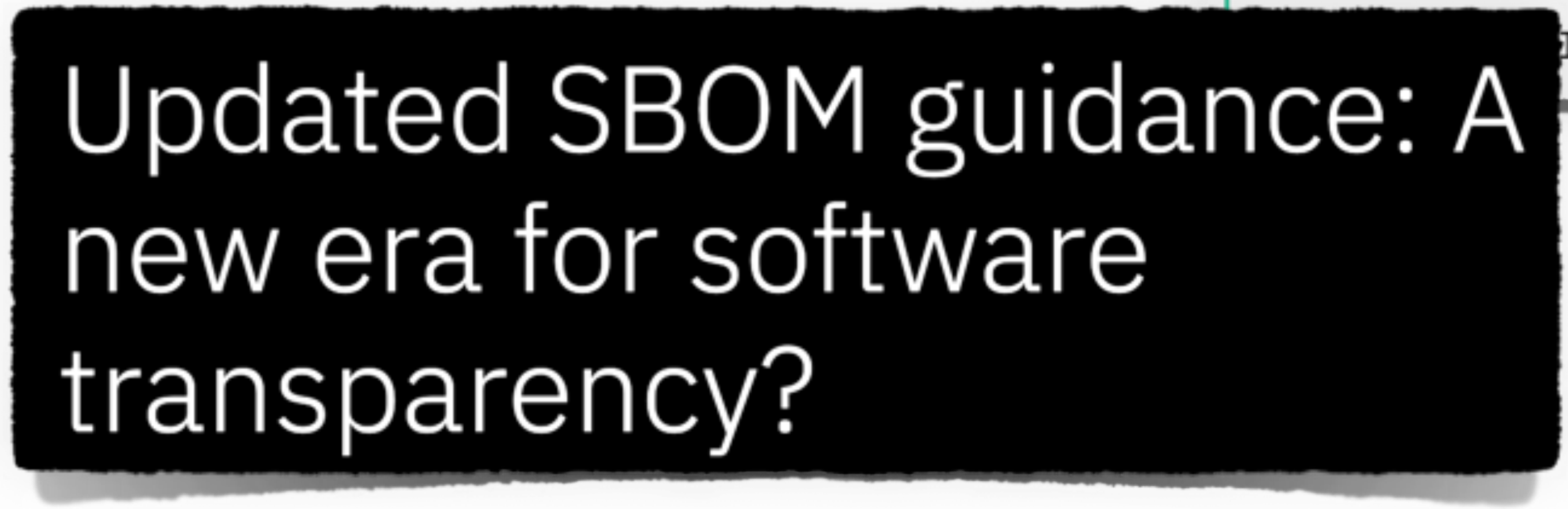
BY: MIKE VIZARD ON FEBRUARY 12, 2024



SCIENCE POLICY DAY ONE PROJECT

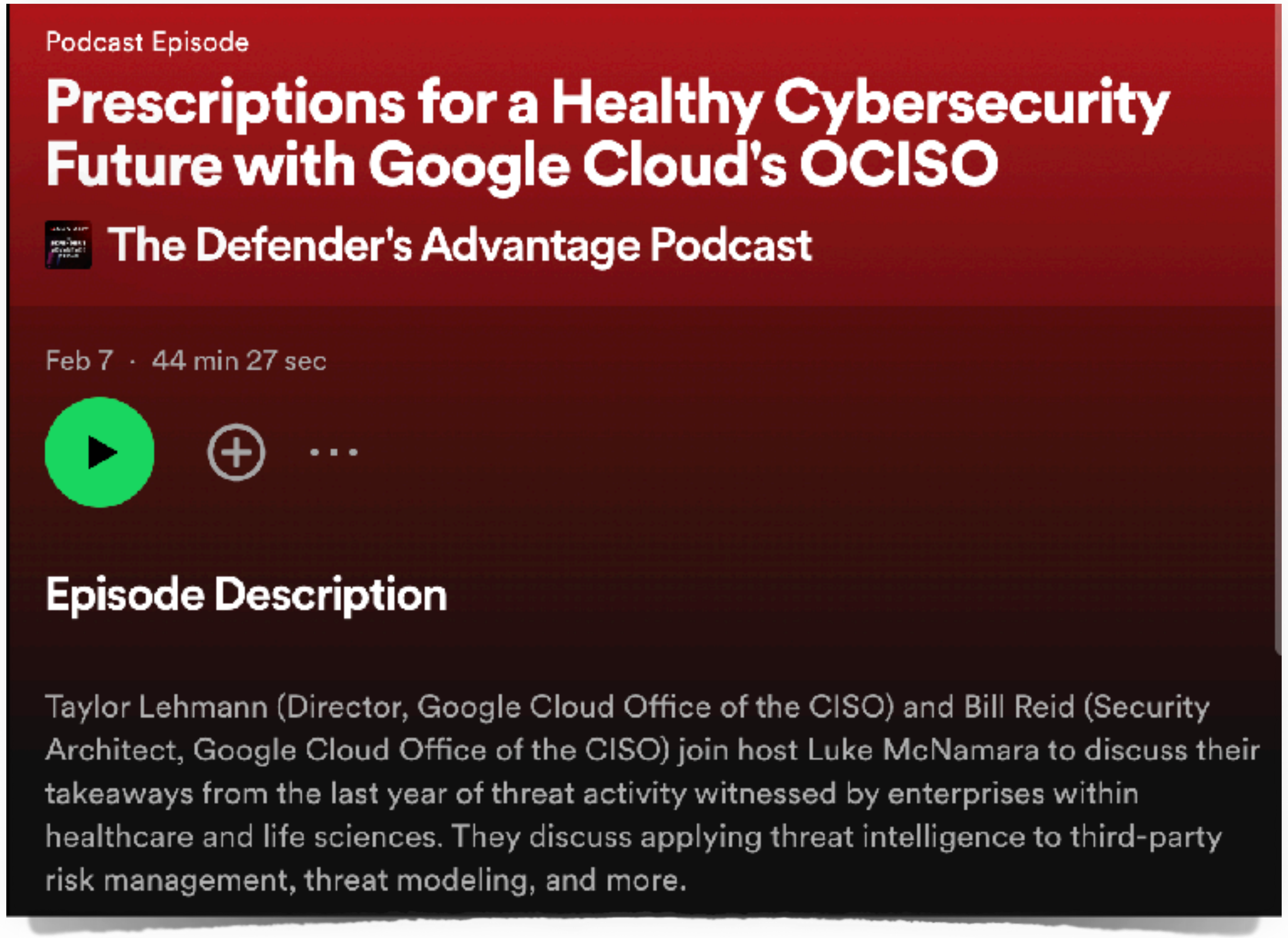
Support Scientific Software Infrastructure By Requiring SBOMs For Federally Funded Research

IN READ | TEXT BY JAMES HOWISON & KARTHIK RAM



Updated SBOM guidance: A new era for software transparency?

PODCASTS & ACADEMIC PAPERS



Podcast Episode

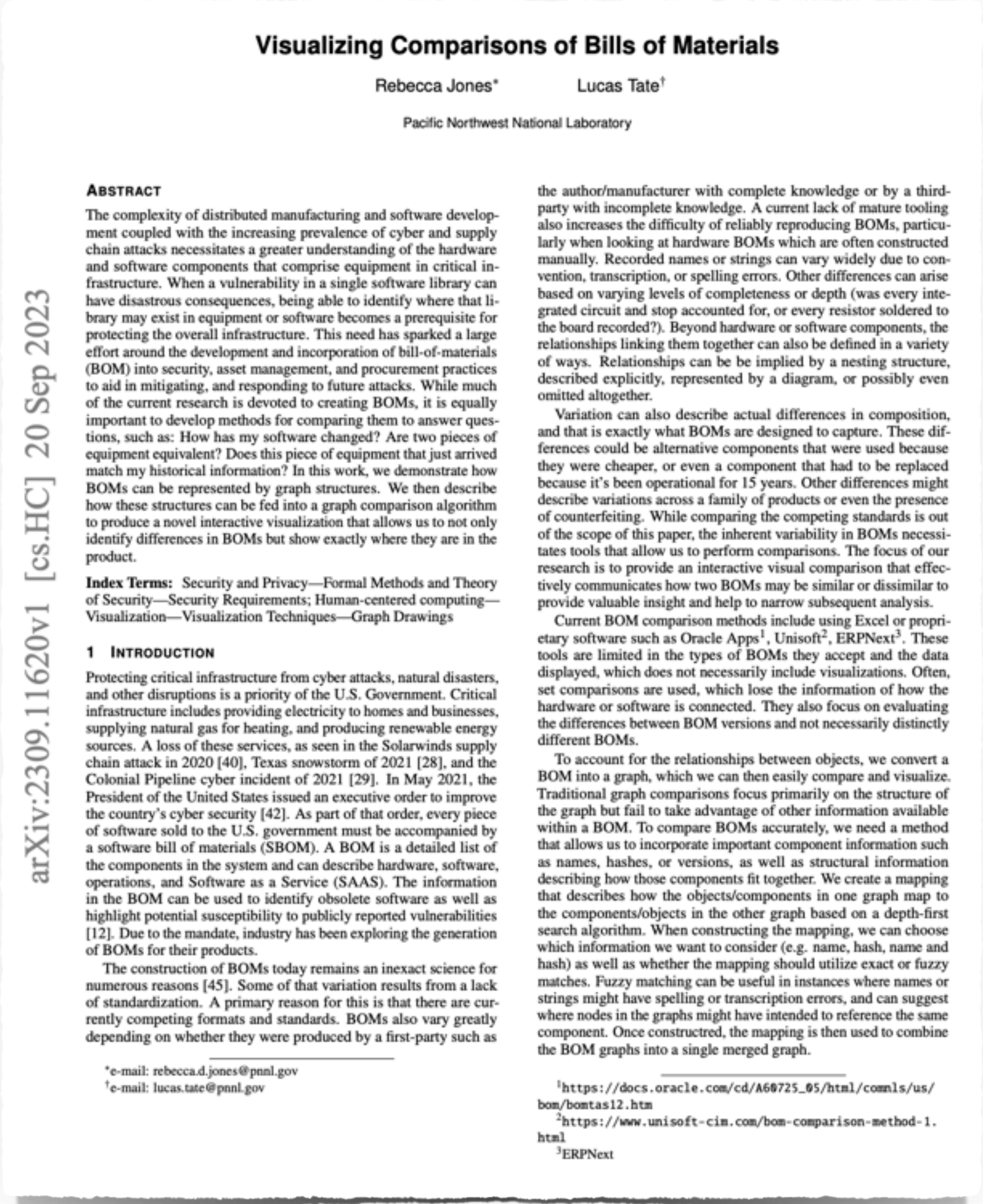
Prescriptions for a Healthy Cybersecurity Future with Google Cloud's OCISO

The Defender's Advantage Podcast

Feb 7 · 44 min 27 sec

Episode Description

Taylor Lehmann (Director, Google Cloud Office of the CISO) and Bill Reid (Security Architect, Google Cloud Office of the CISO) join host Luke McNamara to discuss their takeaways from the last year of threat activity witnessed by enterprises within healthcare and life sciences. They discuss applying threat intelligence to third-party risk management, threat modeling, and more.



Visualizing Comparisons of Bills of Materials

Rebecca Jones[*] Lucas Tate[†]

Pacific Northwest National Laboratory

arXiv:2309.11620v1 [cs.HC] 20 Sep 2023

Abstract

The complexity of distributed manufacturing and software development coupled with the increasing prevalence of cyber and supply chain attacks necessitates a greater understanding of the hardware and software components that comprise equipment in critical infrastructure. When a vulnerability in a single software library can have disastrous consequences, being able to identify where that library may exist in equipment or software becomes a prerequisite for protecting the overall infrastructure. This need has sparked a large effort around the development and incorporation of bill-of-materials (BOM) into security, asset management, and procurement practices to aid in mitigating, and responding to future attacks. While much of the current research is devoted to creating BOMs, it is equally important to develop methods for comparing them to answer questions, such as: How has my software changed? Are two pieces of equipment equivalent? Does this piece of equipment that just arrived match my historical information? In this work, we demonstrate how BOMs can be represented by graph structures. We then describe how these structures can be fed into a graph comparison algorithm to produce a novel interactive visualization that allows us to not only identify differences in BOMs but show exactly where they are in the product.

Index Terms: Security and Privacy—Formal Methods and Theory of Security—Security Requirements; Human-centered computing—Visualization—Visualization Techniques—Graph Drawings

1 Introduction

Protecting critical infrastructure from cyber attacks, natural disasters, and other disruptions is a priority of the U.S. Government. Critical infrastructure includes providing electricity to homes and businesses, supplying natural gas for heating, and producing renewable energy sources. A loss of these services, as seen in the Solarwinds supply chain attack in 2020 [40], Texas snowstorm of 2021 [28], and the Colonial Pipeline cyber incident of 2021 [29]. In May 2021, the President of the United States issued an executive order to improve the country's cyber security [42]. As part of that order, every piece of software sold to the U.S. government must be accompanied by a software bill of materials (SBOM). A BOM is a detailed list of the components in the system and can describe hardware, software, operations, and Software as a Service (SAAS). The information in the BOM can be used to identify obsolete software as well as highlight potential susceptibility to publicly reported vulnerabilities [12]. Due to the mandate, industry has been exploring the generation of BOMs for their products.

The construction of BOMs today remains an inexact science for numerous reasons [45]. Some of that variation results from a lack of standardization. A primary reason for this is that there are currently competing formats and standards. BOMs also vary greatly depending on whether they were produced by a first-party such as the author/manufacturer with complete knowledge or by a third-party with incomplete knowledge. A current lack of mature tooling also increases the difficulty of reliably reproducing BOMs, particularly when looking at hardware BOMs which are often constructed manually. Recorded names or strings can vary widely due to convention, transcription, or spelling errors. Other differences can arise based on varying levels of completeness or depth (was every integrated circuit and stop accounted for, or every resistor soldered to the board recorded?). Beyond hardware or software components, the relationships linking them together can also be defined in a variety of ways. Relationships can be be implied by a nesting structure, described explicitly, represented by a diagram, or possibly even omitted altogether.

Variation can also describe actual differences in composition, and that is exactly what BOMs are designed to capture. These differences could be alternative components that were used because they were cheaper, or even a component that had to be replaced because it's been operational for 15 years. Other differences might describe variations across a family of products or even the presence of counterfeiting. While comparing the competing standards is out of the scope of this paper, the inherent variability in BOMs necessitates tools that allow us to perform comparisons. The focus of our research is to provide an interactive visual comparison that effectively communicates how two BOMs may be similar or dissimilar to provide valuable insight and help to narrow subsequent analysis.

Current BOM comparison methods include using Excel or proprietary software such as Oracle Apps[1], Unisoft[2], ERPNext[3]. These tools are limited in the types of BOMs they accept and the data displayed, which does not necessarily include visualizations. Often, set comparisons are used, which lose the information of how the hardware or software is connected. They also focus on evaluating the differences between BOM versions and not necessarily distinctly different BOMs.

To account for the relationships between objects, we convert a BOM into a graph, which we can then easily compare and visualize. Traditional graph comparisons focus primarily on the structure of the graph but fail to take advantage of other information available within a BOM. To compare BOMs accurately, we need a method that allows us to incorporate important component information such as names, hashes, or versions, as well as structural information describing how those components fit together. We create a mapping that describes how the objects/components in one graph map to the components/objects in the other graph based on a depth-first search algorithm. When constructing the mapping, we can choose which information we want to consider (e.g. name, hash, name and hash) as well as whether the mapping should utilize exact or fuzzy matches. Fuzzy matching can be useful in instances where names or strings might have spelling or transcription errors, and can suggest where nodes in the graphs might have intended to reference the same component. Once constructred, the mapping is then used to combine the BOM graphs into a single merged graph.

[*] e-mail: rebecca.d.jones@pnnl.gov

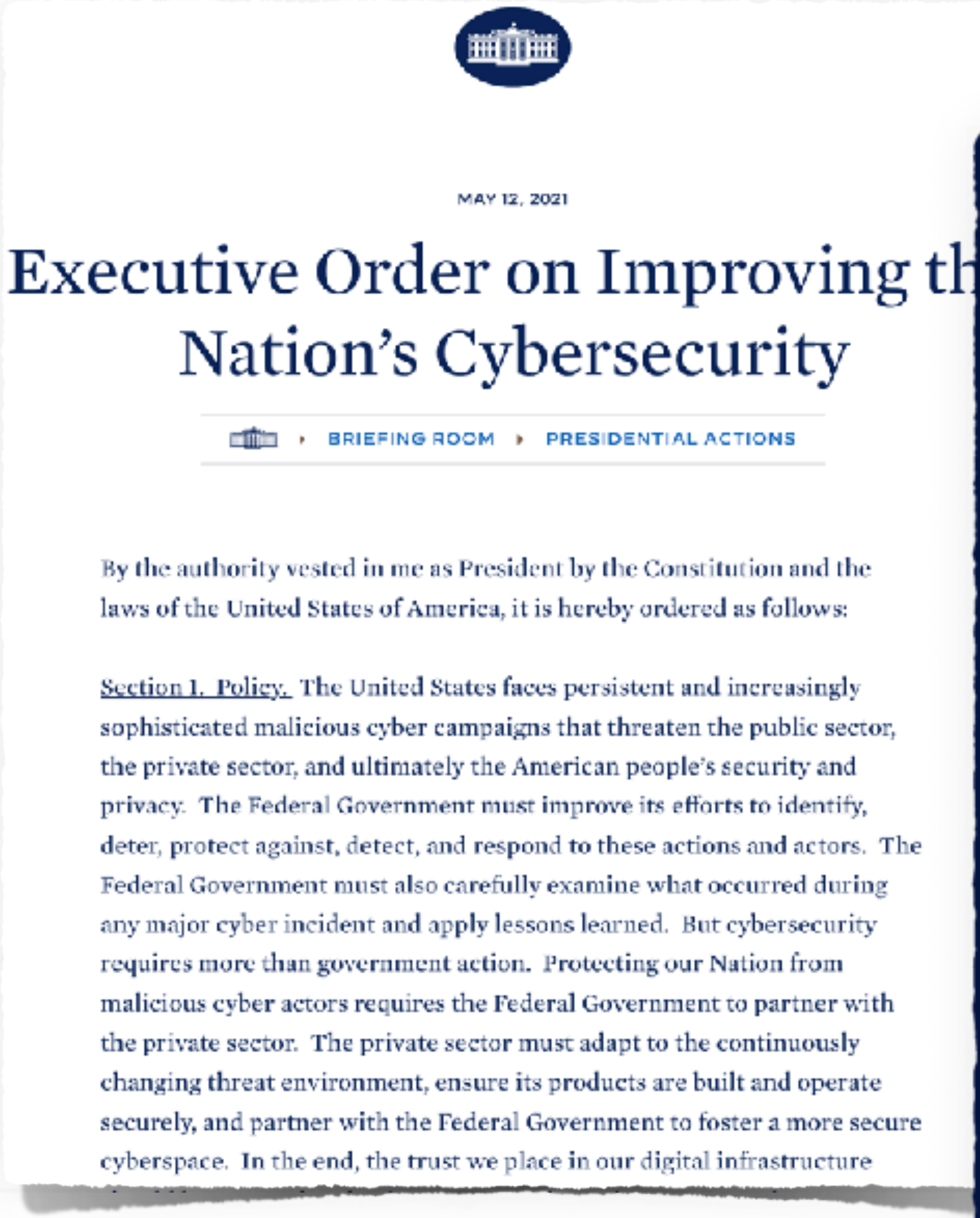
[†] e-mail: lucas.tate@pnnl.gov

[1] `https://docs.oracle.com/cd/A60725_05/html/comnls/us/bom/bomtas12.htm`

[2] `https://www.unisoft-cim.com/bom-comparison-method-1.html`

[3] ERPNext

PUBLIC POLICY



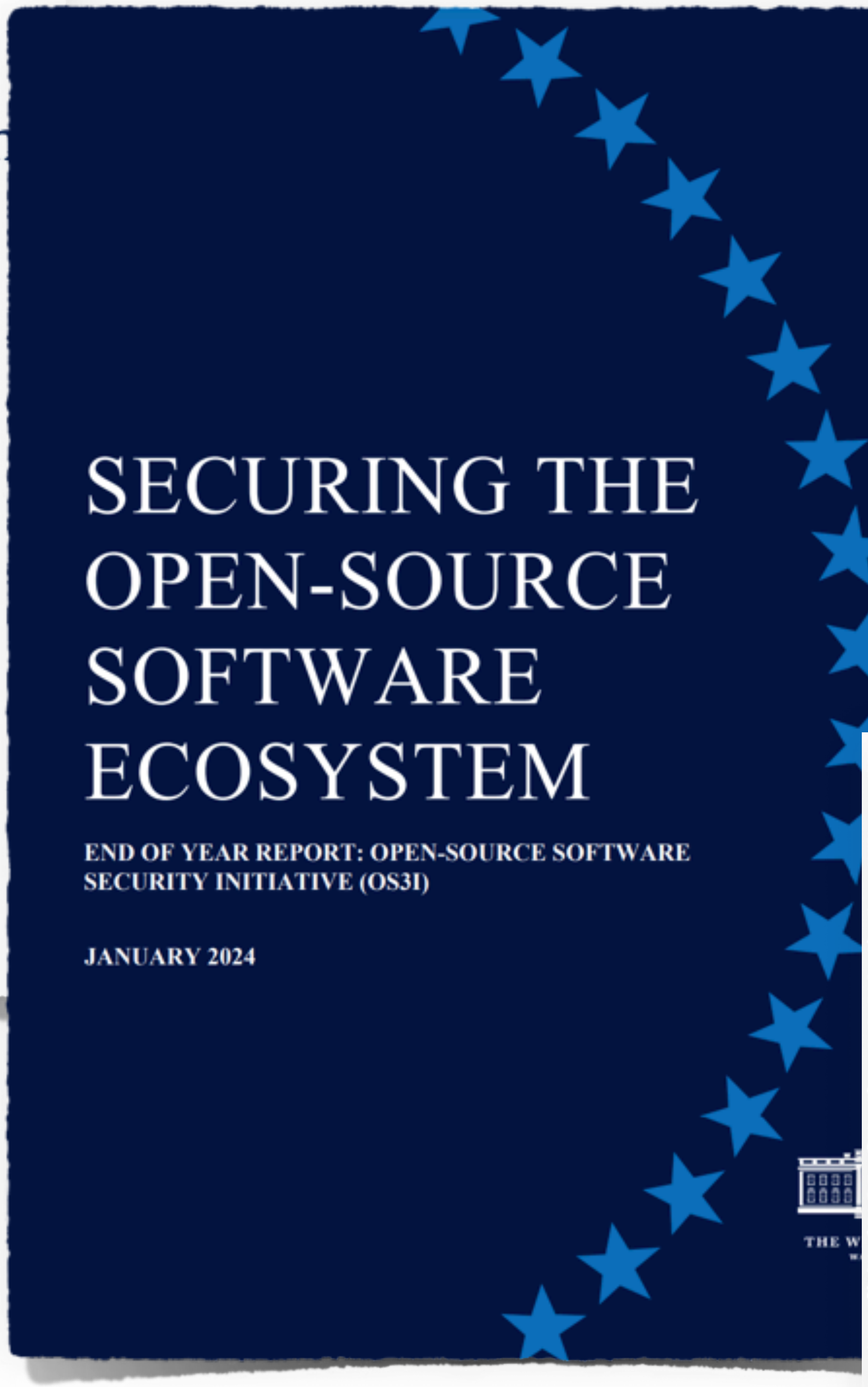
MAY 12, 2021

Executive Order on Improving th Nation’s Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure



SECURING THE OPEN-SOURCE SOFTWARE ECOSYSTEM

END OF YEAR REPORT: OPEN-SOURCE SOFTWARE SECURITY INITIATIVE (OS3I)

JANUARY 2024

Securing Operational Technology: A Deep Dive into the Water Sector

PRESENTATIONS ON PUBLICATIONS

TLP:CLEAR
National Cyber Security Centre
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre
certnz
National Cyber Security Centre

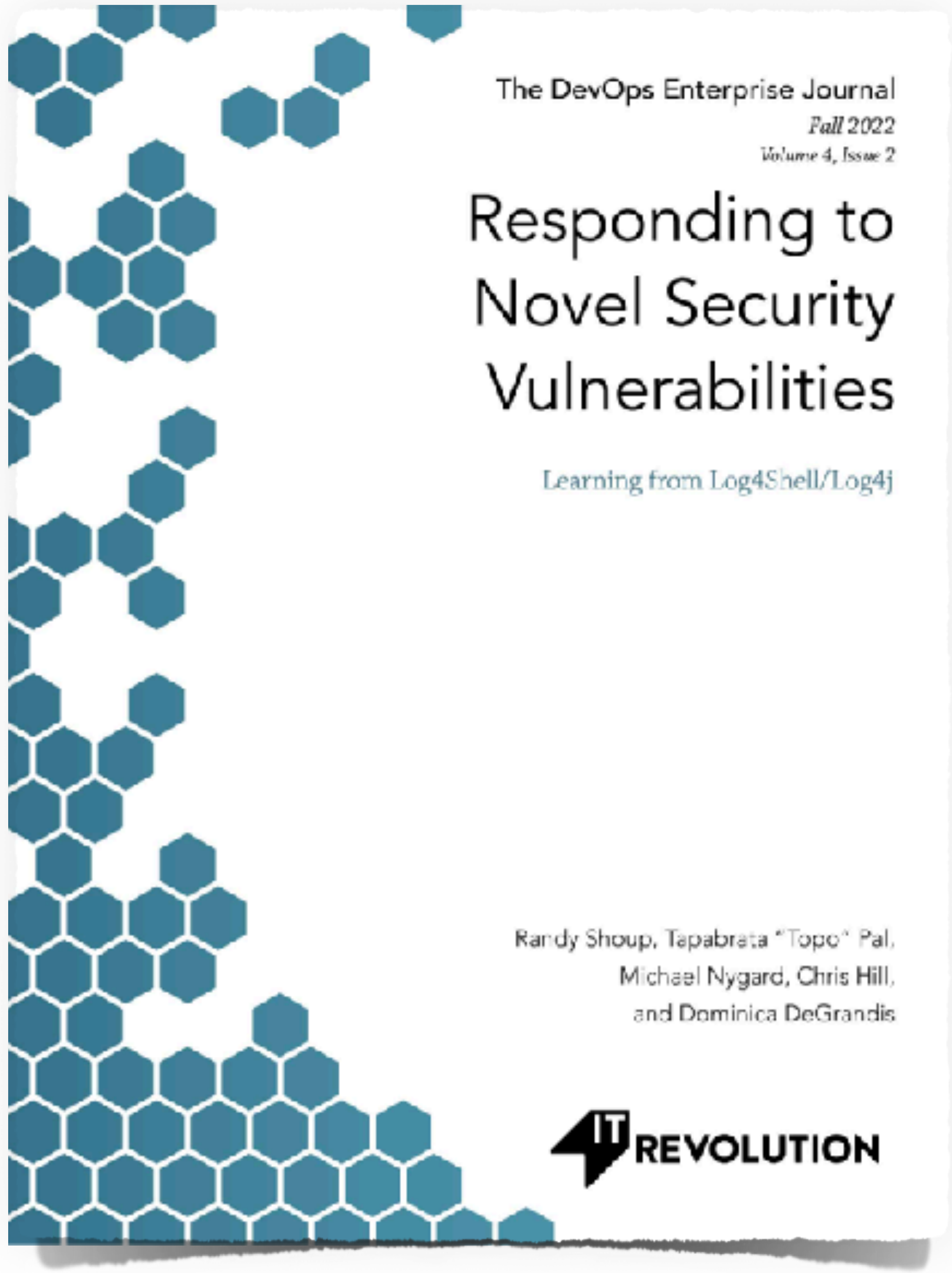
Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publication: April 13, 2023

Cybersecurity and Infrastructure Security Agency

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.



The DevOps Enterprise Journal

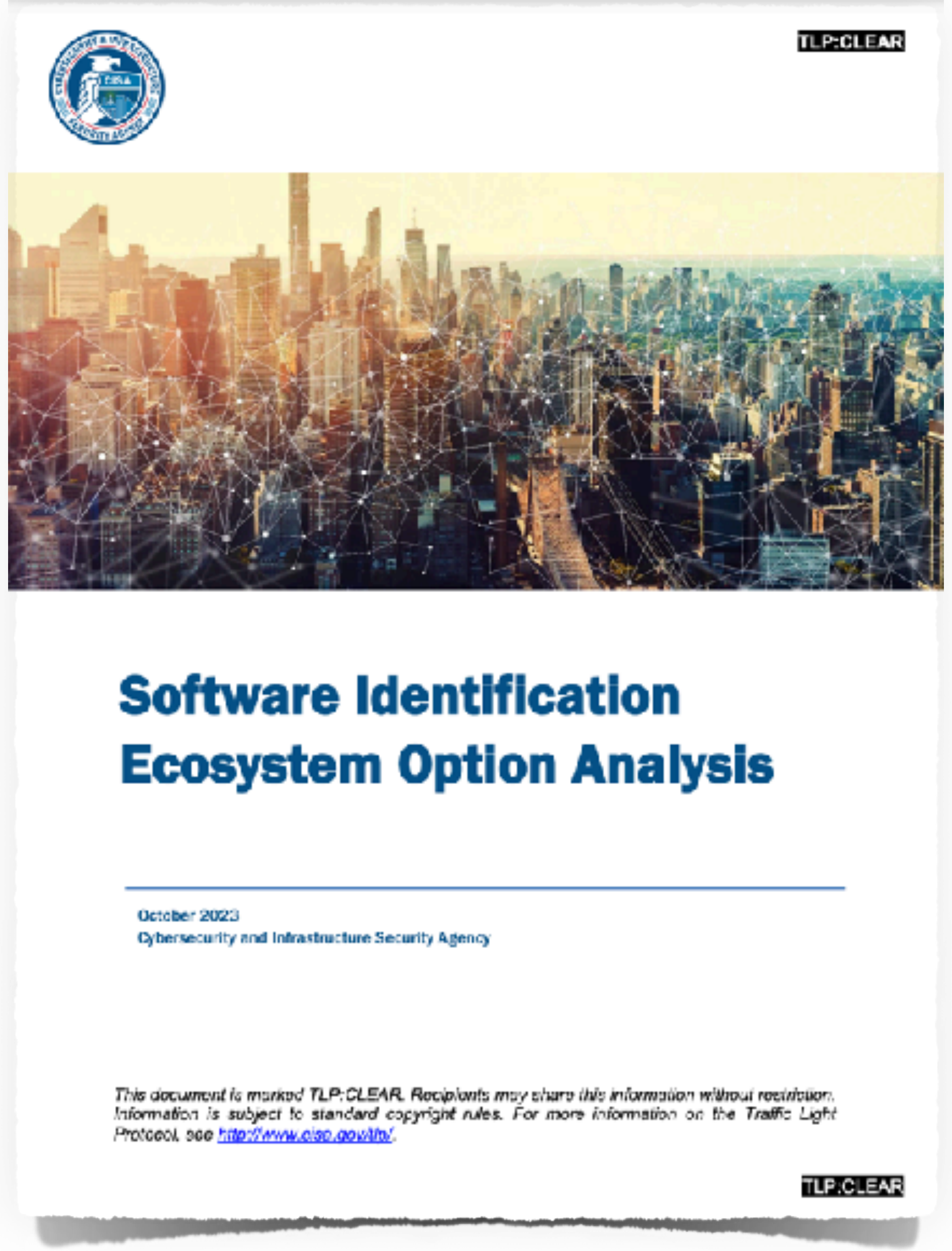
Fall 2022

Volume 4, Issue 2

Responding to Novel Security Vulnerabilities

Learning from Log4Shell/Log4j

Randy Shoup, Tapabrata "Topo" Pal,
Michael Nygard, Chris Hill,
and Dominica DeGrandis



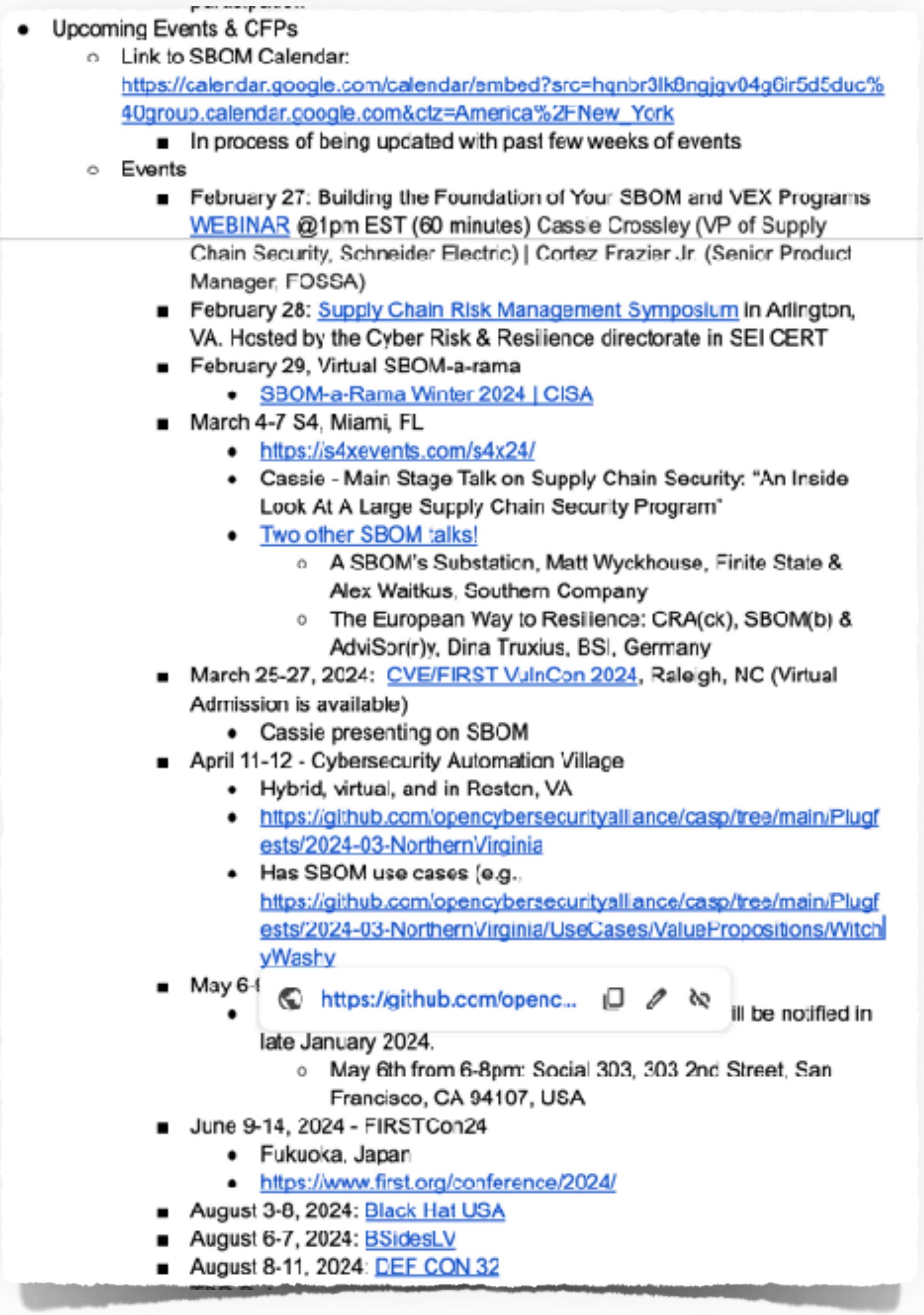
Software Identification Ecosystem Option Analysis

October 2023

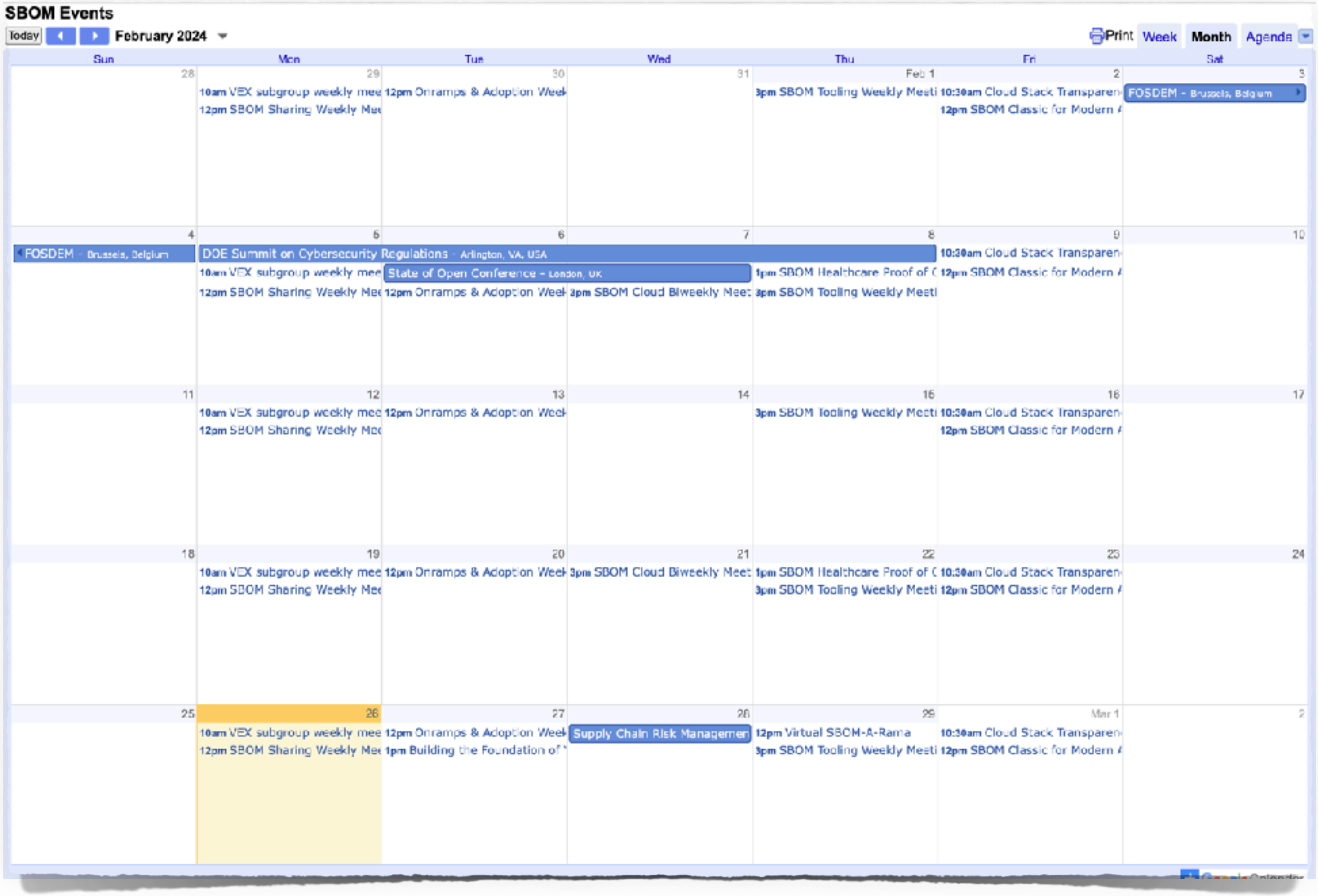
Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

EVENTS & CFPS



- Upcoming Events & CFPs
  - Link to SBOM Calendar: https://calendar.google.com/calendar/embed?src=hqnbr3lk8ngjgv04g6ir5d5duc%40group.calendar.google.com&ctz=America%2FNew_York
    - In process of being updated with past few weeks of events
  - Events
    - February 27: Building the Foundation of Your SBOM and VEX Programs WEBINAR @1pm EST (60 minutes) Cassie Crossley (VP of Supply Chain Security, Schneider Electric) | Cortez Frazier Jr. (Senior Product Manager, FOSSA)
    - February 28: Supply Chain Risk Management Symposium in Arlington, VA. Hosted by the Cyber Risk & Resilience directorate in SEI CERT
    - February 29, Virtual SBOM-a-rama
      - SBOM-a-Rama Winter 2024 | CISA
    - March 4-7 S4, Miami, FL
      - https://s4xevents.com/s4x24/
      - Cassie - Main Stage Talk on Supply Chain Security: "An Inside Look At A Large Supply Chain Security Program"
      - Two other SBOM talks!
        - A SBOM's Substation, Matt Wyckhouse, Finite State & Alex Waitkus, Southern Company
        - The European Way to Resilience: CRA(ck), SBOM(b) & AdviSor(r)y, Dina Truxius, BSI, Germany
    - March 25-27, 2024: CVE/FIRST VulnCon 2024, Raleigh, NC (Virtual Admission is available)
      - Cassie presenting on SBOM
    - April 11-12 - Cybersecurity Automation Village
      - Hybrid, virtual, and in Reston, VA
      - https://github.com/opencybersecurityalliance/casp/tree/main/Plugfests/2024-03-NorthernVirginia
      - Has SBOM use cases (e.g., https://github.com/opencybersecurityalliance/casp/tree/main/Plugfests/2024-03-NorthernVirginia/UseCases/ValuePropositions/WitchyWashy
    - May 6-
      - https://github.com/openc... ill be notified in late January 2024.
        - May 6th from 6-8pm: Social 303, 303 2nd Street, San Francisco, CA 94107, USA
    - June 9-14, 2024 - FIRSTCon24
      - Fukuoka, Japan
      - https://www.first.org/conference/2024/
    - August 3-8, 2024: Black Hat USA
    - August 6-7, 2024: BSidesLV
    - August 8-11, 2024: DEF CON 32



SBOM Events

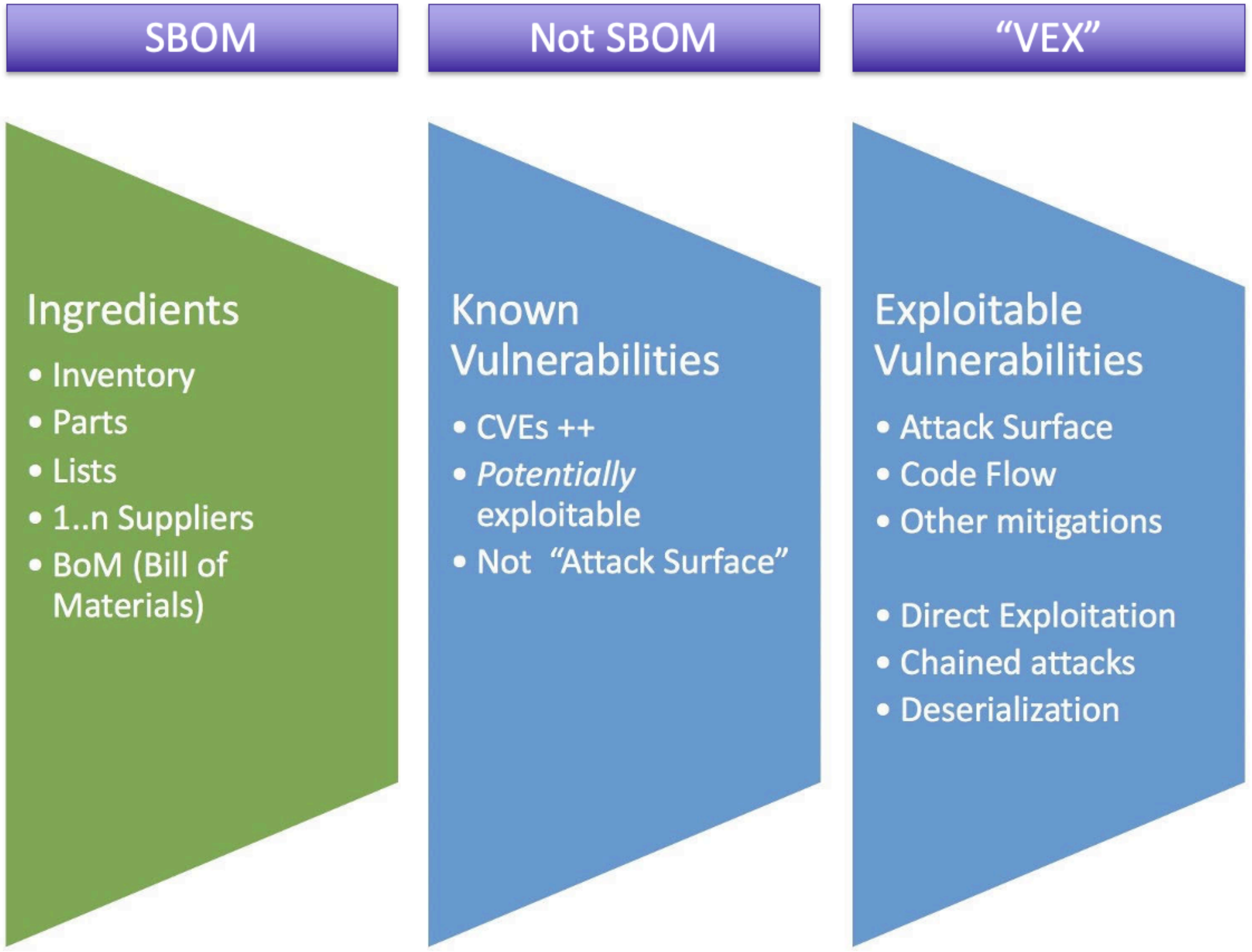
Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29 10am VEX subgroup weekly mee 12pm SBOM Sharing Weekly Mee	30 12pm Onramps & Adoption Week	31	Feb 1 3pm SBOM Tooling Weekly Meeti	2 10:30am Cloud Stack Transparen 12pm SBOM Classic for Modern A	3 FOSDEM - Brussels, Belgium
4 FOSDEM - Brussels, Belgium	5 DOE Summit on Cybersecurity Regulations - Arlington, VA, USA 10am VEX subgroup weekly mee 12pm SBOM Sharing Weekly Mee	6 State of Open Conference - London, UK 12pm Onramps & Adoption Week	7 3pm SBOM Cloud Biweekly Meet	8 1pm SBOM Healthcare Proof of C 3pm SBOM Tooling Weekly Meeti	9 10:30am Cloud Stack Transparen 12pm SBOM Classic for Modern A	10
11	12 10am VEX subgroup weekly mee 12pm SBOM Sharing Weekly Mee	13 12pm Onramps & Adoption Week	14	15 3pm SBOM Tooling Weekly Meeti	16 10:30am Cloud Stack Transparen 12pm SBOM Classic for Modern A	17
18	19 10am VEX subgroup weekly mee 12pm SBOM Sharing Weekly Mee	20 12pm Onramps & Adoption Week	21 3pm SBOM Cloud Biweekly Meet	22 1pm SBOM Healthcare Proof of C 3pm SBOM Tooling Weekly Meeti	23 10:30am Cloud Stack Transparen 12pm SBOM Classic for Modern A	24
25	26 10am VEX subgroup weekly mee 12pm SBOM Sharing Weekly Mee	27 12pm Onramps & Adoption Week 1pm Building the Foundation of Y	28 Supply Chain Risk Managemen	29 12pm Virtual SBOM-A-Rama 3pm SBOM Tooling Weekly Meeti	Mar 1 10:30am Cloud Stack Transparen 12pm SBOM Classic for Modern A	2

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

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

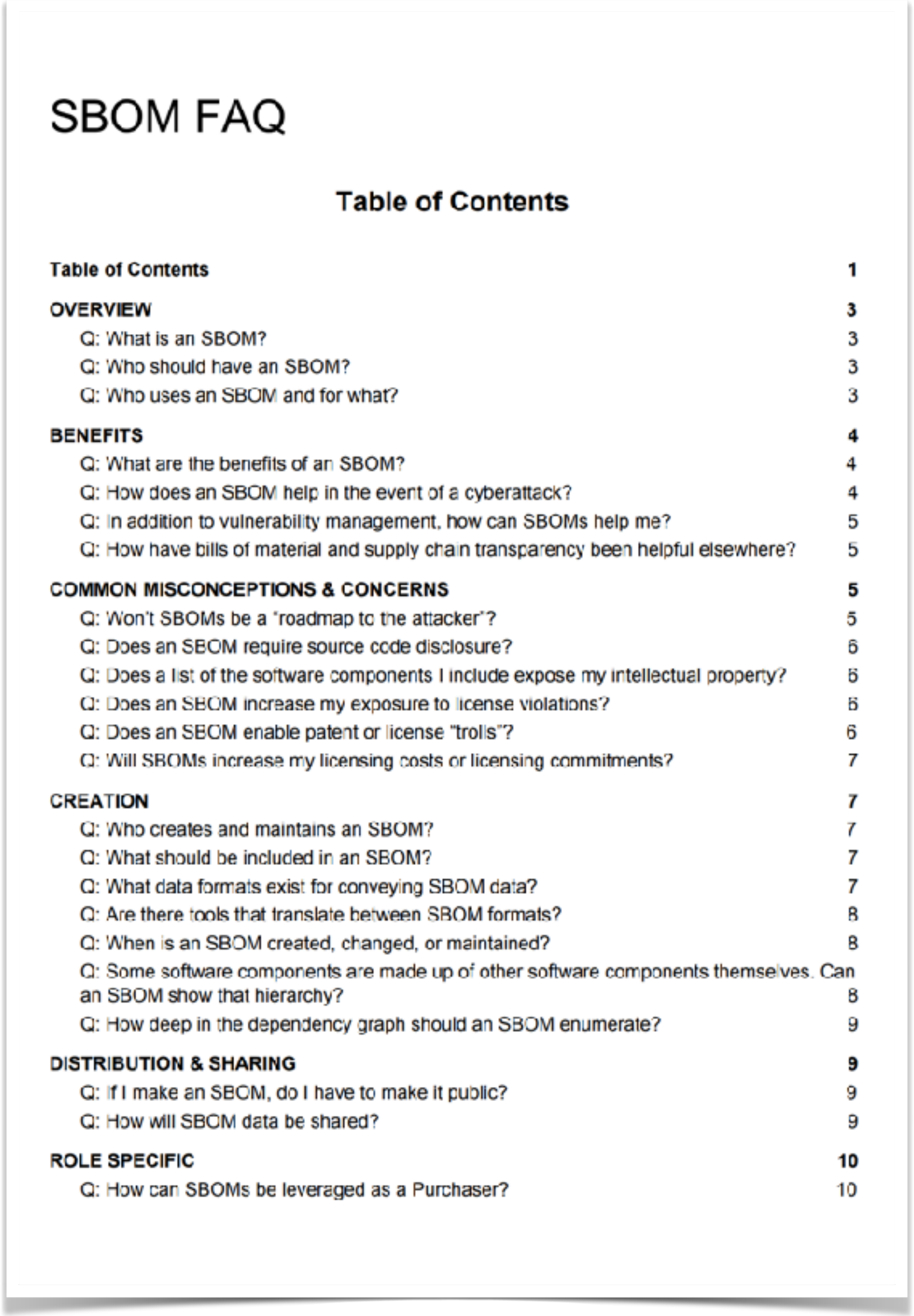
- Direct Exploitation
- Chained attacks
- Deserialization

IMG SRC: Josh Corman NTIA.gov 2018

Excerpt from "The Opposite of Transparency" https://youtu.be/qk2vo7ir1cI

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



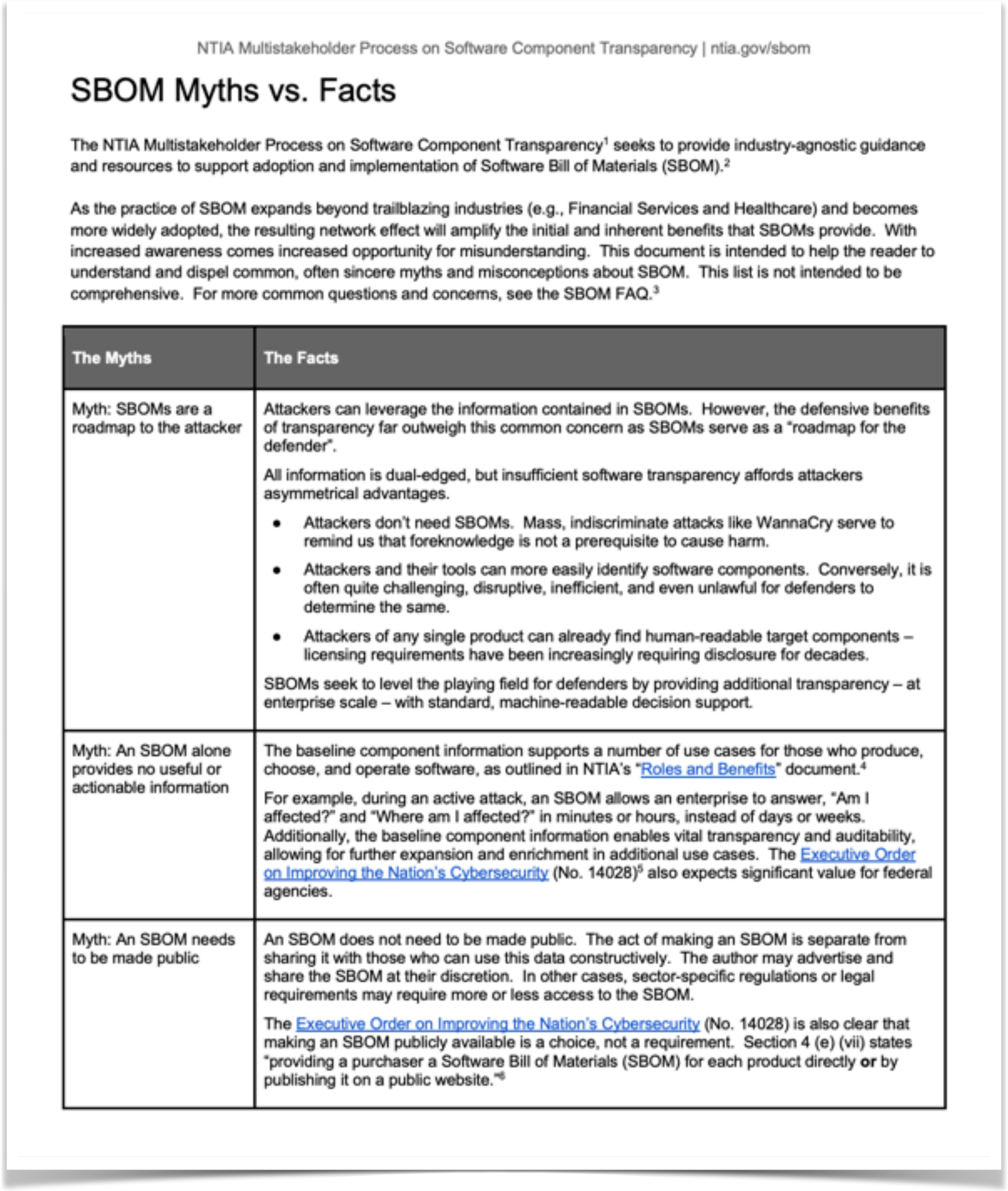
SBOM FAQ

Table of Contents

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

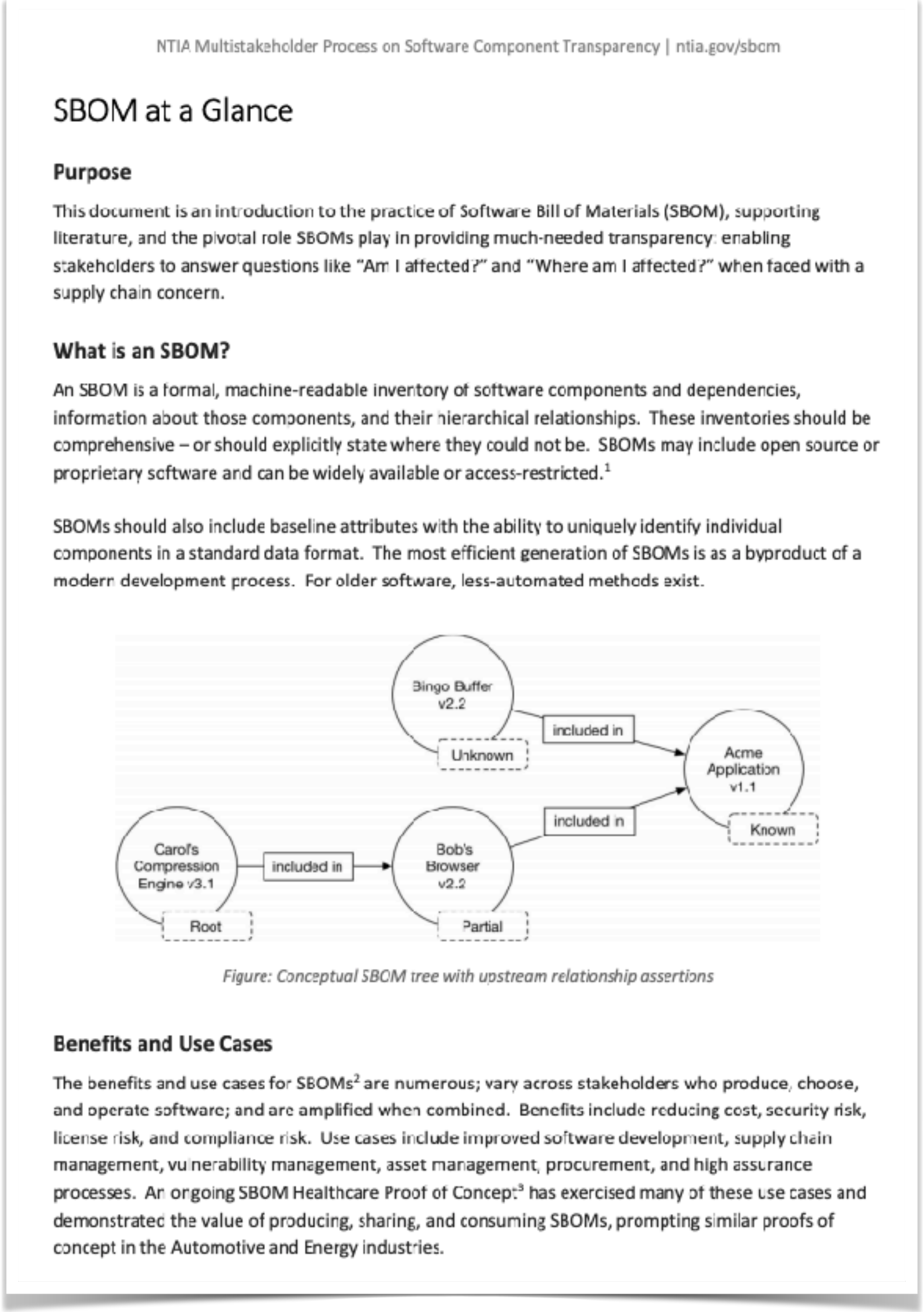
The NTIA Multistakeholder Process on Software Component Transparency[1] seeks to provide industry-agnostic guidance and resources to support adoption and implementation of Software Bill of Materials (SBOM).[2]

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. • 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) (vii) states "providing a purchaser a Software Bill of Materials (SBOM) for each product directly **or** by publishing it on a public website."[6]

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



NTIA Multistakeholder Process on Software Component Transparency | 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.

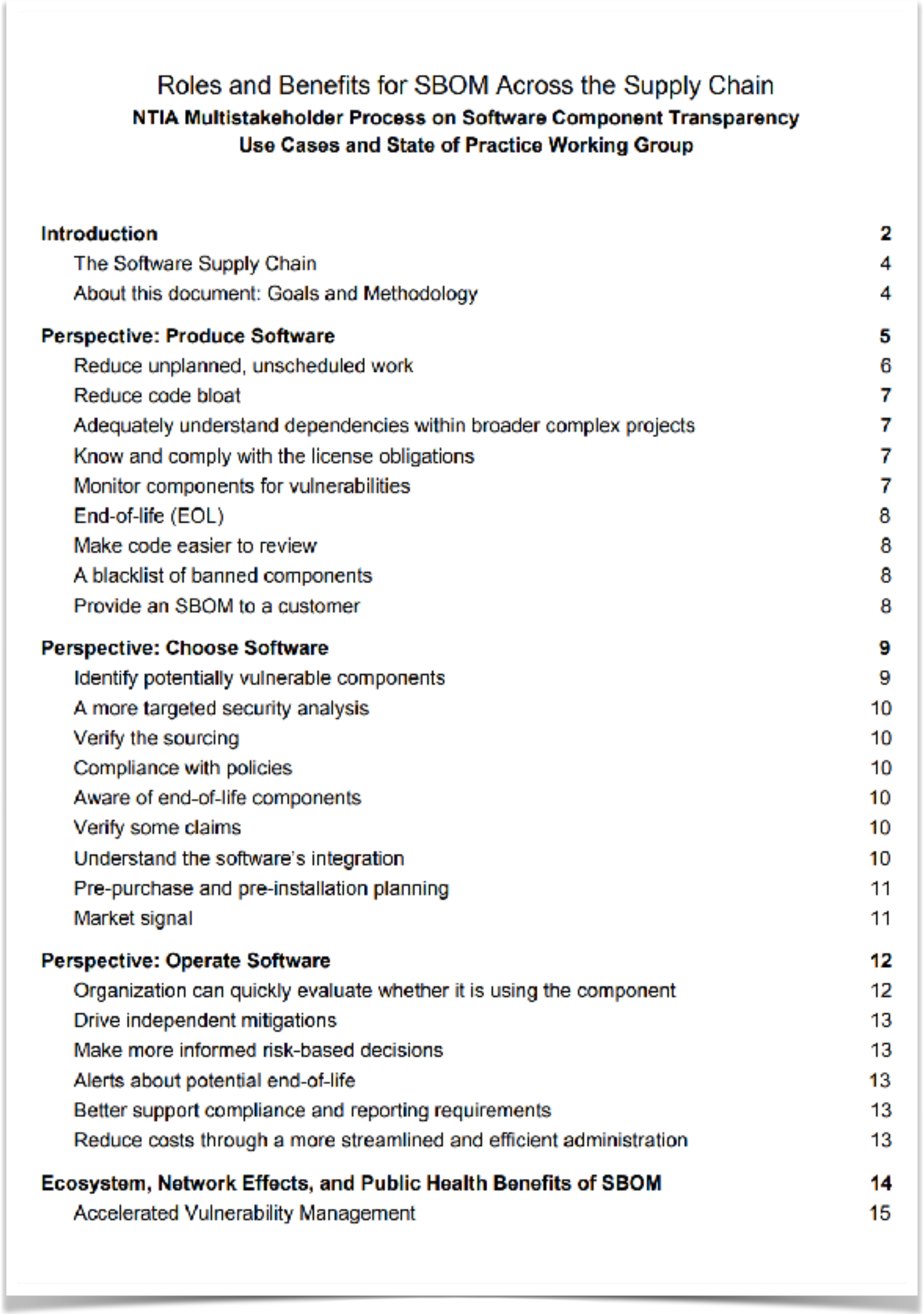
Figure: Conceptual SBOM tree with upstream relationship assertions

Benefits and Use Cases

The benefits and use cases for SBOMs[2] 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 Concept[3] 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.

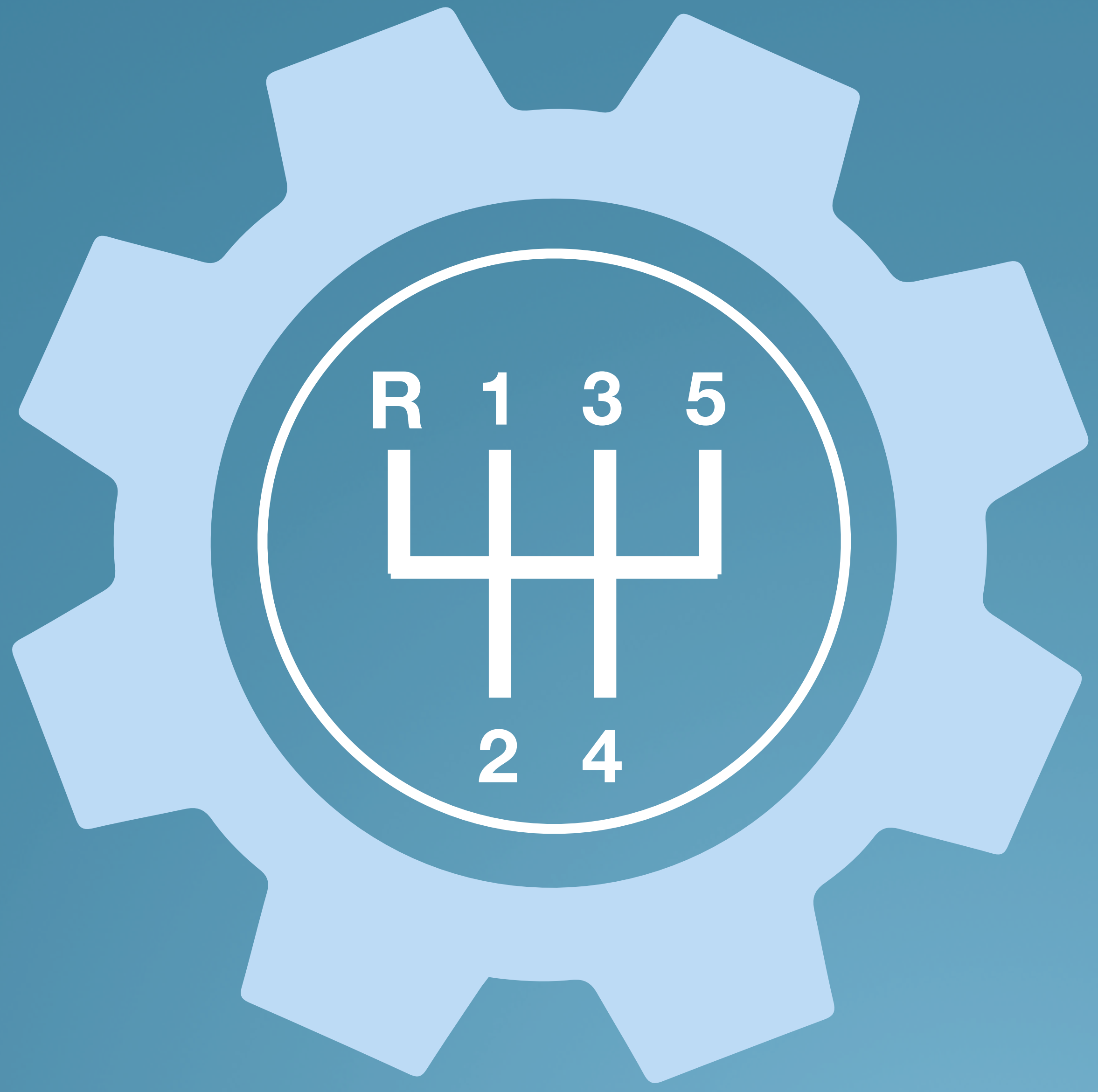
USE CASES, ROLES & BENEFITS

- 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

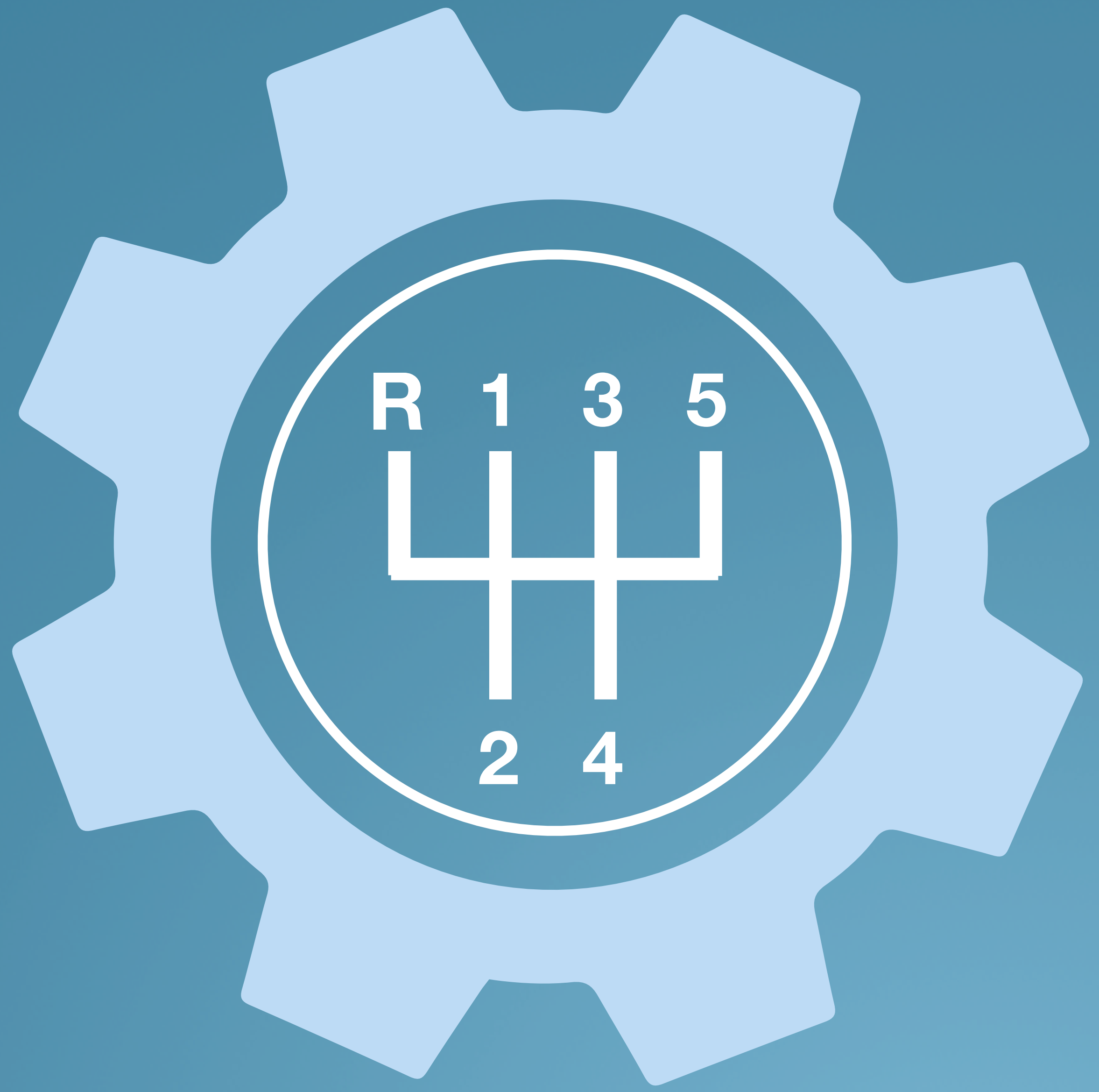


R 1 3 5
2 4

Produce

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

[write/create/assemble/package]



Produce

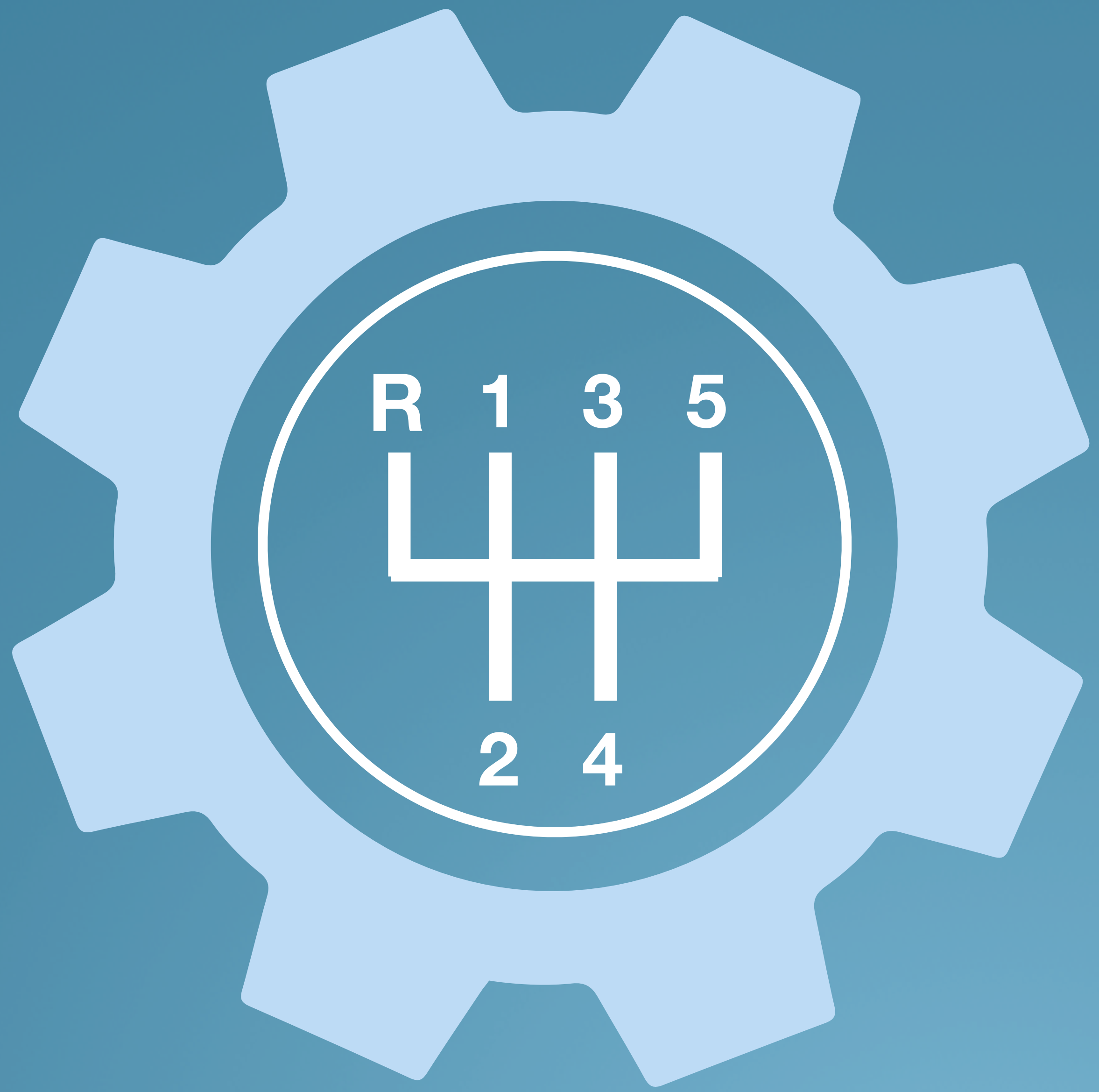
The person or organization that creates a software component or software for use by others

[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]

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

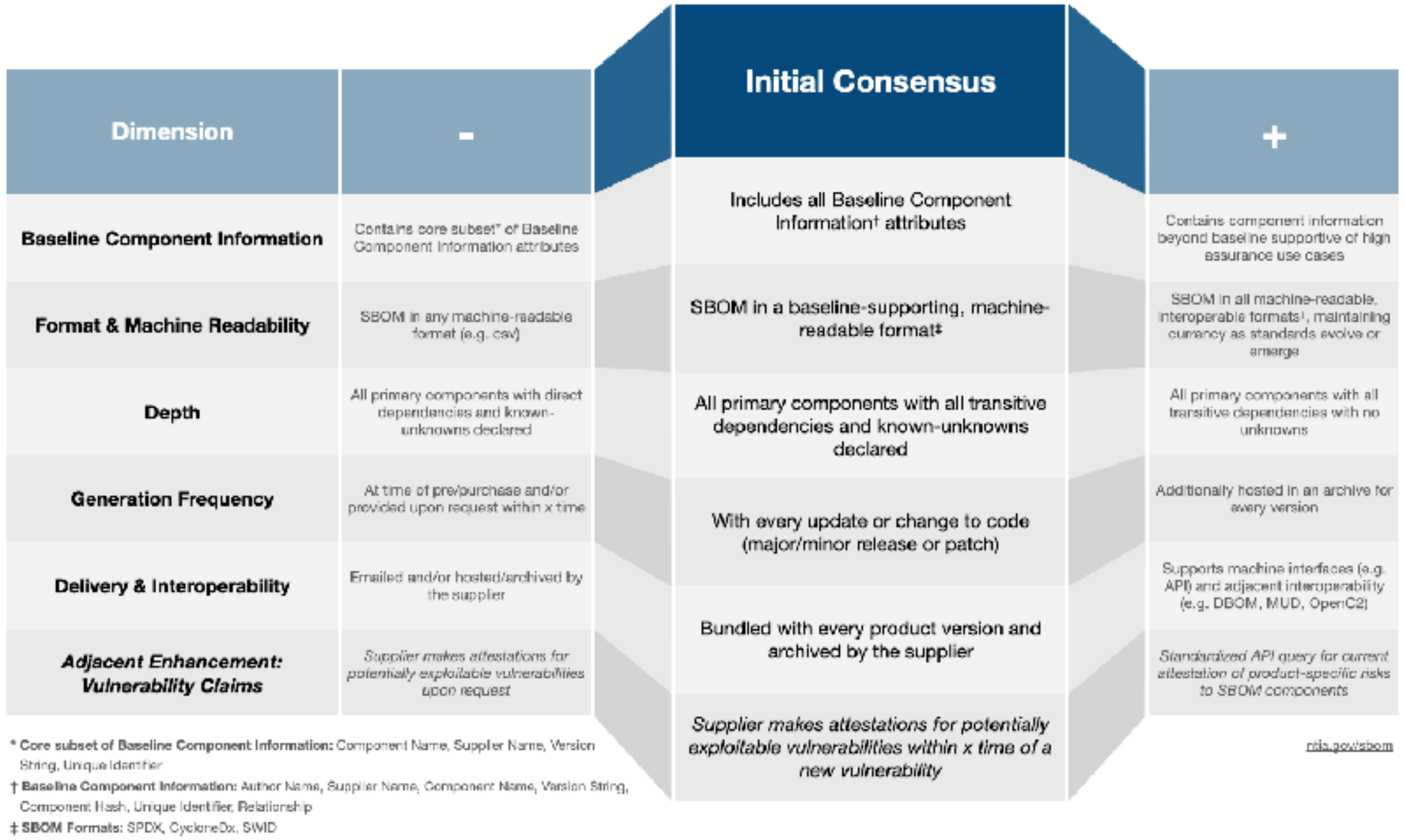
	Produce	Choose	Operate
Crawl	NTIA A&A Participants	NTIA A&A Participants	NTIA A&A Participants
Walk			
Run			

	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

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 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

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	*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	*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	*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	*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	*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	*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	*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*

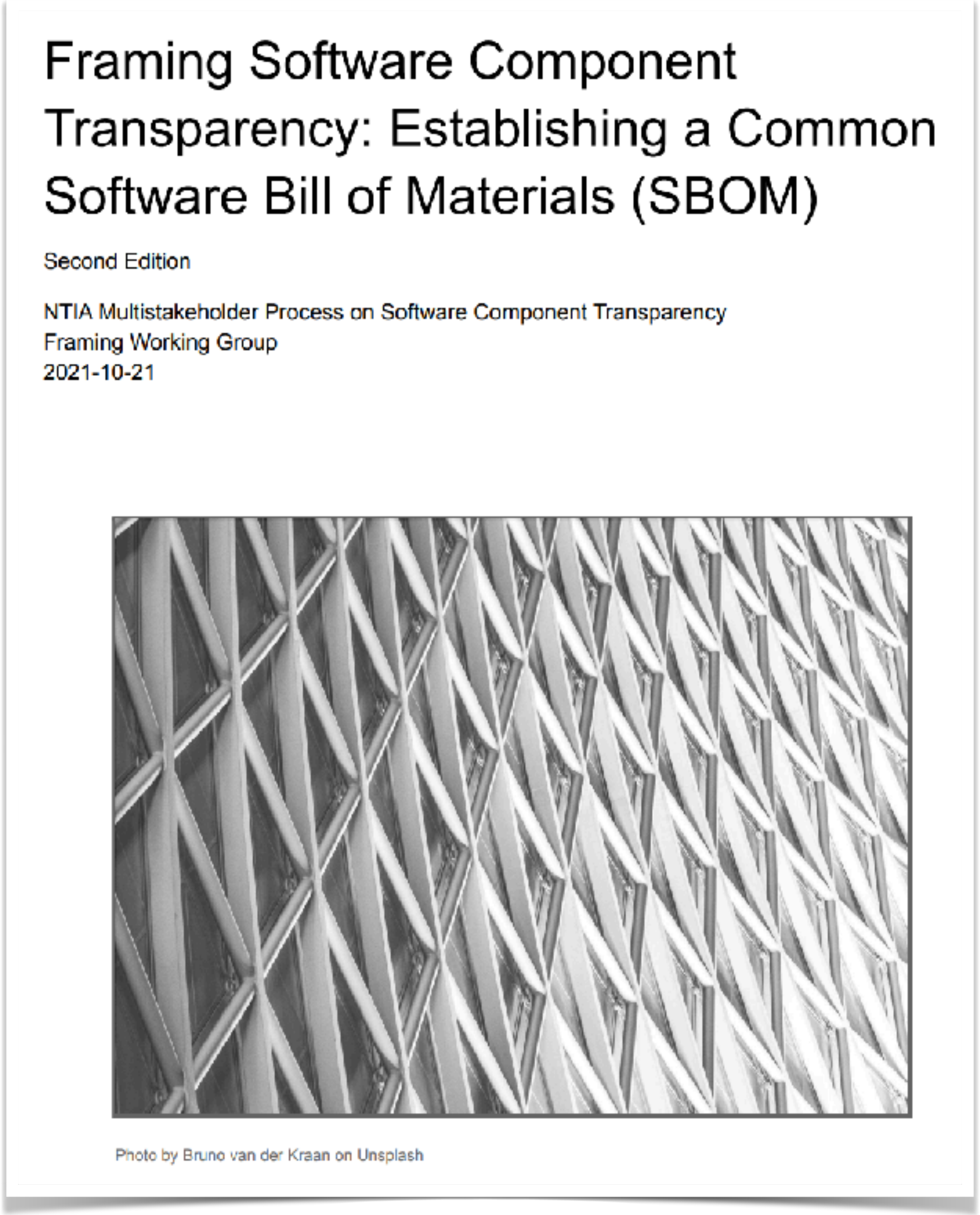
* **Core subset of Baseline Component Information:** Component Name, Supplier Name, Version String, Unique Identifier

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

‡ **SBOM Formats:** SPDX, CycloneDx, SWID

FRAMING SOFTWARE COMPONENT TRANSPARENCY

- NTIA Framing Working Group
- Identifies SBOM Elements, Baseline Attributes, Component Relationships, Existing Formats, Creation and Exchange Processes, and Terminology
- Published on ntia.gov/sbom



Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)

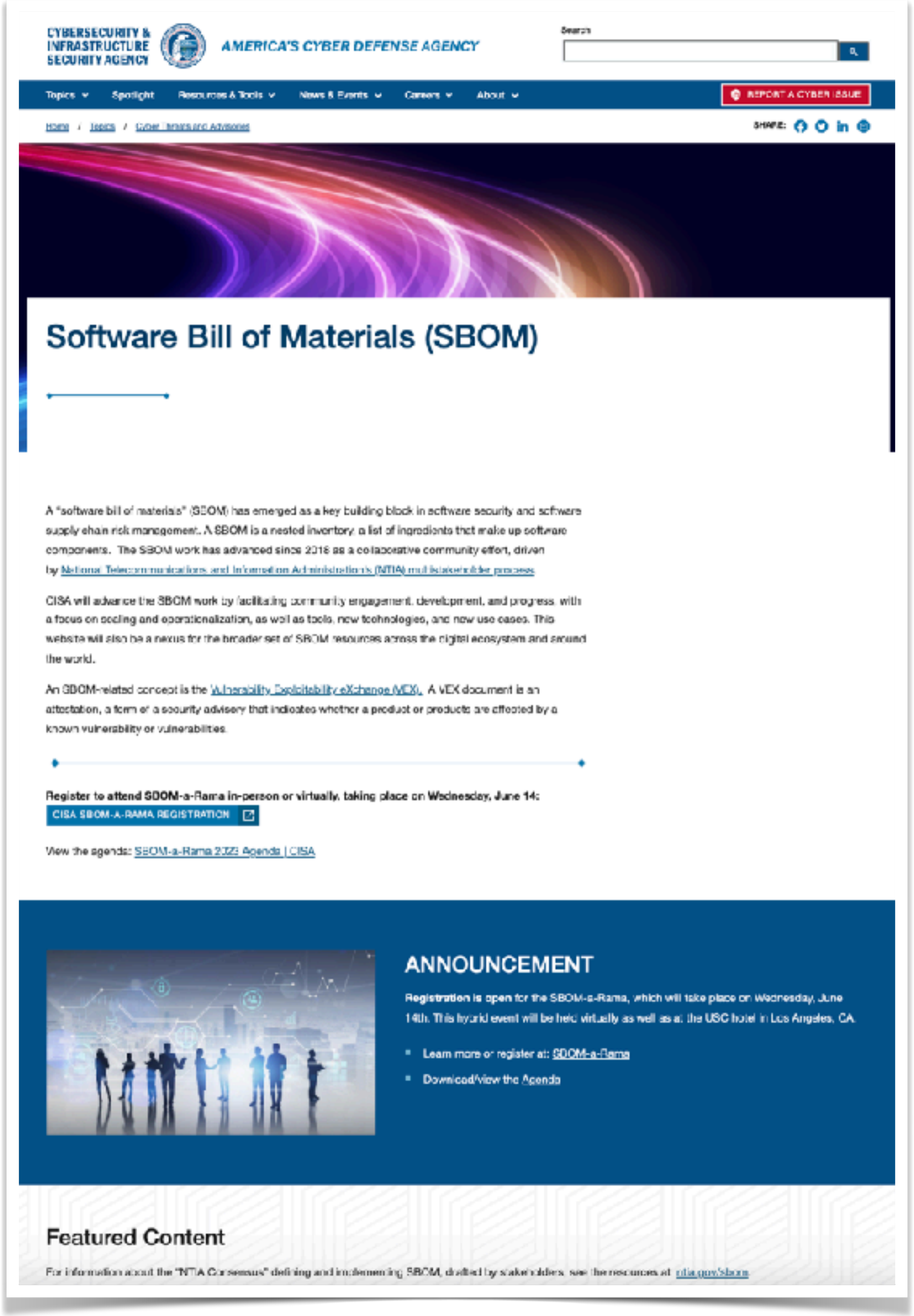
Second Edition

NTIA Multistakeholder Process on Software Component Transparency
Framing Working Group
2021-10-21

Photo by Bruno van der Kraan on Unsplash

CISA RESOURCES

- Working Group Drafted:
  - Guidance on Assembling a Group of Products
  - 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 Identification Ecosystem Option Analysis
  - Software Bill of Materials (SBOM) Sharing Lifecycle Report
- Published on cisa.gov/sbom


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home / Topics / Cyber Threats and Advisories
SHARE:

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 nested inventory, a list of ingredients that make up software components. The SBOM work has advanced since 2018 as a collaborative community effort, driven by National Telecommunications and Information Administration's (NTIA) multistakeholder process.

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 2023 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

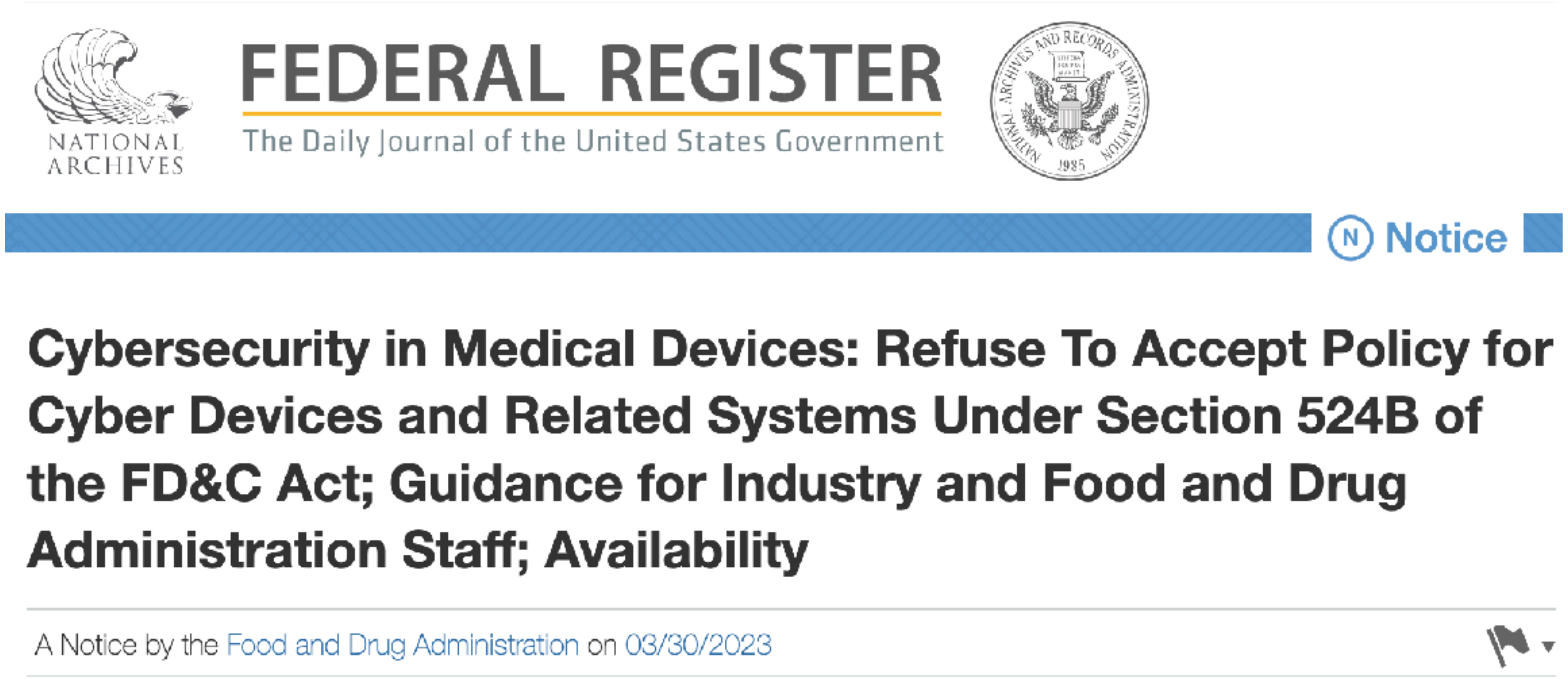
Featured Content

For information about the "NTIA Consensus" defining and implementing SBOM, drafted by stakeholders, see the resources at ntia.gov/sbom.

UPDATES

SINCE JUNE’23 SBOM-A-RAMA

FDA – PATCH ACT



NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

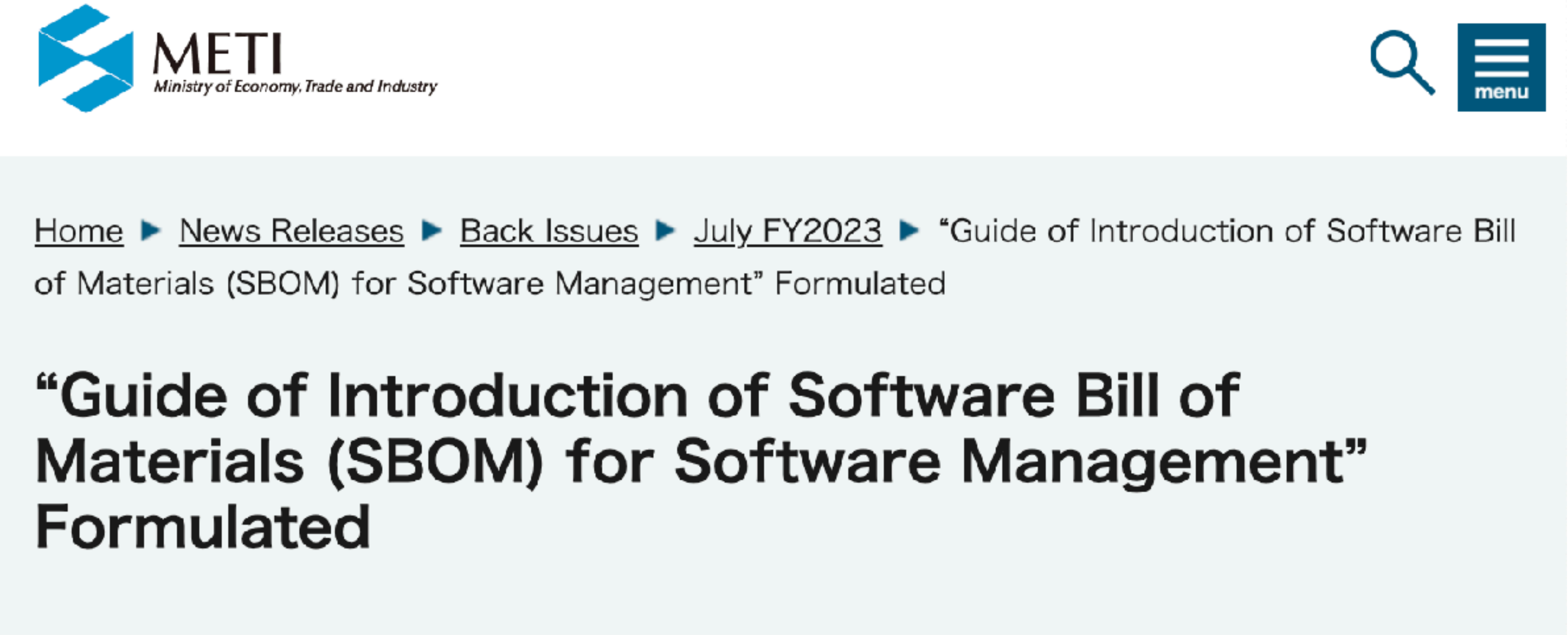
Ⓝ Notice

Cybersecurity in Medical Devices: Refuse To Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act; Guidance for Industry and Food and Drug Administration Staff; Availability

A Notice by the Food and Drug Administration on 03/30/2023

FDA Refuse to Accept Policy

JAPAN – MINISTRY OF ECONOMY, TRADE, AND INDUSTRY

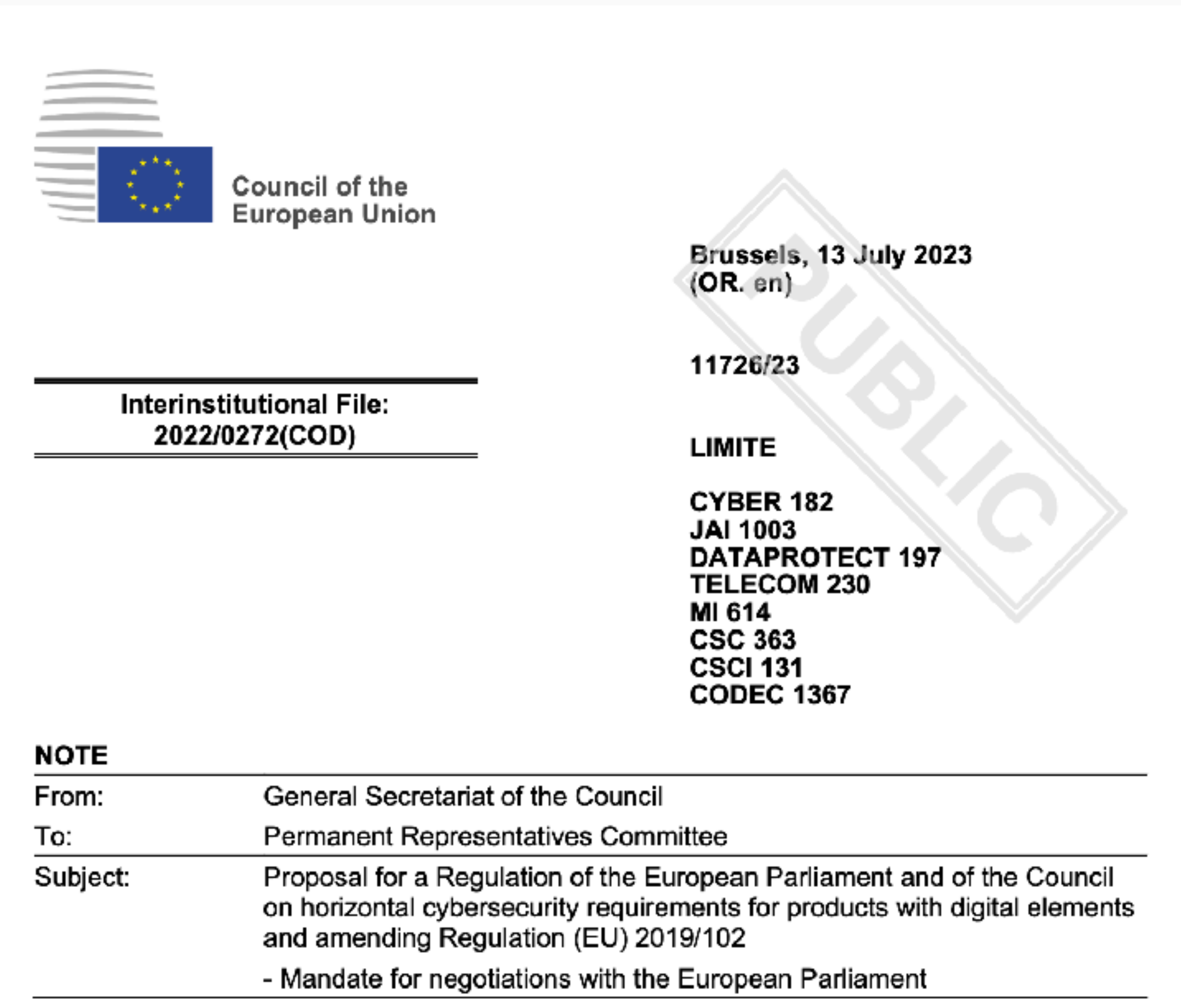


Home ▶ News Releases ▶ Back Issues ▶ July FY2023 ▶ “Guide of Introduction of Software Bill of Materials (SBOM) for Software Management” Formulated

“Guide of Introduction of Software Bill of Materials (SBOM) for Software Management” Formulated

METI SBOM Publication

EU – CYBER RESILIENCE ACT



Council of the European Union

Brussels, 13 July 2023
(OR. en)

11726/23

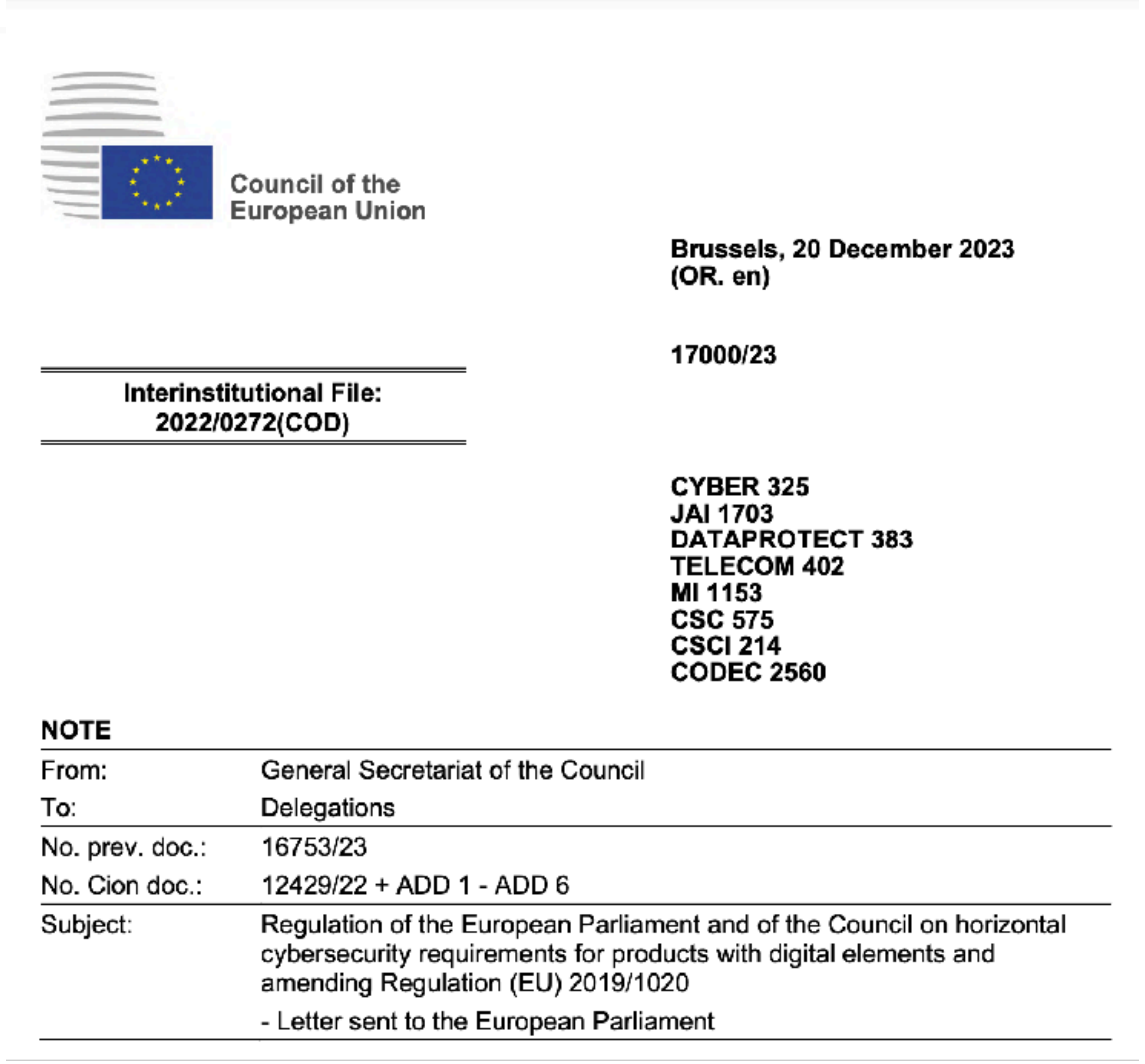
LIMITE

CYBER 182
JAI 1003
DATAPROTECT 197
TELECOM 230
MI 614
CSC 363
CSCI 131
CODEC 1367

Interinstitutional File:
2022/0272(COD)

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
Subject:	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 - Mandate for negotiations with the European Parliament



Council of the European Union

Brussels, 20 December 2023
(OR. en)

17000/23

CYBER 325
JAI 1703
DATAPROTECT 383
TELECOM 402
MI 1153
CSC 575
CSCI 214
CODEC 2560

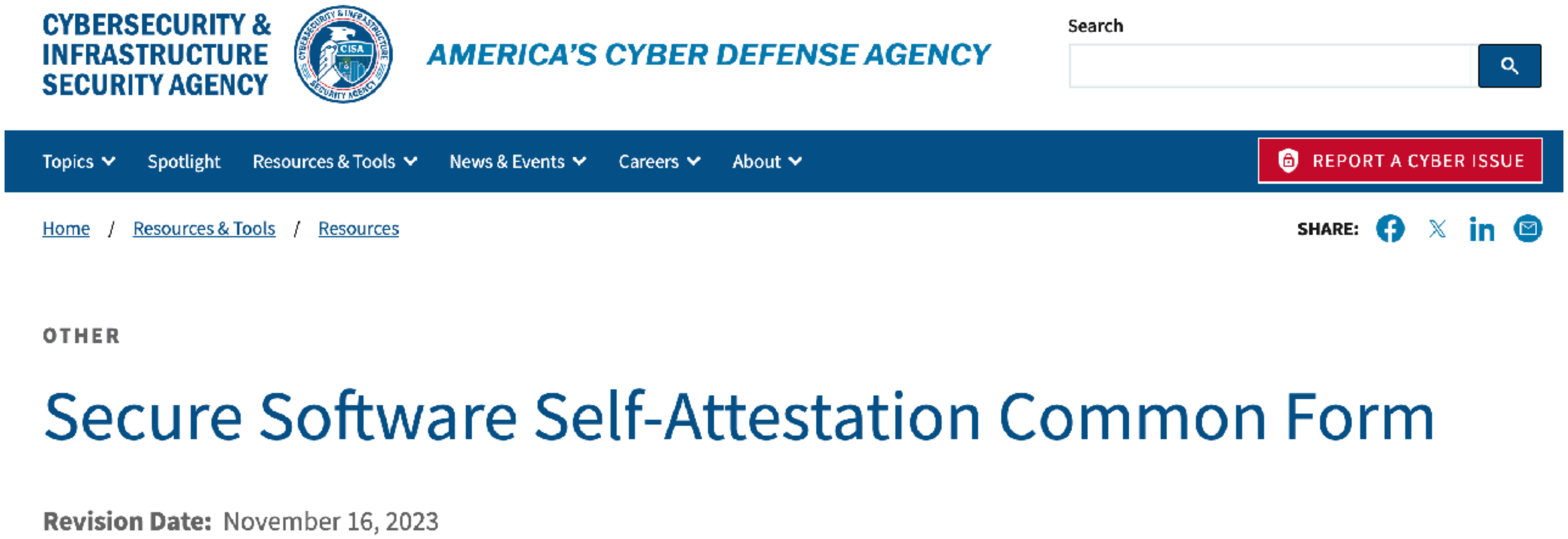
Interinstitutional File:
2022/0272(COD)

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	16753/23
No. Cion doc.:	12429/22 + ADD 1 - ADD 6
Subject:	Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - Letter sent to the European Parliament

EU CRA - Mandate for Negotiations with Parliament & Agreement Letter

CISA – SOFTWARE ATTESTATION FORM



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home / Resources & Tools / Resources
SHARE:

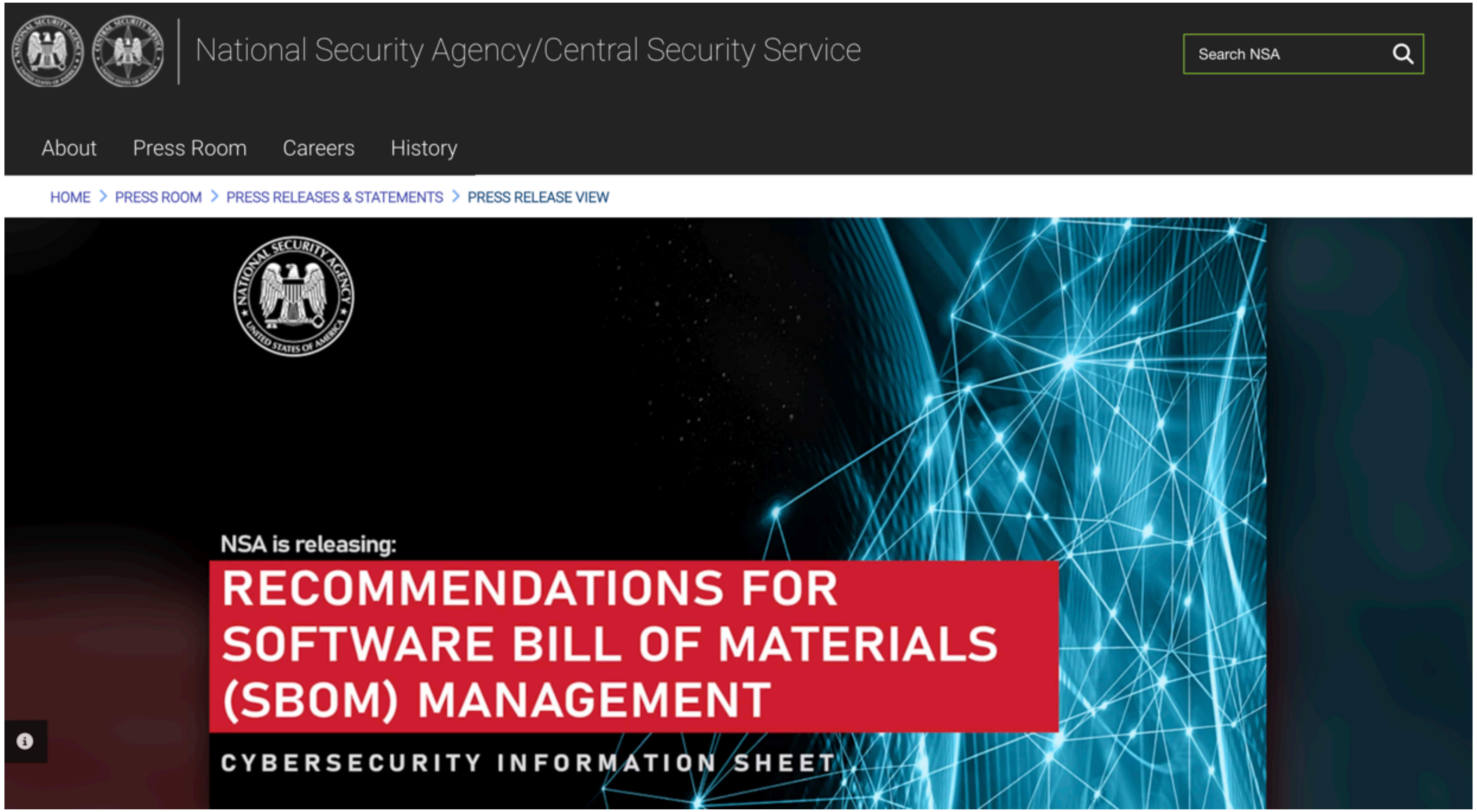
OTHER

Secure Software Self-Attestation Common Form

Revision Date: November 16, 2023

CISA Secure Software Self-Attestation & Comment Period

NSA – SBOM RECOMMENDATIONS



National Security Agency/Central Security Service

Search NSA

About Press Room Careers History

HOME > PRESS ROOM > PRESS RELEASES & STATEMENTS > PRESS RELEASE VIEW

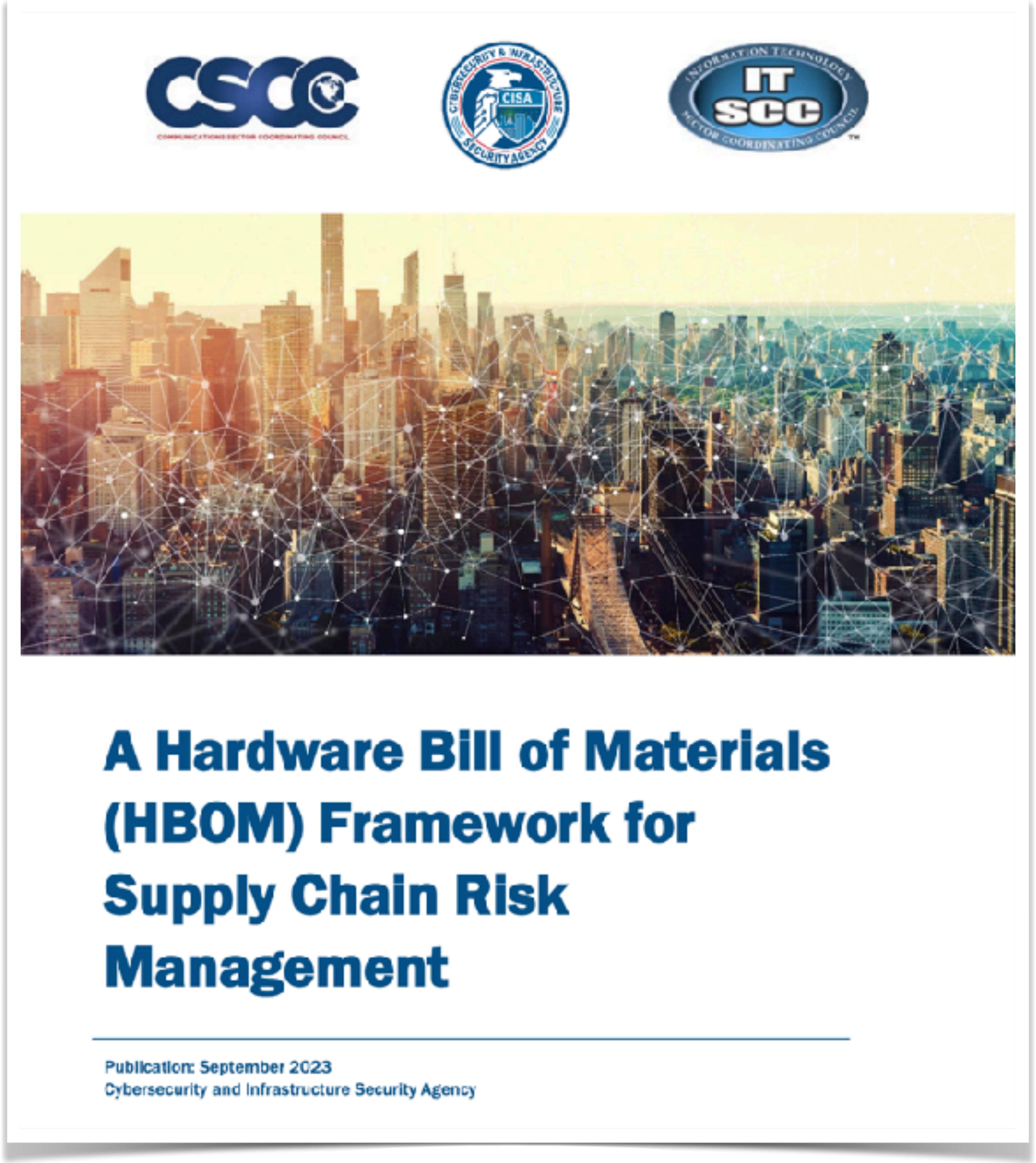
NSA is releasing:

RECOMMENDATIONS FOR SOFTWARE BILL OF MATERIALS (SBOM) MANAGEMENT

CYBERSECURITY INFORMATION SHEET

NSA - Recommendations for Software Bill of Materials

DOD – HARDWARE BILL OF MATERIALS

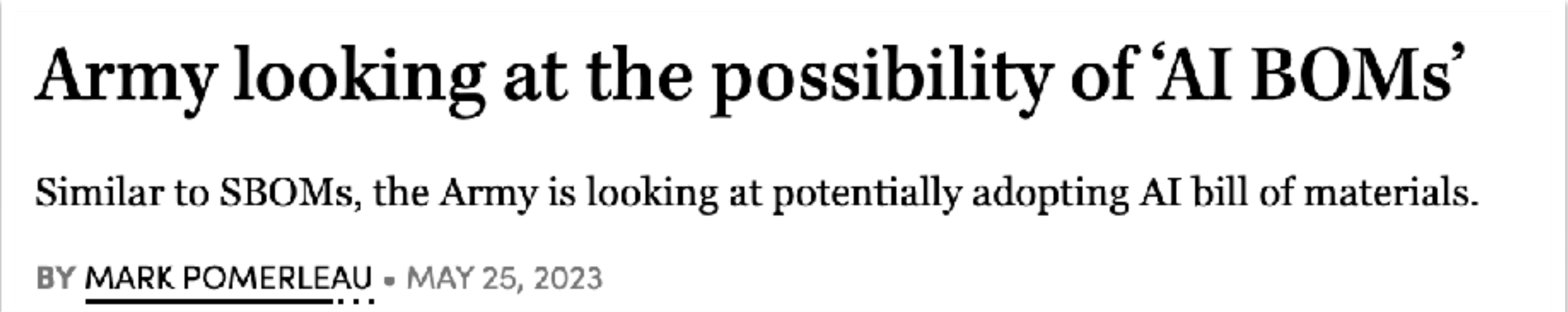


A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management

Publication: September 2023
Cybersecurity and Infrastructure Security Agency

DOD - HBOM

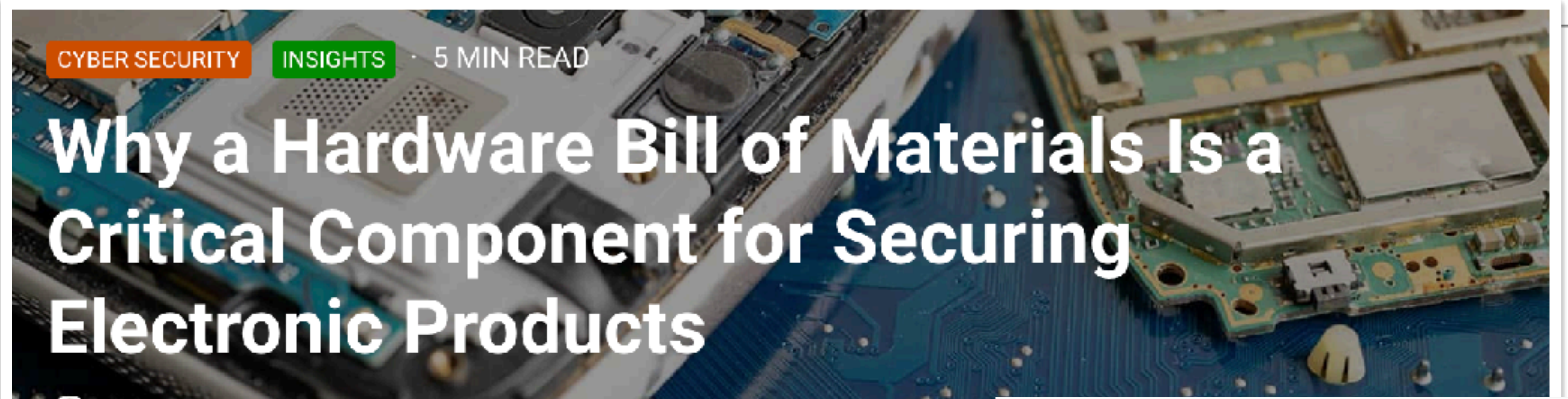
ALL THE BOMS



Army looking at the possibility of 'AI BOMs'

Similar to SBOMs, the Army is looking at potentially adopting AI bill of materials.

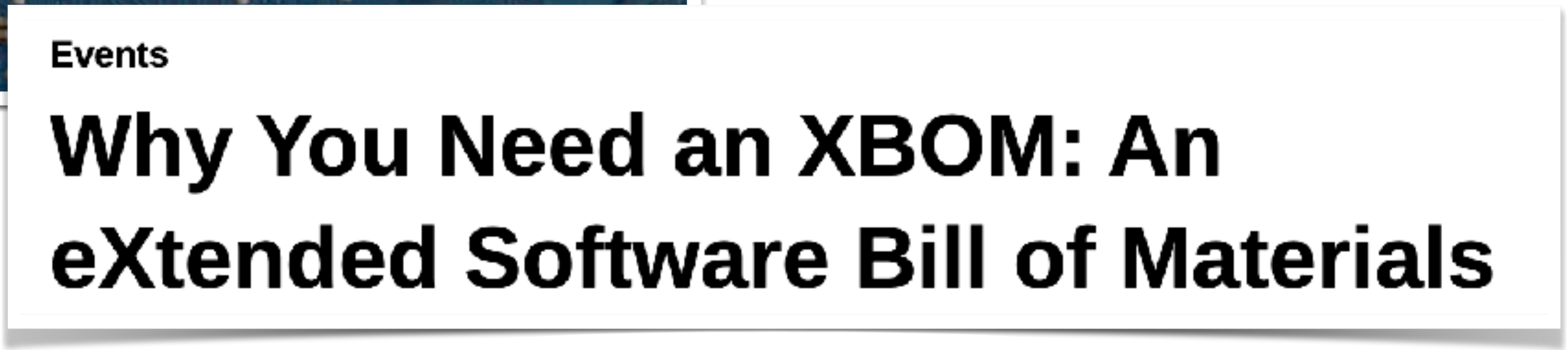
BY MARK POMERLEAU • MAY 25, 2023



CYBER SECURITY INSIGHTS · 5 MIN READ

Why a Hardware Bill of Materials Is a Critical Component for Securing Electronic Products

ANDREAS KUEHLMANN · OCTOBER 28, 2022

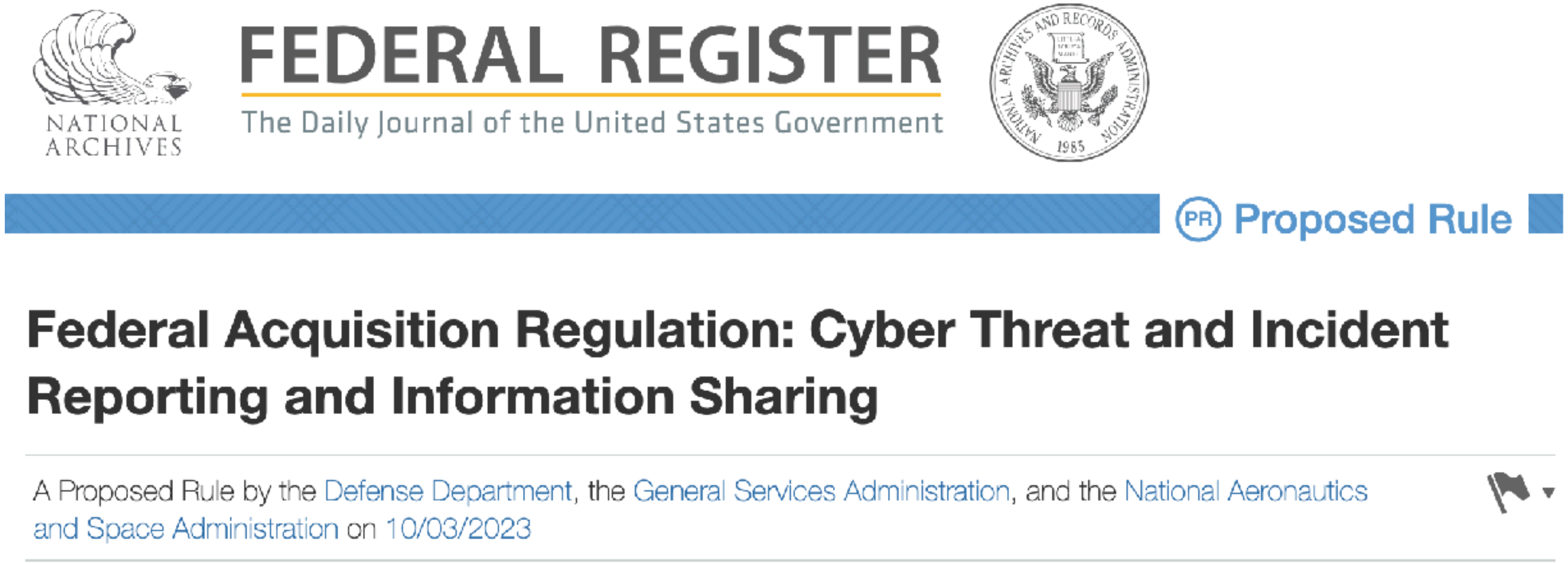


Events

Why You Need an XBOM: An eXtended Software Bill of Materials

SPDX CycloneDX

FAR – PROPOSED RULE & COMMENTS



NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

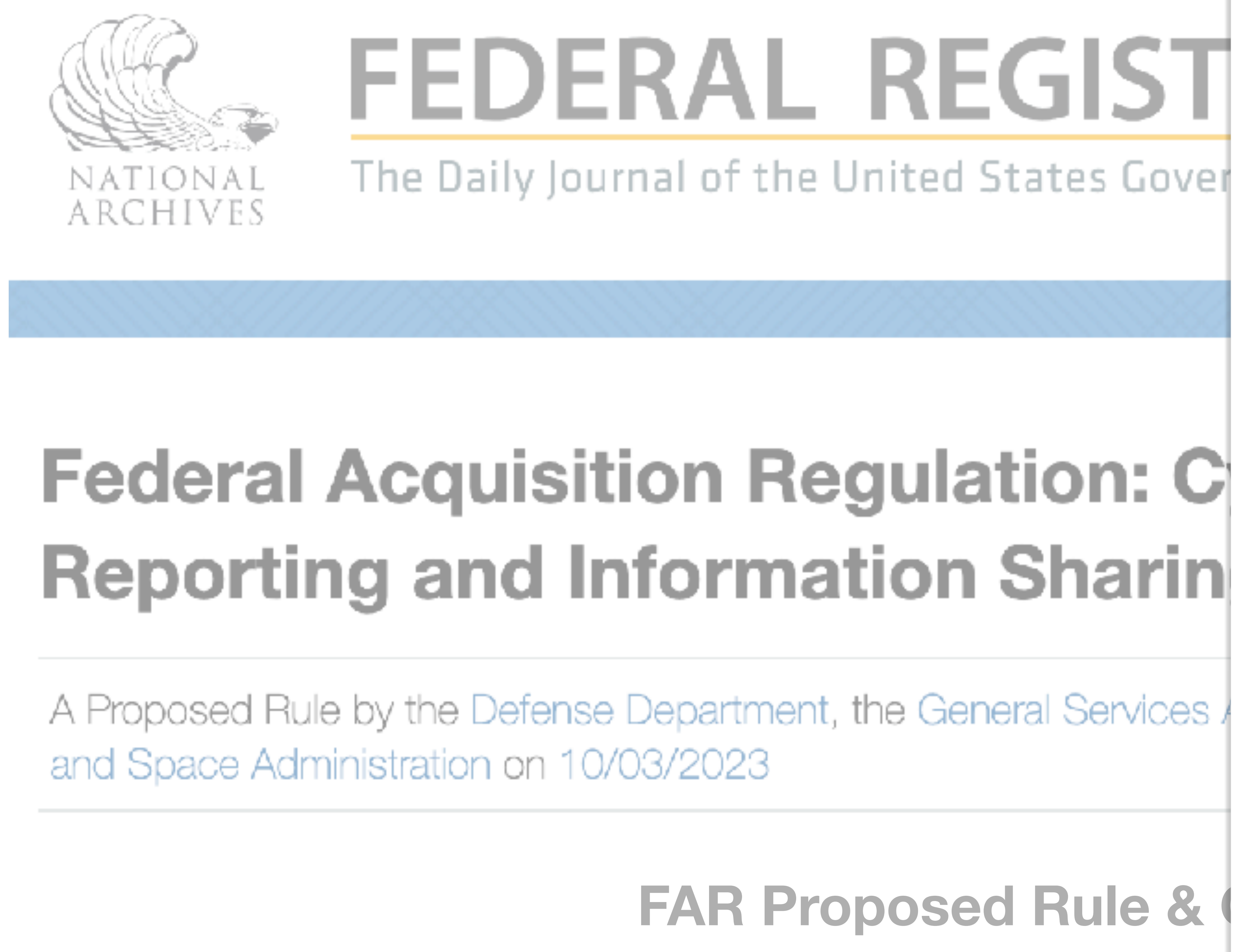
PR Proposed Rule

Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing

A Proposed Rule by the Defense Department, the General Services Administration, and the National Aeronautics and Space Administration on 10/03/2023

FAR Proposed Rule & Comment Period

FAR – PROPOSED RULE & COMMENTS



NATIONAL ARCHIVES

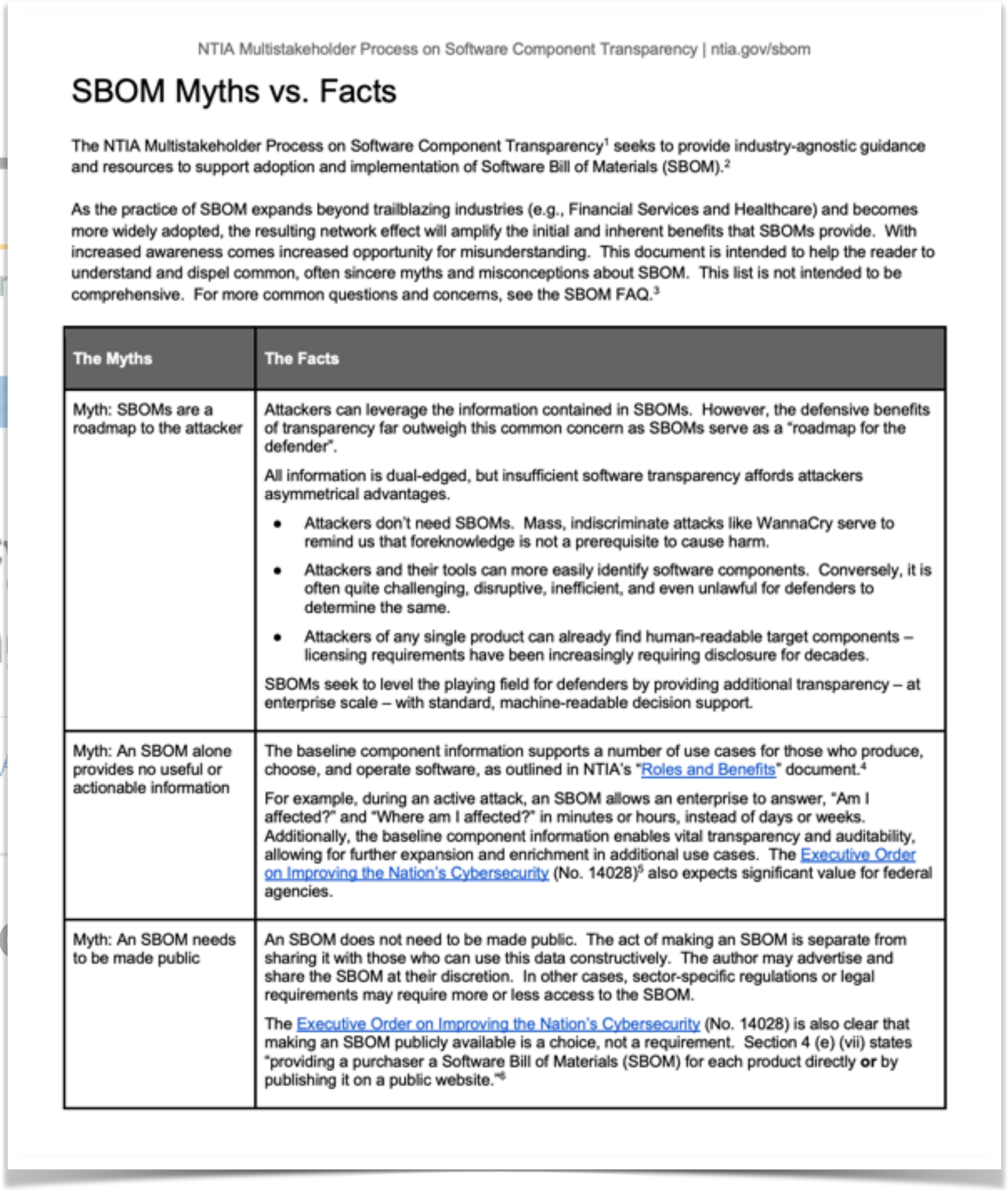
FEDERAL REGIST

The Daily Journal of the United States Gover

Federal Acquisition Regulation: C Reporting and Information Sharin

A Proposed Rule by the Defense Department, the General Services and Space Administration on 10/03/2023

FAR Proposed Rule &



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

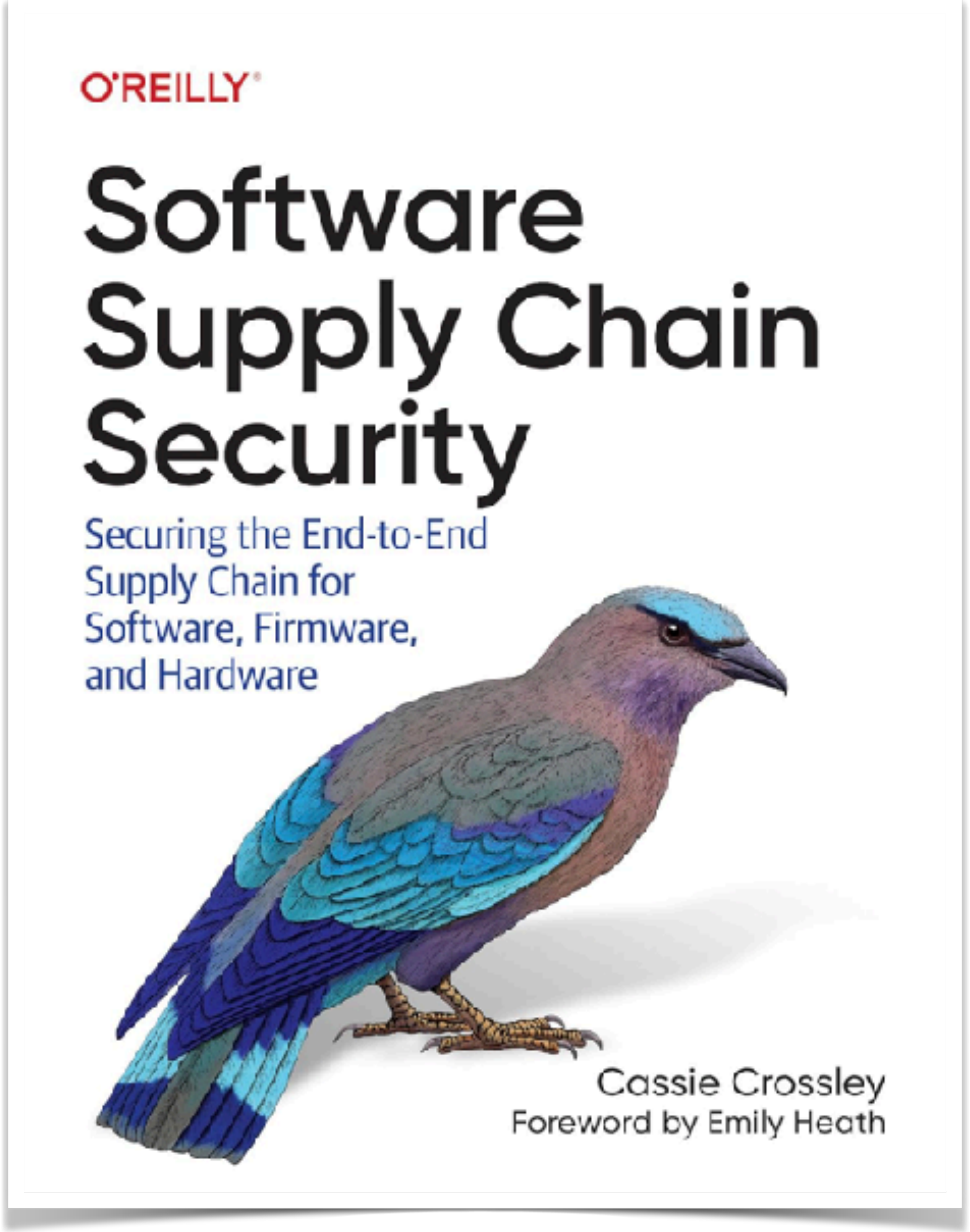
SBOM Myths vs. Facts

The NTIA Multistakeholder Process on Software Component Transparency[1] 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. • 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) (vii) states "providing a purchaser a Software Bill of Materials (SBOM) for each product directly **or** by publishing it on a public website."[6]

BOOKS

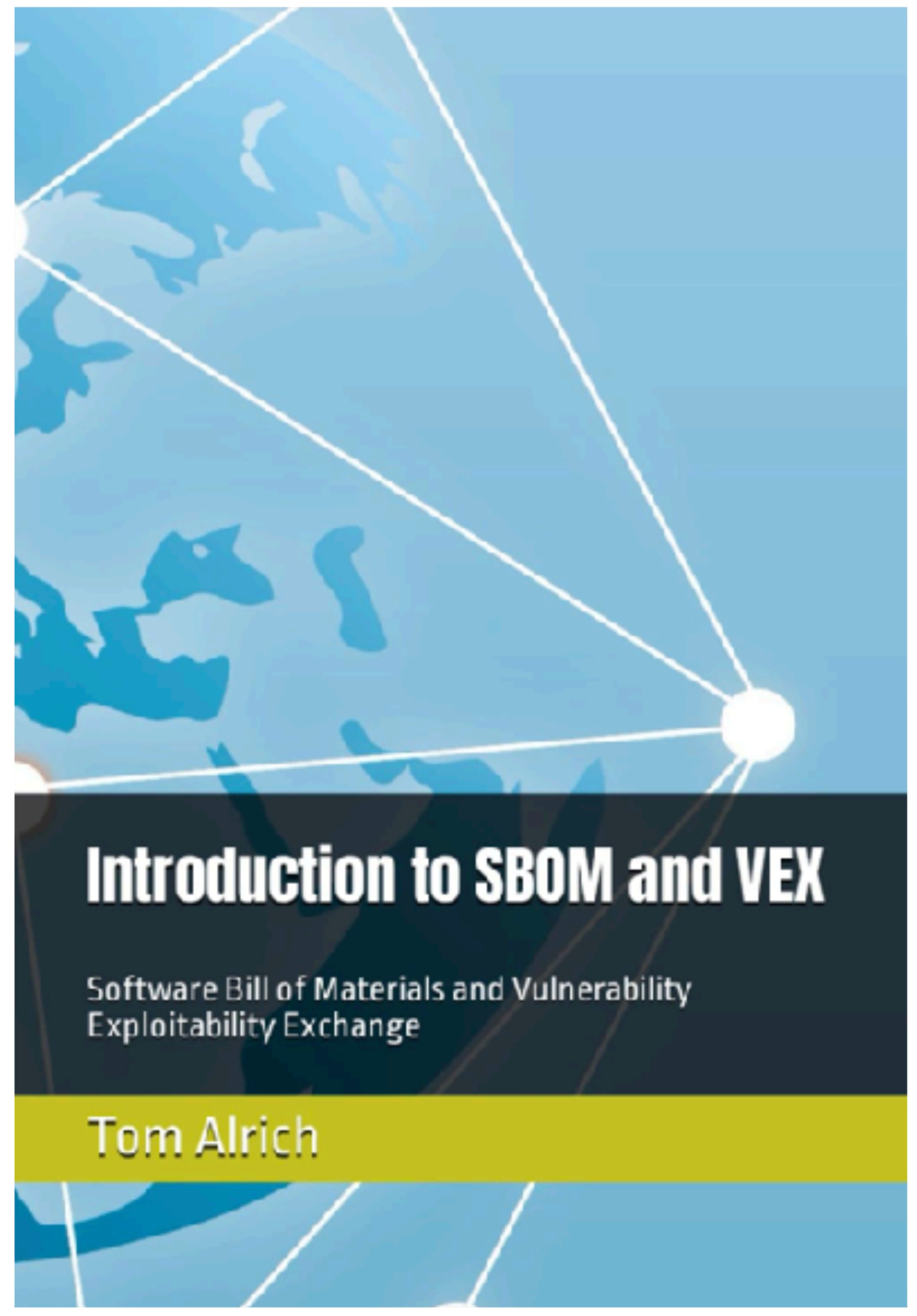


O'REILLY

Software Supply Chain Security

Securing the End-to-End Supply Chain for Software, Firmware, and Hardware

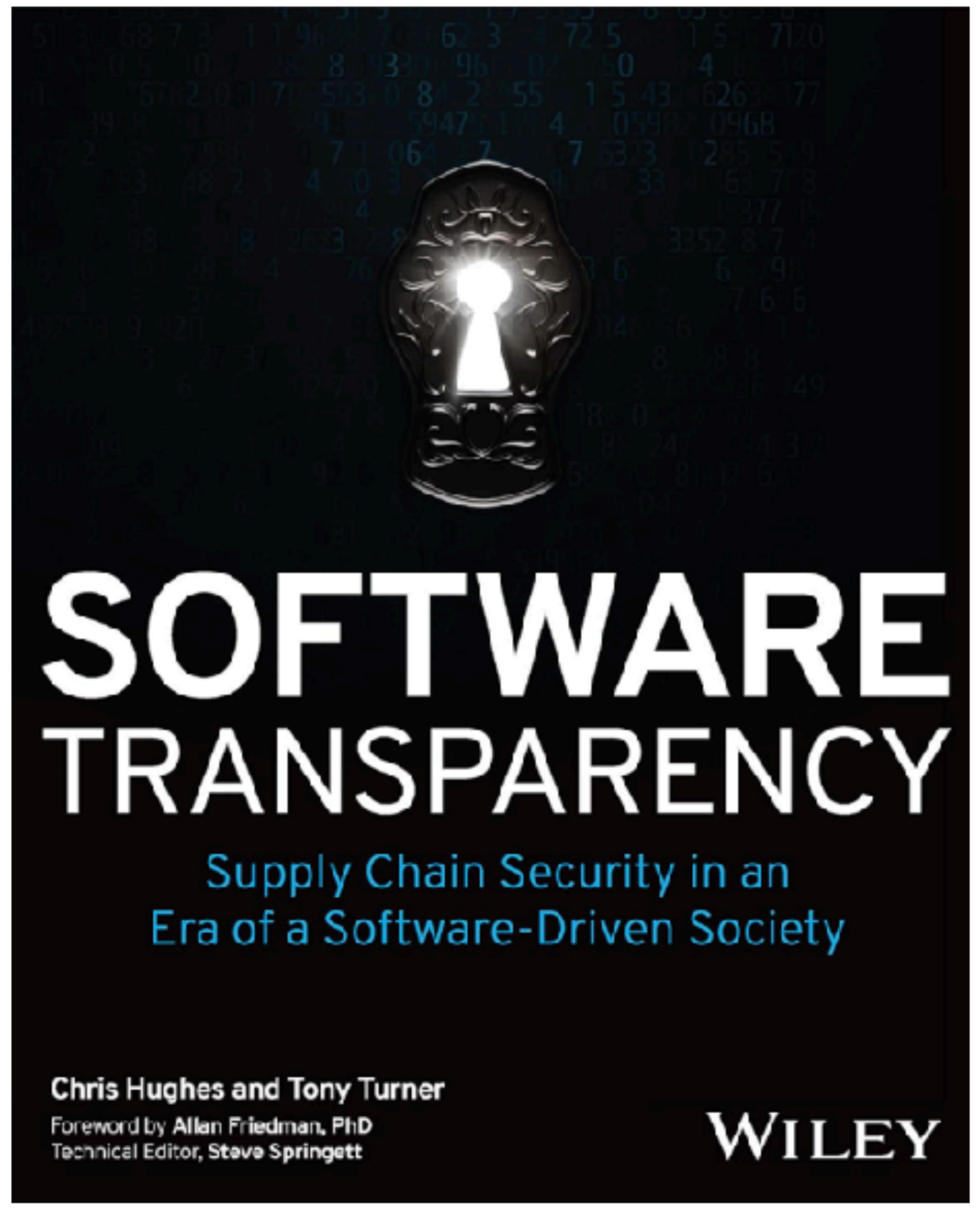
Cassie Crossley
Foreword by Emily Heath



Introduction to SBOM and VEX

Software Bill of Materials and Vulnerability Exploitability Exchange

Tom Alrich



SOFTWARE TRANSPARENCY

Supply Chain Security in an Era of a Software-Driven Society

Chris Hughes and Tony Turner
Foreword by Allan Friedman, PhD
Technical Editor, Steve Springett

WILEY

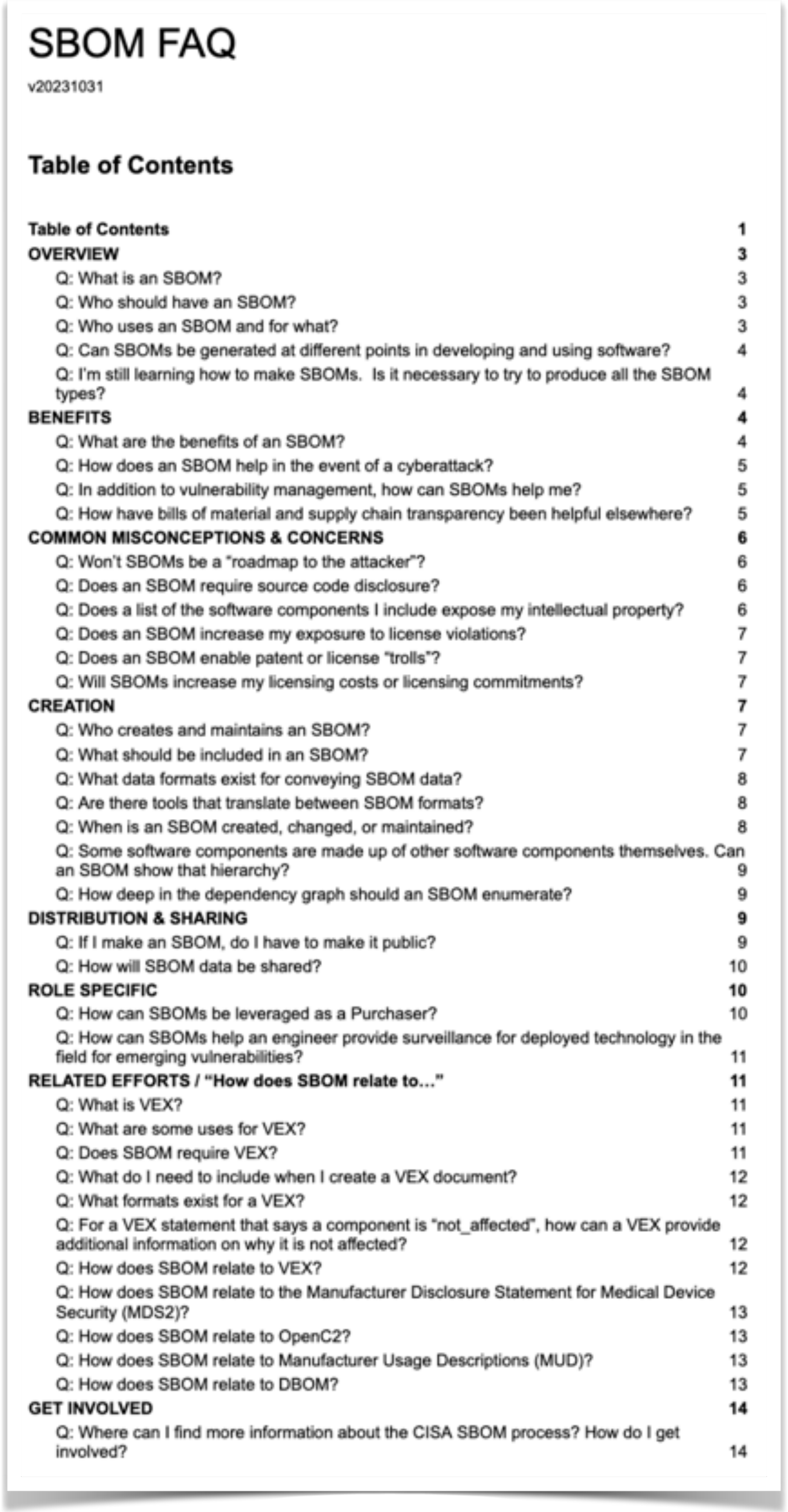
CURRENT FOCUS

CURRENT PUBLICATION PIPELINE

- Updated FAQ
- Equipping the Buyer - Procurement/Acquisition
- Equipping the Board of Directors on increasing obligations

FAQ

- Awaiting Publication
  - Nine new questions
- Additional updates planned post-publication

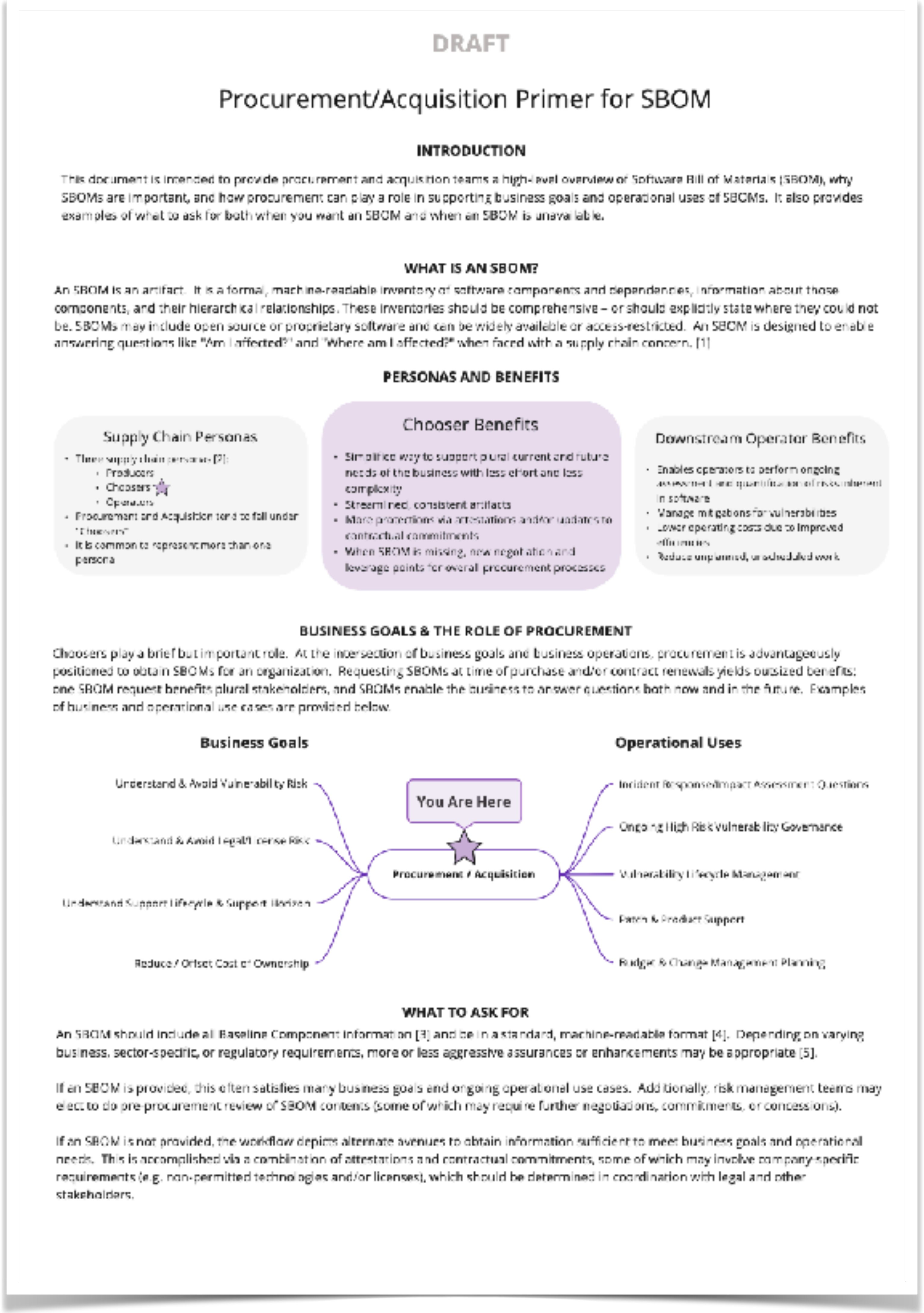


SBOM FAQ

v20231031

Table of Contents

PROCUREMENT/ACQUISITION PRIMER



DRAFT

Procurement/Acquisition Primer for SBOM

INTRODUCTION

This document is intended to provide procurement and acquisition teams a high-level overview of Software Bill of Materials (SBOM), why SBOMs are important, and how procurement can play a role in supporting business goals and operational uses of SBOMs. It also provides examples of what to ask for both when you want an SBOM and when an SBOM is unavailable.

WHAT IS AN SBOM?

An SBOM is an artifact. It 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. An SBOM is designed to enable answering questions like "Am I affected?" and "Where am I affected?" when faced with a supply chain concern. [1]

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 risk 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.

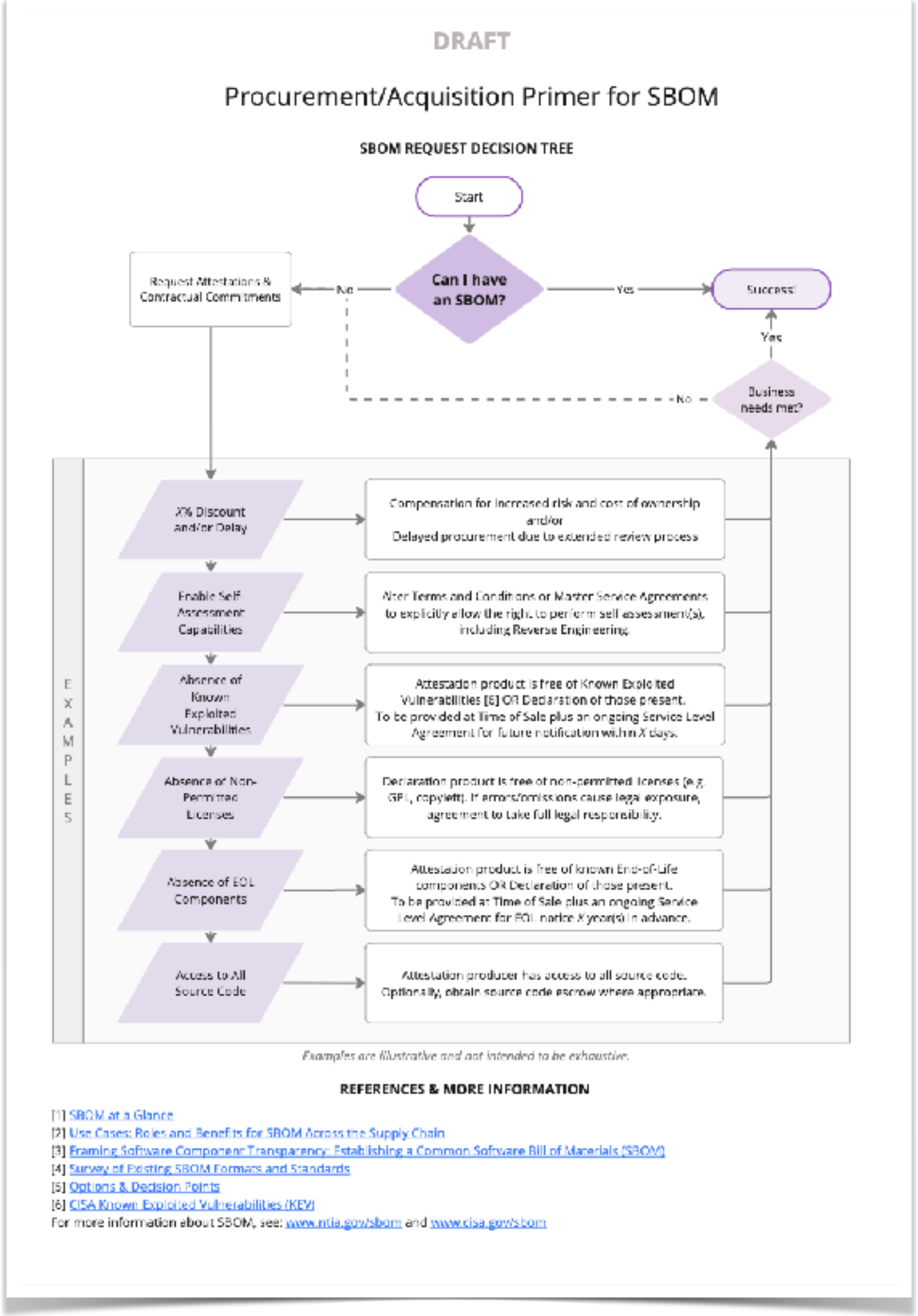
Business Goals
Operational Uses
Understand & Avoid Vulnerability Risk
Understand & Avoid Legal/License Risk
Understand Support Lifecycle & Support Horizon
Reduce / Offset Cost of Ownership
You Are Here
Procurement / Acquisition
Incident Response/Impact Assessment Questions
Ongoing High Risk Vulnerability Governance
Vulnerability Lifecycle Management
Patch & Product Support
Budget & Change Management Planning

WHAT TO ASK FOR

An SBOM should include all Baseline Component Information [3] and be in a standard, machine-readable format [4]. Depending on varying business, sector-specific, or regulatory requirements, more or less aggressive assurances or enhancements may be appropriate [5].

If an SBOM is provided, this often satisfies many business goals and ongoing operational use cases. Additionally, risk management teams may elect to do pre-procurement review of SBOM contents (some of which may require further negotiations, commitments, or concessions).

If an SBOM is not provided, the workflow depicts alternate avenues to obtain information sufficient to meet business goals and operational needs. This is accomplished via a combination of attestations and contractual commitments, some of which may involve company-specific requirements (e.g. non-permitted technologies and/or licenses), which should be determined in coordination with legal and other stakeholders.



DRAFT

Procurement/Acquisition Primer for SBOM

SBOM REQUEST DECISION TREE

Start
Can I have an SBOM?
Yes
Success!
No
Request Attestations & Contractual Commitments
Business needs met?
Yes
No
EXAMPLES
X% Discount and/or Delay
Compensation for increased risk and cost of ownership and/or Delayed procurement due to extended review process
Enable Self Assessment Capabilities
Alter Terms and Conditions or Master Service Agreements to explicitly allow the right to perform self assessment(s), including Reverse Engineering.
Absence of Known Exploited Vulnerabilities
Attestation product is free of Known Exploited Vulnerabilities [6] OR Declaration of those present. To be provided at Time of Sale plus an ongoing Service Level Agreement for future notification within X days.
Absence of Non-Permitted Licenses
Declaration product is free of non-permitted licenses (e.g. GPL, copyleft). If errors/omissions cause legal exposure, agreement to take full legal responsibility.
Absence of EOL Components
Attestation product is free of known End-of-Life components OR Declaration of those present. To be provided at Time of Sale plus an ongoing Service Level Agreement for EOL notice X year(s) in advance.
Access to All Source Code
Attestation producer has access to all source code. Optionally, obtain source code escrow where appropriate.

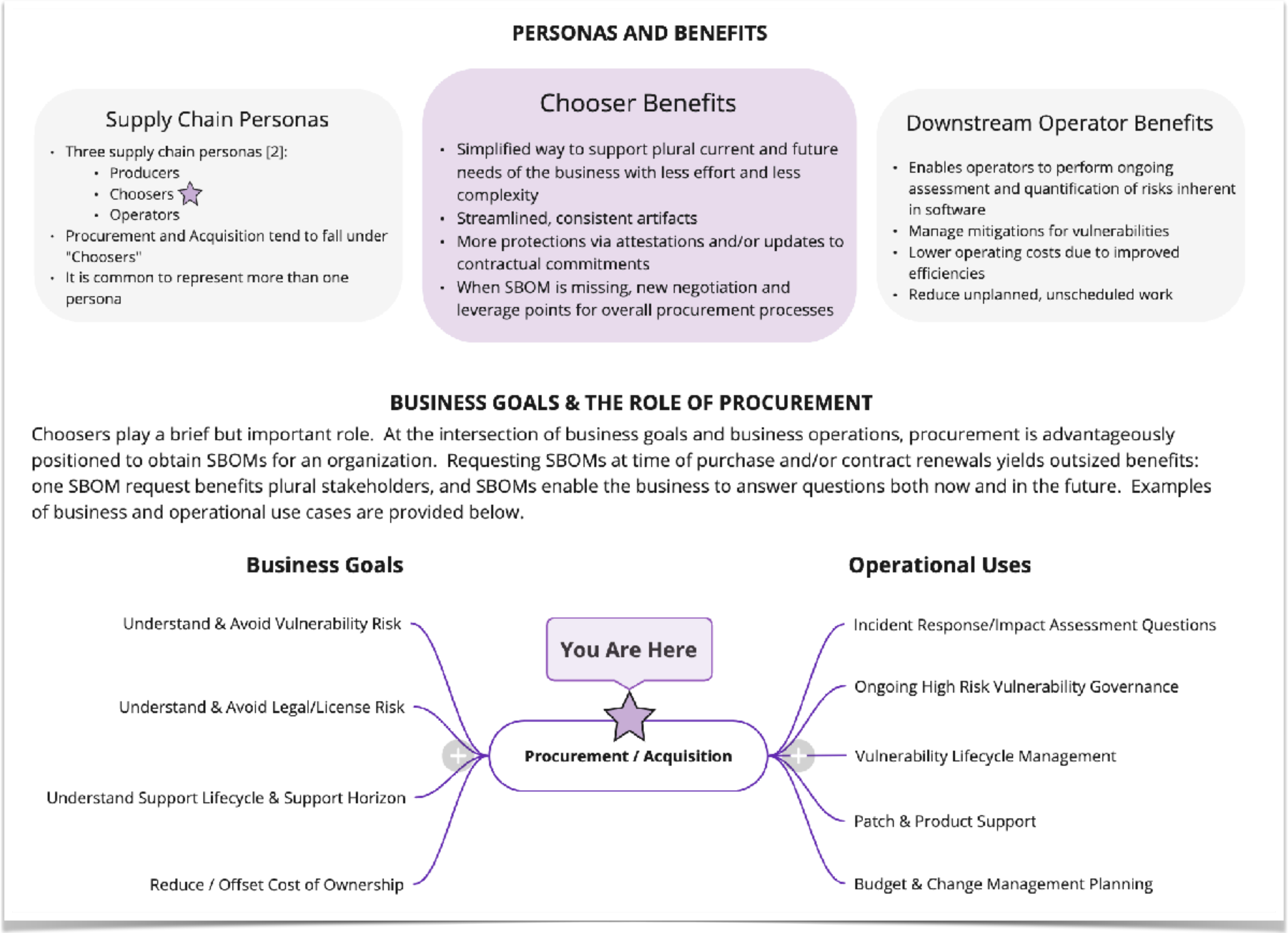
Examples are illustrative and not intended to be exhaustive.

REFERENCES & MORE INFORMATION

[1] SBOM at a Glance
[2] Use Cases: Roles and Benefits for SBOM Across the Supply Chain
[3] Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)
[4] Survey of Existing SBOM Formats and Standards
[5] Options & Decision Points
[6] CISA Known Exploited Vulnerabilities (KEV)

For more information about SBOM, see: www.ntia.gov/sbom and www.cisa.gov/sbom

PROCUREMENT/ACQUISITION PRIMER



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

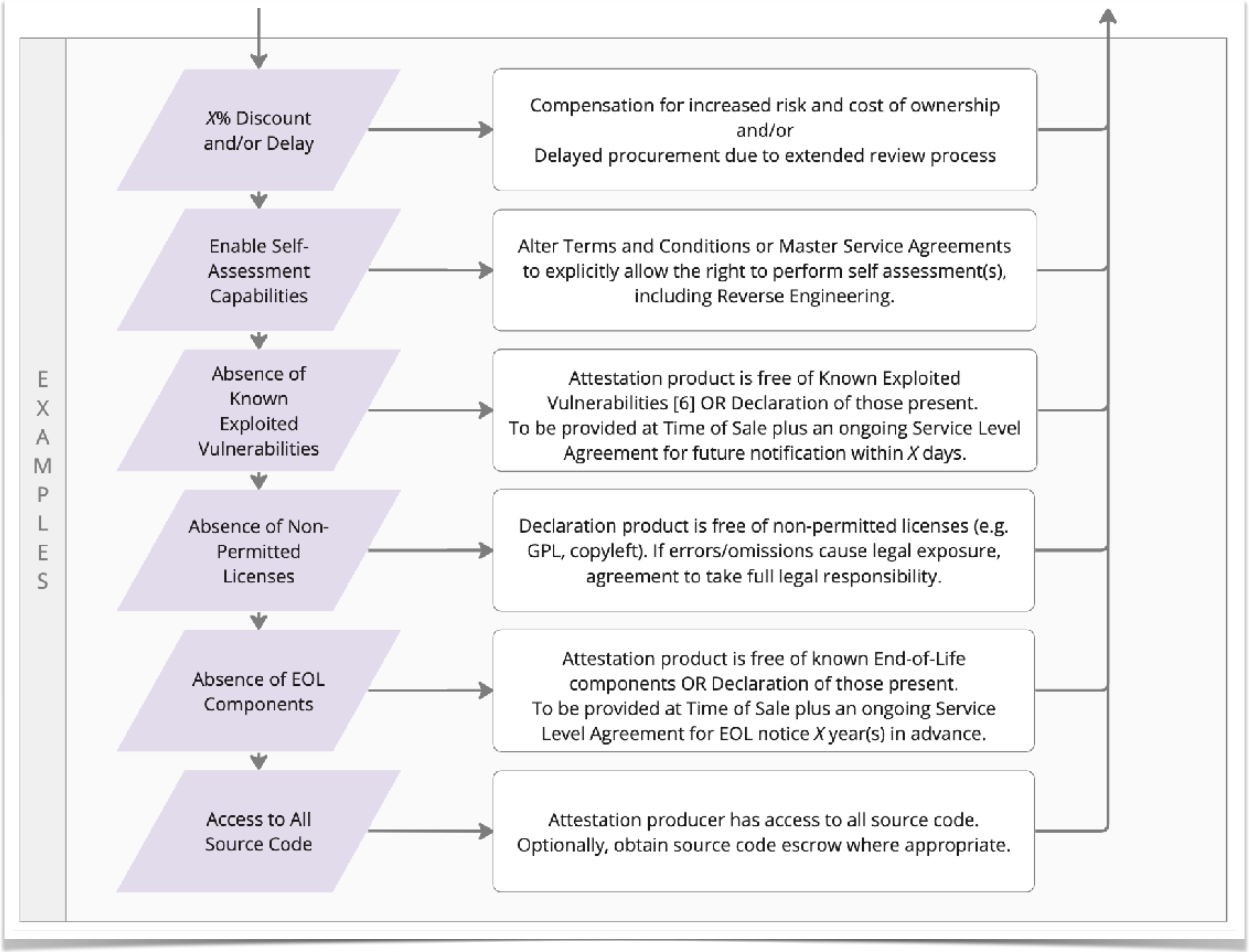
- Enables operators to perform ongoing assessment and quantification of risks inherent in software
- Manage mitigations for vulnerabilities
- Lower operating costs due to improved efficiencies
- Reduce unplanned, unscheduled work

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.

Business Goals
Understand & Avoid Vulnerability Risk
Understand & Avoid Legal/License Risk
Understand Support Lifecycle & Support Horizon
Reduce / Offset Cost of Ownership
You Are Here
Procurement / Acquisition
Operational Uses
Incident Response/Impact Assessment Questions
Ongoing High Risk Vulnerability Governance
Vulnerability Lifecycle Management
Patch & Product Support
Budget & Change Management Planning

PROCUREMENT/ACQUISITION PRIMER



X% Discount and/or Delay

Compensation for increased risk and cost of ownership
and/or
Delayed procurement due to extended review process

Enable Self-Assessment Capabilities

Alter Terms and Conditions or Master Service Agreements to explicitly allow the right to perform self assessment(s), including Reverse Engineering.

Absence of Known Exploited Vulnerabilities

Attestation product is free of Known Exploited Vulnerabilities [6] OR Declaration of those present. To be provided at Time of Sale plus an ongoing Service Level Agreement for future notification within *X* days.

Absence of Non-Permitted Licenses

Declaration product is free of non-permitted licenses (e.g. GPL, copyleft). If errors/omissions cause legal exposure, agreement to take full legal responsibility.

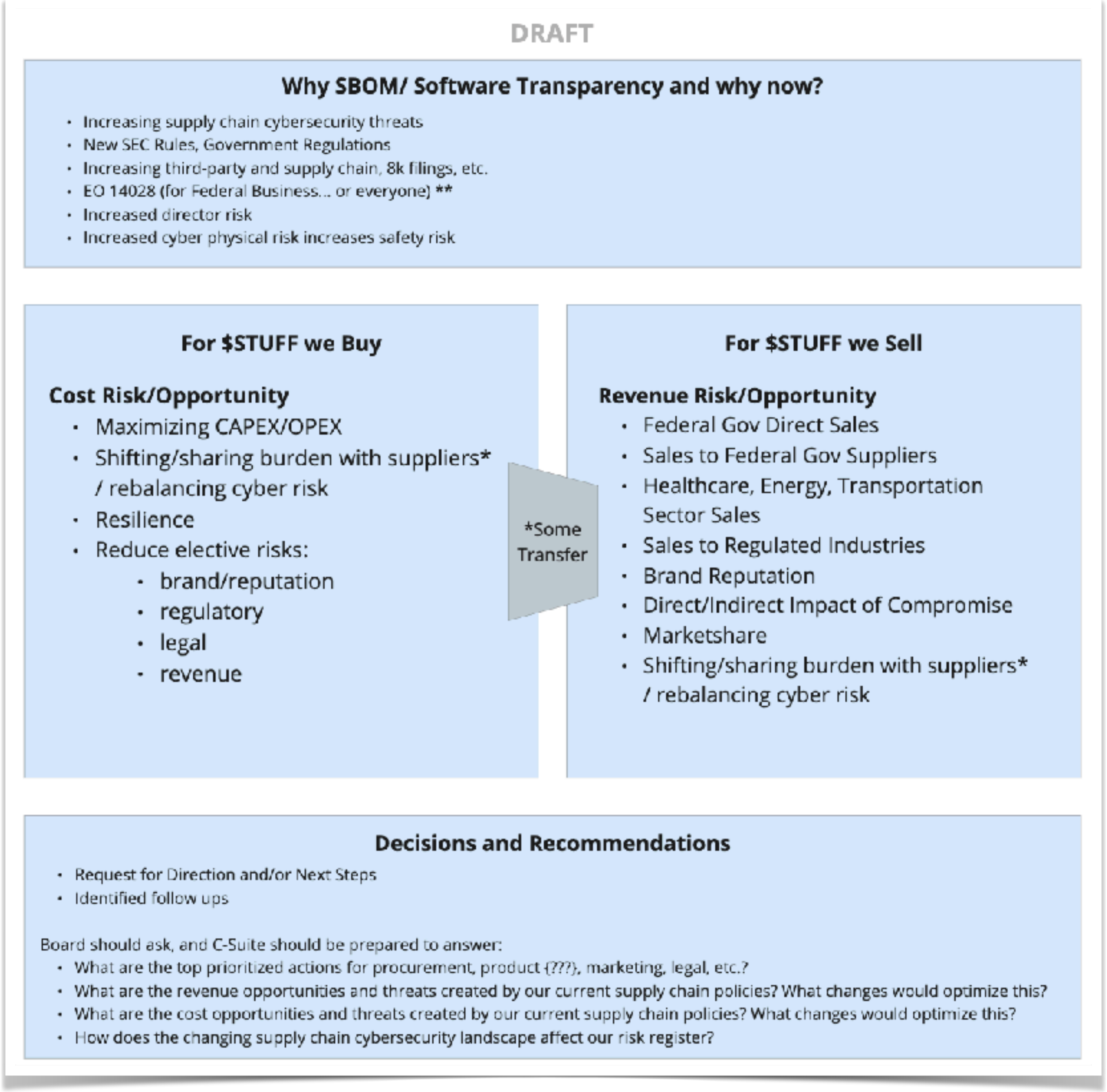
Absence of EOL Components

Attestation product is free of known End-of-Life components OR Declaration of those present. To be provided at Time of Sale plus an ongoing Service Level Agreement for EOL notice *X* year(s) in advance.

Access to All Source Code

Attestation producer has access to all source code. Optionally, obtain source code escrow where appropriate.

SBOM FOR BOARD OF DIRECTORS



DRAFT

Why SBOM/ Software Transparency and why now?

- Increasing supply chain cybersecurity threats
- New SEC Rules, Government Regulations
- Increasing third-party and supply chain, 8k filings, etc.
- EO 14028 (for Federal Business... or everyone) **
- Increased director risk
- Increased cyber physical risk increases safety risk

For $STUFF we Buy

Cost Risk/Opportunity

- Maximizing CAPEX/OPEX
- Shifting/sharing burden with suppliers* / rebalancing cyber risk
- Resilience
- Reduce elective risks:
  - brand/reputation
  - regulatory
  - legal
  - revenue

*Some Transfer

For $STUFF we Sell

Revenue Risk/Opportunity

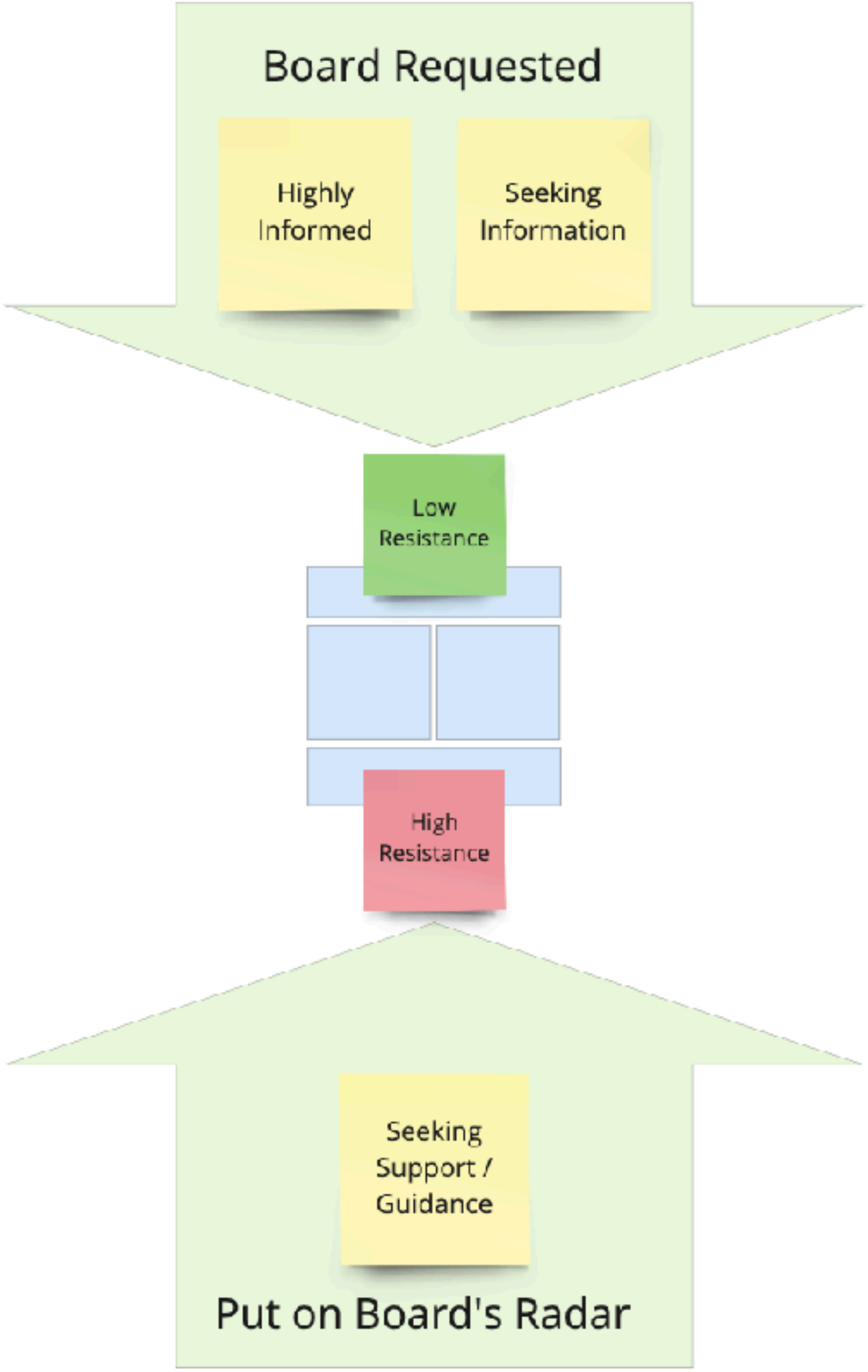
- Federal Gov Direct Sales
- Sales to Federal Gov Suppliers
- Healthcare, Energy, Transportation Sector Sales
- Sales to Regulated Industries
- Brand Reputation
- Direct/Indirect Impact of Compromise
- Marketshare
- Shifting/sharing burden with suppliers* / rebalancing cyber risk

Decisions and Recommendations

- Request for Direction and/or Next Steps
- Identified follow ups

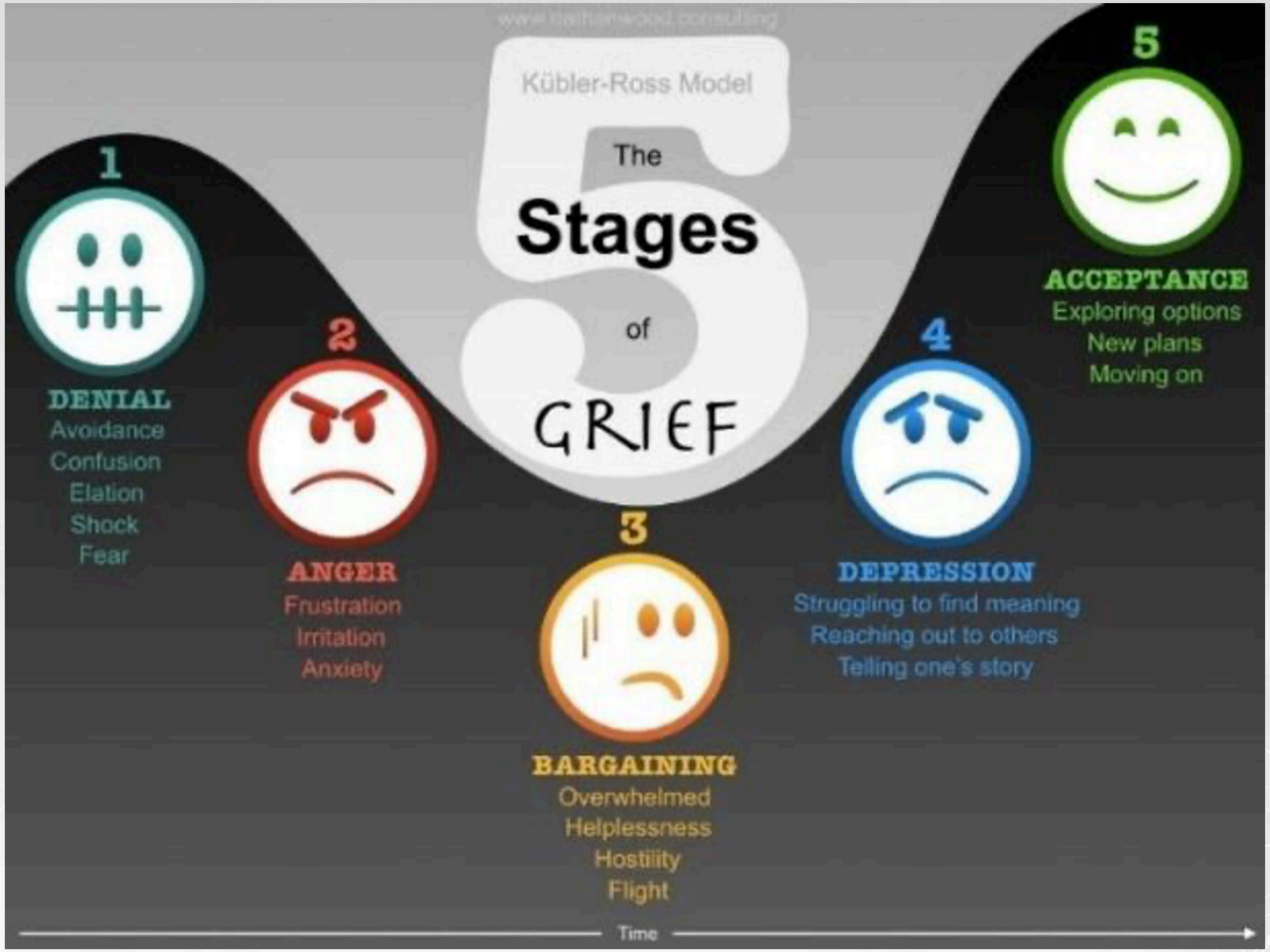
Board should ask, and C-Suite should be prepared to answer:

- What are the top prioritized actions for procurement, product (???), marketing, legal, etc.?
- What are the revenue opportunities and threats created by our current supply chain policies? What changes would optimize this?
- What are the cost opportunities and threats created by our current supply chain policies? What changes would optimize this?
- How does the changing supply chain cybersecurity landscape affect our risk register?



FUTURE INITIATIVES & SAMPLE NOMINATIONS FOR 2024

- 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



Excerpt from "The Opposite of Transparency" https://youtu.be/qk2vo7ir1cI

TRANSPARENCY IS COMING

Generated by Font-Generator.com

iamthecavalry.org

I AM THE Cavalry

Excerpt from “The Opposite of Transparency” https://youtu.be/qk2vo7ir1cI

SBOM IS COMING

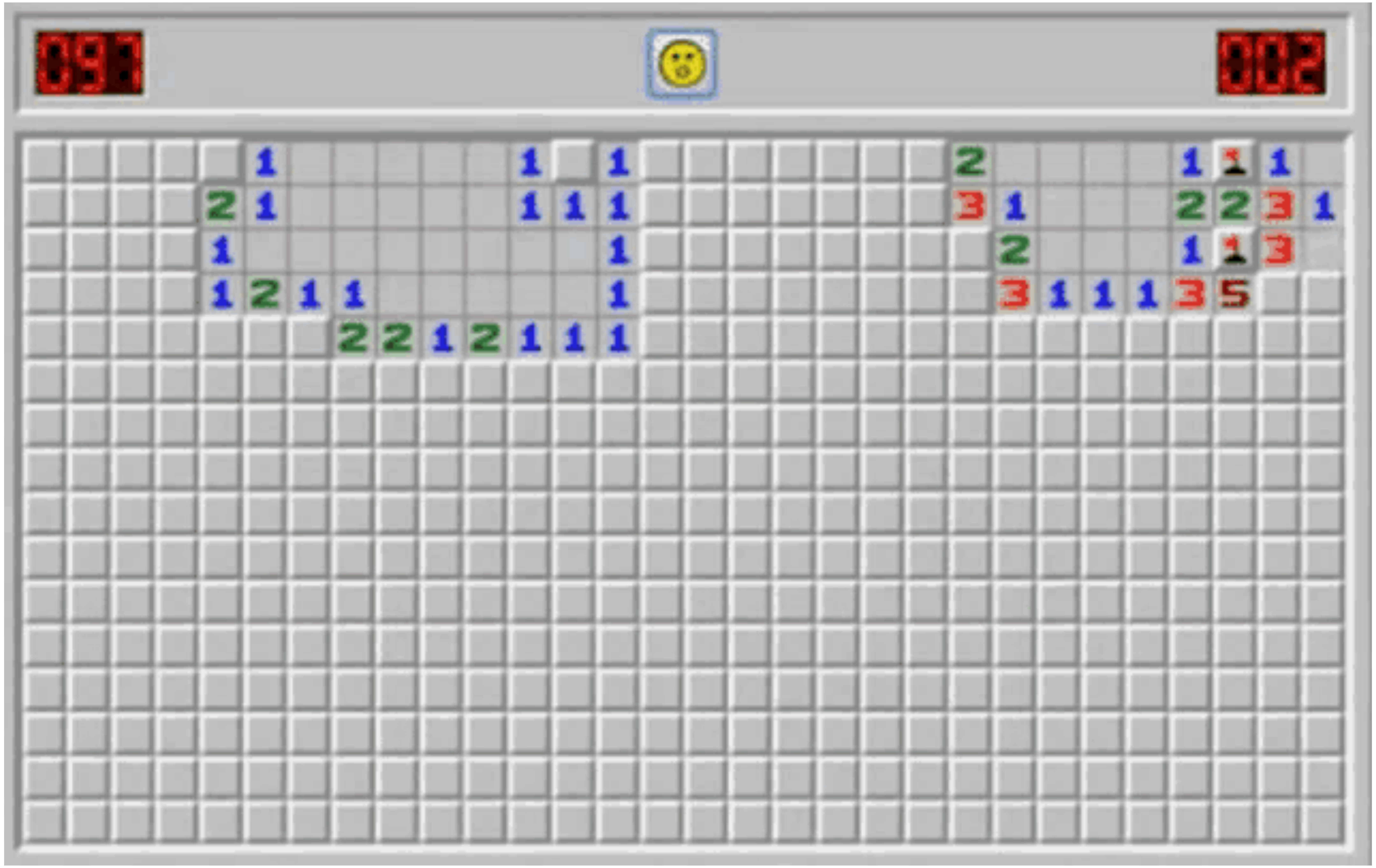
Generated by Font-Generator.com

iamthecavalry.org

I AM THE Cavalry

Excerpt from “The Opposite of Transparency” https://youtu.be/qk2vo7ir1cI

BOMBS – VISIBILITY VS OPACITY



~~Symptoms (& smokescreens?)~~ Heart of the Hydra

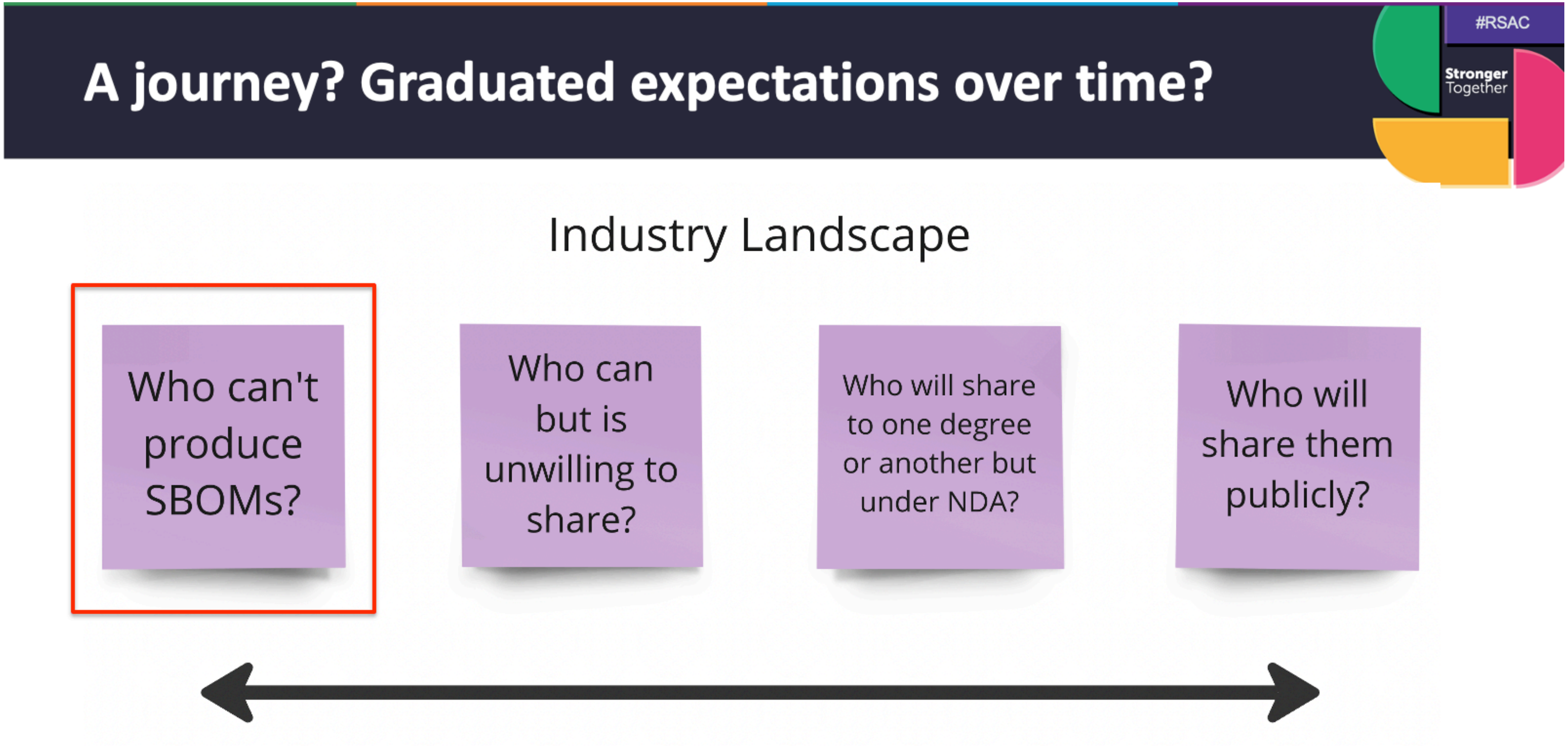
1) License violations

2) “Unfixable” issues

3) Ongoing scrutiny / accountability

4) $Other

Excerpt from “The Opposite of Transparency” https://youtu.be/qk2vo7ir1cI



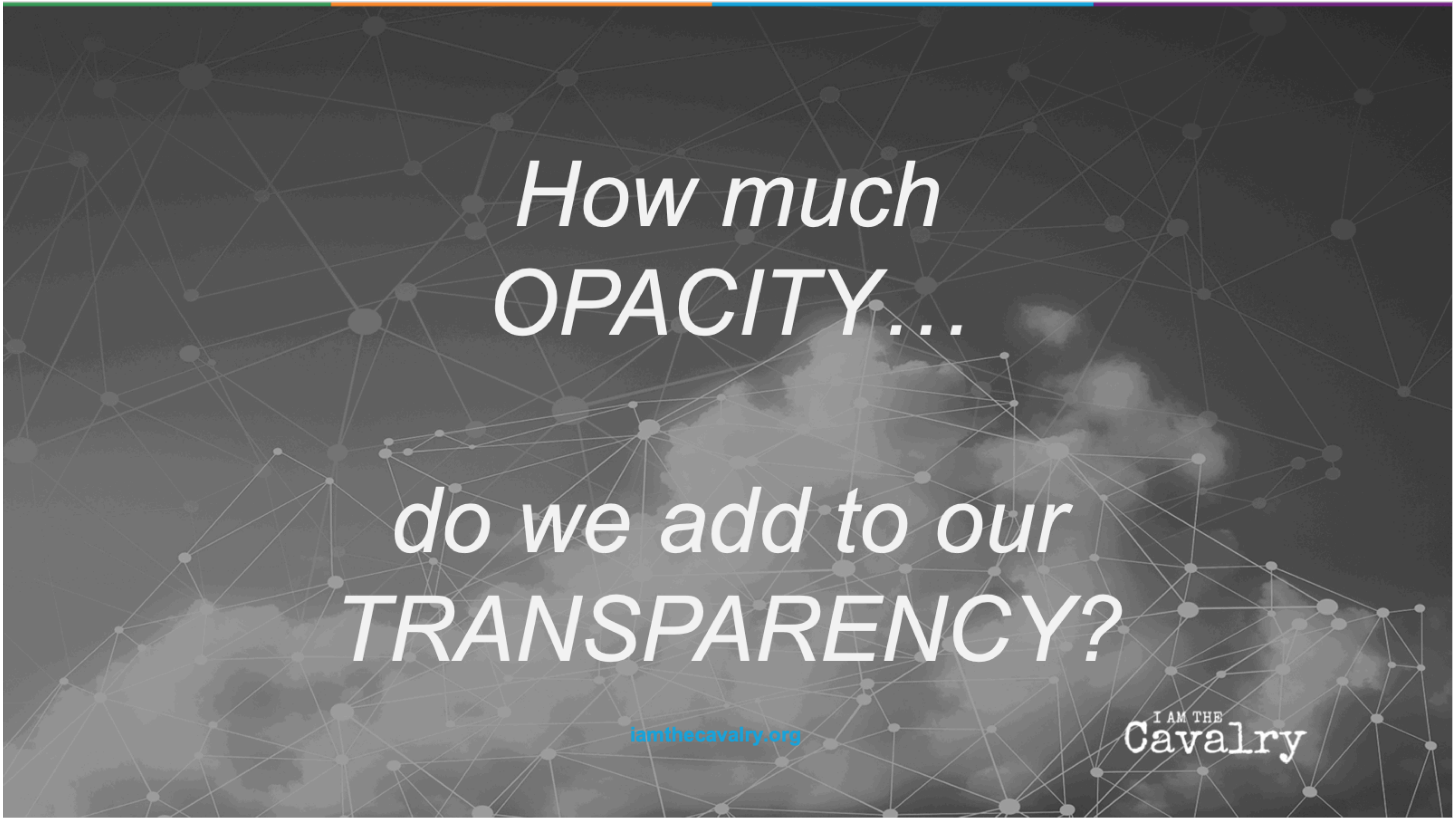
A journey? Graduated expectations over time?

#RSAC Stronger Together

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/qk2vo7ir1cI



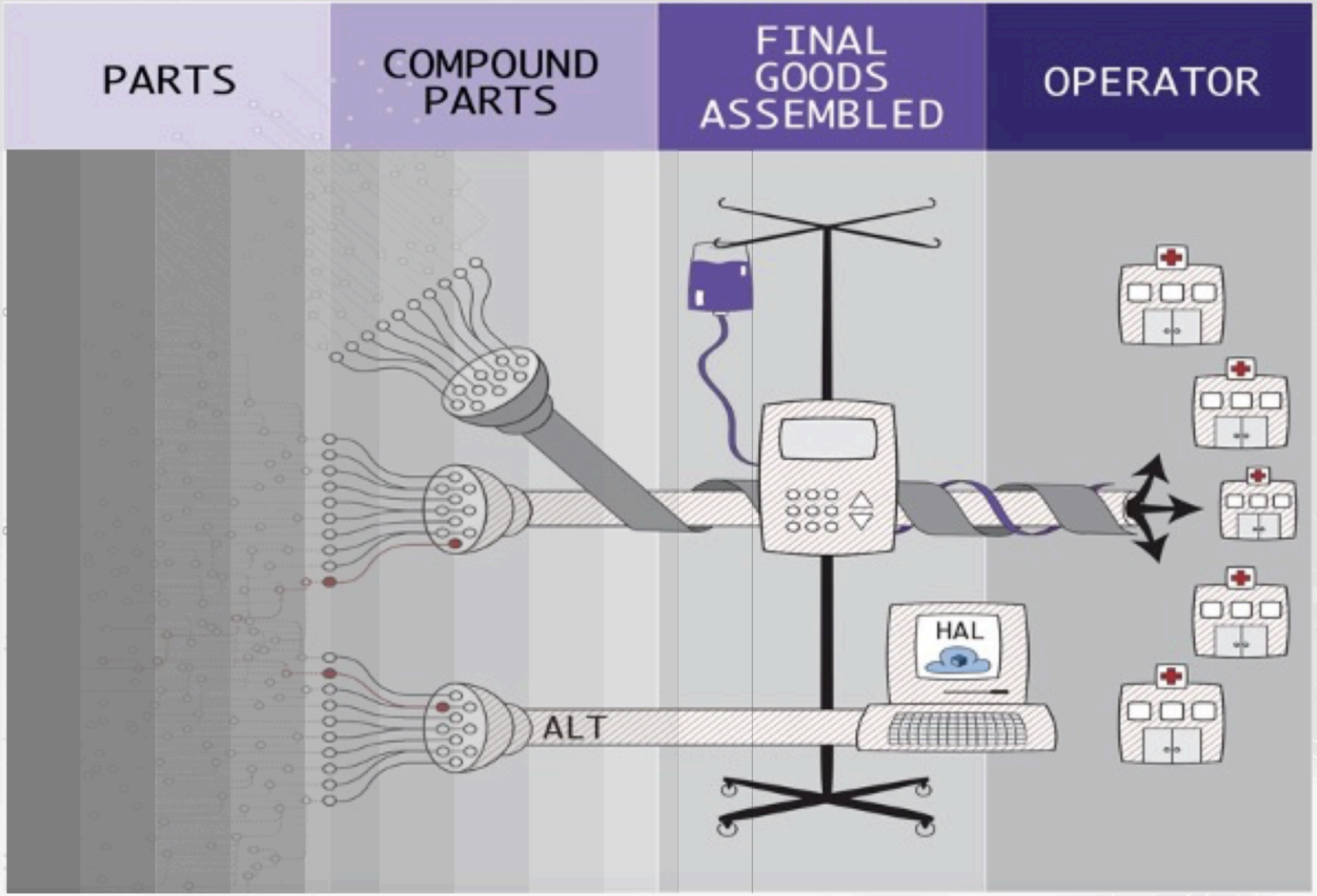
How much
OPACITY…

do we add to our
TRANSPARENCY?

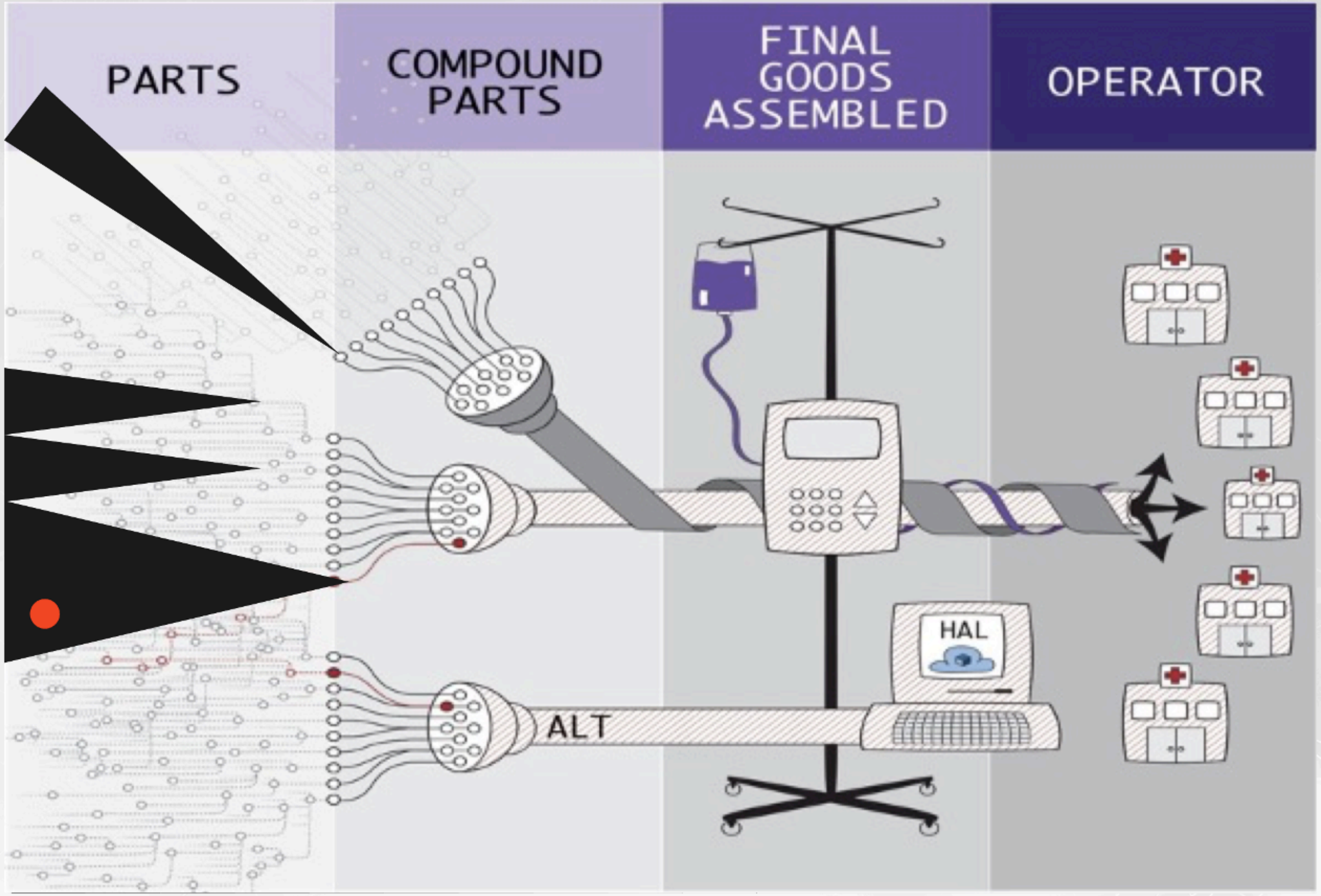
iamthecavalry.org

I AM THE Cavalry

Excerpt from “The Opposite of Transparency” https://youtu.be/qk2vo7ir1cI

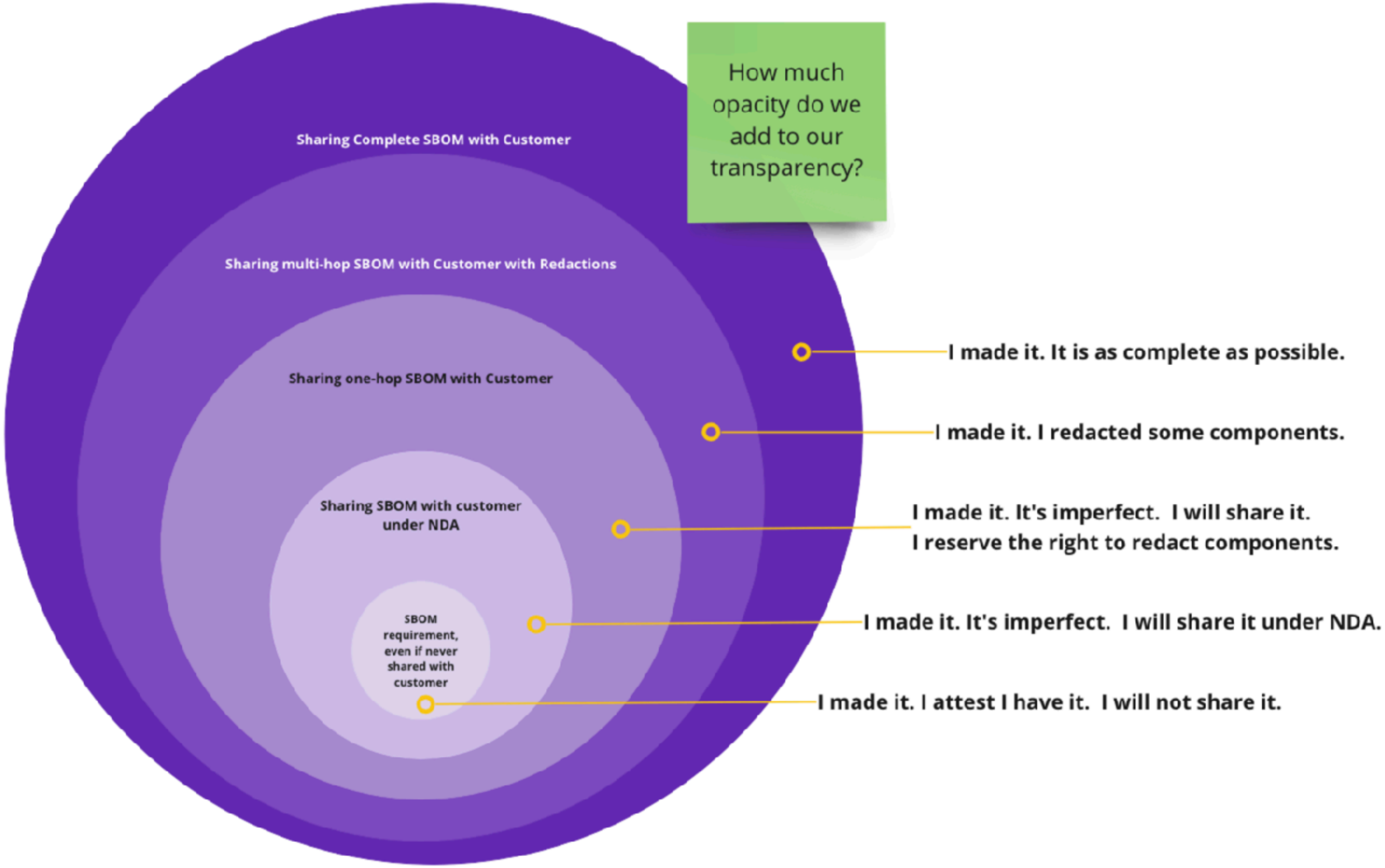


Excerpt from "The Opposite of Transparency" https://youtu.be/qk2vo7ir1cI



Excerpt from "The Opposite of Transparency" https://youtu.be/qk2vo7ir1cI

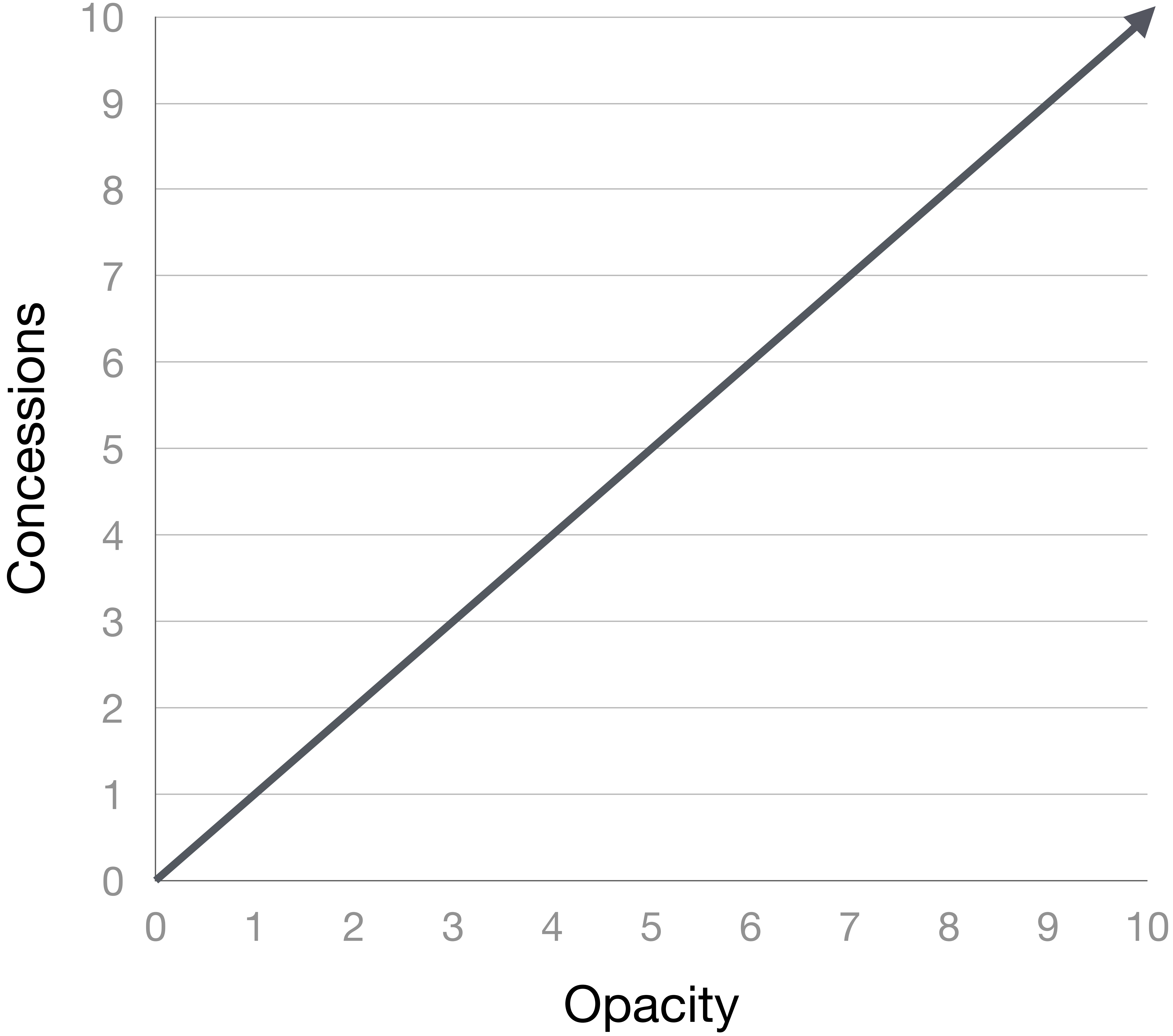
Rings of Expanding Value for SBOM



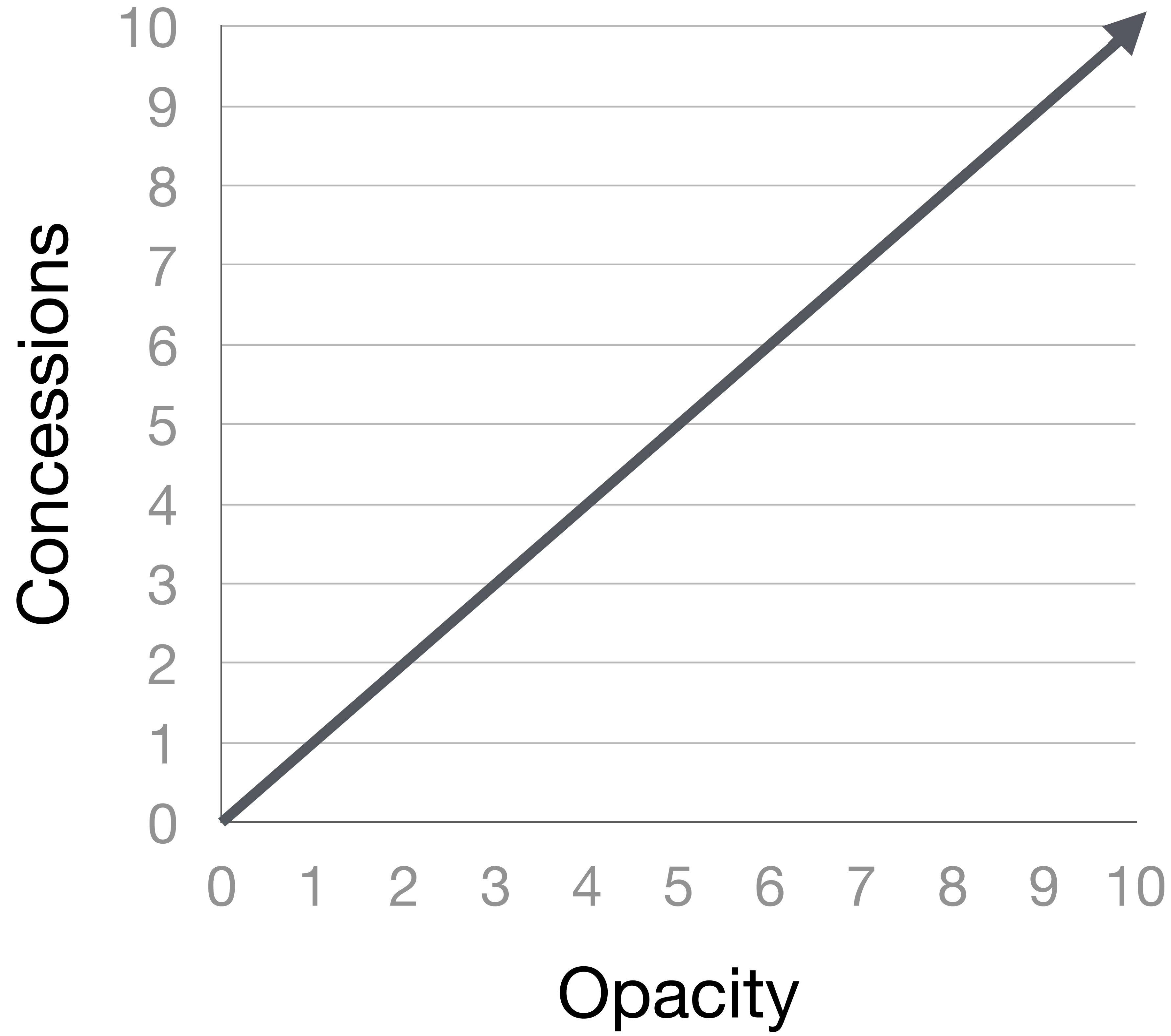
Sharing Complete SBOM with Customer
Sharing multi-hop SBOM with Customer with Redactions
Sharing one-hop SBOM with Customer
Sharing SBOM with customer under NDA
SBOM requirement, even if never shared with customer
How much opacity do we add to our transparency?
I made it. It is as complete as possible.
I made it. I redacted some components.
I made it. It's imperfect. I will share it.
I reserve the right to redact components.
I made it. It's imperfect. I will share it under NDA.
I made it. I attest I have it. I will not share it.

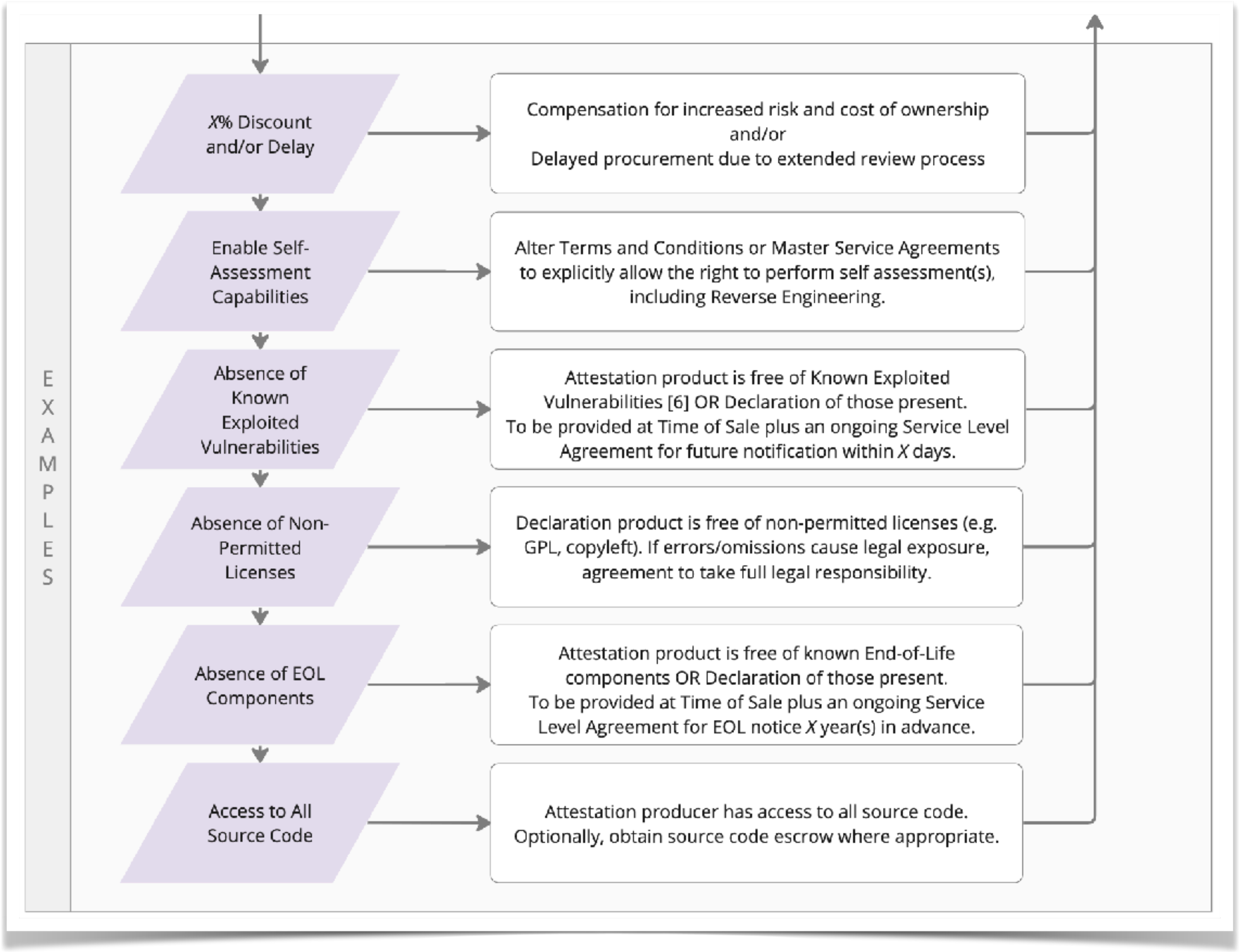
Excerpt from "The Opposite of Transparency" https://youtu.be/qk2vo7ir1cI

PROPORTIONAL OPACITY & CONCESSIONS



PROPORTIONAL OPACITY & CONCESSIONS




EXAMPLES

X% Discount and/or Delay → Compensation for increased risk and cost of ownership and/or Delayed procurement due to extended review process

Enable Self-Assessment Capabilities → Alter Terms and Conditions or Master Service Agreements to explicitly allow the right to perform self assessment(s), including Reverse Engineering.

Absence of Known Exploited Vulnerabilities → Attestation product is free of Known Exploited Vulnerabilities [6] OR Declaration of those present. To be provided at Time of Sale plus an ongoing Service Level Agreement for future notification within *X* days.

Absence of Non-Permitted Licenses → Declaration product is free of non-permitted licenses (e.g. GPL, copyleft). If errors/omissions cause legal exposure, agreement to take full legal responsibility.

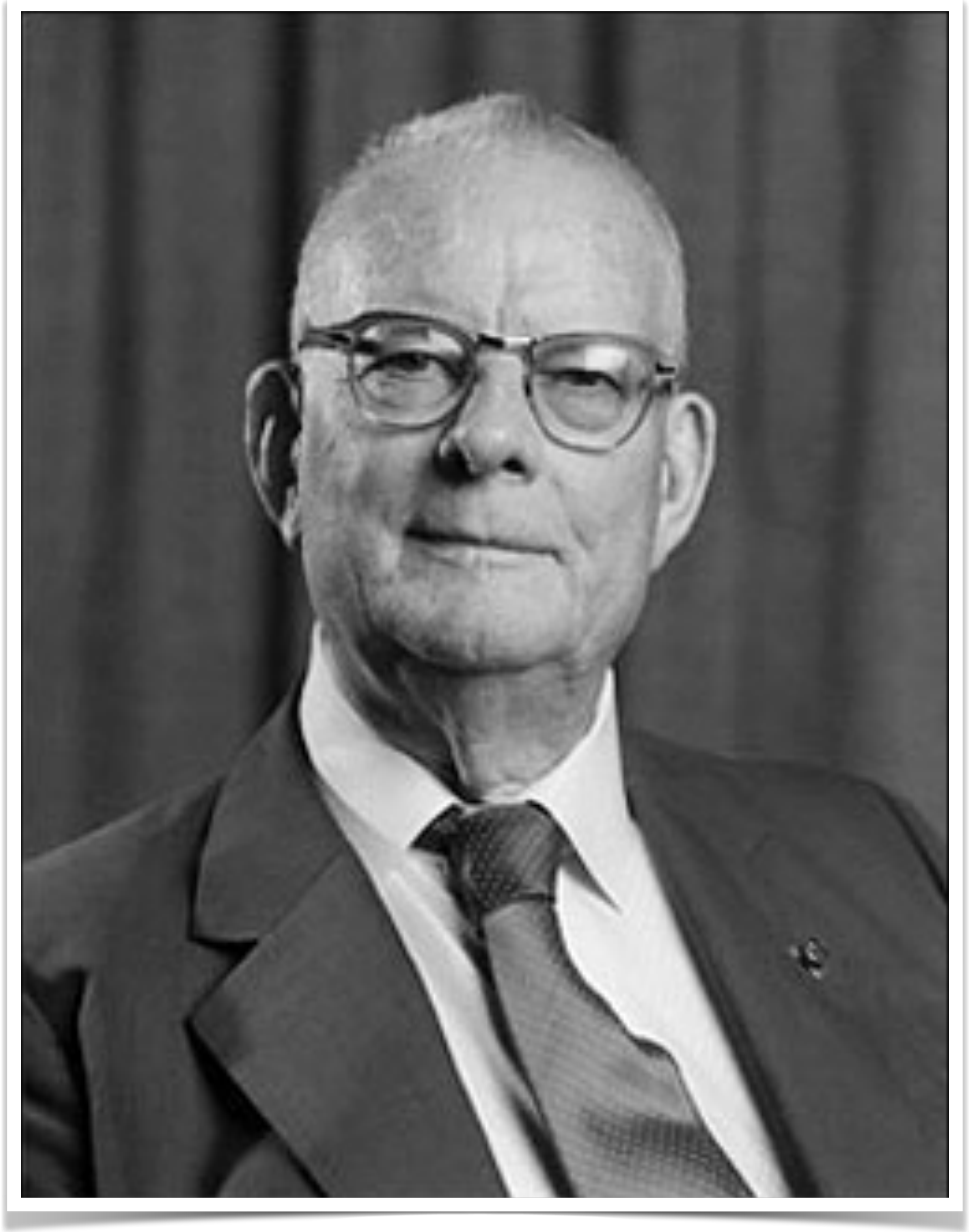
Absence of EOL Components → Attestation product is free of known End-of-Life components OR Declaration of those present. To be provided at Time of Sale plus an ongoing Service Level Agreement for EOL notice *X* year(s) in advance.

Access to All Source Code → Attestation producer has access to all source code. Optionally, obtain source code escrow where appropriate.

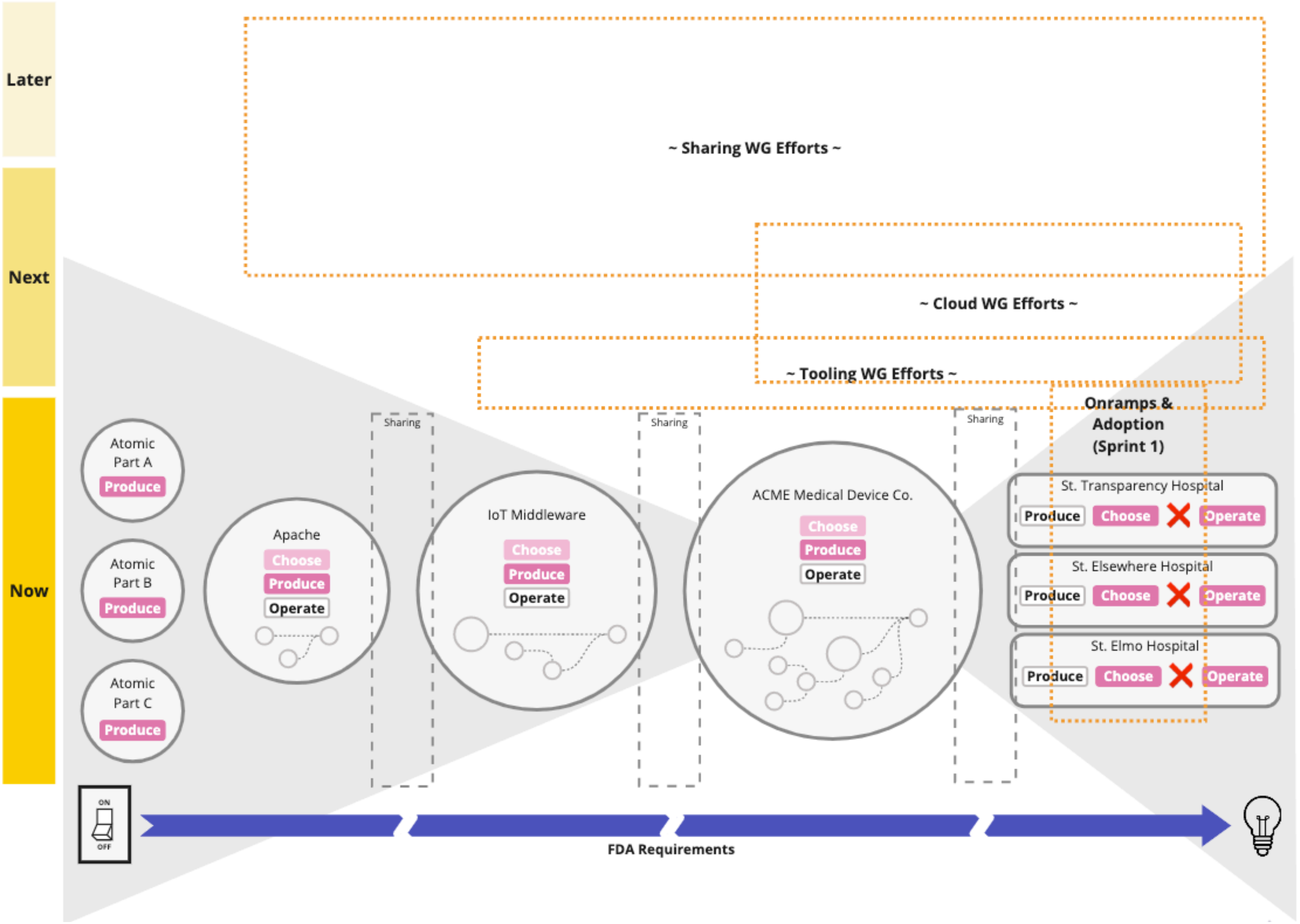
W. EDWARDS DEMING

"It is not necessary to change. Survival is not mandatory."

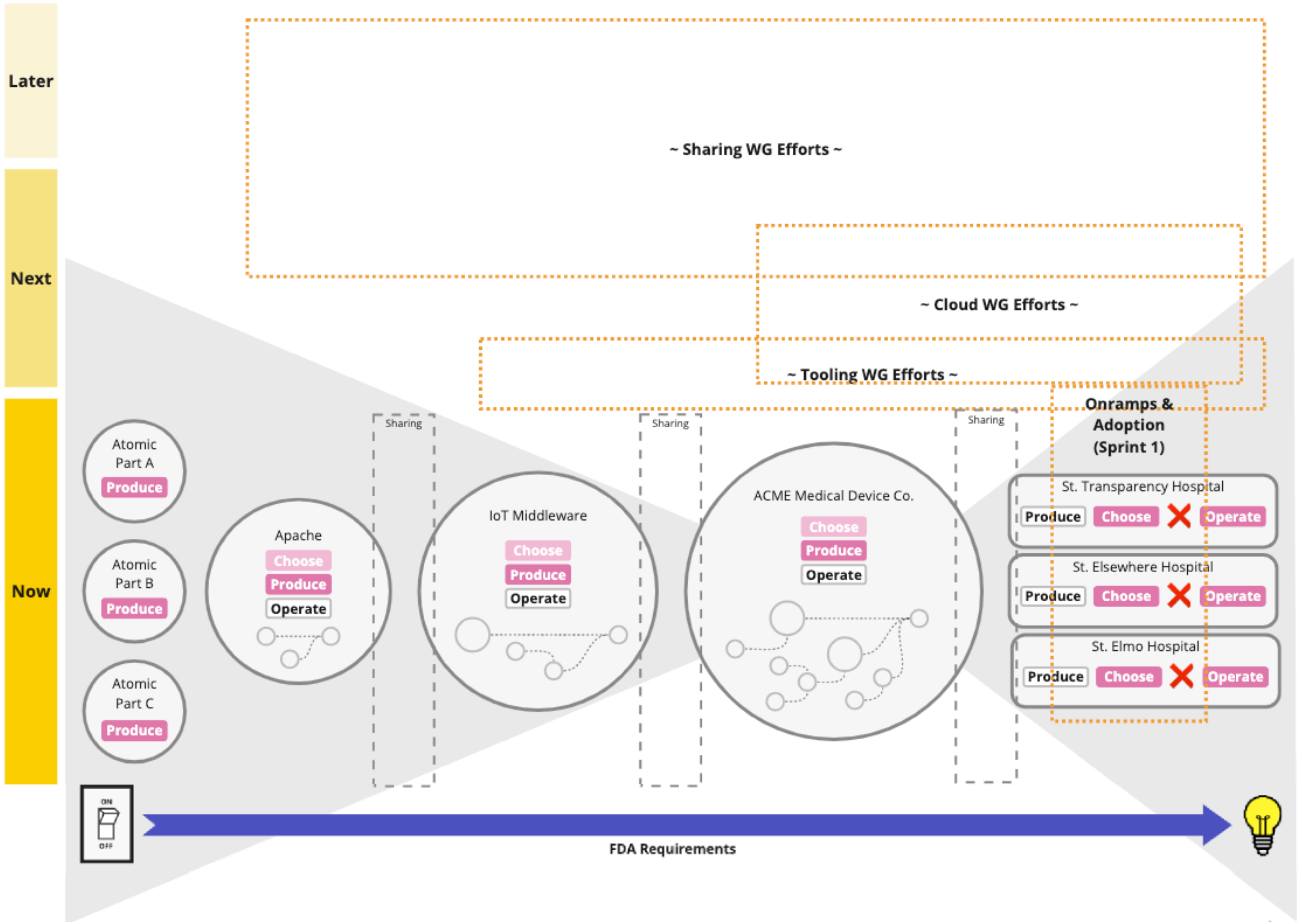
– W. Edwards Deming



FDA USE CASE / UNIFIED FIELD THEORY



FDA USE CASE / UNIFIED FIELD THEORY



Later

Next

Now

~ Sharing WG Efforts ~

~ Cloud WG Efforts ~

~ Tooling WG Efforts ~

Atomic Part A
Produce

Atomic Part B
Produce

Atomic Part C
Produce

Apache
Choose
Produce
Operate

Sharing

IoT Middleware
Choose
Produce
Operate

Sharing

ACME Medical Device Co.
Choose
Produce
Operate

Sharing

Onramps & Adoption (Sprint 1)

St. Transparency Hospital
Produce Choose ❌ Operate

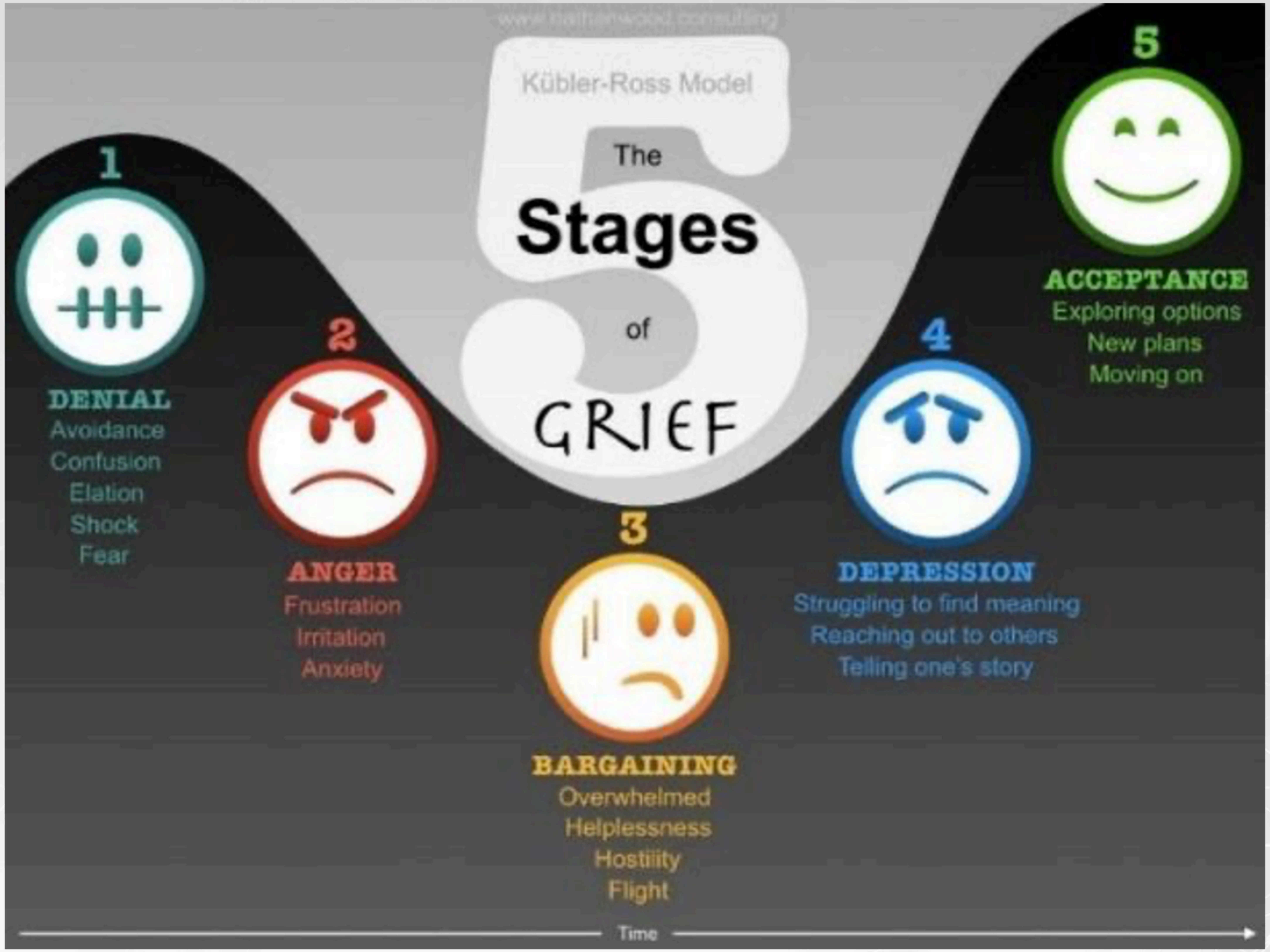
St. Elsewhere Hospital
Produce Choose ❌ Operate

St. Elmo Hospital
Produce Choose ❌ Operate

ON
OFF

FDA Requirements

INCREASING STIMULI



Excerpt from "The Opposite of Transparency" https://youtu.be/qk2vo7ir1cI

COMMUNITY ASK

- How you can help Onramps & Adoption:
  - We are seeking **new participants** and **project leads** for ongoing efforts
    - Testimonials
    - Incident Response
    - Board of Directors
    - Creative Colleagues (e.g. marketing, design, developer relations)
  - Submit upcoming events to the SBOM Calendar

- 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?

COMMUNITY ASK

Ask for an SBOM

from all your suppliers

RESOURCES

- NTIA Publications
  www.ntia.gov/sbom
- CISA Publications
  www.cisa.gov/sbom
- 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