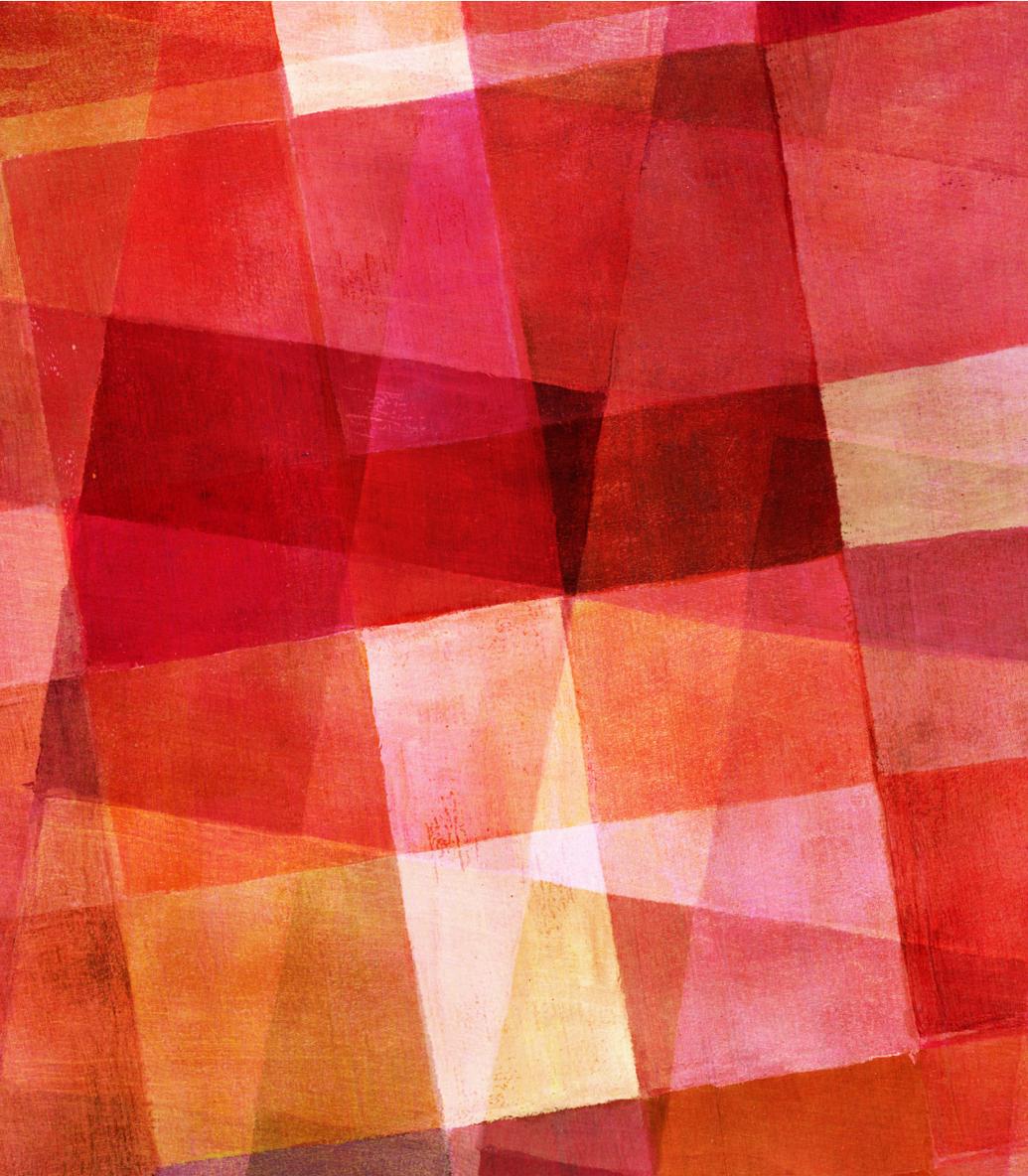


February 13, 2020

AWARENESS & ADOPTION

NTIA Software Component Transparency
Audra Hatch, Joshua Corman



OVERVIEW

- ▶ Awareness & Adoption Mission
- ▶ High Level Approach to Goals
- ▶ What We're Working On
- ▶ Future Initiatives & Wishlist
- ▶ Asks of other NTIA Groups & Community



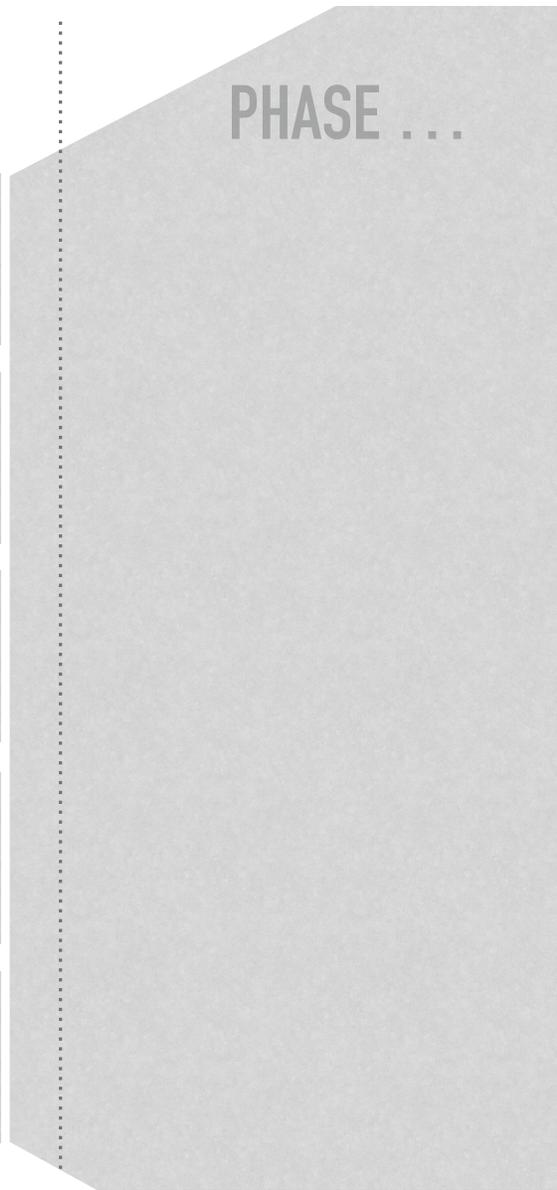
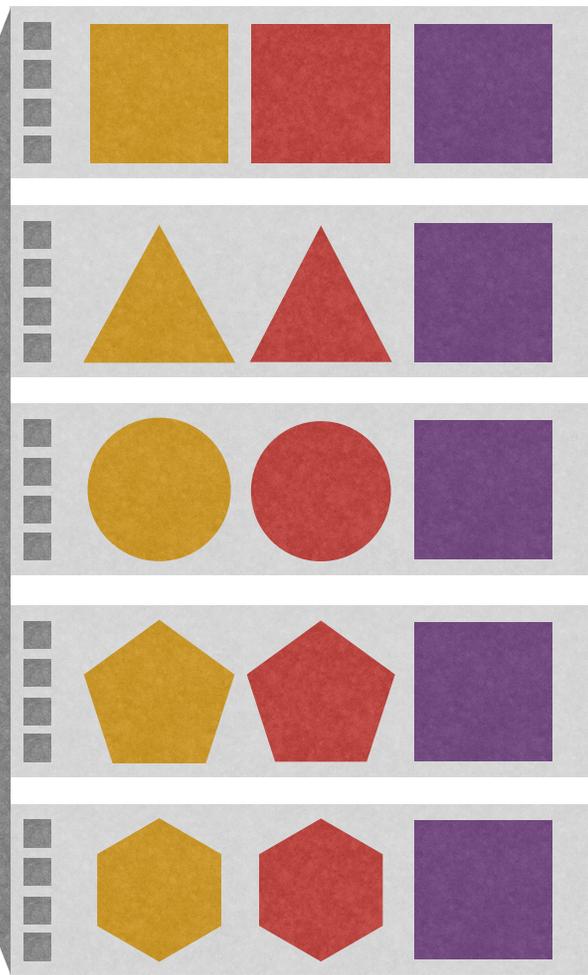
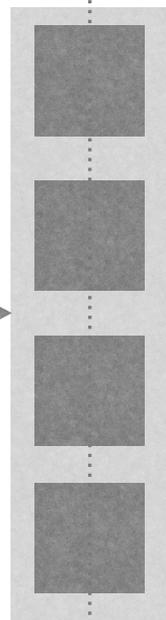
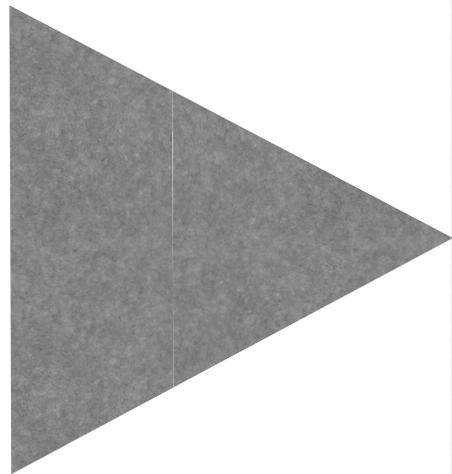
AWARENESS & ADOPTION MISSION

- Work will focus on promoting SBOM as an idea and a practice.
- Tasks identified include:
 - building a broader outreach strategy with outreach targets;
 - shorter documents with specific outreach goals for sectors, organizational role, etc;
 - coordinating with related efforts;
 - more explicit business cases for SBOM adoption.

PHASE I

PHASE II

PHASE ...





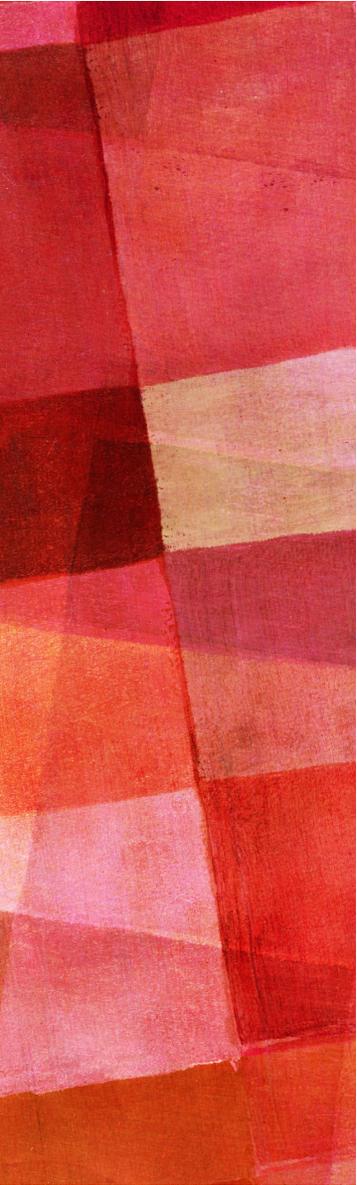
HIGH LEVEL APPROACH TO GOALS

- ▶ Outreach / Increase Awareness
 - ▶ Let people know about SBOM
 - ▶ Conference Presentations, Webinars, etc.
 - ▶ Connect People
 - ▶ Invitation to NTIA groups & documents, other networking, etc.
- ▶ Increase Adoption
 - ▶ Address early questions about SBOM
 - ▶ Provide fit-for-purpose “getting started” materials
 - ▶ Journeys: Crawl / Walk / Run



WHAT WE'RE WORKING ON

- ▶ FAQ - Broad Categories:
 - ▶ Dominant, broad questions
 - ▶ Myths & Concerns about SBOM
 - ▶ SBOM Implementation
 - ▶ Role-Specific
- ▶ Two-pager Documents - Targeted to specific audience or perspective
- ▶ Outreach Opportunities - List of Conferences and Entities to engage on SBOM



WHAT WE'RE WORKING ON

► FAQ Examples

Q: What is an SBOM?

A: A software bill of materials (SBOM) is an inventory of the software components, assemblies, subassemblies, parts and components, as well as the relationships of each, included in a software product. An SBOM tries to describe these components and their relationship to sufficiently understand the software product.

Q: What are the benefits of an SBOM?

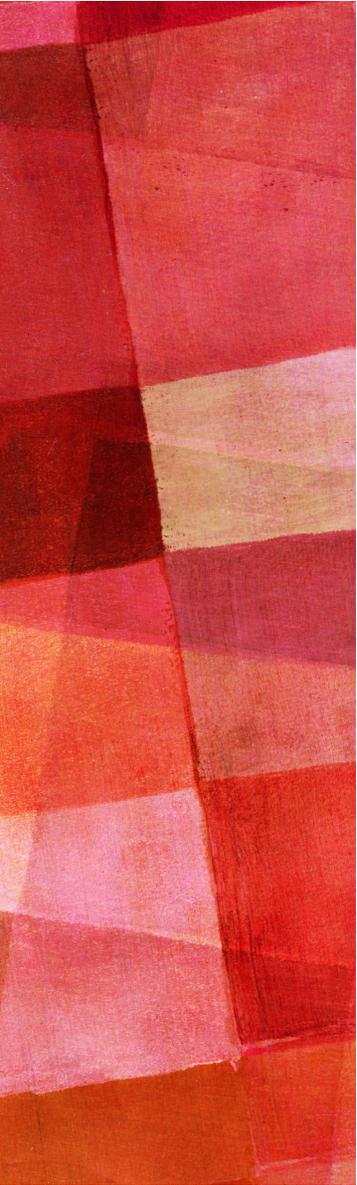
A: The benefits of an SBOM are many, and they include:

- Avoid known vulnerabilities
- Quantify and manage licenses
- Identify compliance requirements earlier in the lifecycle
- Less unplanned, unscheduled work

These benefits can be seen by those who develop software, those who select or purchase software, and those who operate software, across every sector. For a complete discussion of all the benefits please see the following document: [Roles and Benefits for SBOM Across the Supply Chain](#)

Q: Do SBOMs change?

A: Since an SBOM reflects the state of the software, a new SBOM should be created for every new release of a component. Changes to components require corresponding changes to SBOMs. Changes to components are often noted as updates, upgrades, releases, and patches. Moreover, an SBOM should be created or updated when information about included components changes, even if the components themselves have not changed. For example, an SBOM should be updated when an included component is changed and also when a supplier starts providing or provides new SBOM information. Maintaining current SBOM information is essential. (More information is available in [Section 4.2 of this document](#).)



FUTURE INITIATIVES & WISHLIST

- ▶ Need for seamless navigation through NTIA SBOM Documents
- ▶ Slide Decks
 - ▶ e.g. “Introduction to SBOM” deck(s)
 - ▶ Compilation of existing slide decks as a general resource for supporting creation of new presentations
- ▶ Graphics Resource Folder
- ▶ Stages of SBOM: Crawl / Walk / Run - Resource to aid in identifying “Next Steps”



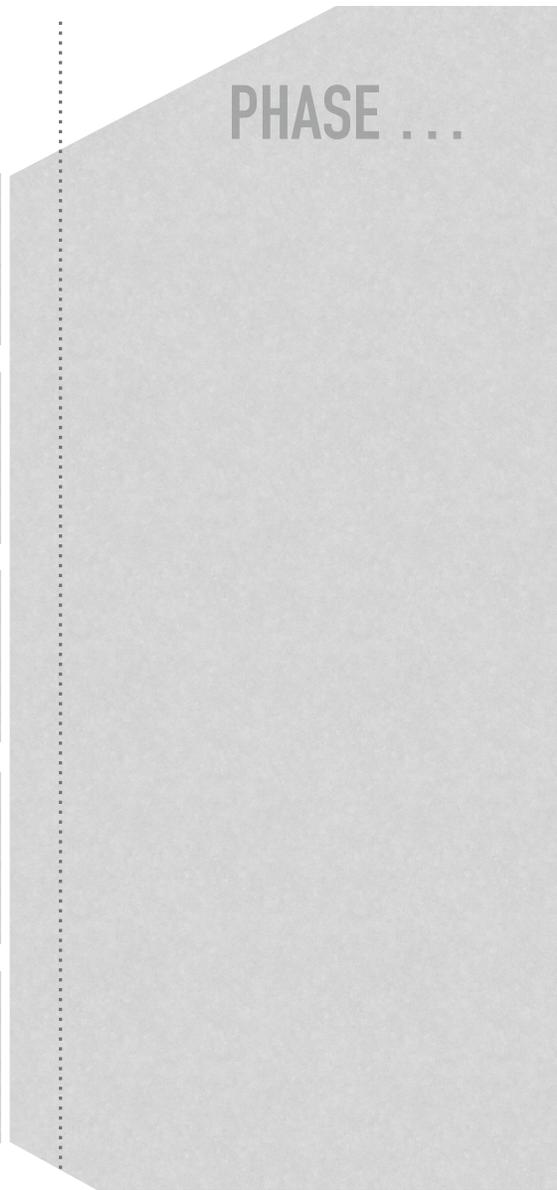
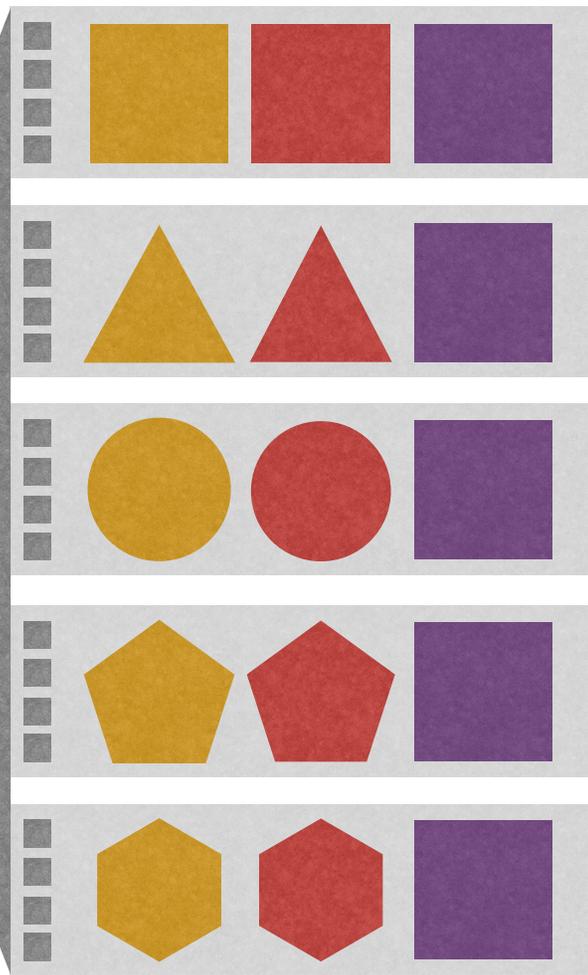
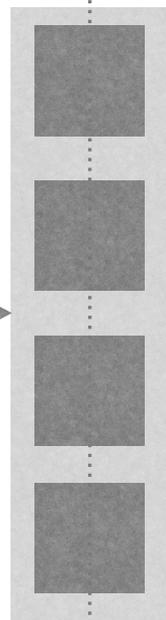
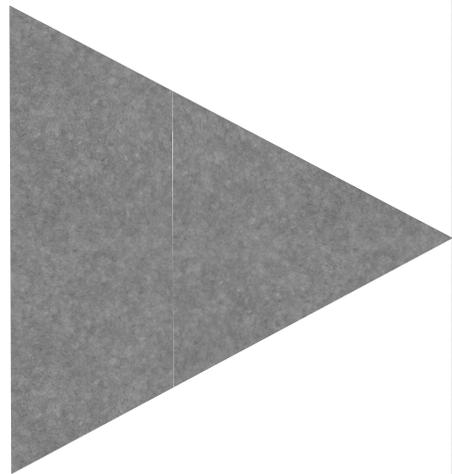
ASKS OF OTHER NTIA GROUPS & COMMUNITY

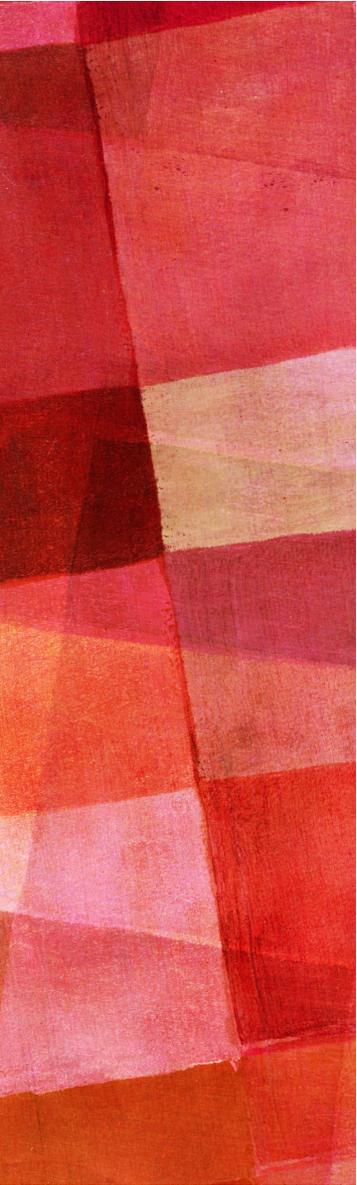
- ▶ SBOM Resources: What do you want?
 - ▶ e.g. Slide decks
- ▶ What are we not yet working on that would be helpful?
- ▶ We need: Industry-specific Translators & Guides
- ▶ Expect Experimentation & Iteration
 - ▶ Come help us!

PHASE I

PHASE II

PHASE ...





RESOURCES

- ▶ Awareness & Adoption Meeting
 - ▶ Fridays at 1:00 PM ET
- ▶ Google Drive Folder:
 - ▶ <http://bit.ly/sbom-awareness-google-drive>
- ▶ Meeting Notes: <http://bit.ly/sbom-awareness-meeting-notes>
- ▶ FAQ: <http://bit.ly/sbom-awareness-faq>