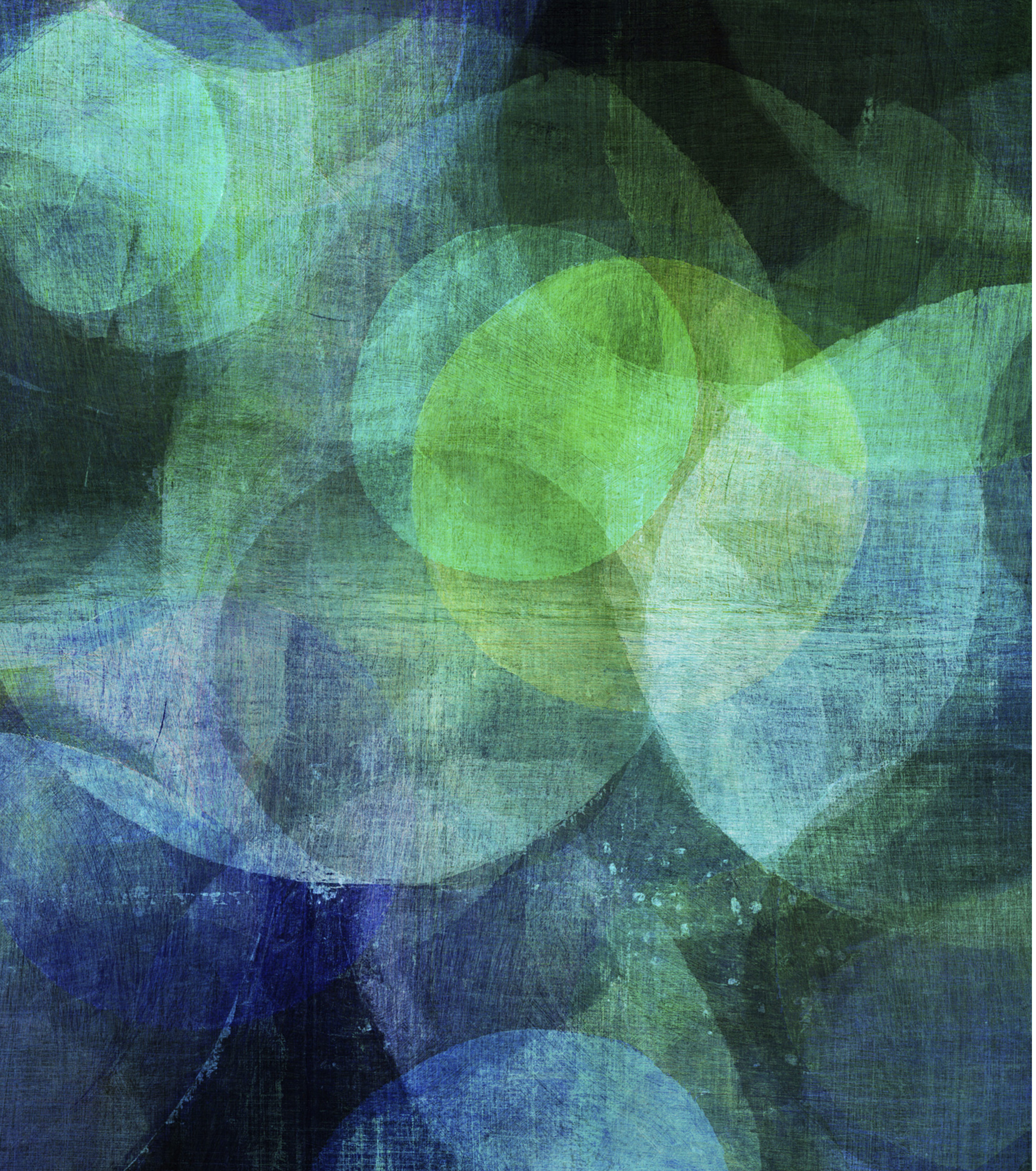
April 15, 2020

AWARENESS & ADOPTION

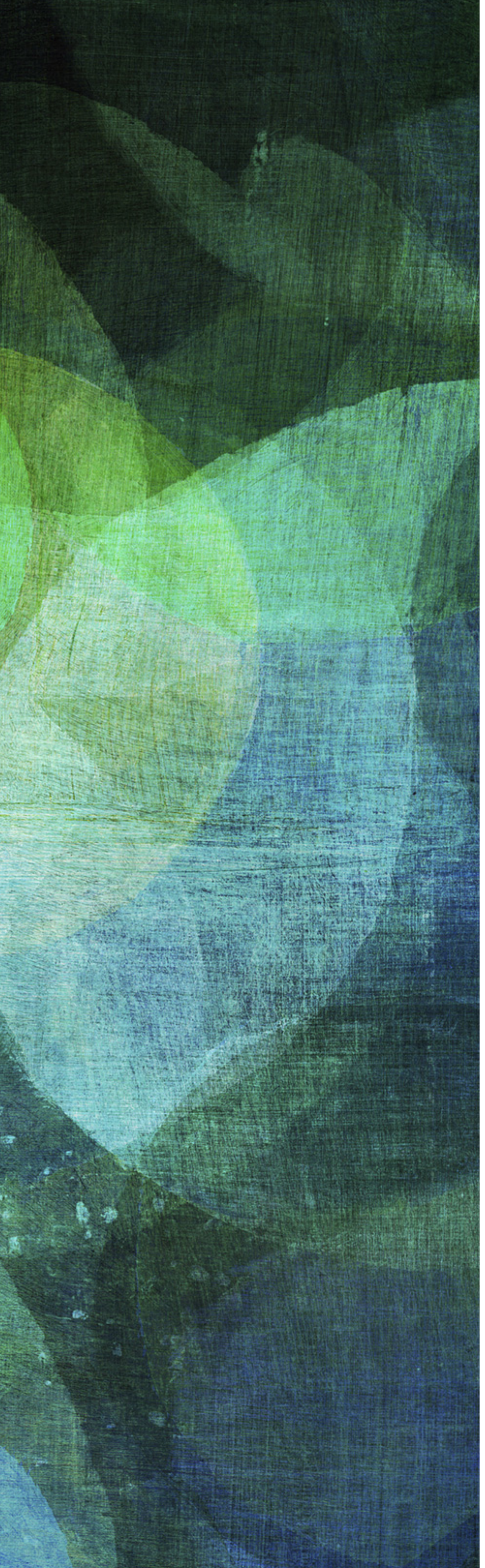
NTIA Software Component Transparency

Audra Hatch, Joshua Corman



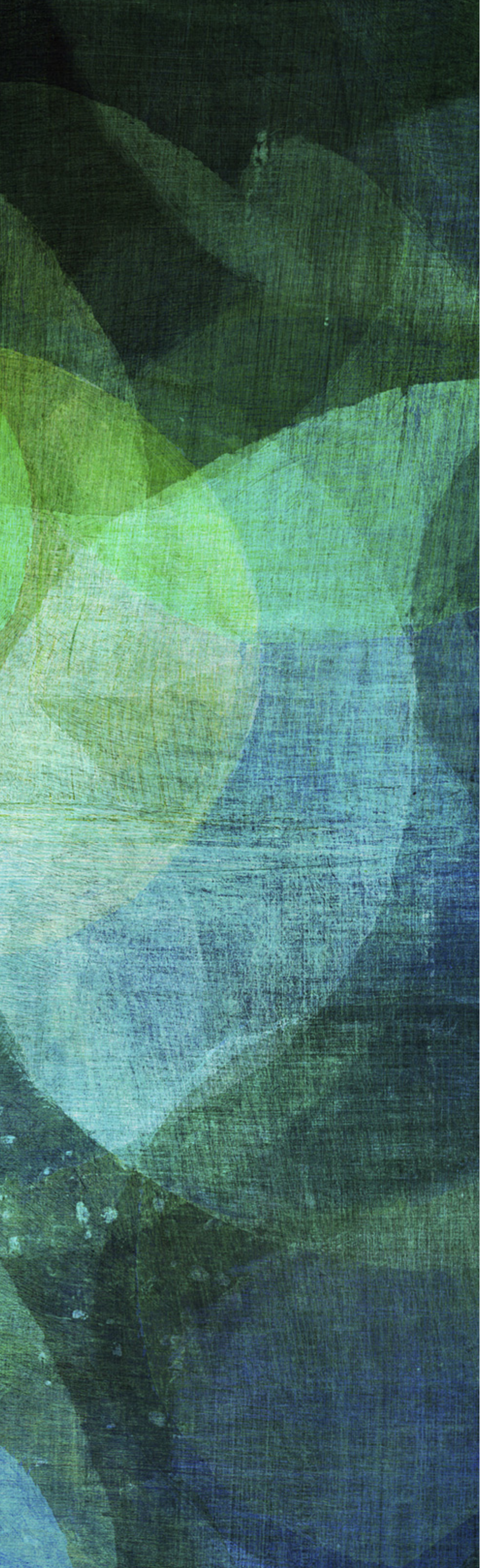
OVERVIEW

- Recap: Mission and Goals
- What We’re Working On
    - Today’s Deliverables
    - Ongoing Efforts
- Community Ask
- Resources



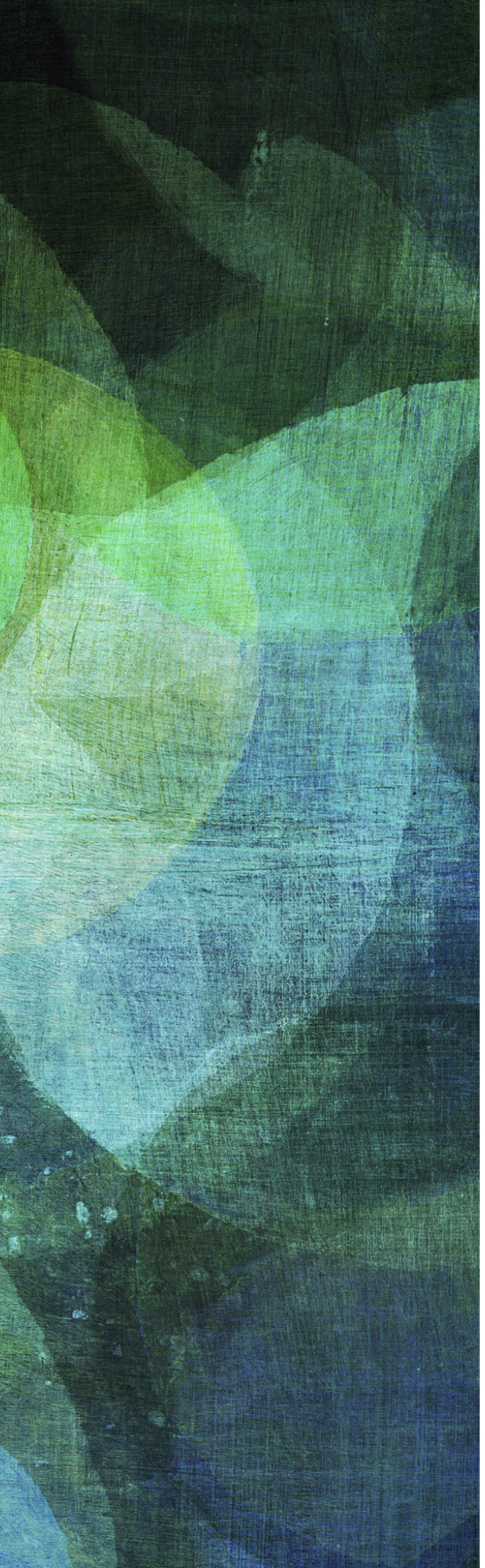
RECAP: AWARENESS & ADOPTION MISSION

- 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.



RECAP: 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

- Today's Deliverables:
  - FAQ - Current Release
  - DRAFT Generic Two-Pager
  - Recent Public SBOM Recordings
- Ongoing Efforts:
  - FAQ - Backlog and Active Development
  - SBOM Two-pager Documents - Tailored to industry and/or role
  - Graphics Repository
  - Short SBOM "Explainer" Videos
  - Knowledge Base - Searchable, cross-linked Phase I Documents
  - Virtual Engagement Opportunities

FAQ - CURRENT RELEASE

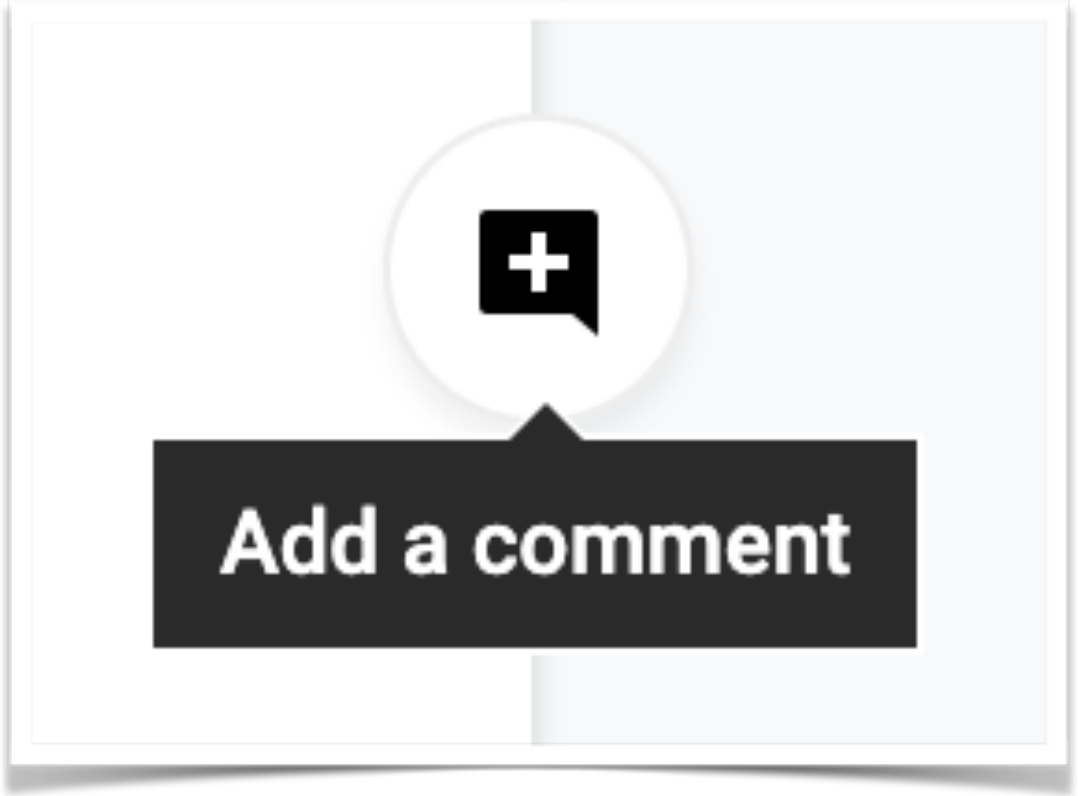
- April 15 Version - Questions prepared for feedback
- Broad Categories:
  - General Questions
  - Concerns about SBOM
  - SBOM Implementation
  - Role-Specific
- Backlog and Active Development:
  - Questions that need additional work prior to distribution to the broader working groups

FAQ FEEDBACK

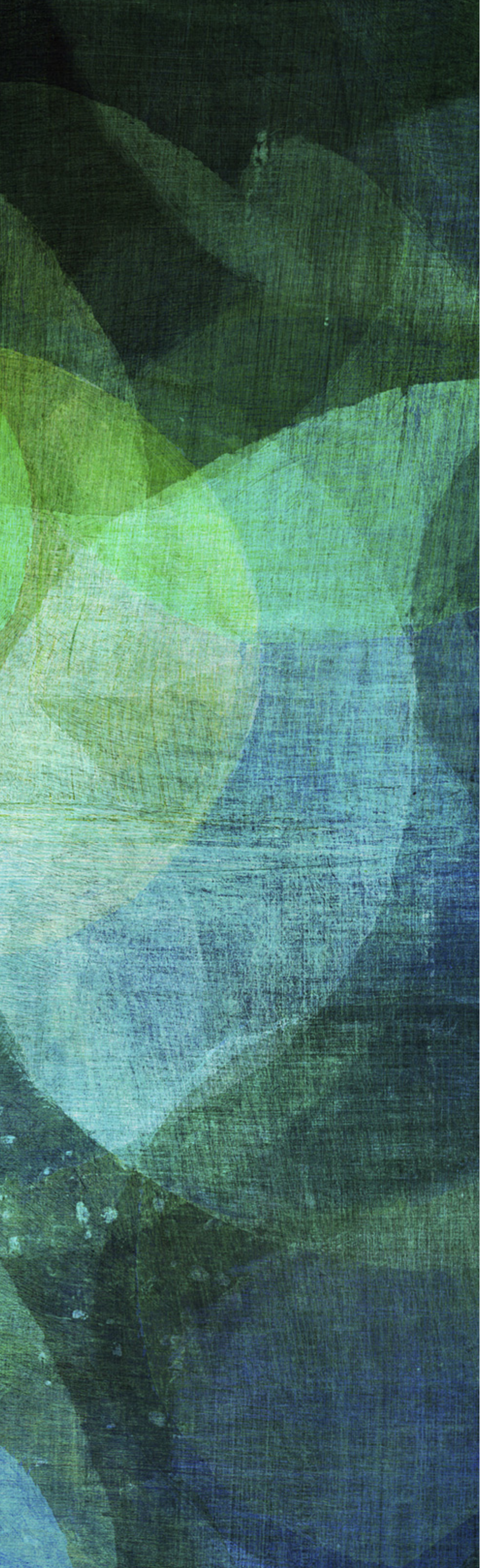
- April 15 Version - Questions prepared for feedback: https://bit.ly/sbom-awareness-faq-april15

- Feedback Due: May 1, 2020

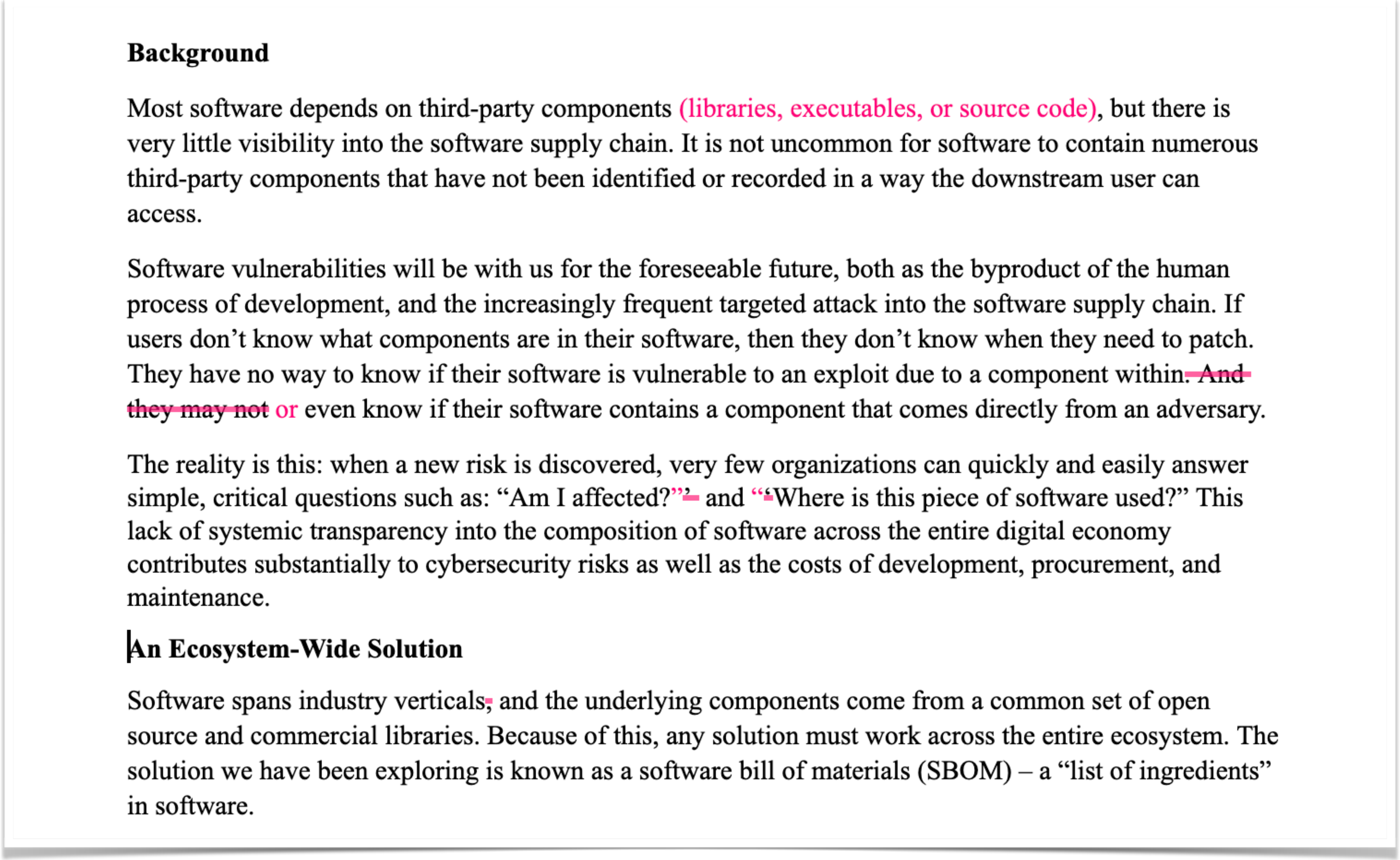
- Please provide feedback via “Add a comment” on Google Document:



- Please also nominate new FAQ questions!



DRAFT GENERIC TWO-PAGER



Background

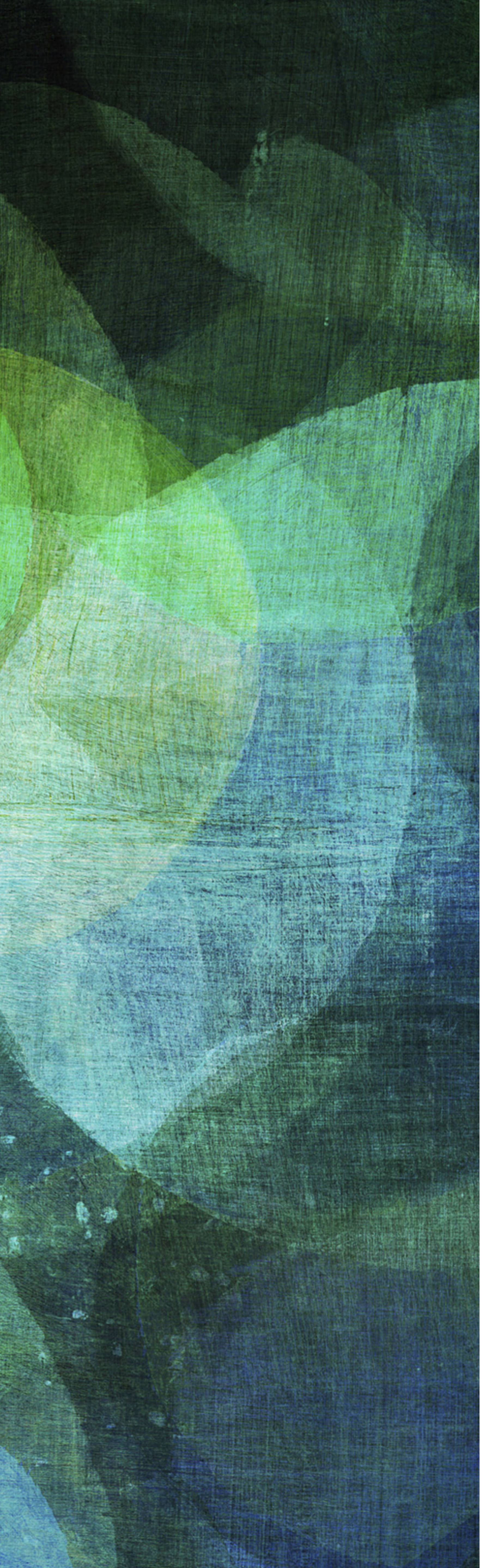
Most software depends on third-party components (libraries, executables, or source code), but there is very little visibility into the software supply chain. It is not uncommon for software to contain numerous third-party components that have not been identified or recorded in a way the downstream user can access.

Software vulnerabilities will be with us for the foreseeable future, both as the byproduct of the human process of development, and the increasingly frequent targeted attack into the software supply chain. If users don’t know what components are in their software, then they don’t know when they need to patch. They have no way to know if their software is vulnerable to an exploit due to a component within~~. And they may not~~ or even know if their software contains a component that comes directly from an adversary.

The reality is this: when a new risk is discovered, very few organizations can quickly and easily answer simple, critical questions such as: “Am I affected?”~~”~~ and “~~“~~Where is this piece of software used?” This lack of systemic transparency into the composition of software across the entire digital economy contributes substantially to cybersecurity risks as well as the costs of development, procurement, and maintenance.

An Ecosystem-Wide Solution

Software spans industry verticals~~,~~ and the underlying components come from a common set of open source and commercial libraries. Because of this, any solution must work across the entire ecosystem. The solution we have been exploring is known as a software bill of materials (SBOM) – a “list of ingredients” in software.

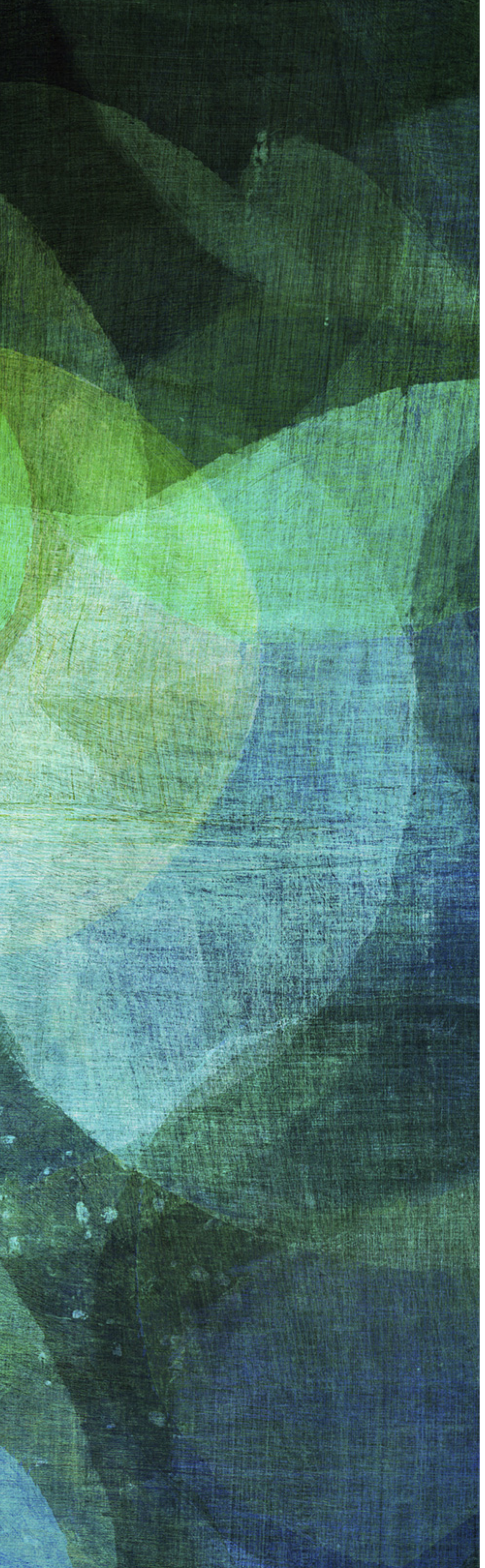


RECENT PUBLIC SBOM RECORDINGS

- February 2020 - RSAC: Allan Friedman (31min)
  "What's in the Box? Software Bill of Materials for IoT"
  https://www.rsaconference.com/industry-topics/presentation/whats-in-the-box-software-bill-of-materials-for-iot

- January 2020 - ShmooCon: Audie, Josh Corman (20min)
  https://www.youtube.com/watch?v=RxYK2vyQKWo

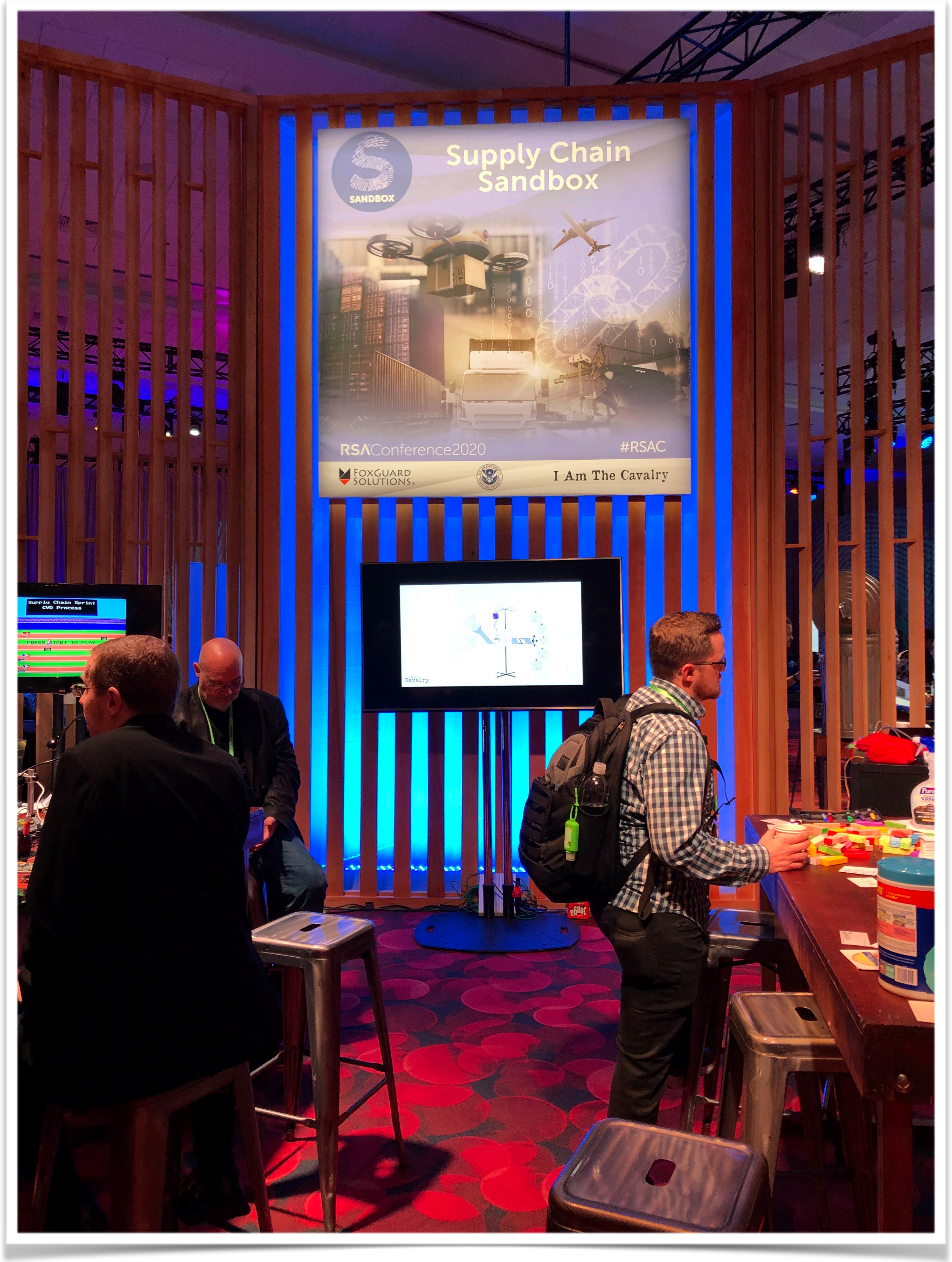
- December 2019 - Application Security Weekly Podcast: Allan Friedman (37min)
  "Software Bill of Materials (SBOM) - Allan Friedman - ASW #88"
  https://www.youtube.com/watch?v=RxYK2vyQKWo



ONGOING EFFORTS

- DRAFT Generic Two-Pager https://docs.google.com/document/d/1BEf-lthbIkOHwD7vjwpGUzVEc3Icp7bW8WSiWIs7D10/edit
- Graphics Repository: https://bit.ly/sbom-awareness-graphics
- Short SBOM “Explainer” Videos
- Knowledge Base - Searchable, cross-linked Phase I Documents
- Virtual Engagement Opportunities
  - Webinars, Podcasts, Virtual Conferences, Other

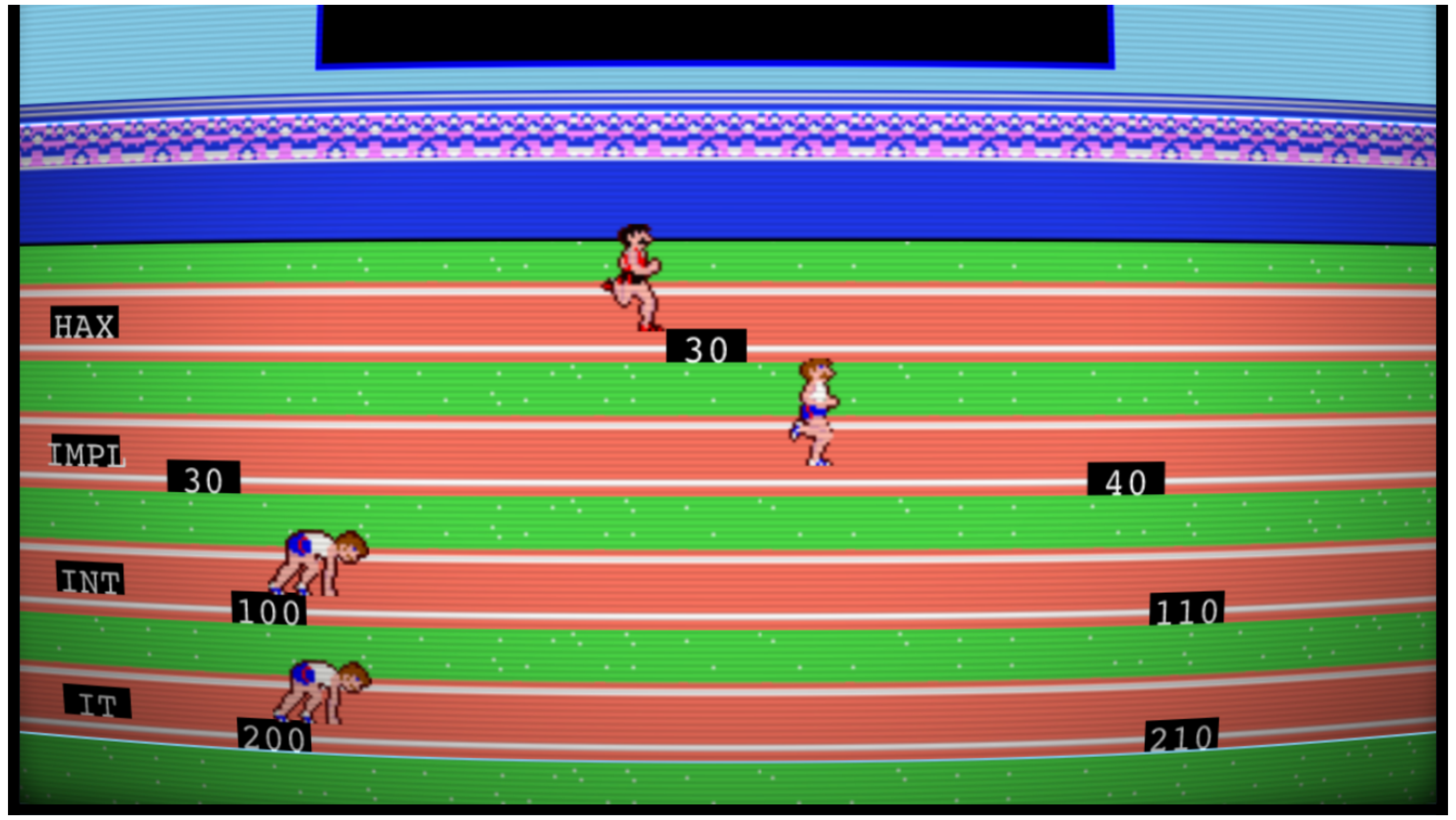
MULTIMEDIA



supplychainsandbox.org

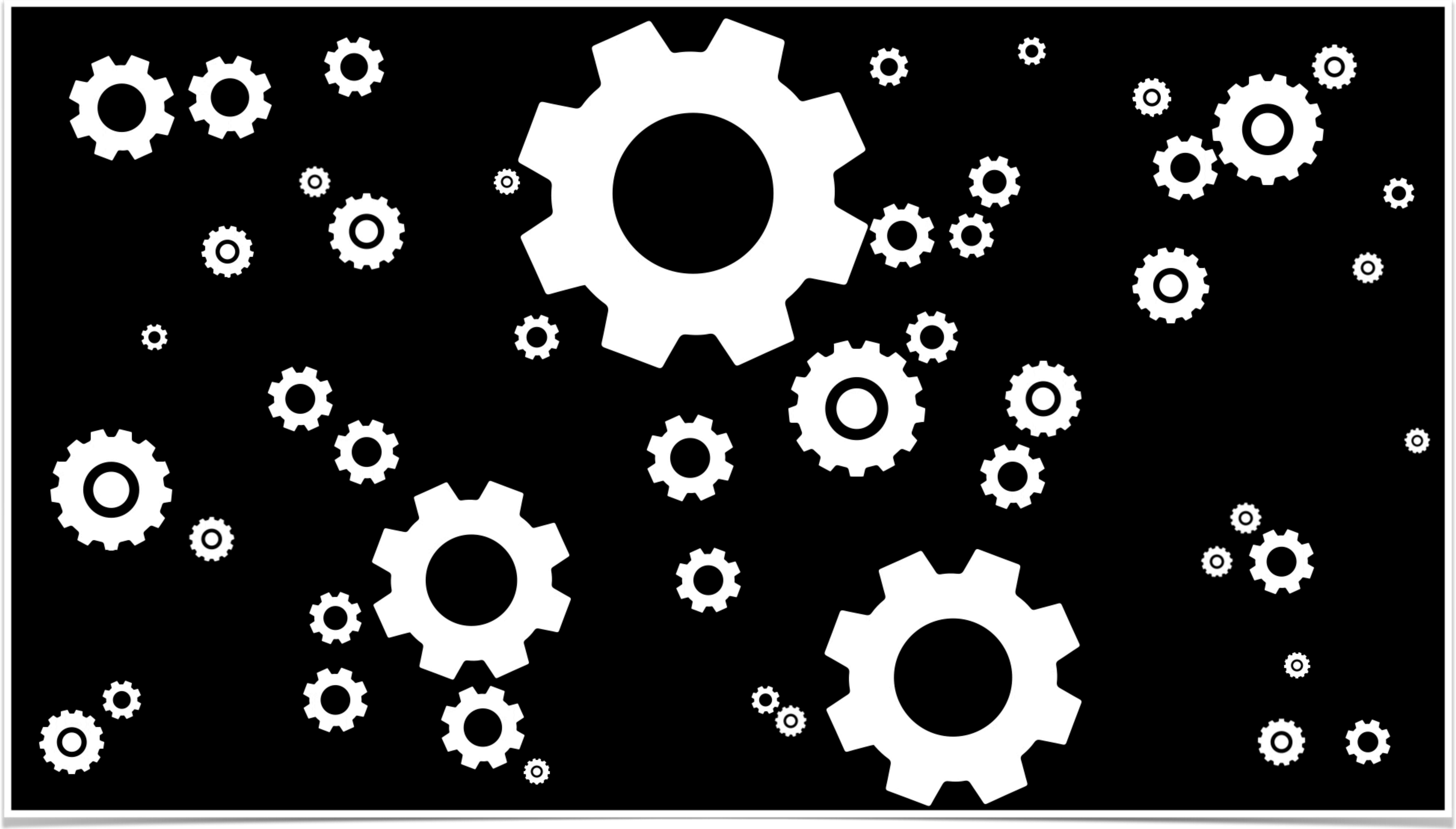
Supply Chain Sprint

1 Player
3 Player
Cheat Codes

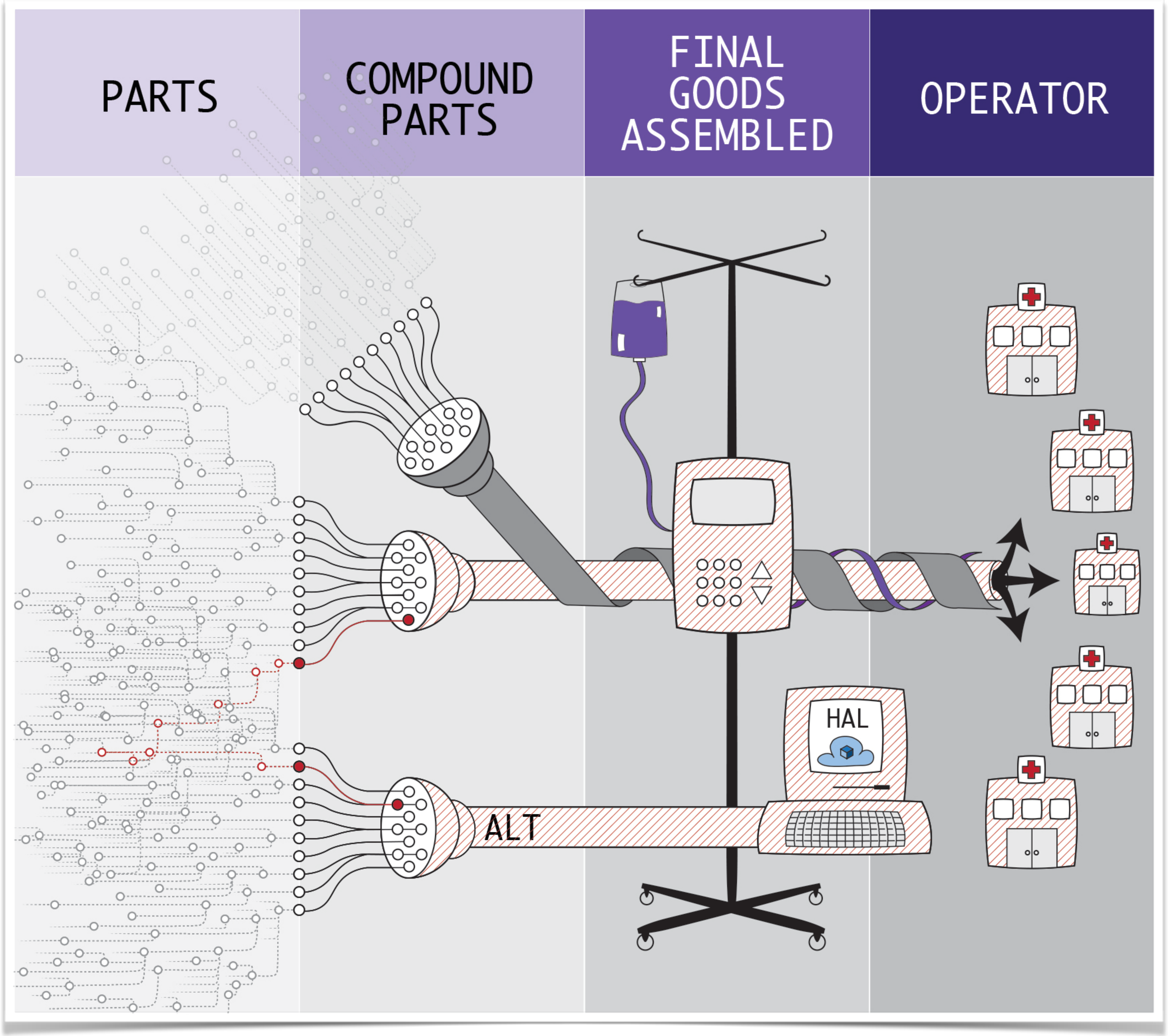


supplychainsprint.com

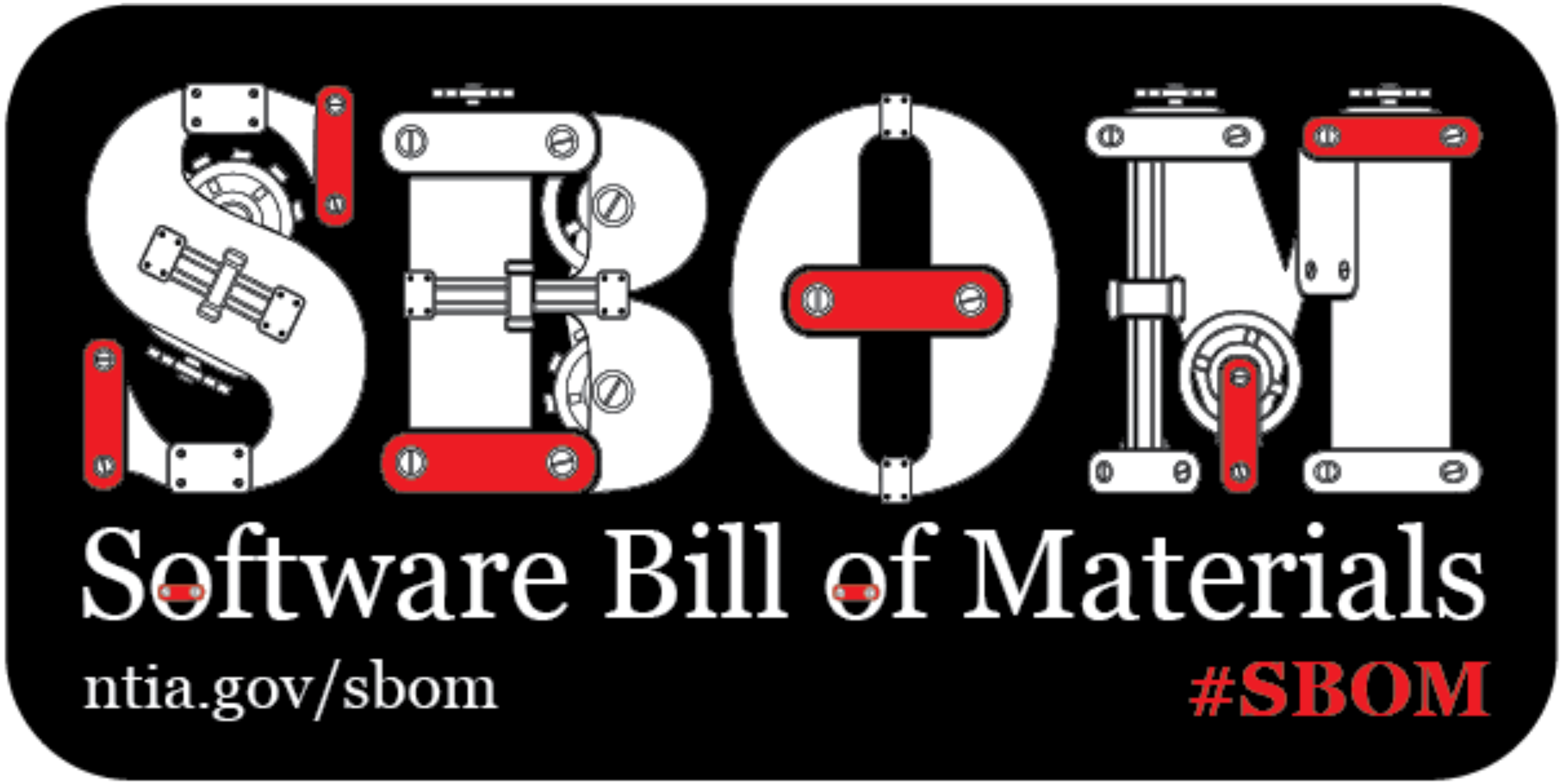
MULTIMEDIA

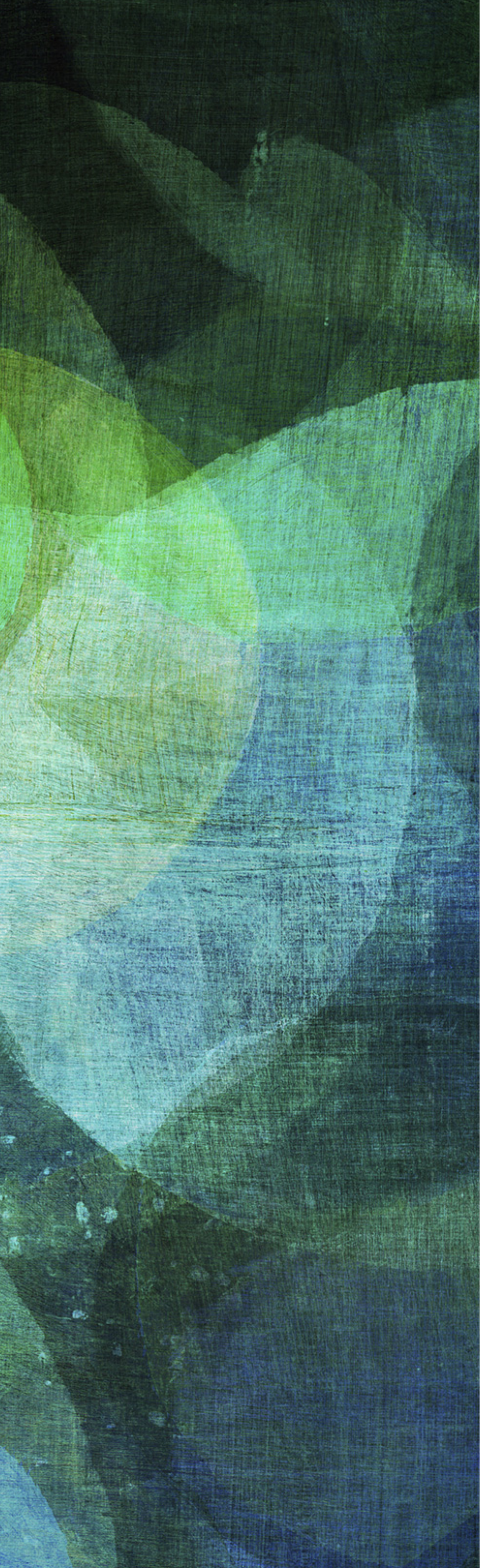


MULTIMEDIA


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
HAL
ALT

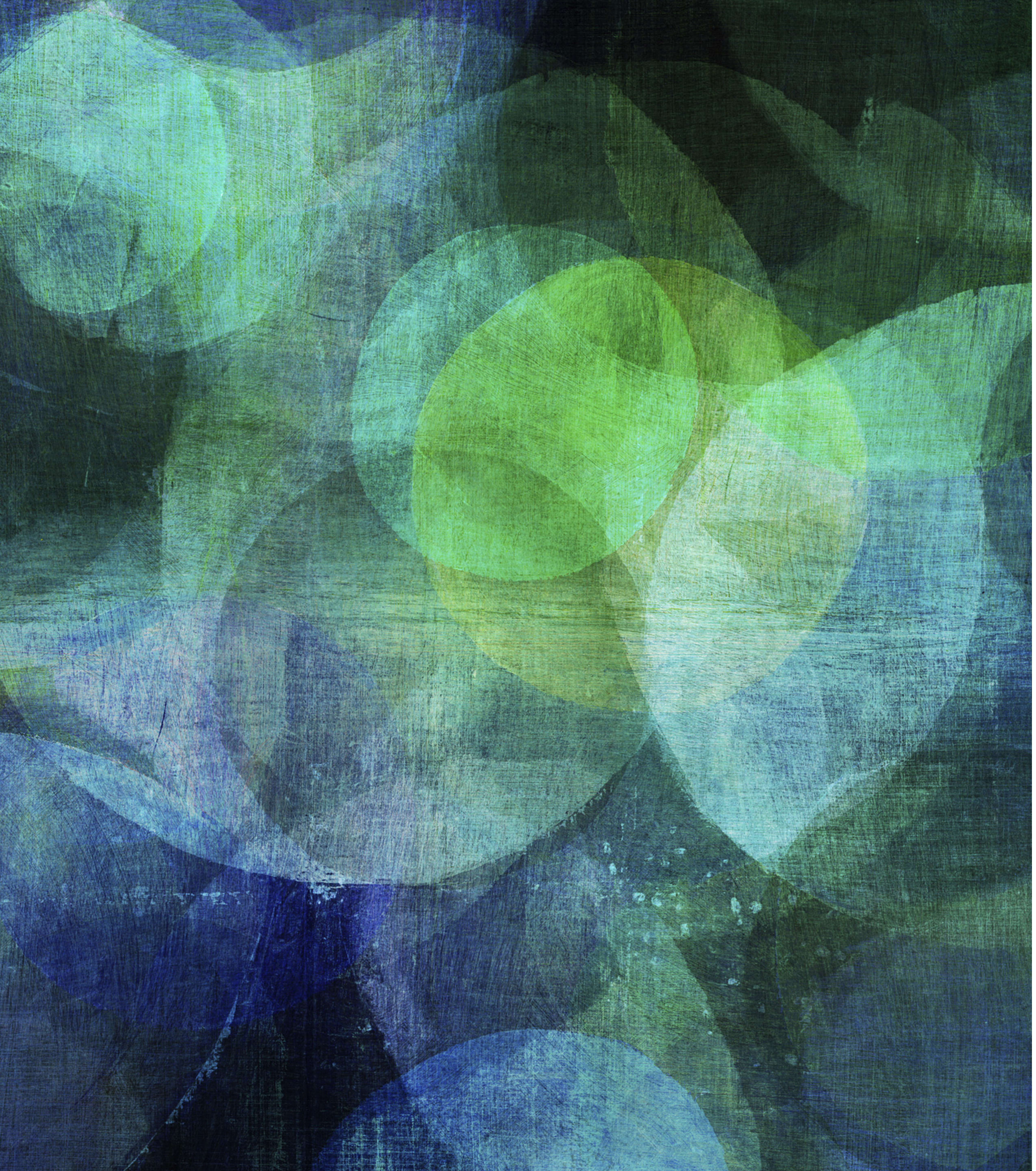
MULTIMEDIA





COMMUNITY ASK

- How you can help Awareness & Adoption:
  - Please provide feedback on FAQ.
  - Watch and share public recordings.
  - Introductions to creative colleagues and contributors (e.g. marketing, design, developer relations, etc.)
- How can Awareness & Adoption help you?
  - What other resources do you need?
- Get creative with outreach in the time of corona!



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