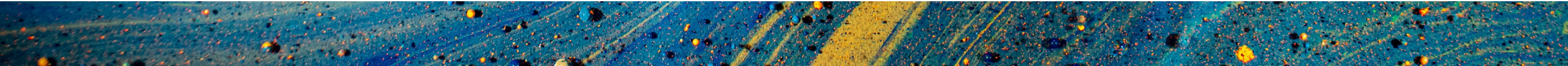


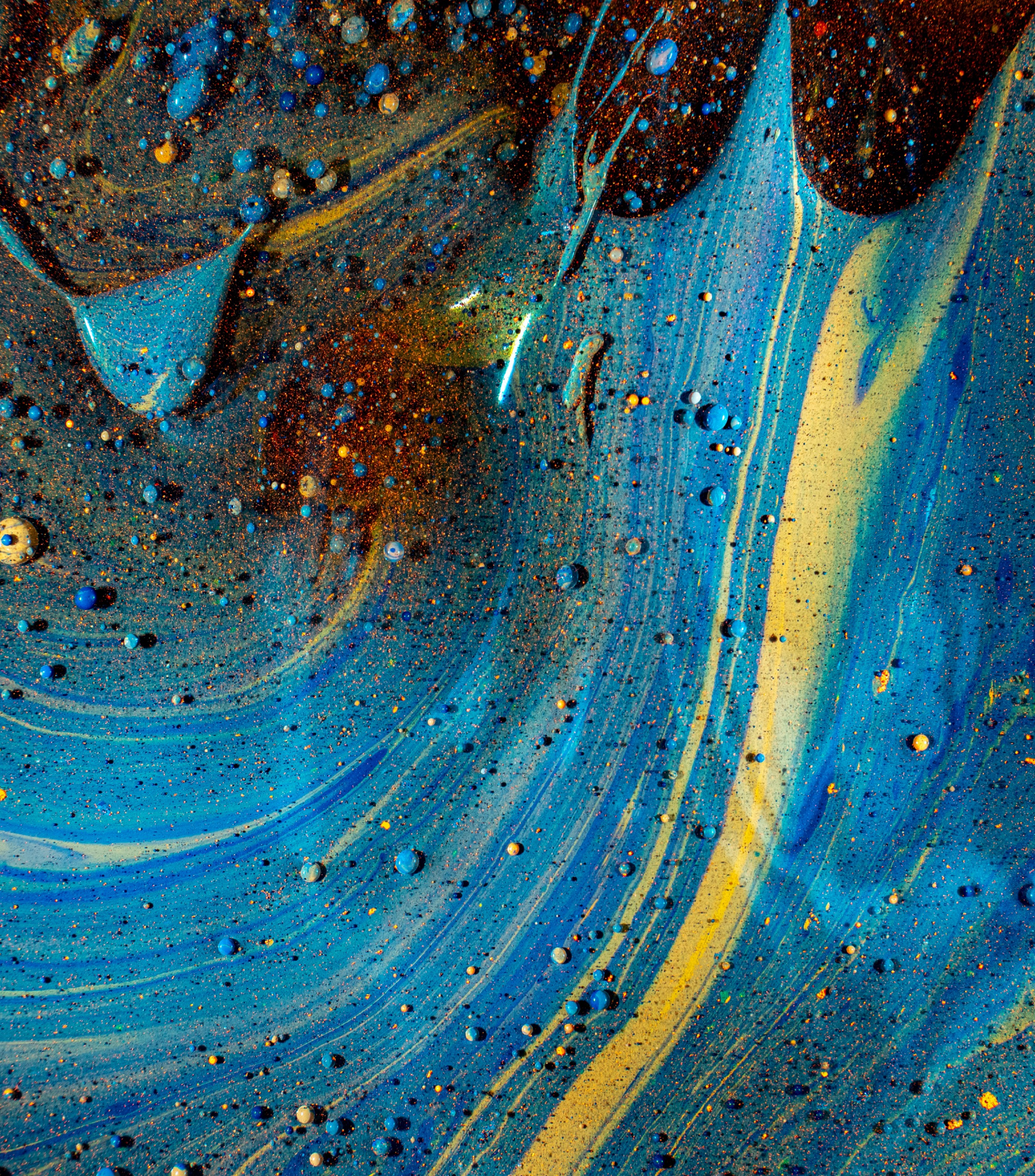
January 13, 2021

AWARENESS & ADOPTION

NTIA Software Component Transparency

Audra Hatch, Joshua Corman





OVERVIEW

- Recap: Mission and Goals
- 2020 Year in Review
- What We're Working On
 - Today's Highlights
 - Ongoing Efforts
 - Future Initiatives
- Community Ask
- Resources



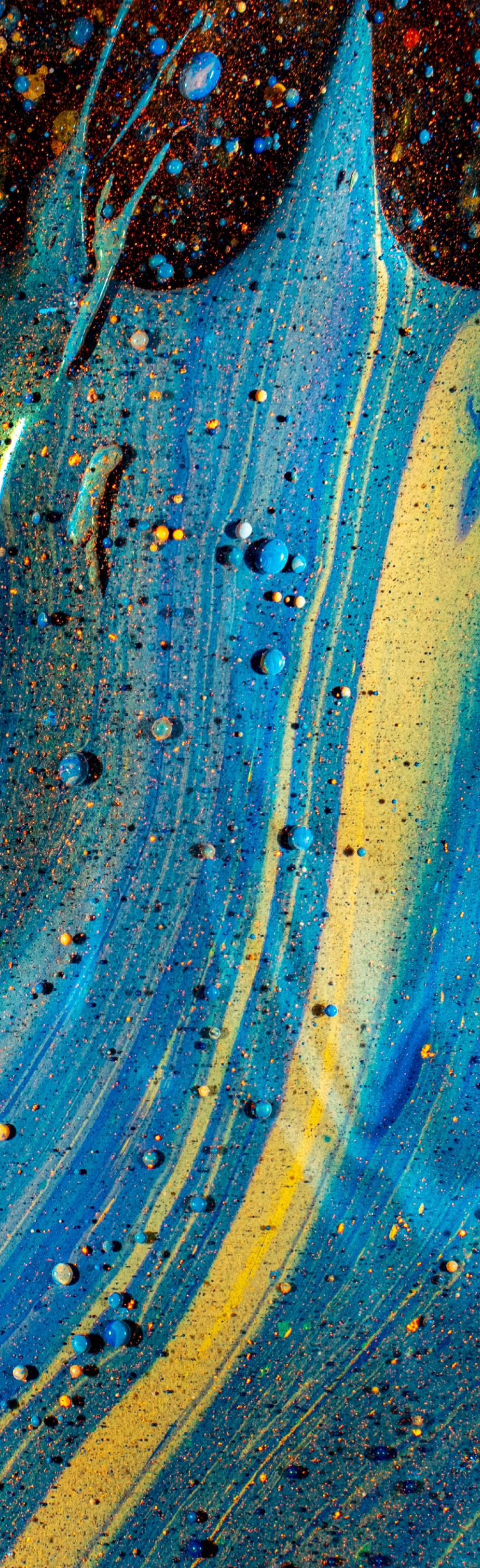
RECAP: AWARENESS & ADOPTION MISSION

- ▶ 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



WHERE TO START: README

- ▶ README file containing links to documents and ongoing efforts in the NTIA SBOM Awareness & Adoption Working Group Google Drive:
 - ▶ <https://bit.ly/sbom-awareness-readme>

My Drive > NTIA SBOM: Practices / Awareness & Adoption

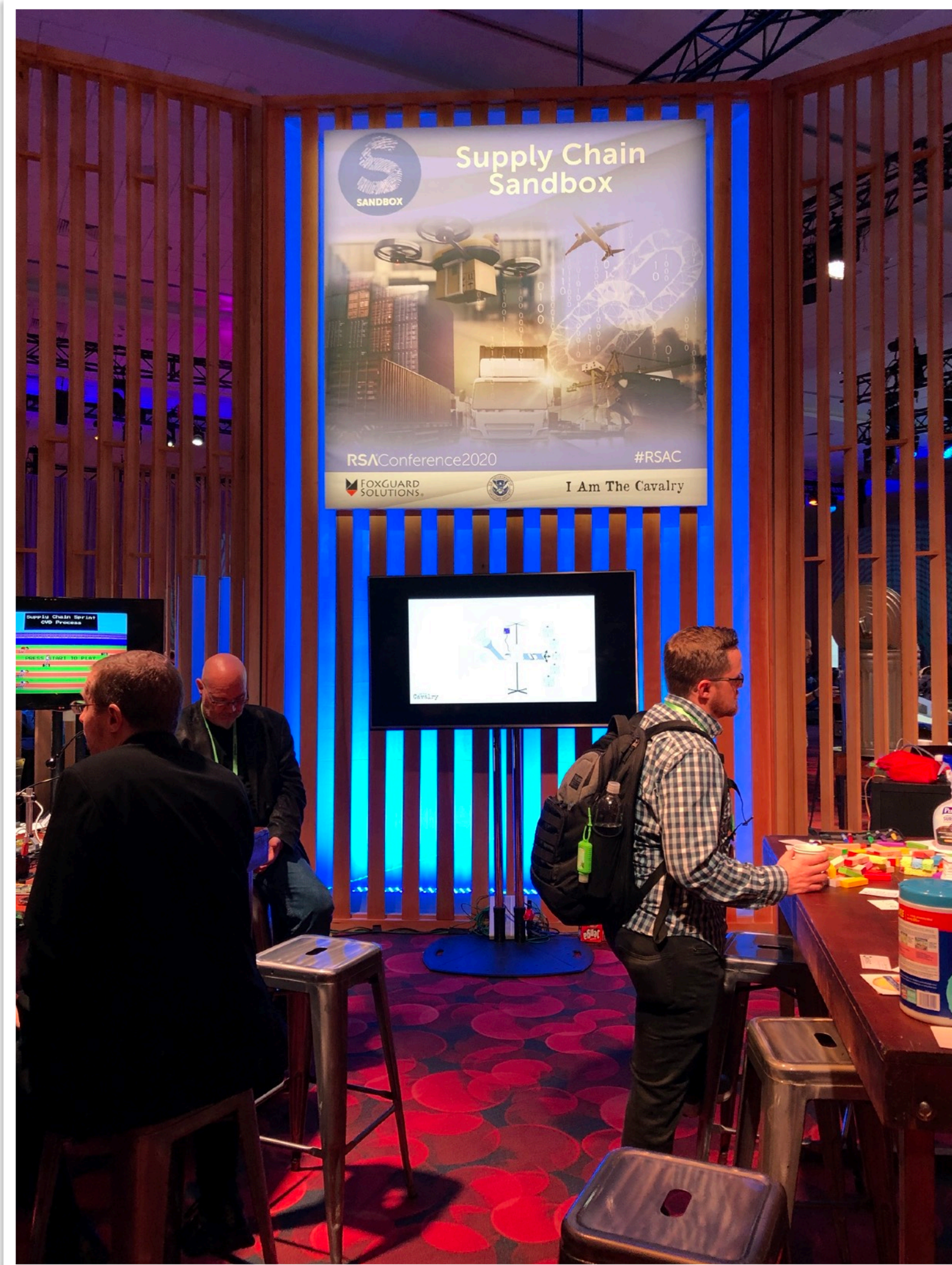
| Name ↑ | Owner | Last modified | File size |
|---|-----------------|-----------------|-----------|
| Archived Documents | me | Mar 24, 2020 me | – |
| Graphics | me | Dec 5, 2019 me | – |
| Meeting Notes | me | Nov 22, 2019 me | – |
| Outreach Strategy | me | Nov 22, 2019 me | – |
| Slide Decks | me | Mar 19, 2020 me | – |
| Copy of SBOM FAQ - Fork for July 9 Meeting | me | Jul 2, 2020 me | – |
| Copy of SBOM Two-Pager Overview - Fork for July 9 Meeting | me | 6:37 PM me | – |
| NTIA SBOM - phase two goals.pptx | me | May 6, 2020 me | 446 KB |
| README | me | Jul 2, 2020 me | – |
| SBOM Business Two-Pager | Duncan Sparrell | 7:03 PM me | – |
| SBOM Explainer Videos | me | 6:49 PM me | – |
| SBOM FAQ | me | Jul 2, 2020 me | – |



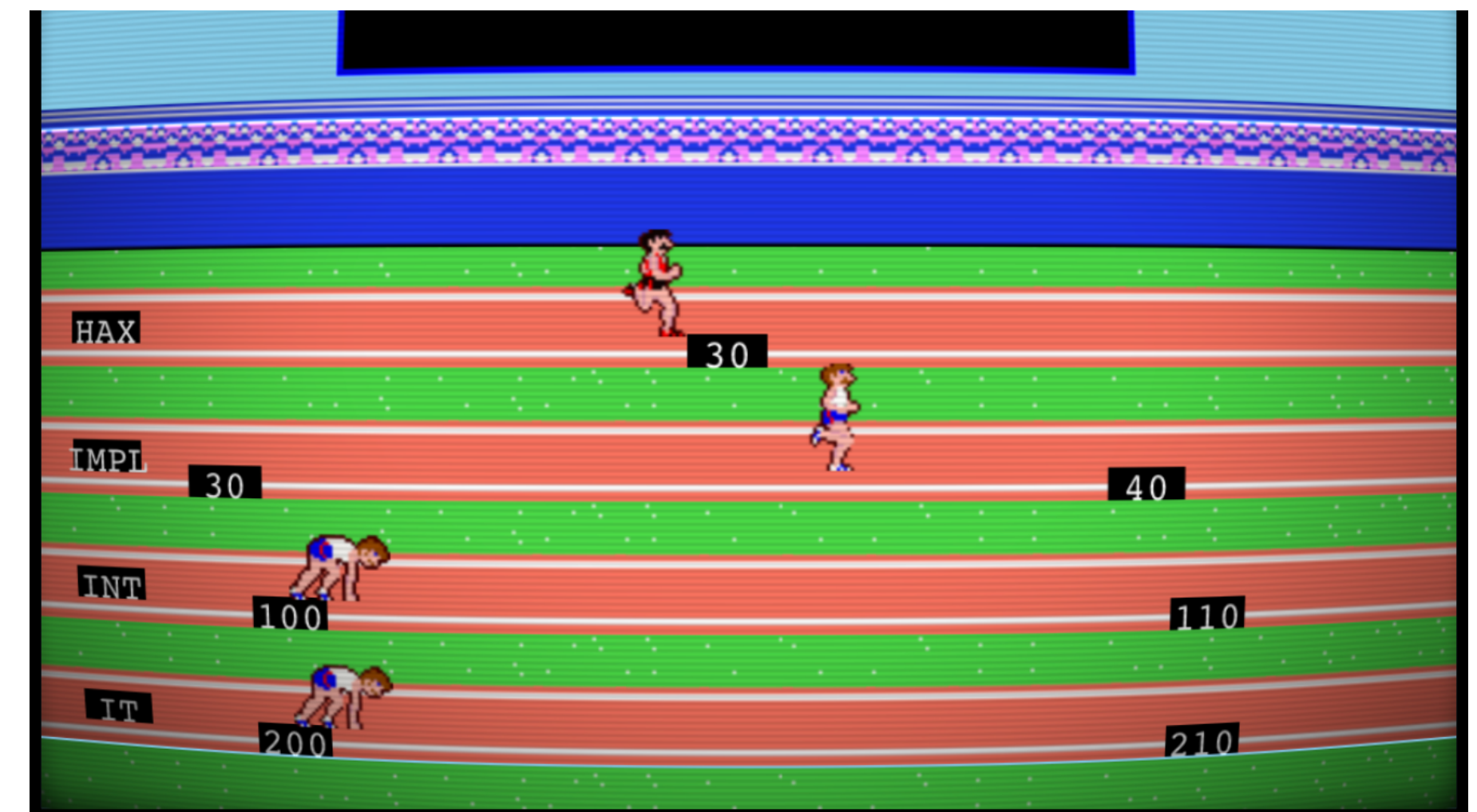
2020 AWARENESS & ADOPTION YEAR IN REVIEW

- ▶ Published Deliverables:
 - ▶ NTIA Website Update
 - ▶ FAQ - NTIA Website & GitHub
 - ▶ Overview Two-Pager
 - ▶ SBOM Explainer Videos
 - ▶ SBOM Calendar
- ▶ Supply Chain Cybersecurity Events & Disclosures
 - ▶ SolarWinds*
 - ▶ Amnesia33
 - ▶ Ripple20
- ▶ Proofs of Concept, Events, and Virtual Engagement Opportunities
 - ▶ Supply Chain Sandbox at RSA
 - ▶ Double-digit SBOM Recordings, Presentations, and Podcasts in 2020
 - ▶ Community Survey on SBOM Process
 - ▶ Auto ISAC Proof of Concept Kickoff
 - ▶ Planning for Energy Proof of Concept

SUPPLY CHAIN SANDBOX



supplychainsandbox.org



supplychainsprint.com



WHAT WE'RE WORKING ON

➤ Today's Highlights:

- Explainer Videos on YouTube
- SBOM Survey Results
- Auto ISAC Update
- Procurement Strategy Overview

➤ Ongoing Efforts:

- FAQ
- SBOM Calendar
- News, Recordings, & Presentations
- Business Two-Pagers
- Virtual Engagement Opportunities
- POC Conversations & Expansions
- Graphics & Slide Repositories
- Knowledge Base
- SBOM-Adjacent Topics
- Questions For Your Suppliers

➤ Future Initiatives:

- Journeys & Playbooks
- SBOM Starter Slides
- Additional Explainer Videos
- Proof of Concept Virtual Summit
- Ideas for 2021

DELIVERABLES AND STATUS

| Deliverable | On Deck | Development | In Review | Released |
|--|---------|-------------|-----------|----------|
| FAQ | | X | | X |
| FAQ on GitHub | | | | X |
| SBOM Overview Two-Pager | v 2 | | | X |
| Explainer Videos | X | | | X* |
| SBOM Calendar | | | | X |
| SBOM News | | X | | * |
| Recordings & Presentations | | X | | * |
| Community Survey on SBOM Process | | | X | * |
| SBOM Business Two-Pagers | | X | | |
| Virtual Engagement Opportunities | | X | | |
| Proof of Concept Conversations & Expansions | | X | | |
| Graphics & Slide Repositories | | X | | * |
| Knowledge Base | | X | | |
| SBOM-Adjacent Topics Spreadsheet | | X | | |
| Questions for your Suppliers | | X | | |
| Procurement Strategy Two-Pager | | X | | |
| SBOM Starter Slides | | X | | |
| Journeys & Playbooks | X | | | |
| Proof of Concept Virtual Summit | X | | | |

PHASE I SBOM EXPLAINER VIDEOS

► Available on YouTube:

► <https://www.youtube.com/playlist?list=PLO2lqCK7WyTDpVmcHsy6R2HWftFkUp6zG>

Software Bill of Materials (SBOM)

6 videos • 120 views • Last updated on Dec 21, 2020

SBOM Explainer Videos

NTIAgov SUBSCRIBE

- 1 SBOM Explainer: What Is SBOM? Part 1 NTIAgov 4:41
- 2 SBOM Explainer: What is an SBOM? Part 2 NTIAgov 4:11
- 3 SBOM Explainer: What is an SBOM? Part 3 NTIAgov 2:55
- 4 SBOM Explainer: Introduction to Use Cases & State of Practice Working Group NTIAgov 4:51
- 5 SBOM Explainer: Introduction to Formats and Tooling Working Group NTIAgov 5:03
- 6 SBOM Explainer: Introduction to Healthcare Proof of Concept Working Group NTIAgov 5:48

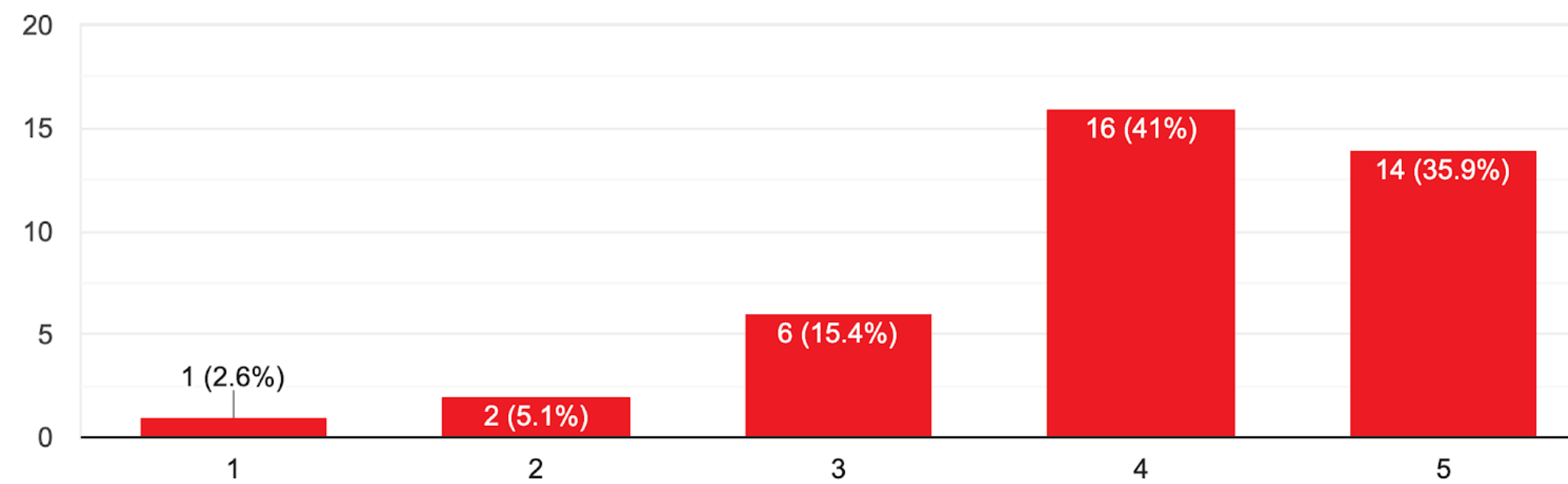
► Also linked to on ntia.gov/sbom

COMMUNITY SURVEY ON SBOM PROCESS

- ▶ Link to survey results:
 - ▶ <http://bit.ly/sbom-awareness-survey-2020>

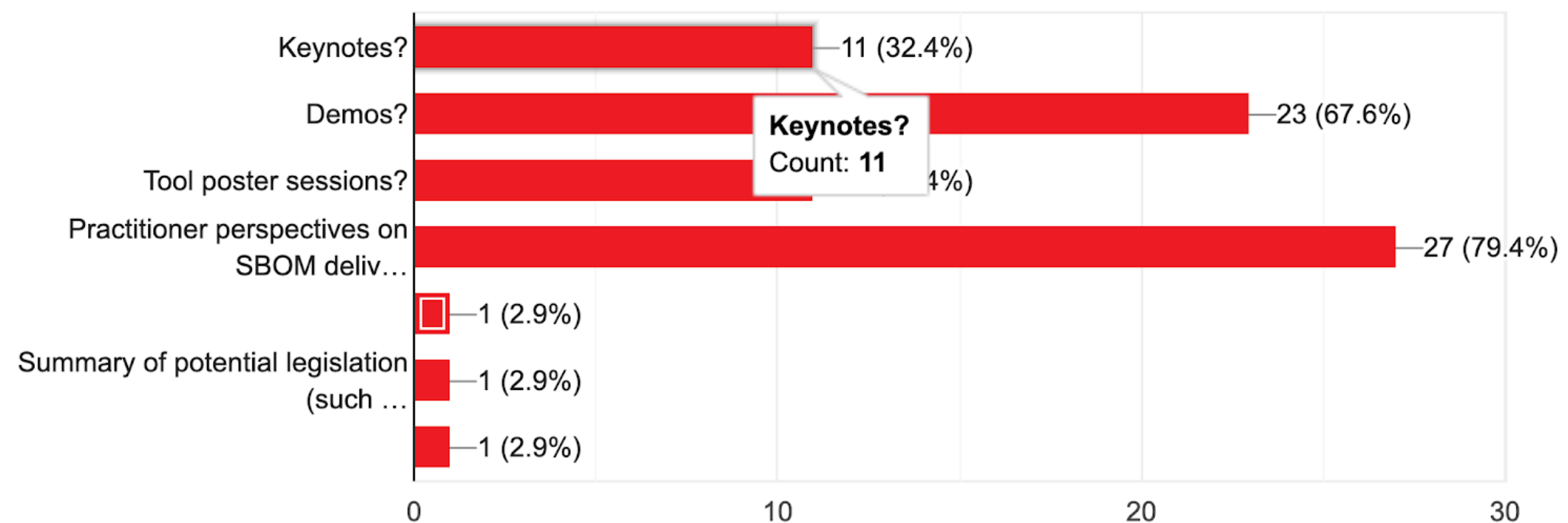
How satisfied are you with the quarterly multistakeholder community meetings in 2020?

39 responses



What else would you like to see at the quarterly meetings? (select all that apply)

34 responses





FAQ & OVERVIEW TWO-PAGER

➤ Published on NTIA SBOM Website:

➤ ntia.gov/sbom

➤ GitHub Mirror of FAQ:

➤ <https://github.com/sparrell/NtiaSbomFaq>

SBOM EVENTS CALENDAR

SBOM Events

Today ◀ ▶ October 2020

Print Week Month Agenda

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|--------------------------|---|--|---|---|-----|
| 27 | 28 | 29 | 30 | Oct 1 | 2 | 3 |
| | | | | 1pm NTIA SBOM Healthcar | 1pm NITA SBOM Awarenes 2pm NTIA SBOM Framing | |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | 1pm NTIA SBOM Healthcar | 11am NTIA SBOM Formats 1pm NITA SBOM Awarenes 2pm NTIA SBOM Framing | |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| | | 8am CISQ - 8th Annual Cy 11:30am WHAT'S IN MY SO | 6:30am INTERSCT 7:30am What's in the box: | 6:30am INTERSCT 1pm NTIA SBOM Healthcar | 1pm NITA SBOM Awarenes 2pm NTIA SBOM Framing | |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| | 4:30pm Secure Guild 2020 | | | 12pm NTIA SBOM Virtual M 1pm NTIA SBOM Healthcar | 11am NTIA SBOM Formats 1pm NITA SBOM Awarenes 2pm NTIA SBOM Framing | |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| | | | OpenC2 SBOM Event - Vi 2pm OpenC2 Keynote: Ne | 1pm NTIA SBOM Healthcar | 1pm NITA SBOM Awarenes 2pm NTIA SBOM Framing | |

Events shown in time zone: Eastern Time - New York

+ Google Calendar



SBOM EVENTS CALENDAR

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



SBOM RESOURCES

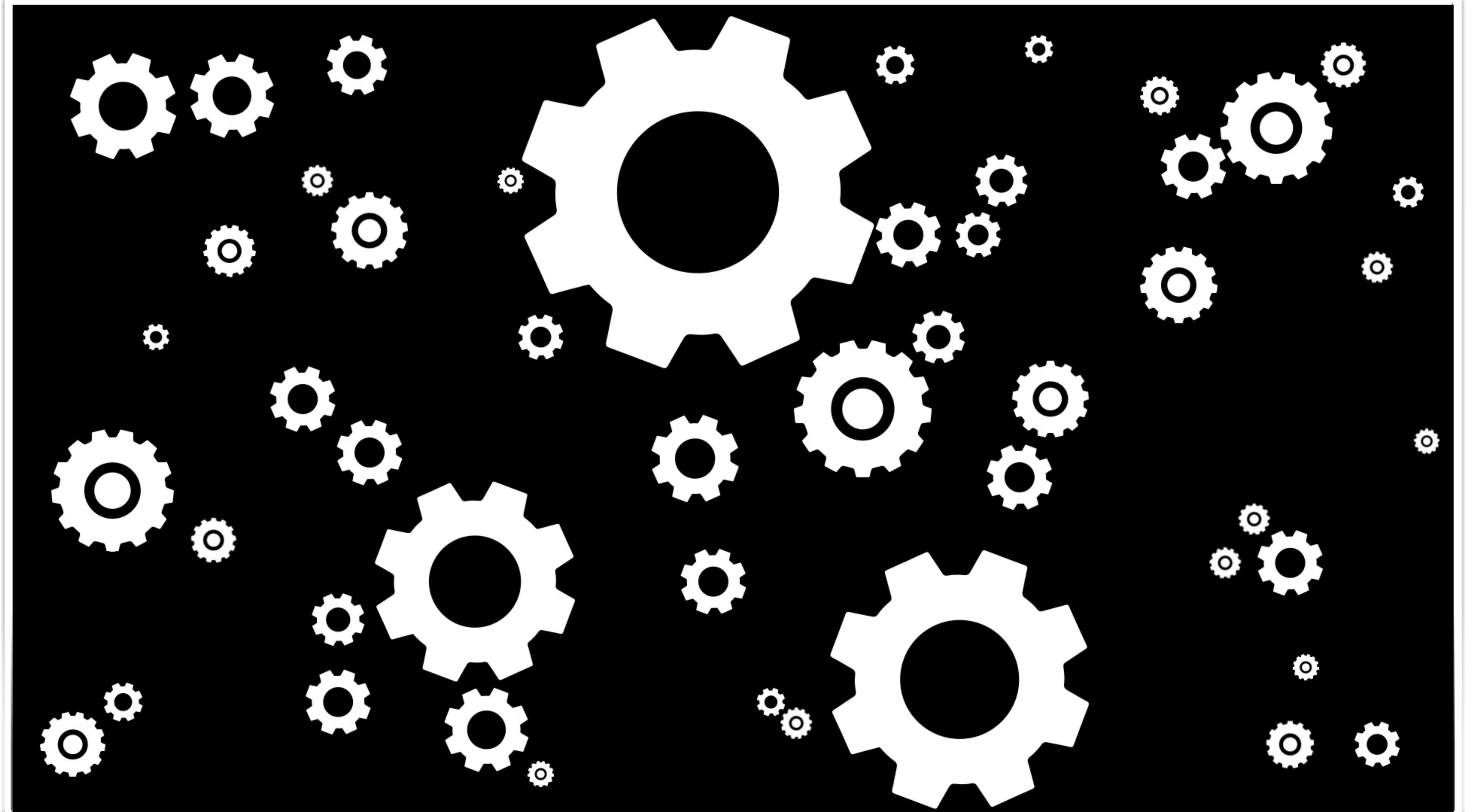
- SBOM News:
 - <https://bit.ly/sbom-awareness-news>
- SBOM Recordings, Presentations, and Podcasts:
 - <https://bit.ly/sbom-awareness-recordings>
- If you have a news story, recording, presentation, or podcast to add to the lists, please submit a comment in the Google Doc.



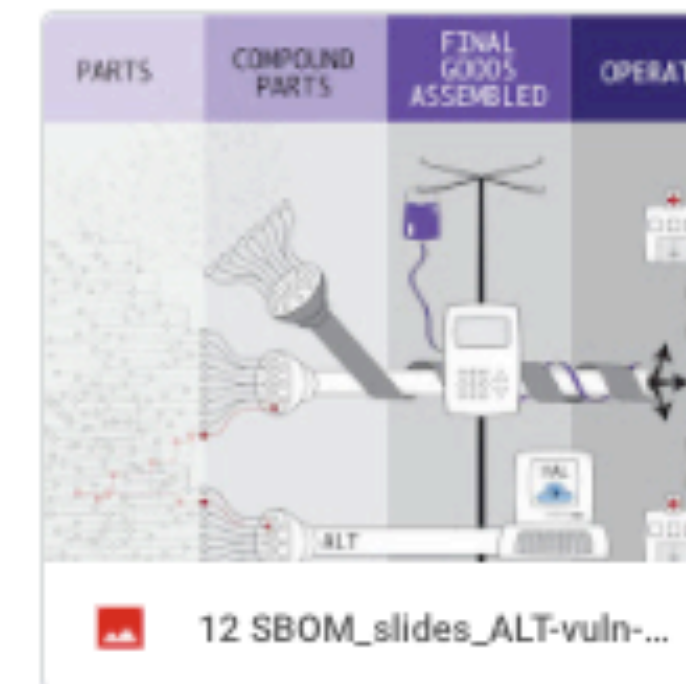
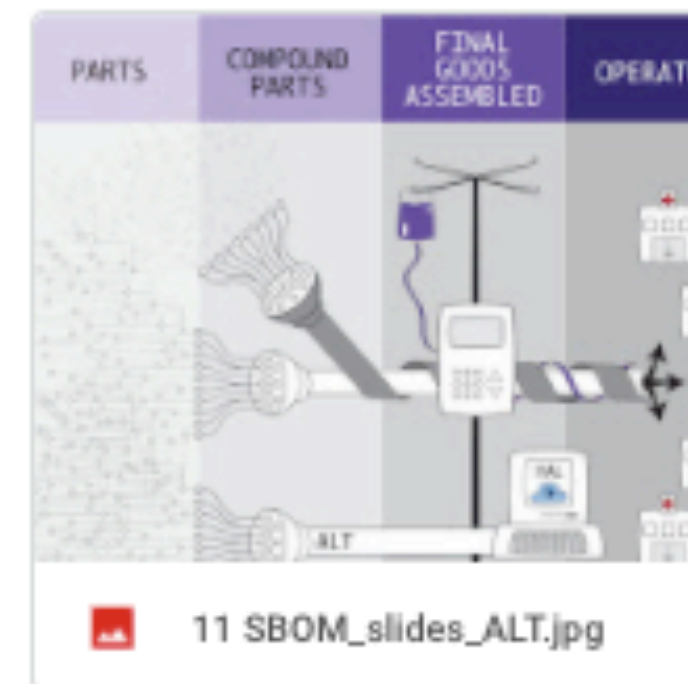
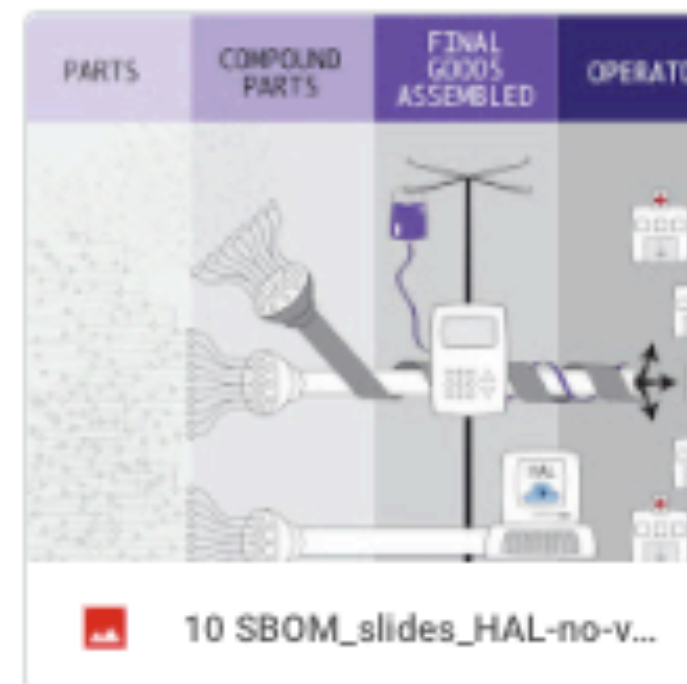
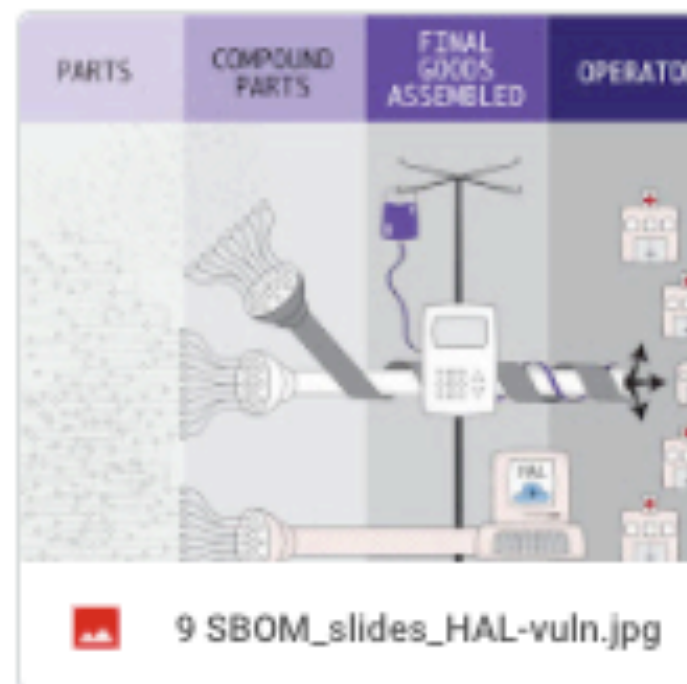
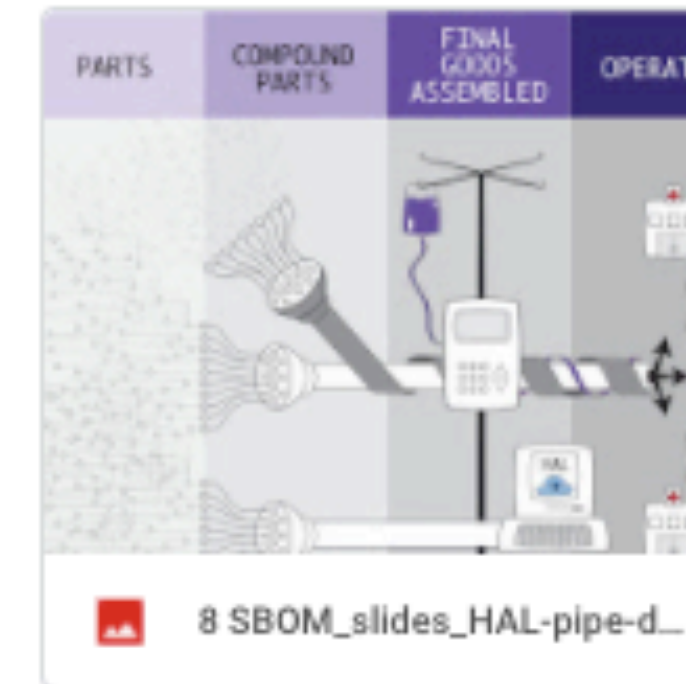
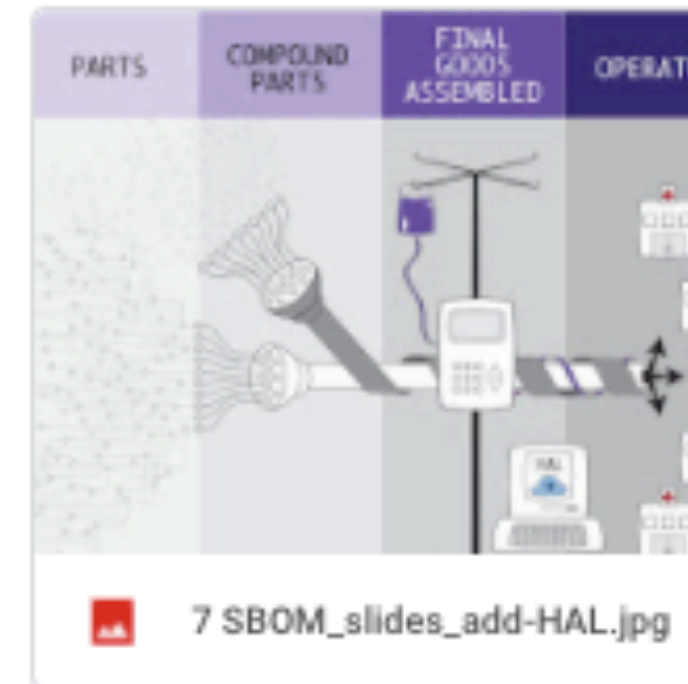
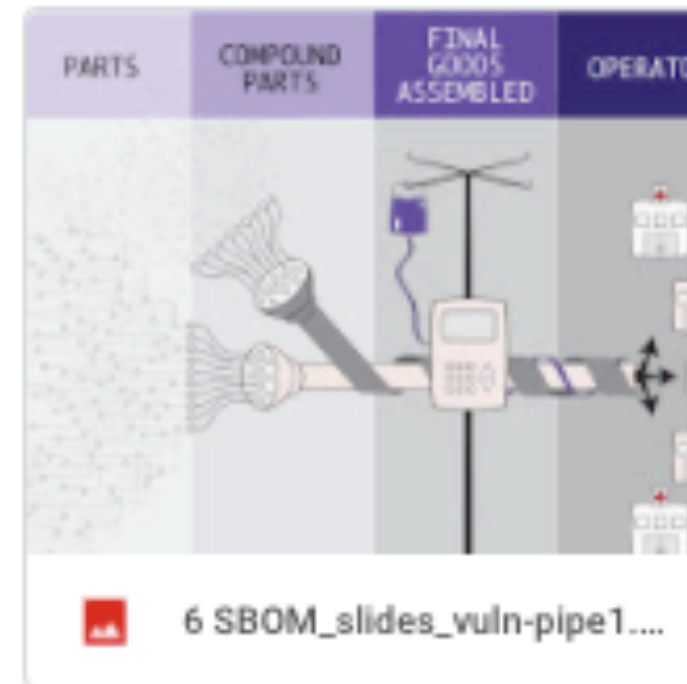
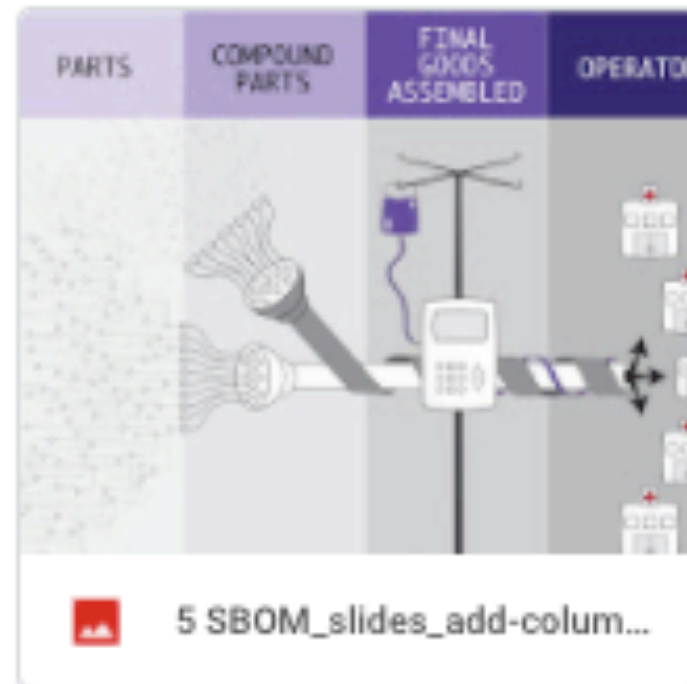
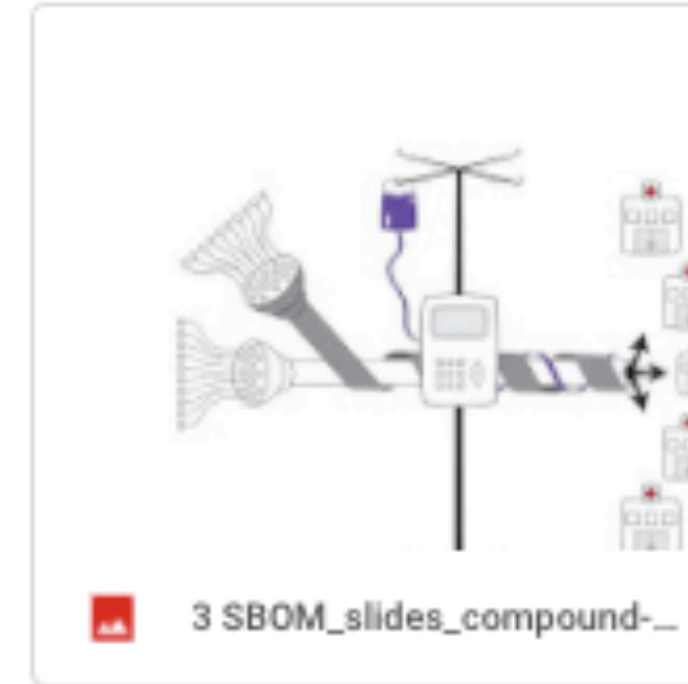
ONGOING EFFORTS

- Two-Pagers
 - Procurement Strategy
 - Business Two-Pager being reworked into two documents:
 - Business Customer
 - Producer
- SBOM-Adjacent Topics Spreadsheet
- Virtual Engagement Opportunities
 - Webinars, Podcasts, Virtual Conferences, Other
- Proof of Concept Conversations & Expansions
- Graphics Repository:
 - <https://bit.ly/sbom-awareness-graphics>
- Slides Repository:
 - <http://bit.ly/sbom-awareness-slides>
- Knowledge Base - Searchable, cross-linked Phase I Documents

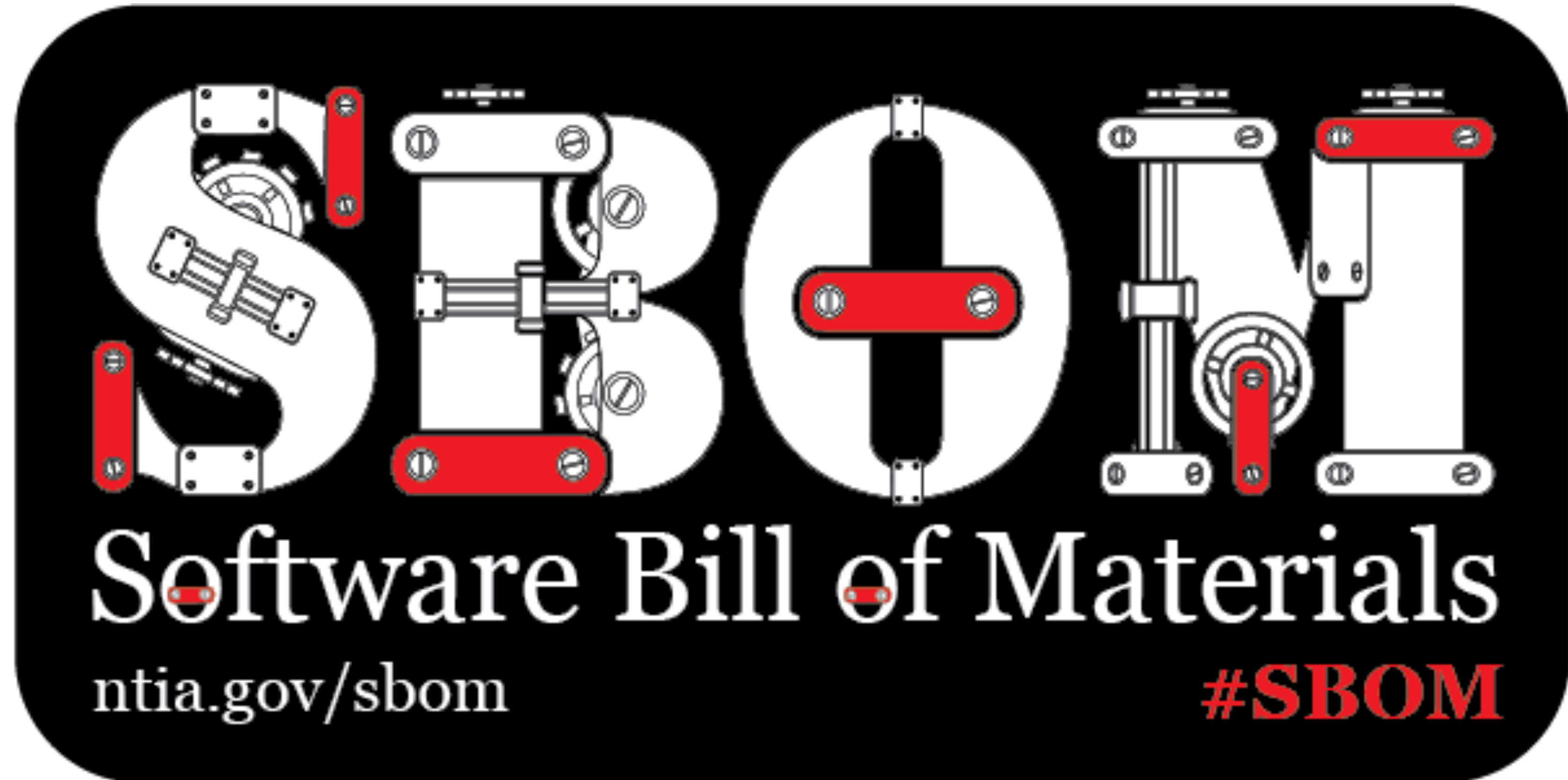
MULTIMEDIA



MULTIMEDIA

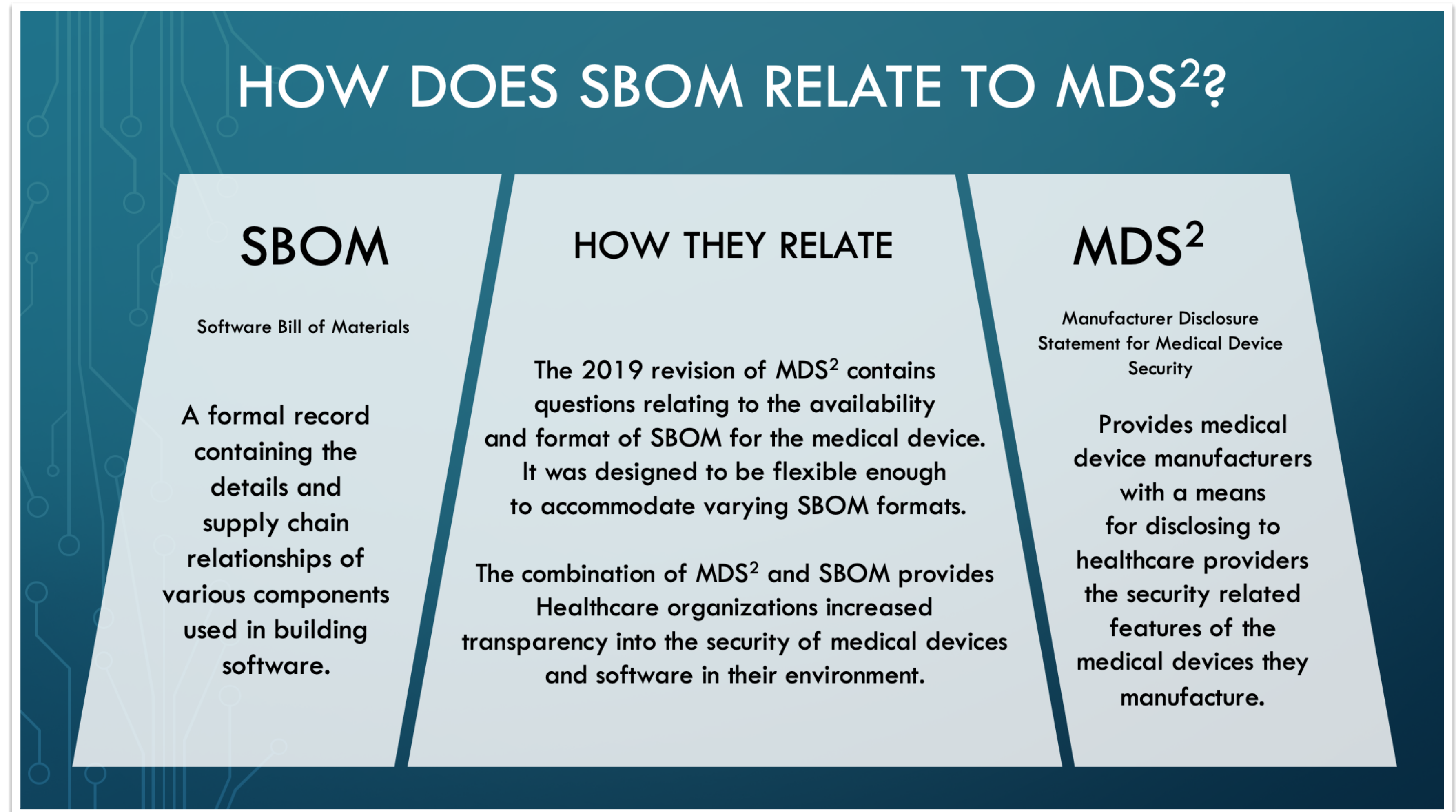


MULTIMEDIA



“HOW DOES SBOM RELATE TO...”

- PowerPoint Template: <http://bit.ly/sbom-relates-to-ppt>





SBOM-ADJACENT TOPICS SPREADSHEET

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



QUESTIONS FOR YOUR SUPPLIERS

- ▶ Link to document listing questions to ask your suppliers about SBOM:
 - ▶ <http://bit.ly/sbom-questions-for-suppliers>

Do you have an SBOM?

If Yes:

- Is it machine readable?
- What format(s) are your SBOM(s)?
 - SWID
 - SPDX
 - CycloneDx
 - Other
- Does the SBOM include subcomponents?
 - If yes, how many levels?
 - Does the SBOM include indications of completeness?

If No:

- How do you track components for compliance?
- Do you have an approved list of components?
- Do you have a list of components that developers are not allowed to use (non-permitted technology list)?
- Do you use any SCA tools?
- Do you have a customer communication plan for vulnerabilities in your upstream components?
- Do you intend to create an SBOM in the future?
- Will you be willing to confirm an SBOM generated by a 3rd party?



FUTURE INITIATIVES & IDEAS FOR 2021

- ▶ SBOM Procurement Strategy
- ▶ SBOM Starter Slides
- ▶ NTIA GitHub
- ▶ Additional SBOM Surveys
- ▶ Journeys & Playbooks
- ▶ Additional Explainer Videos
- ▶ Revisit Outreach Strategy
- ▶ Proof of Concept Virtual Summit
- ▶ Other Virtual Conference Opportunities
- ▶ SBOM SWAG



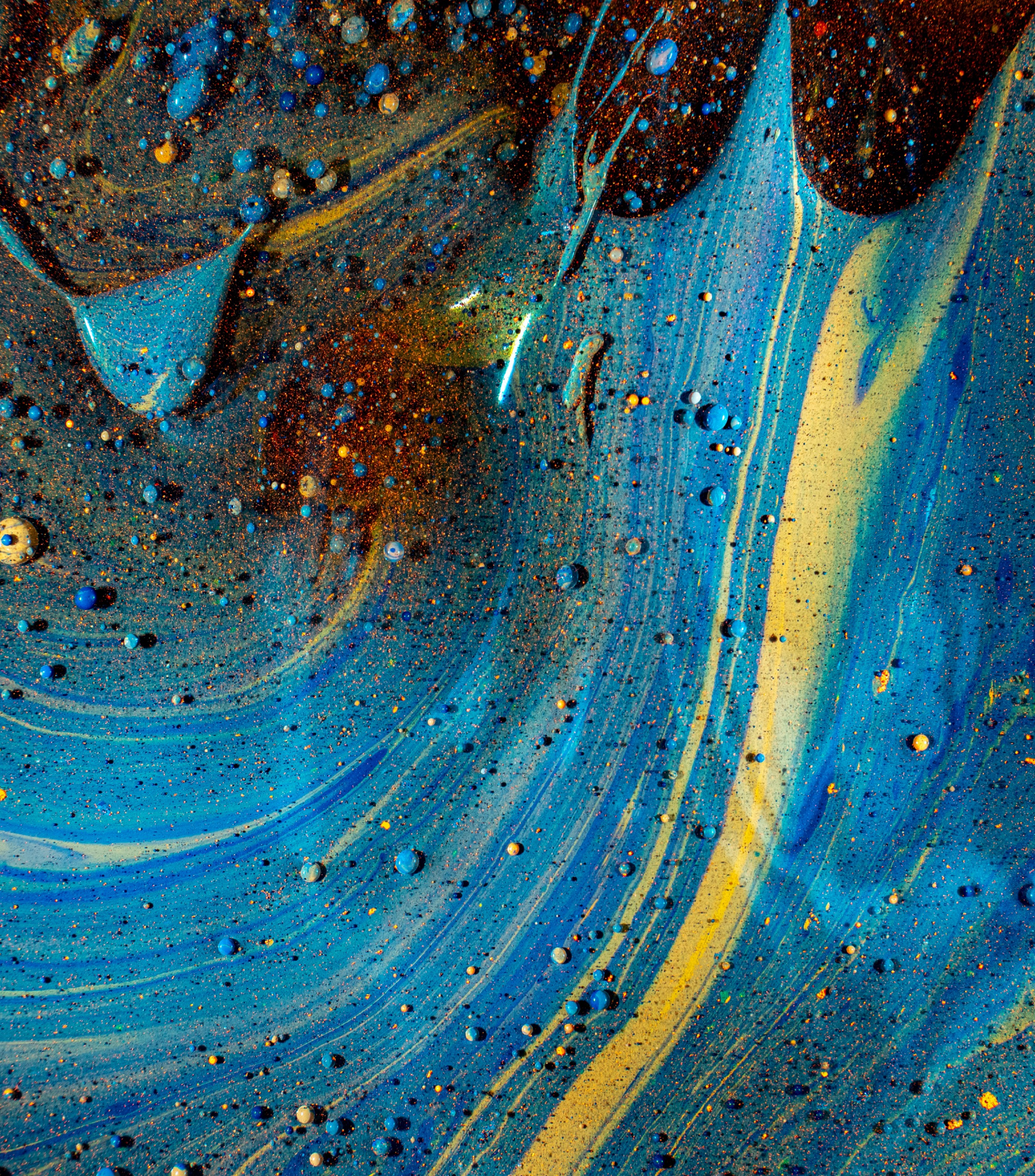
FUTURE INITIATIVES & IDEAS FOR 2021

- ▶ SBOM Procurement Strategy ★
- ▶ SBOM Starter Slides ★
- ▶ NTIA GitHub
- ▶ Additional SBOM Surveys
- ▶ Journeys & Playbooks
- ▶ Additional Explainer Videos
- ▶ Revisit Outreach Strategy ★
- ▶ Proof of Concept Virtual Summit
- ▶ Other Virtual Conference Opportunities
- ▶ SBOM SWAG



COMMUNITY ASK

- ▶ How you can help Awareness & Adoption:
 - ▶ We are seeking **new participants** and **project leads** for ongoing efforts
 - ▶ Please provide feedback on new FAQ questions
 - ▶ Watch, share, and **add to** list of public recordings
 - ▶ Submit upcoming events to the SBOM Calendar
 - ▶ Introductions to creative colleagues and contributors (e.g. marketing, design, developer relations, etc.) + new industry participants
- ▶ How can Awareness & Adoption help you?
 - ▶ What other resources do you need?
 - ▶ How can we improve existing resources?
 - ▶ Do our future initiatives and priorities align with yours?



RESOURCES

➤ README:

➤ <https://bit.ly/sbom-awareness-readme>

➤ Google Drive Folder:

➤ <http://bit.ly/sbom-awareness-google-drive>

➤ Meeting Notes:

➤ <http://bit.ly/sbom-awareness-meeting-notes>



JOIN US

- Awareness & Adoption Meeting
 - Fridays at 1:00 PM ET
 - Join the working group:
<https://lists.sei.cmu.edu/mailman/listinfo/ntia-sbom-practices>
- Mailing List
 - ntia-sbom-practices@cert.org



AUTOMOTIVE INDUSTRY SBOM PROJECT – PROLOGUE (1/3)

- Disclaimer
- From NHTSA “Cybersecurity Best Practices for the Safety of Modern Vehicles,” Draft 2020 Update – released for public comment January 2020:
 - 4.2.6 *Inventory and Management of Software Assets on Vehicles*
 - [G.10] *Manufacturers should maintain a database of operational software components^{19,20} used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle’s lifetime.*
 - [G.11] *Manufacturers should track sufficient details related to software components,²¹ such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,²² manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.*



AUTOMOTIVE INDUSTRY SBOM PROJECT - WHAT? (2/3)

- ▶ A supplier-led project to:
 - ▶ Study and understand SBOM principles and operations
 - ▶ Align and emulate - NTIA, FDA/Healthcare, other agencies/industries
 - ▶ Make the case for SBOM in the auto industry
 - ▶ Unified voice from suppliers
 - ▶ Practical approach and solution with input from customers/partners
 - ▶ Perform exercises in implementation
 - ▶ Recommend and get agreement from industry
 - ▶ Encourage/foster voluntary adoption by suppliers



AUTOMOTIVE – TASKS AND DELIVERABLES – HOW? (3/3)

- Learn: 3 x1 hour tutorials by NTIA Healthcare MSP leaders (complete)
- Cycle:
 - Planning: Timelines, resources, example components, logistics, metrics, formats, tools, other (Cycle 1 underway)
 - Execution: Build SBOMs and conduct exercises
 - Review: Post-mortem, lessons learned
 - Adjust: Improvements, streamlining
- Report: Supplier recommendations for industry standards to automakers (~12 months)

GUIDELINES FOR SBOM INCLUSION IN YOUR SOFTWARE LICENSE AND MAINTENANCE AGREEMENTS (SLMA)



Each term and condition (T&Cs) in the SLMA serve as negotiation levers

- When one party is asked to concede on a given T&C, the expectation is that the other party also offers some concession as well
- The buyer must have sufficient starting leverage or influence to extract concessions on the T&Cs

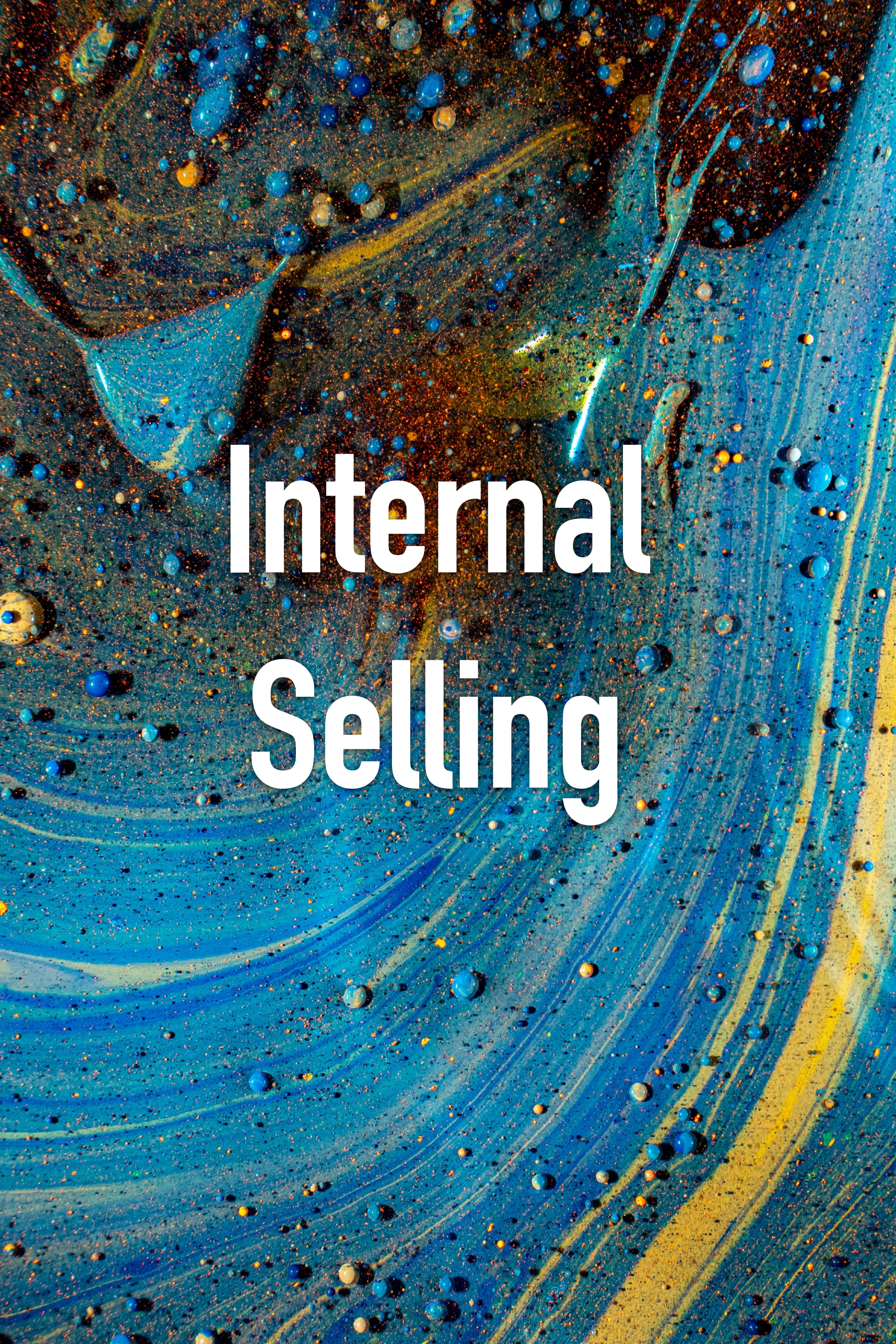


The T&Cs should make it explicitly clear that the SBOM is a best practice intended to reduce risk to the buyer

- The lack of an SBOM transfers risk from the software manufacturer to the buyer
- Thus, the buyer should be appropriately compensated for that transfer of risk
- Compensation can come in various forms such as cost reduction, additional services, and extended support

Possible T&Cs

| | SBOM Formats | Update Frequency | Vulnerable Components | Handling Newly Discovered Vulnerable Components |
|-----------------------|---|--------------------|--|---|
| Very aggressive | SBOM in a specific format (e.g., CycloneDX, SWID, SPDX) | With every release | No known vulnerable components at time of delivery | Update within 30 days |
| Moderately aggressive | SBOM in any machine readable format (e.g., txt, csv) | | | Update within 90 days |
| Not aggressive | SBOM in any format (e.g., paper, PDF) | Upon purchase | No known vulnerable components at time of build | Remediate in next planned release |



Internal Selling

Show

Show how an SBOM offers many benefits in the same way that food quality increased with a listing of ingredients

Share

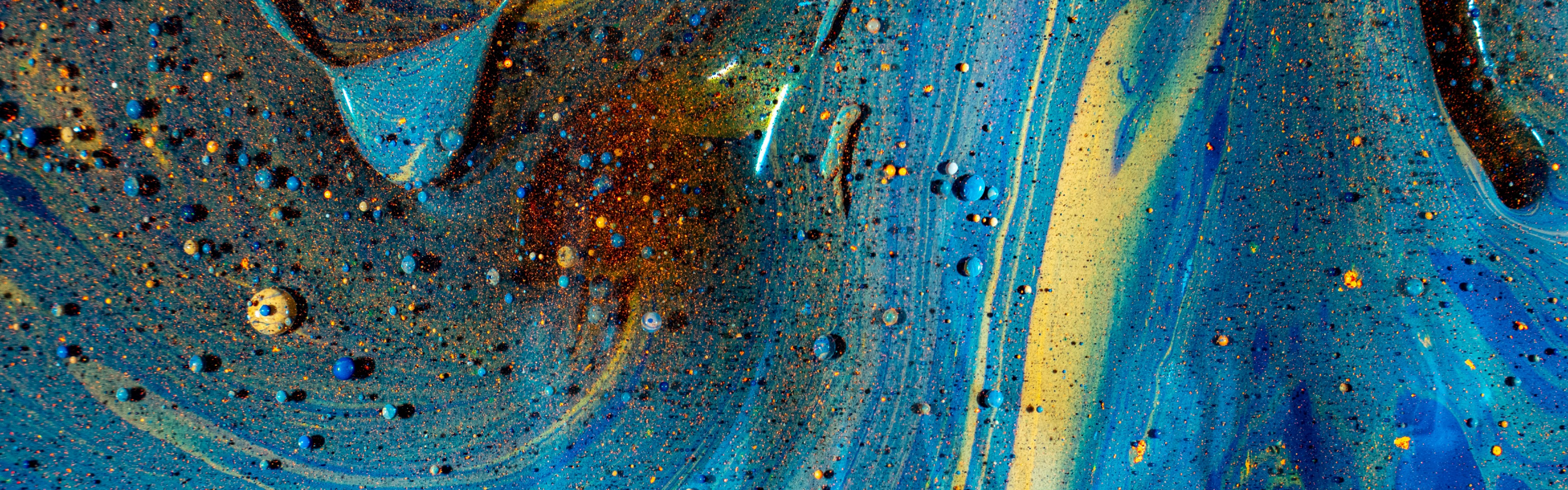
Share stories (Struts, Heartbleed, etc.) about how our risk exposure increased due to the difficulty of finding vulnerable software products without an SBOM

Start

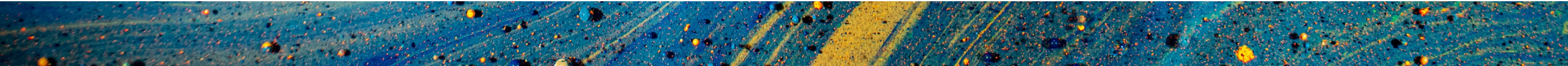
Start with software vendors where you have leverage and set a precedent internally

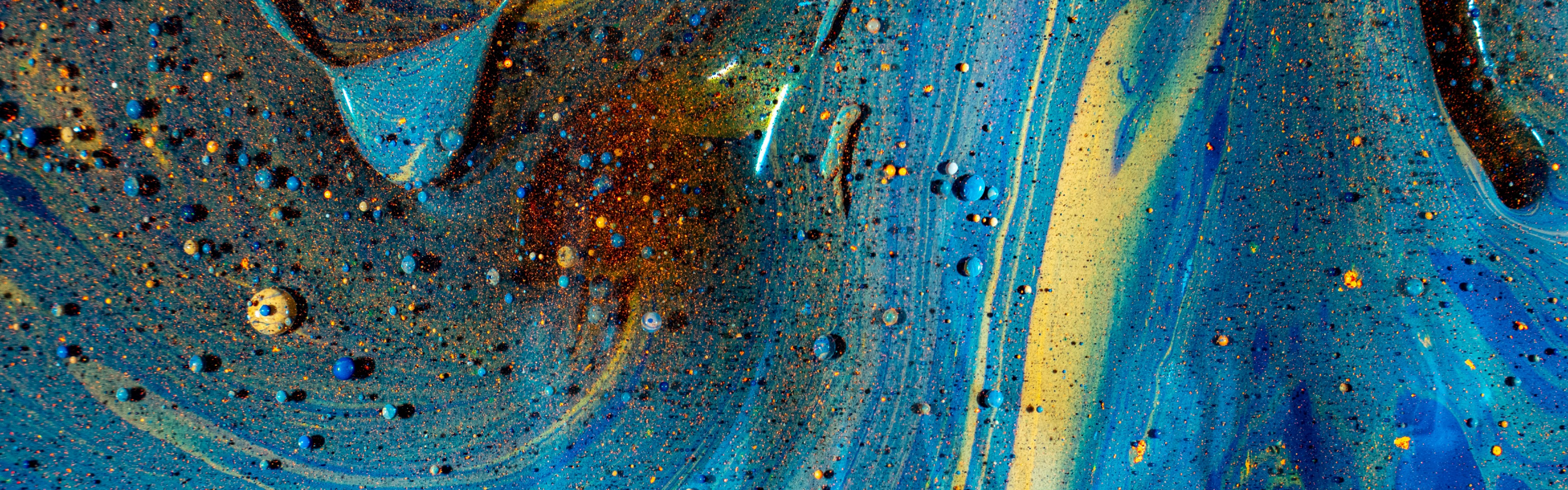
Partner

Partner with other stakeholders who will champion the cause of an SBOM (e.g., supply chain / third party assessment teams)



THANK YOU!





Q & A

