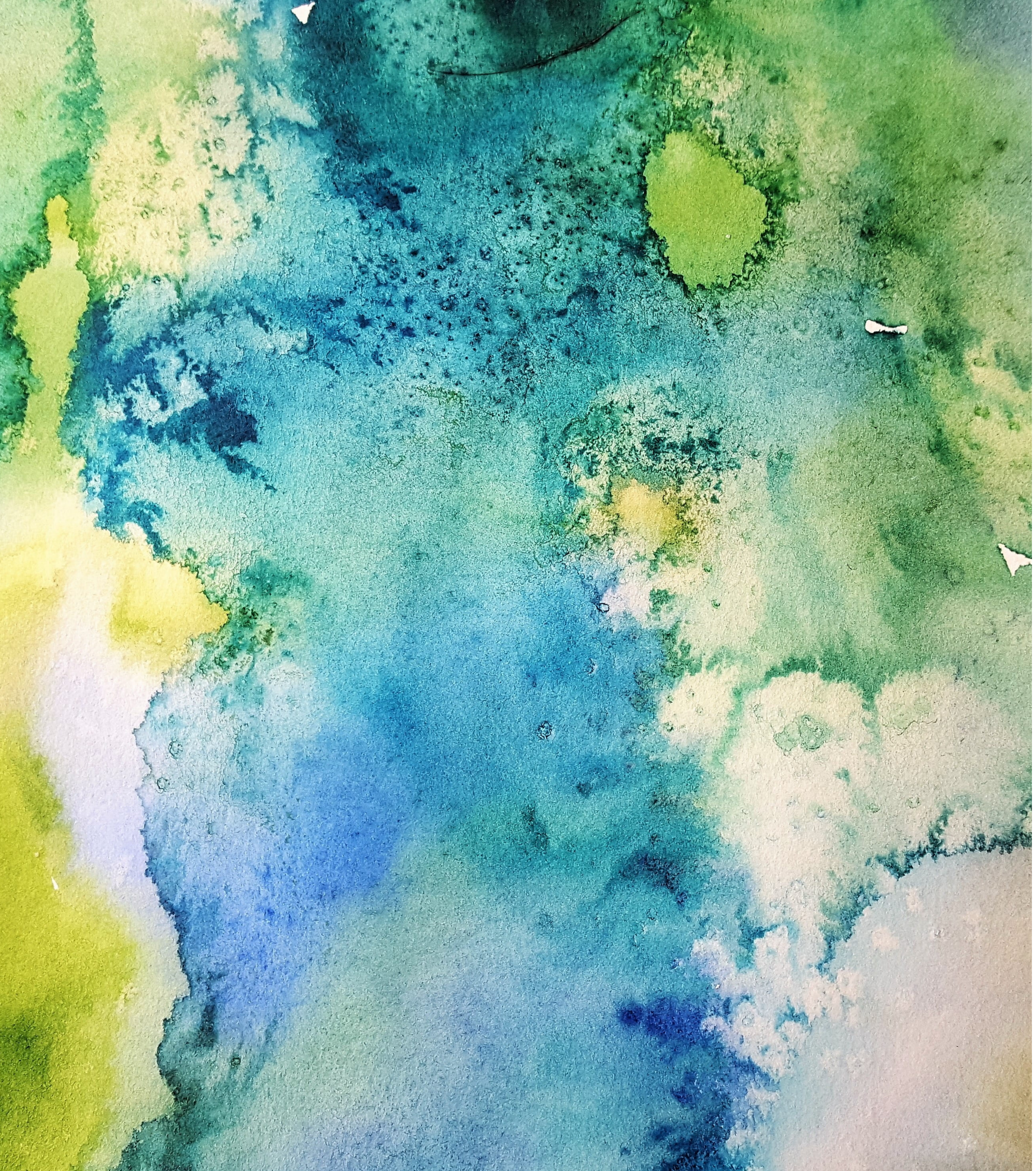
October 22, 2020

AWARENESS & ADOPTION

NTIA Software Component Transparency

Audra Hatch, Joshua Corman



OVERVIEW

- Recap: Mission and Goals
- What We’re Working On
  - Current Deliverables
  - Ongoing Efforts
  - Future Initiatives
- Community Ask
- Resources

RECAP: AWARENESS & ADOPTION MISSION

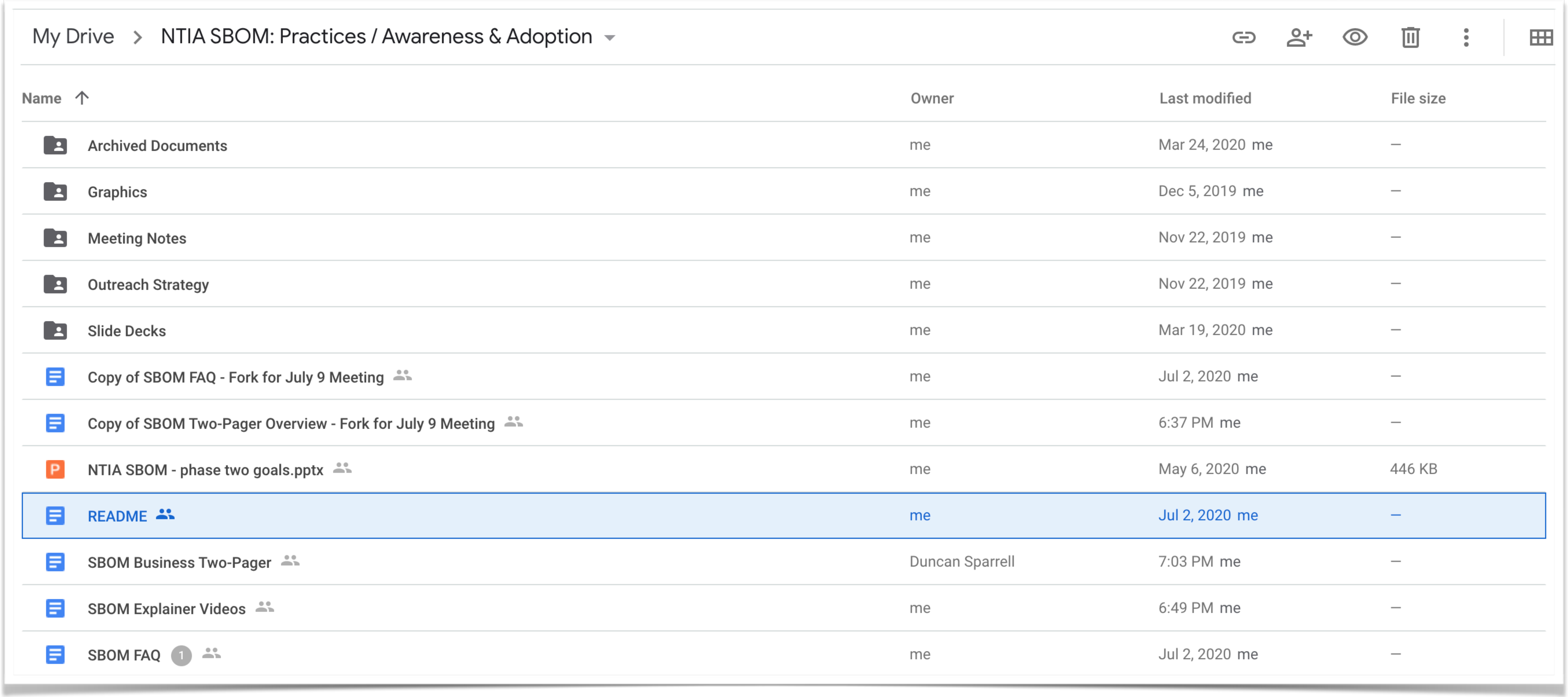
- Work will focus on promoting SBOM as an idea and a practice.
- Tasks identified include:
  - Building a broader outreach strategy with outreach targets
  - Shorter documents with specific outreach goals for sectors, organizational role, etc.
  - Coordinating with related efforts
  - More explicit business 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 1	me	Jul 2, 2020 me	–

WHAT WE'RE WORKING ON

- **Current Deliverables:**
  - FAQ
  - Overview Two-Pager
  - SBOM Calendar
  - News
  - Recordings & Presentations
  - Explainer Videos

- **Additional Ongoing Efforts:**
  - Business Two-Pagers
  - Virtual Engagement Opportunities
  - POC Conversations & Expansions
  - Graphics & Slide Repositories
  - Knowledge Base
  - SBOM-Adjacent Topics
  - Questions For Your Suppliers

- **Future Initiatives:**
  - Contract Language
  - Journeys & Playbooks
  - SBOM Starter Slides
  - Additional Explainer Videos
  - Proof of Concept Virtual Summit

DELIVERABLES AND STATUS

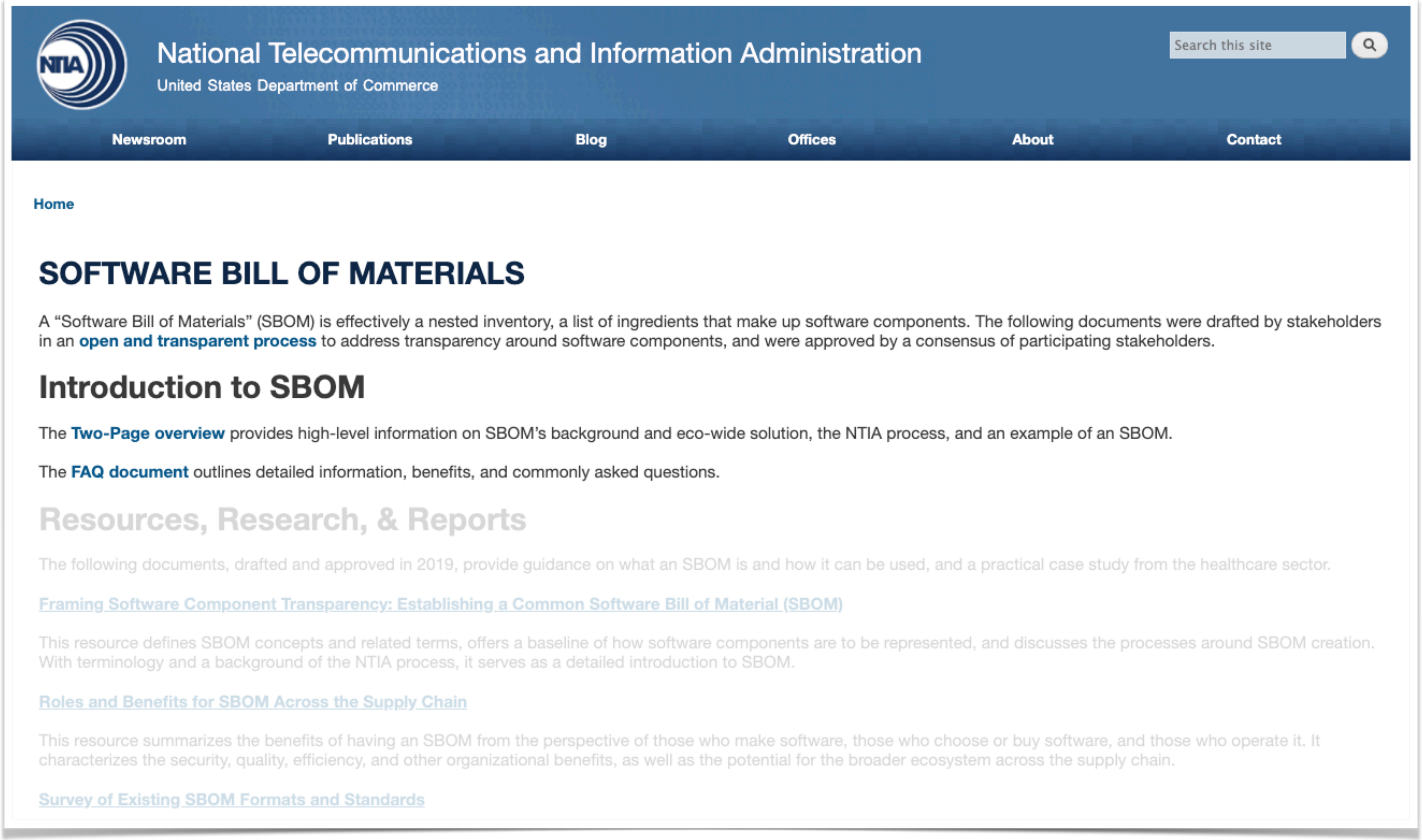
Deliverable	On Deck	Development	In Review	Released
FAQ		X	v 3	X
FAQ on GitHub				X
SBOM Overview Two-Pager	v 2			X
Explainer Videos	X		X	*
SBOM Calendar				X
SBOM News		X		*
Recordings & Presentations		X		*
SBOM Business Two-Pagers		X		
Virtual Engagement Opportunities		X		
Proof of Concept Conversations & Expansions		X		
Graphics & Slide Repositories		X		*
Knowledge Base		X		
SBOM-Adjacent Topics Spreadsheet		X		
Questions for your Suppliers		X		
Contract Language	X			
Journeys & Playbooks	X			
SBOM Starter Slides	X			
Proof of Concept Virtual Summit	X			

* Available and continuously updated in Google Drive

FAQ

- Published at Updated NTIA SBOM Website: ntia.gov/sbom
- GitHub Mirror
- Third Release (v 3)
  - 6 New Questions
  - New “How does SBOM relate to…” Category

NTIA SBOM WEBSITE UPDATE



National Telecommunications and Information Administration
United States Department of Commerce

SOFTWARE BILL OF MATERIALS

A "Software Bill of Materials" (SBOM) is effectively a nested inventory, a list of ingredients that make up software components. The following documents were drafted by stakeholders in an open and transparent process to address transparency around software components, and were approved by a consensus of participating stakeholders.

Introduction to SBOM

The Two-Page overview provides high-level information on SBOM's background and eco-wide solution, the NTIA process, and an example of an SBOM.

The FAQ document outlines detailed information, benefits, and commonly asked questions.

Resources, Research, & Reports

The following documents, drafted and approved in 2019, provide guidance on what an SBOM is and how it can be used, and a practical case study from the healthcare sector.

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

This resource defines SBOM concepts and related terms, offers a baseline of how software components are to be represented, and discusses the processes around SBOM creation. With terminology and a background of the NTIA process, it serves as a detailed introduction to SBOM.

Roles and Benefits for SBOM Across the Supply Chain

This resource summarizes the benefits of having an SBOM from the perspective of those who make software, those who choose or buy software, and those who operate it. It characterizes the security, quality, efficiency, and other organizational benefits, as well as the potential for the broader ecosystem across the supply chain.

Survey of Existing SBOM Formats and Standards

FAQ - PUBLISHED

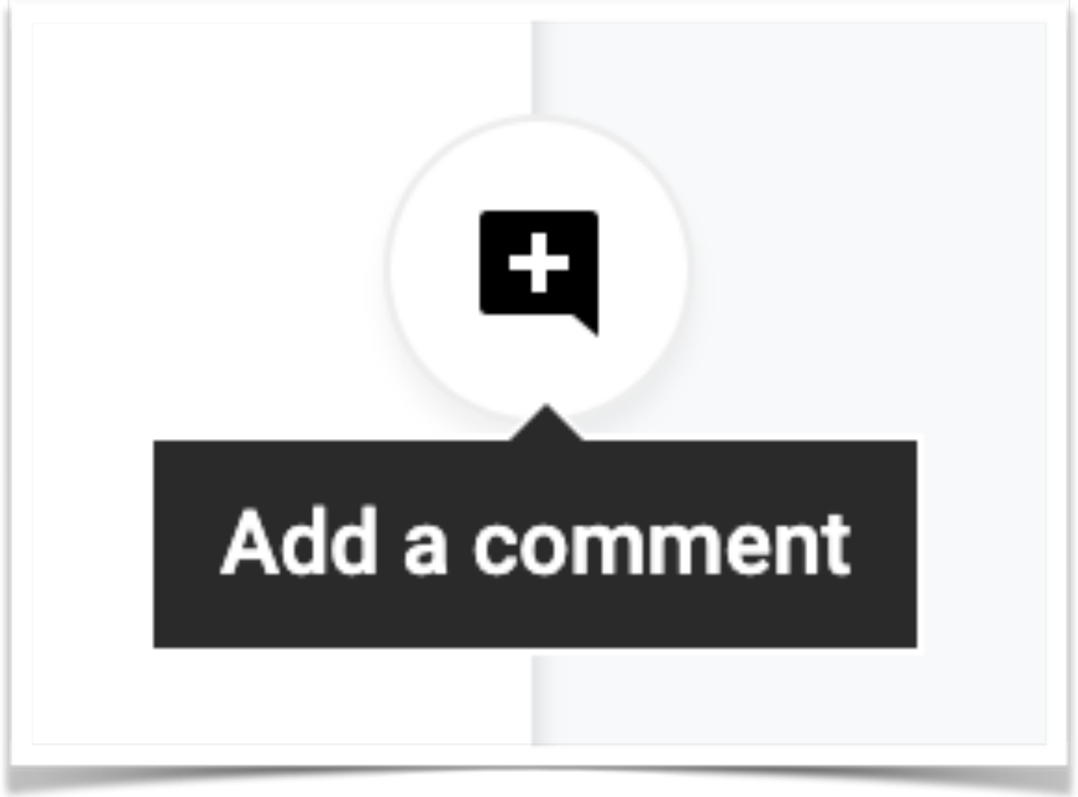
- Current Published Version - Available at ntia.gov/sbom
- Categories:
  - Overview
  - Benefits
  - Common Misconceptions & Concerns
  - Creation
  - Distribution & Sharing
  - Role Specific
  - Get Involved

FAQ – GITHUB MIRROR

- Current NTIA Published Version Mirrored on GitHub:
  - https://github.com/sparrell/NtiaSbomFaq
- Opportunity for broader community engagement
- Process:
  - Generate an Issue: To record a problem or a missing question
  - Pull Request: To propose a change to an existing question
  - Awareness & Adoption working group reviews Issues and Pull Requests
  - Approved changes are applied to Google Doc, circulated for broader working group review, and then published to the NTIA website

FAQ – THIRD RELEASE FEEDBACK

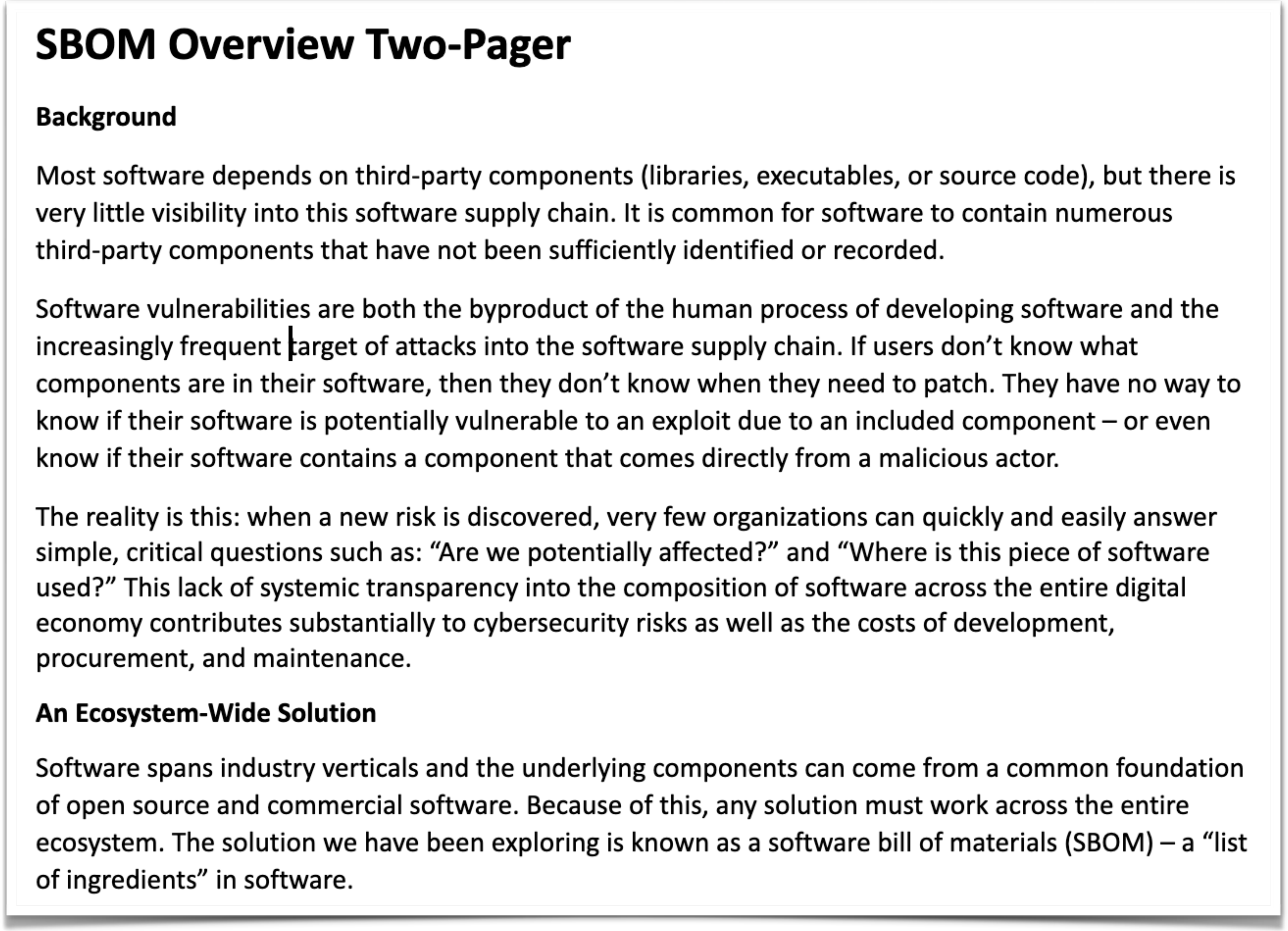
- October 22 Version:
  - https://bit.ly/sbom-awareness-faq-october22
- Feedback Due: November 6, 2020
- Please provide feedback via "Add a comment" on Google Document:



- Please also nominate new FAQ questions and/or categories!

SBOM OVERVIEW TWO-PAGER

- Published at ntia.gov/sbom



SBOM Overview Two-Pager

Background

Most software depends on third-party components (libraries, executables, or source code), but there is very little visibility into this software supply chain. It is common for software to contain numerous third-party components that have not been sufficiently identified or recorded.

Software vulnerabilities are both the byproduct of the human process of developing software and the increasingly frequent target of attacks 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 potentially vulnerable to an exploit due to an included component – or even know if their software contains a component that comes directly from a malicious actor.

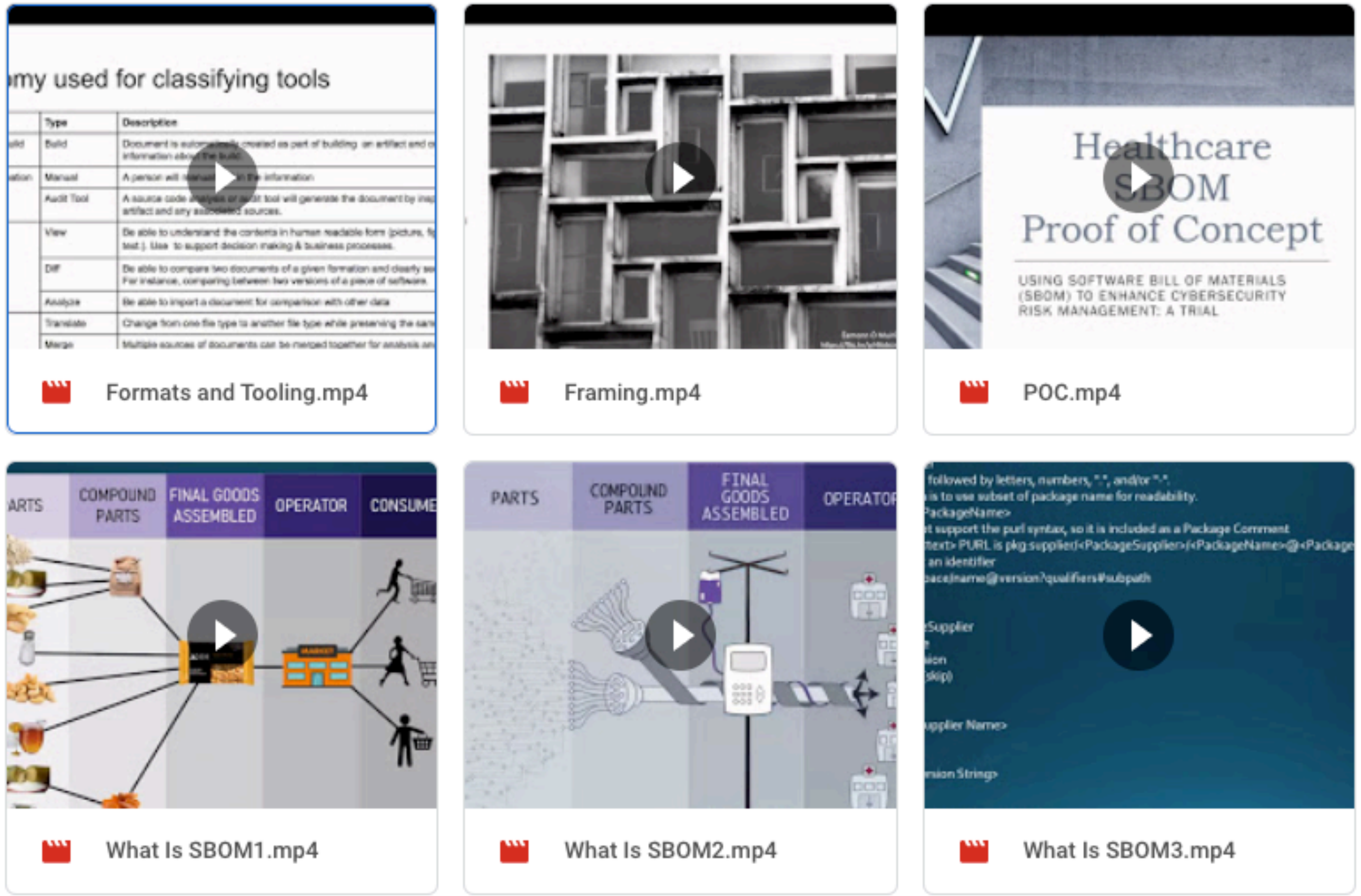
The reality is this: when a new risk is discovered, very few organizations can quickly and easily answer simple, critical questions such as: "Are we potentially affected?" and "Where is this piece of software used?" This lack of systemic transparency into the composition of software across the entire 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 can come from a common foundation of open source and commercial software. 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.

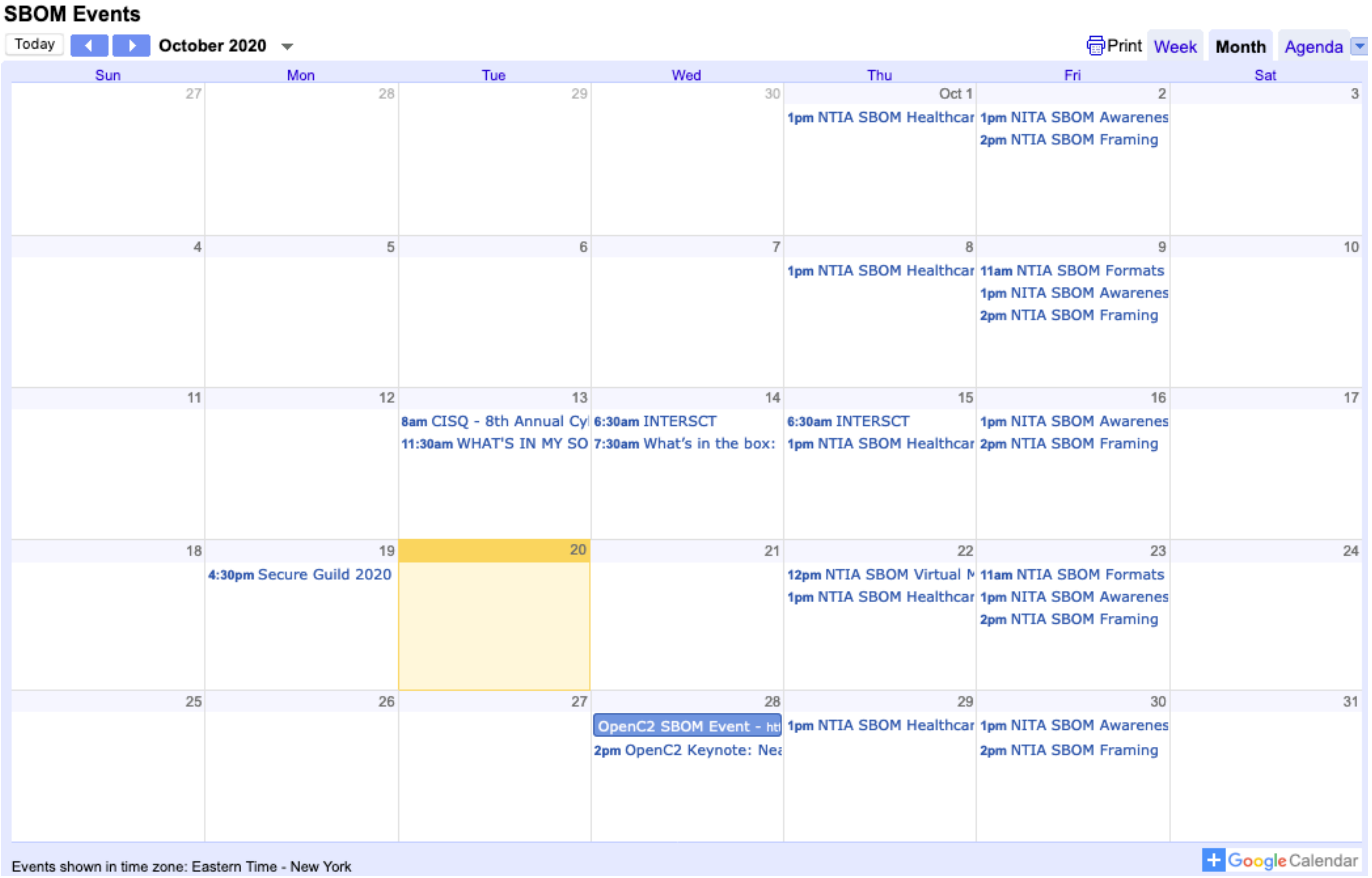
PHASE I SBOM EXPLAINER VIDEOS

- Completed Explainer Video Links and Space for Feedback:
  - https://bit.ly/sbom-awareness-explainer-videos



- Pursuing publishing on ntia.gov/sbom

SBOM EVENTS CALENDAR



SBOM Events

October 2020

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

Events shown in time zone: Eastern Time - New York

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 NEWS

- October 9, 2020 - "Don’t Drop the SBOM! Creating a Usable (and Useful) Software Bill of Materials for Your Medical Device”, Michelle Jump https://www.linkedin.com/posts/michellejump_sbom-softwaretransparency-activity-6720381952240738304-3rj1
- October 7, 2020 - “How To Prove (Or Improve) The Trustworthiness Of Your Medical Devices”, John Giantsidis https://www.meddeviceonline.com/doc/how-to-prove-or-improve-the-trustworthiness-of-your-medical-devices-0001
- October 6, 2020 - “Working together to secure our expanding connected health future”, Kelly Rozumalski https://www.helpnetsecurity.com/2020/10/06/working-together-to-secure-our-expanding-connected-health-future/
- September 24, 2020 - “Five big questions as America votes: Cybersecurity” https://www.atlanticcouncil.org/blogs/new-atlanticist/five-big-questions-as-america-votes-cybersecurity/
- September 23, 2020 - “A powerful example of why we need SBOM”, Tom Alrich https://tomalrichblog.blogspot.com/2020/09/a-powerful-example-of-why-we-need-sboms.html
- September 23, 2020 - “To improve DevSecOps, set application security priorities”, Taylor Armerding https://www.scmagazine.com/home/sponsor-content/to-improve-devsecops-set-application-security-priorities/
- September 9, 2020 - “Critical Flaws in 3rd-Party Code Allow Takeover of Industrial Control Systems”, Lindsey O’Donnell https://threatpost.com/severe-industrial-bugs-takeover-critical-systems/159068

SBOM NEWS

- Link to document listing recent SBOM News:
  - https://bit.ly/sbom-awareness-news

- If you have a news story to add to the list, please submit a comment in the Google Doc.

RECENT PUBLIC SBOM RECORDINGS

- October 2020 - CSIAC Webinars: Allan Friedman (1 h)
  “Software Bill of Materials (SBOM)”
  https://www.csiac.org/podcast/software-bill-of-materials-sbom/

- October 2020 - CISQ Webinar: Robert Martin, Bill Curtis (51 min)
  “Introducing the Tool-to-Tool Software Bill of Materials Specification”
  https://www.it-cisq.org/webinars/software-bill-of-materials.htm

- September 2020 - CISA CYBERSUMMIT 2020: Daniel Kroese, Kate Stewart, Allan Friedman, Trey Herr (40 min)
  “Promoting Security in the Software Supply Chain”
  https://www.cisa.gov/cybersummit-2020-day-two-leading-digital-transformation

- August 2020 - Brakeing Down Security Podcast (44 min)
  “2020-031-Allan Friedman, SBOM, software transparency, and knowing how the sausage is made”
  https://brakeingsecurity.com/2020-031-allan-friedman-sbom-software-transparency-and-knowing-how-the-sausage-is-made

- July 2020 - Brakeing Down Security Podcast (1 h)
  “2020-028-Shlomi Oberman, RIPPLE20, supply chain security discussion, software bill of materials”
  https://brakeingsecurity.com/2020-028-shlomi-oberman-ripple20-supply-chain-security-discussion-software-bill-of-materials

- May 2020 - InSecurity Podcast (1 h 16 min)
  “Chris Blask and Fred Cohen on DBOM and the Record of Everything”
  https://blogs.blackberry.com/en/2020/05/insecurity-podcast-chris-blask-and-fred-cohen-on-dbom-and-the-record-of-everything

SBOM RECORDINGS, PRESENTATIONS, AND PODCASTS

- Link to document listing SBOM Recordings, Presentations, and Podcasts:
  - https://bit.ly/sbom-awareness-recordings
- If you have a recording, presentation, or podcast to add to the list, please submit a comment in the Google Doc.
- #AllanDoesntScale

ONGOING EFFORTS

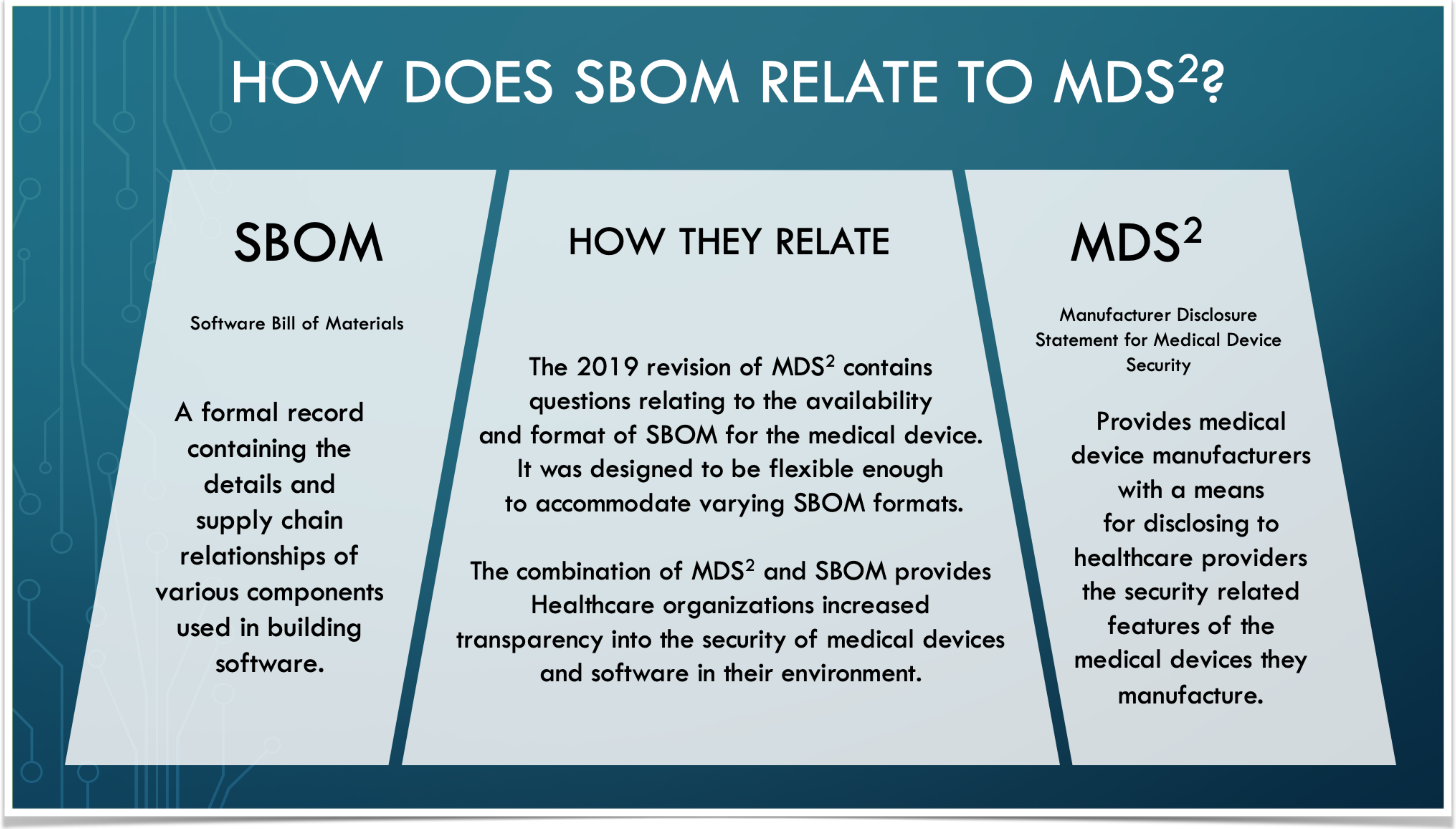
- Business Two-Pagers
  - Reworking into two documents:
    - Business Customer
    - Producer
- Virtual Engagement Opportunities
  - Webinars, Podcasts, Virtual Conferences, Other
- Proof of Concept Conversations & Expansions
- Graphics Repository:
  - https://bit.ly/sbom-awareness-graphics
- Slides Repository:
  - http://bit.ly/sbom-awareness-slides
- Knowledge Base - Searchable, cross-linked Phase I Documents

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

"HOW DOES SBOM RELATE TO…"

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



HOW DOES SBOM RELATE TO MDS^2?

SBOM

Software Bill of Materials

A formal record containing the details and supply chain relationships of various components used in building software.

HOW THEY RELATE

The 2019 revision of MDS^2 contains questions relating to the availability and format of SBOM for the medical device. It was designed to be flexible enough to accommodate varying SBOM formats.

The combination of MDS^2 and SBOM provides Healthcare organizations increased transparency into the security of medical devices and software in their environment.

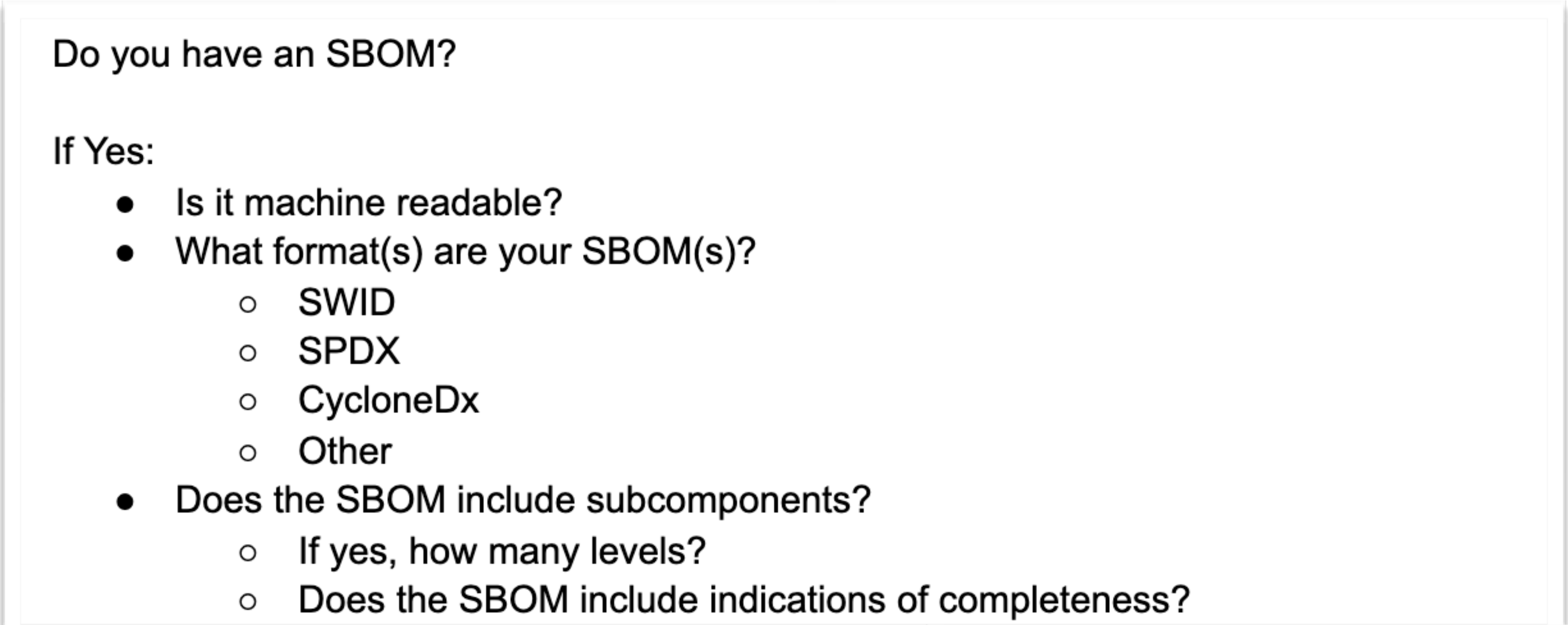
MDS^2

Manufacturer Disclosure Statement for Medical Device Security

Provides medical device manufacturers with a means for disclosing to healthcare providers the security related features of the medical devices they manufacture.

QUESTIONS FOR YOUR SUPPLIERS

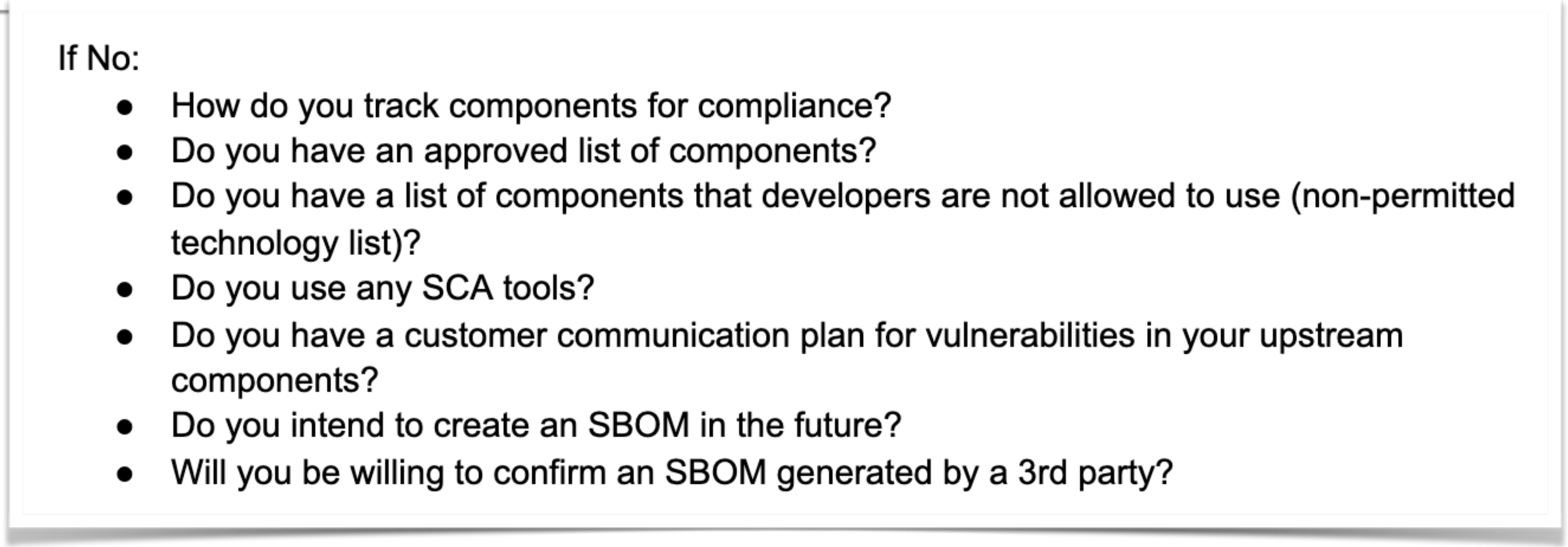
- Link to document listing questions to ask your suppliers about SBOM:
  - http://bit.ly/sbom-questions-for-suppliers



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

- ➤ SBOM Contract Language
- ➤ Journeys & Playbooks
- ➤ SBOM Starter Slides
- ➤ Additional Explainer Videos
- ➤ Proof of Concept Virtual Summit

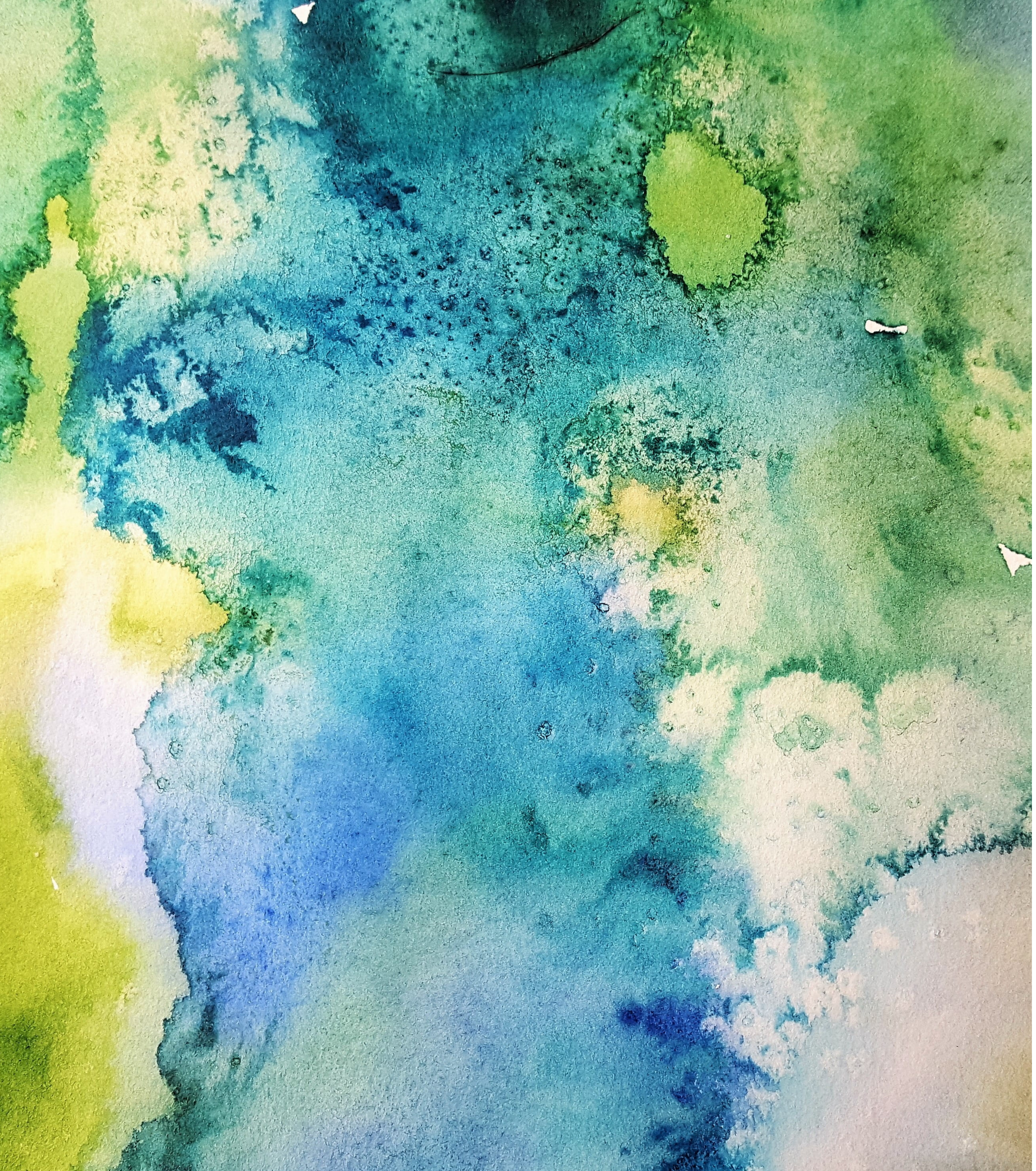
RECAP: HOW-TO-POC VIRTUAL SUMMIT

- Collaboration with Healthcare Proof of Concept (POC)
- Goal: To encourage and engage other industries to leverage the POC approach and template pioneered by the Healthcare Industry for additional proofs of concept
- Please nominate and introduce industries and stakeholders who may be a good fit for a Proof of Concept
  - Optimal targets include industries that are relatively mature in their use of traditional BOMs and/or those who are increasingly affected by supply chain vulnerabilities (e.g. Urgent/11, Ripple20)
  - e.g. Automotive, Aviation, Energy, Oil & Gas, etc.

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

- Awareness & Adoption Meeting
  - Fridays at 1:00 PM ET
- 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

THANK YOU!