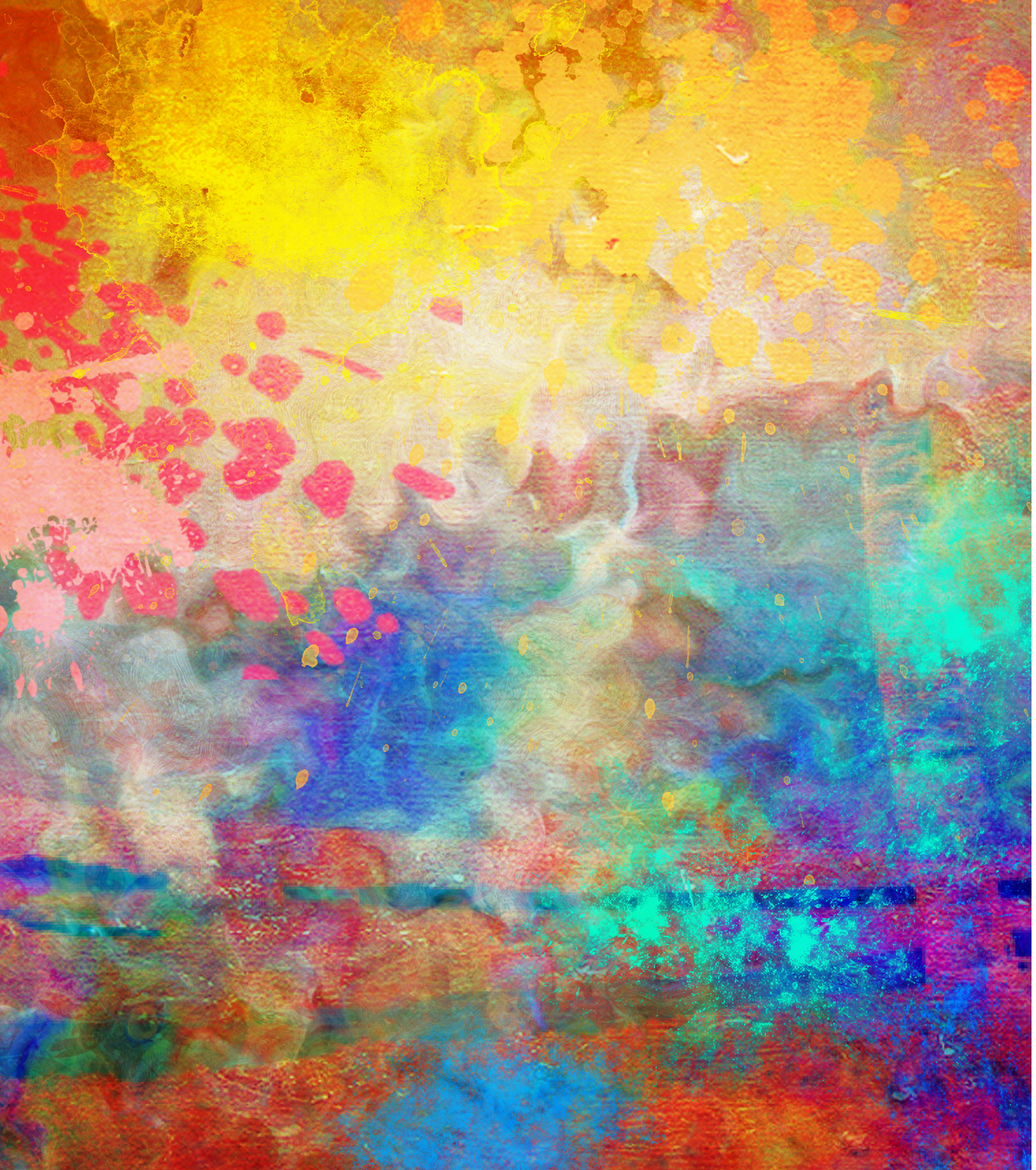
July 9, 2020

AWARENESS & ADOPTION

NTIA Software Component Transparency

Audra Hatch, Joshua Corman



OVERVIEW

- Recap: Mission and Goals
- What We're Working On
  - Current Deliverables
  - Ongoing Efforts
- 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

- **Current Deliverables:**
  - FAQ - Second Release
  - SBOM Overview Two-Pager
  - Phase I SBOM Explainer Videos
  - Recent Public SBOM Recordings
  - README
- **Ongoing Efforts:**
  - FAQ - Backlog and Work-In-Progress
  - SBOM Business Two-Pager
  - SBOM Documents - Tailored to industry and/or role
  - Graphics Repository
  - Additional SBOM Explainer Videos
  - Knowledge Base - Searchable, cross-linked Phase I Documents
  - Virtual Engagement Opportunities
  - How-To-POC Virtual Summit

DELIVERABLES AND STATUS

Deliverable	Development	In Review	Released
FAQ	X	v 2	
SBOM Overview Two-Pager	X	X	
SBOM Business Two-Pager	X		
Explainer Videos	X	X	
Graphics Repository	X		*
Recordings & Presentations	X		*
Knowledge Base - Searchable, cross-linked Phase I Documents	X		
Outreach Opportunities	X		

* Available and continuously updated in Google Drive

FAQ - SECOND RELEASE

- July 9 Version - 23 Questions prepared for feedback
- Broad Categories:
  - General Questions
  - Concerns about SBOMs
  - Details of SBOM Execution
  - Role-Specific
- Backlog and Work-In-Progress:
  - Questions that need additional work prior to distribution to the broader working groups

FAQ – SECOND RELEASE FEEDBACK

- July 9 Version - Questions prepared for feedback: https://bit.ly/sbom-awareness-faq-july9
- Feedback Due: July 24, 2020
- Please provide feedback via “Add a comment” on Google Document:

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

SBOM OVERVIEW TWO-PAGER

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.

SBOM OVERVIEW TWO-PAGER FEEDBACK

- July 9 Version - Two-Pager prepared for feedback: https://bit.ly/sbom-awareness-overview-two-pager-july9
- Feedback Due: July 24, 2020
- Please provide feedback via “Add a comment” on Google Document:

PHASE I SBOM EXPLAINER VIDEOS

- Completed Explainer Video Links and Space for Feedback: https://bit.ly/sbom-awareness-explainer-videos
- Please provide:
  - Feedback on style and approach for future videos
  - Suggestions for future topics and volunteers
- Feedback Due: July 24, 2020
- Many thanks to our editor/producer Chris Gates and to all the cast and crew!

RECENT PUBLIC SBOM RECORDINGS

- May 2020 - Security Nation Podcast: Jen Ellis, Tod Beardsley, Josh Corman, Audra Hatch (38 min)
  “Advocating for Tech Literacy and Transparency”
  https://www.rapid7.com/resources/security-nation-i-am-the-cavalry/

- 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

- February 2020 - BSidesSF: Allan Friedman
  “Someone Set Us Up the SBOM - How Software Transparency Can Help Save the World”
  https://www.youtube.com/watch?v=9j1KYLfklMQ

- 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

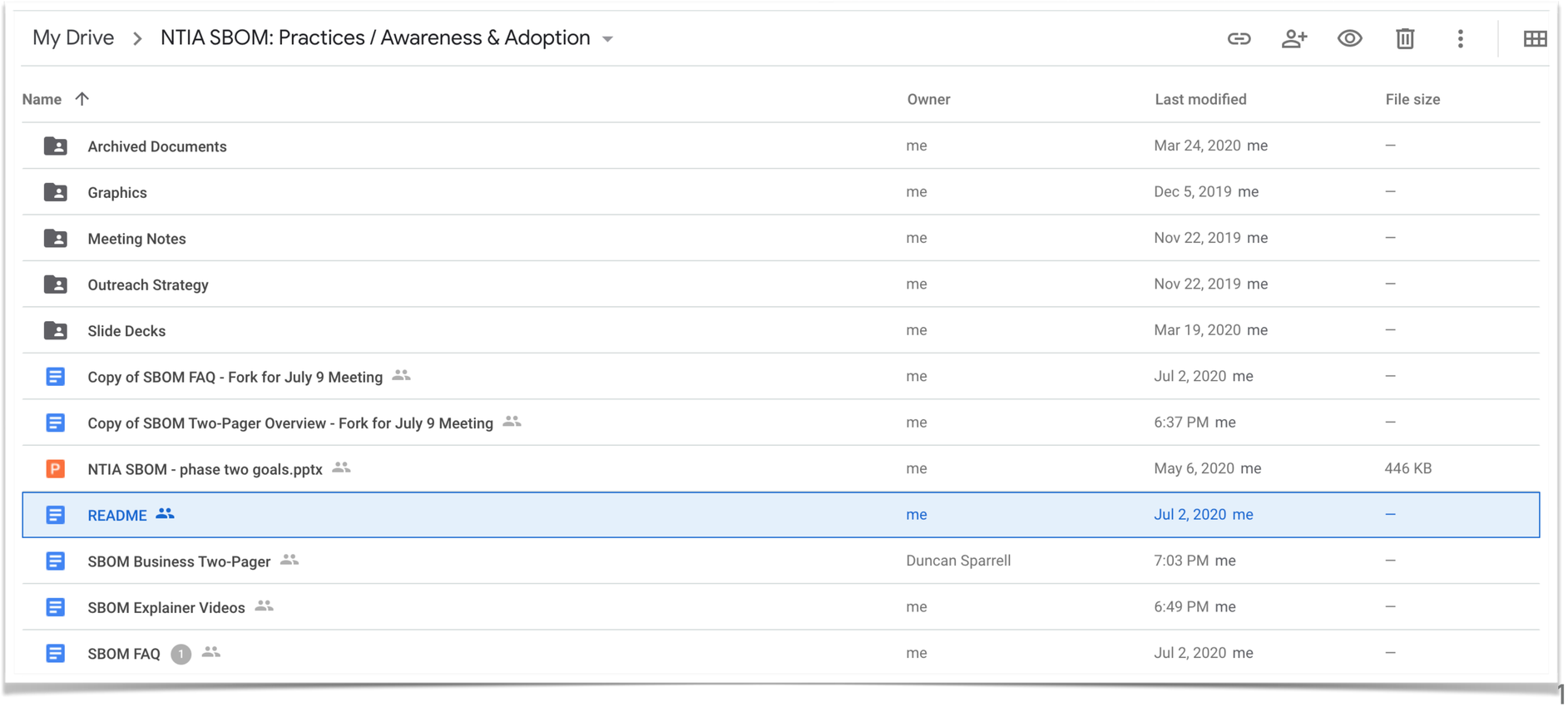
SBOM RECORDINGS, PRESENTATIONS, AND PODCASTS

- Link to document listing SBOM Recordings, Presentations, and Podcasts:
  - https://bit.ly/sbom-awareness-recordings

- #AllanDoesntScale

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



ONGOING EFFORTS

- DRAFT Business Two-Pager
  https://docs.google.com/document/d/151kAUnyqTAAAVtF5q7IXTfG1HiHjsgQbveLGtYLb8Z4/edit?usp=sharing

- Graphics Repository:
  https://bit.ly/sbom-awareness-graphics

- Additional SBOM Explainer Videos

- Knowledge Base - Searchable, cross-linked Phase I Documents

- Virtual Engagement Opportunities
  - Webinars, Podcasts, Virtual Conferences, Other

HOW-TO-POC VIRTUAL SUMMIT

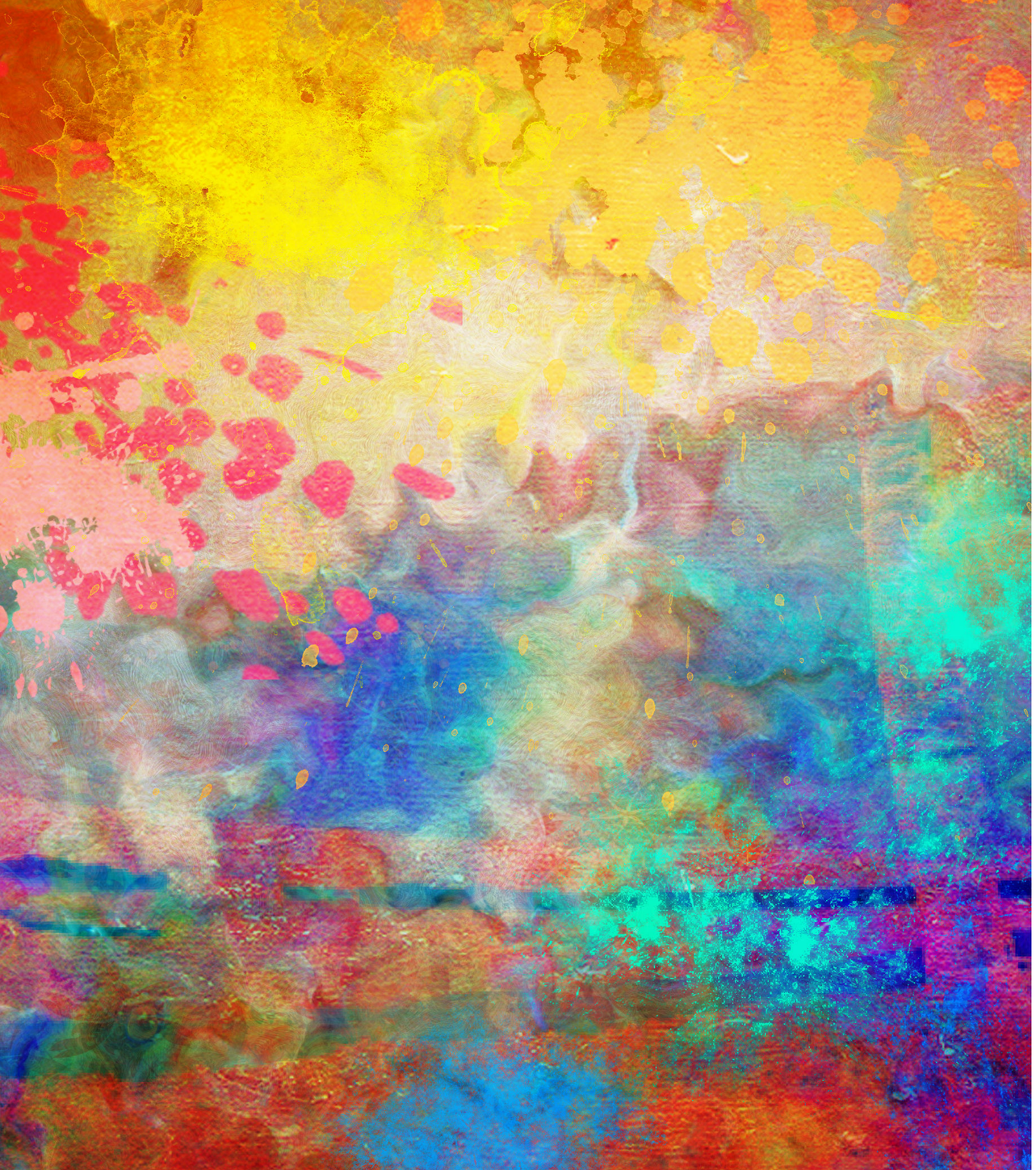
- Collaboration with Healthcare Proof of Concept (POC)
- Goal: To encourage and engage other industries to leverage the POC approach and template pioneered by the Healthcare Industry for additional proofs of concept
- Please nominate and introduce industries and stakeholders who may be a good fit for 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:
  - Please provide feedback on FAQ and SBOM Overview Two-Pager.
  - Watch and share public recordings
  - Create an Explainer Video
  - 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?
  - How can we improve existing resources?

- Get creative with outreach in the time of corona!



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!