



*April 29, 2021*

# AWARENESS & ADOPTION

---

*NTIA Software Component Transparency*

*Audra Hatch, Joshua Corman*





# OVERVIEW

---

- Recap: Mission and Goals
- 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		<a href="#">Link</a> <a href="#">Share</a> <a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>		
Name	Owner	Last modified		File size
 Archived Documents	me	10:00 AM me		—
 Video	Arthur Hicken	Jan 15, 2021 me		—
 Artifacts	me	Nov 12, 2020 me		—
 Slide Decks	me	Mar 19, 2020 me		—
 Graphics	me	Dec 5, 2019 me		—
 Outreach Strategy	me	Nov 22, 2019 me		—
 Meeting Notes	me	Nov 22, 2019 me		—
 SBOM Options and Decision Points 	me	10:27 AM me		—
 SBOM Related Efforts  	me	Apr 26, 2021 me		—
 README 	me	Apr 26, 2021 me		—
 RSAC 2021  	me	Apr 25, 2021		—
 SBOM at a Glance 	me	Apr 14, 2021 me		—
 SBOM FAQ  	me	Apr 9, 2021		—





# WHAT WE'RE WORKING ON

---

## ➤ Today's Highlights:

- SBOM at a Glance
- SBOM Options & Decision Points Graphic
- Asking for SBOMs
- Supplying SBOMs
- SBOM Related Efforts
- FAQ
- Graphics Repository
- Slide Repository

## ➤ Ongoing Efforts:

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

## ➤ Future Initiatives:

- Use Case Repository
- 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	X
FAQ on GitHub				X
SBOM at a Glance				X
SBOM Options & Decision Points				X
NTIA SBOM Overview Two-Pager	v 2			X
Explainer Videos	X			X*
SBOM Calendar				X
SBOM Related Efforts			X	
SBOM News		X		*
Recordings & Presentations		X		*
Graphics & Slide Repositories		X		*
Community Survey on SBOM Process			X	*
SBOM Business Two-Pagers		X		
Virtual Engagement Opportunities		X		
Proof of Concept Conversations & Expansions		X		
Knowledge Base		X		
SBOM-Adjacent Topics Spreadsheet		X		
Questions for your Suppliers		X		
SBOM Starter Slides		X		
Asking for SBOMs	X			
Supplying SBOMs	X			
Journeys & Playbooks	X			
Proof of Concept Virtual Summit	X			

\* Available and/or continuously updated in Google Drive



# SBOM AT A GLANCE

- Intro to SBOMs, supporting literature, and the pivotal role of SBOMs for supply chain transparency
  - What is an SBOM?
  - Benefits & Use Cases
  - Baseline Component Information
  - Machine-Readable Formats & Tools
  - Sharing & Exchanging
  - Learn More
- Published on [ntia.gov/sbom](https://ntia.gov/sbom)

NTIA Multistakeholder Process on Software Component Transparency | [ntia.gov/sbom](https://ntia.gov/sbom)

## SBOM at a Glance

### Purpose

This document is an introduction to the practice of Software Bill of Materials (SBOM), supporting literature, and the pivotal role SBOMs play in providing much-needed transparency: enabling stakeholders to answer questions like “Am I affected?” and “Where am I affected?” when faced with a supply chain concern.

### What is an SBOM?

An SBOM is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships. These inventories should be comprehensive – or should explicitly state where they could not be. SBOMs may include open source or proprietary software and can be widely available or access-restricted.<sup>1</sup>

SBOMs should also include baseline attributes with the ability to uniquely identify individual components in a standard data format. The most efficient generation of SBOMs is as a byproduct of a modern development process. For older software, less-automated methods exist.

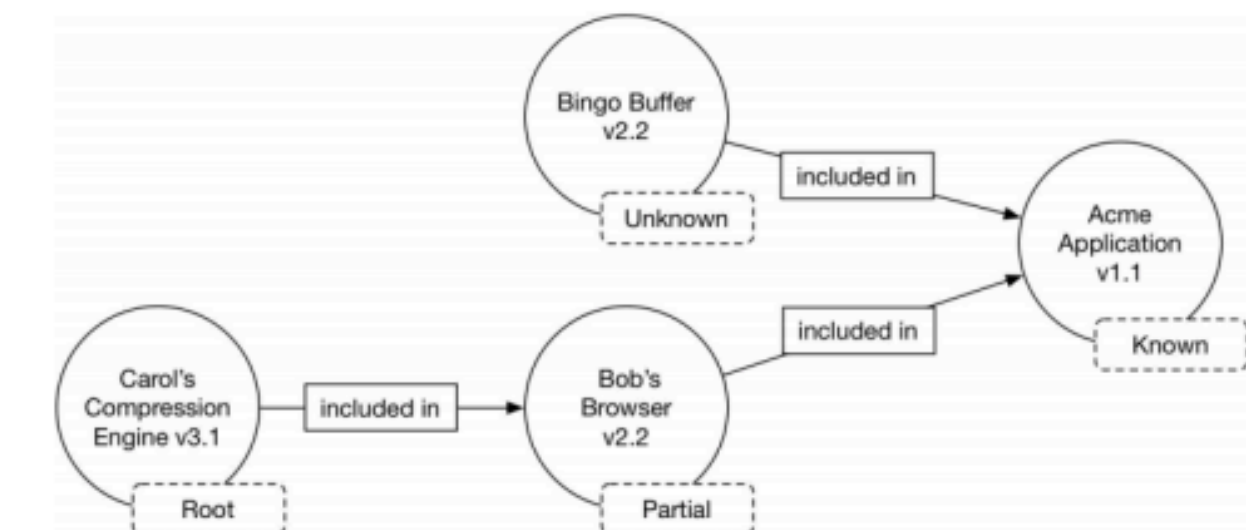


Figure: Conceptual SBOM tree with upstream relationship assertions

### Benefits and Use Cases

The benefits and use cases for SBOMs<sup>2</sup> are numerous; vary across stakeholders who produce, choose, and operate software; and are amplified when combined. Benefits include reducing cost, security risk, license risk, and compliance risk. Use cases include improved software development, supply chain management, vulnerability management, asset management, procurement, and high assurance processes. An ongoing SBOM Healthcare Proof of Concept<sup>3</sup> has exercised many of these use cases and demonstrated the value of producing, sharing, and consuming SBOMs, prompting similar proofs of concept in the Automotive and Energy industries.



# SBOM OPTIONS & DECISION POINTS

- Purpose
  - To frame the dimensions for what is possible with modern development practices
  - To support more consistent and effective articulation of needs between requesters and suppliers of SBOMs

➤ Published on [ntia.gov/sbom](https://ntia.gov/sbom)

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier  
† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship  
‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version

String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM OPTIONS & DECISION POINTS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# PERSPECTIVE: ASKING FOR SBOMS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# PERSPECTIVE: SUPPLYING SBOMS

Dimension	-	Initial Consensus	+
Baseline Component Information	Contains core subset* of Baseline Component Information attributes	Includes all Baseline Component Information† attributes	Contains component information beyond baseline supportive of high assurance use cases
Format & Machine Readability	SBOM in any machine-readable format (e.g. csv)	SBOM in a baseline-supporting, machine-readable format‡	SBOM in all machine-readable, interoperable formats‡, maintaining currency as standards evolve or emerge
Depth	All primary components with direct dependencies and known-unknowns declared	All primary components with all transitive dependencies and known-unknowns declared	All primary components with all transitive dependencies with no unknowns
Generation Frequency	At time of pre/purchase and/or provided upon request within x time	With every update or change to code (major/minor release or patch)	Additionally hosted in an archive for every version
Delivery & Interoperability	Emailed and/or hosted/archived by the supplier	Bundled with every product version and archived by the supplier	Supports machine interfaces (e.g. API) and adjacent interoperability (e.g. DBOM, MUD, OpenC2)
Adjacent Enhancement: Vulnerability Claims	Supplier makes attestations for potentially exploitable vulnerabilities upon request	Supplier makes attestations for potentially exploitable vulnerabilities within x time of a new vulnerability	Standardized API query for current attestation of product-specific risks to SBOM components

\* Core subset of Baseline Component Information: Component Name, Supplier Name, Version String, Unique Identifier

† Baseline Component Information: Author Name, Supplier Name, Component Name, Version String, Component Hash, Unique Identifier, Relationship

‡ SBOM Formats: SPDX, CycloneDx, SWID



# SBOM RELATED EFFORTS

- Originally Appendix I in “Roles and Benefits for SBOM Across the Supply Chain” Phase I document
- Releasing as standalone “SBOM Related Efforts” document
- 15+ Additions and Updates
- <http://bit.ly/sbom-related-efforts>

NTIA Multistakeholder Process on Software Component Transparency | [ntia.gov/sbom](https://ntia.gov/sbom)

Table of Contents

Introduction	3
Atlantic Council “Breaking Trust” Report	3
BSA Framework for Secure Software	4
Building Security in Maturity Model	4
CISQ Trustworthy System Manifesto	4
Cybersecurity Maturity Model Certification (CMMC)	5
Cloud Native Computing Foundation	5
Digital Bill of Materials	5
Edison Electric Institute – Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk	5
ENISA – European Cybersecurity Certification Scheme for Cloud Services	6
ENISA – Guidelines for Securing the Internet of Things	6
FDA Premarket Guidance	7
FS-ISAC Third Party Governance	7
International Organization for Standardization (ISO)	7
ISO/IEC 27002:2005 and 27002:2013 – Code of Practice for Information Security Controls	7
ISO/IEC 5230:2020 – OpenChain Specification	9
ISO/SAE 21434 – Road Vehicles - Cybersecurity Engineering	9
Joint Security Plan	9
Manufacturers Disclosure Statement for Medical Device Security	10
MITRE Deliver Uncompromised	10
Manufacturer Usage Description	10
NERC CIP-013	10
National Cyber Security Centre (NCSC) - Using the Software Bill of Materials for Enhancing Cybersecurity	11
National Highway Traffic Safety Administration – Cybersecurity Best Practices for the Safety of Modern Vehicles	11
NIST’s Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)	12
Open Command and Control	12
OWASP Component Analysis Project	12
OWASP Software Component Verification Standard	12
SAFECode Managing Security Risks Inherent in the Use of Third party Components	13
Software Heritage	13
UL 2900-1 – Standard for Software Cybersecurity for Network-Connectable Products	14
United Nations Economic Commission for Europe WP.29 / R155	14
SBOM Related Efforts	2



# SBOM RELATED EFFORTS – FEEDBACK REQUEST

---

- SBOM Related Efforts prepared for feedback:  
<http://bit.ly/sbom-related-efforts>
- Feedback Due: May 14, 2021
- Please provide feedback via “Add a comment” on Google Document:



- Please also nominate new SBOM-related efforts for inclusion.



# FAQ

- Published on NTIA SBOM Website:
  - [ntia.gov/sbom](https://ntia.gov/sbom)
- GitHub Mirror of FAQ:
  - [https://github.com/NTIADC/SBOM\\_FAQ/](https://github.com/NTIADC/SBOM_FAQ/)

SBOM FAQ

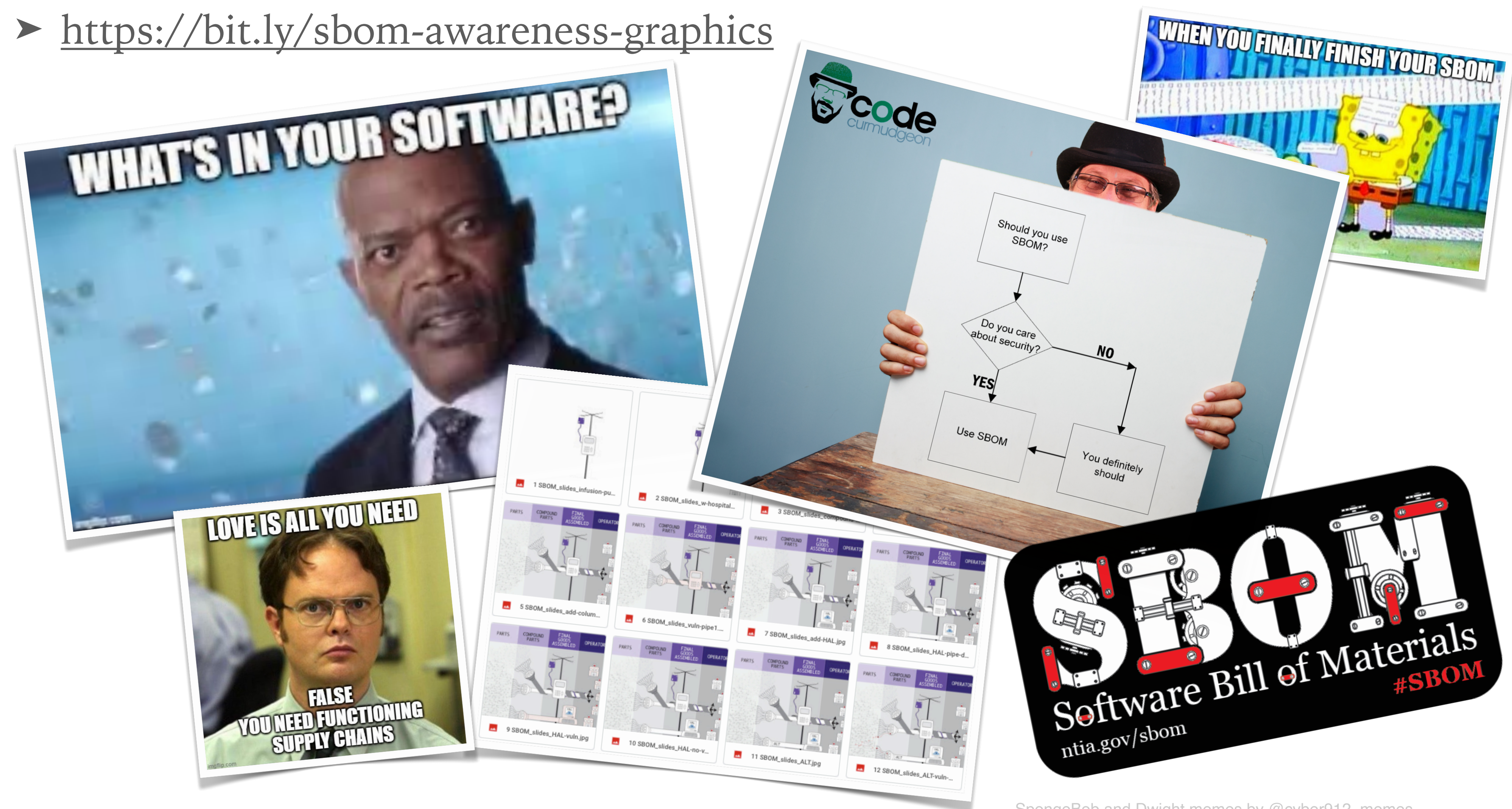
Table of Contents

Table of Contents	1
OVERVIEW	3
Q: What is an SBOM?	3
Q: Who should have an SBOM?	3
Q: Who uses an SBOM and for what?	3
BENEFITS	4
Q: What are the benefits of an SBOM?	4
Q: How does an SBOM help in the event of a cyberattack?	4
Q: In addition to vulnerability management, how can SBOMs help me?	5
Q: How have bills of material and supply chain transparency been helpful elsewhere?	5
COMMON MISCONCEPTIONS & CONCERNS	5
Q: Won't SBOMs be a "roadmap to the attacker"?	5
Q: Does an SBOM require source code disclosure?	6
Q: Does a list of the software components I include expose my intellectual property?	6
Q: Does an SBOM increase my exposure to license violations?	6
Q: Does an SBOM enable patent or license "trolls"?	6
Q: Will SBOMs increase my licensing costs or licensing commitments?	7
CREATION	7
Q: Who creates and maintains an SBOM?	7
Q: What should be included in an SBOM?	7
Q: What data formats exist for conveying SBOM data?	7
Q: Are there tools that translate between SBOM formats?	8
Q: When is an SBOM created, changed, or maintained?	8
Q: Some software components are made up of other software components themselves. Can an SBOM show that hierarchy?	8
Q: How deep in the dependency graph should an SBOM enumerate?	9
DISTRIBUTION & SHARING	9
Q: If I make an SBOM, do I have to make it public?	9
Q: How will SBOM data be shared?	9
ROLE SPECIFIC	10
Q: How can SBOMs be leveraged as a Purchaser?	10



# GRAPHICS REPOSITORY\*

- <https://bit.ly/sbom-awareness-graphics>



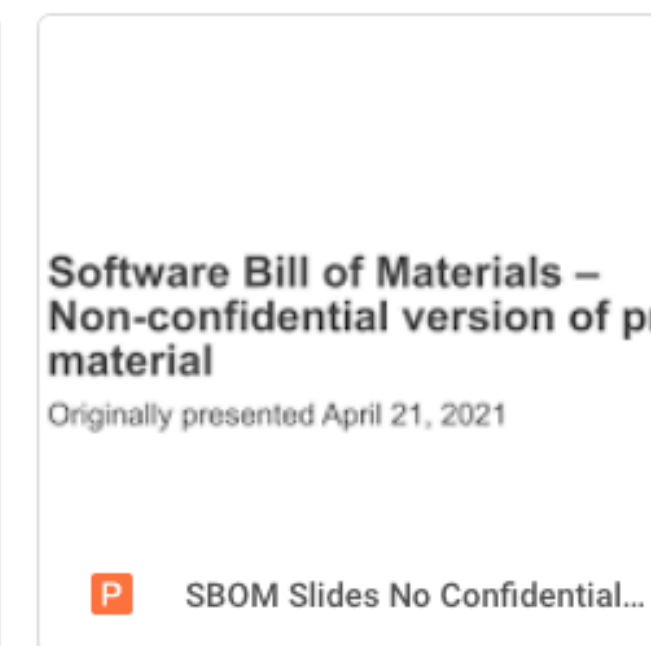
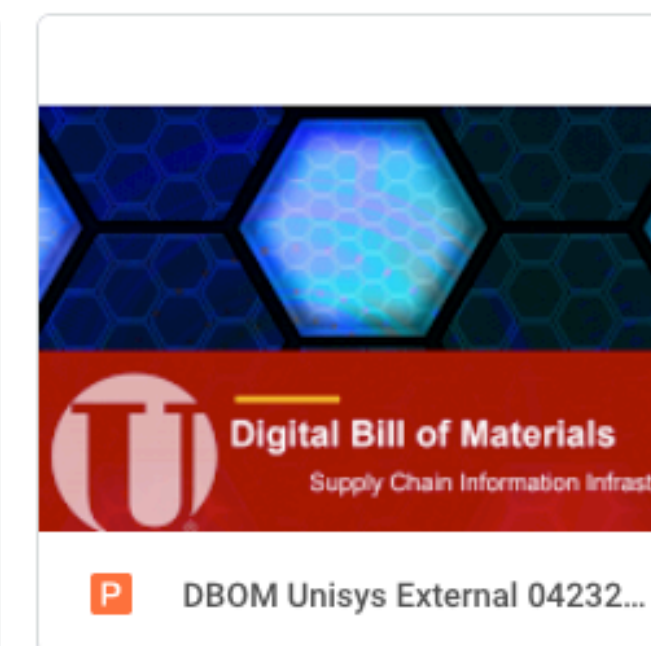
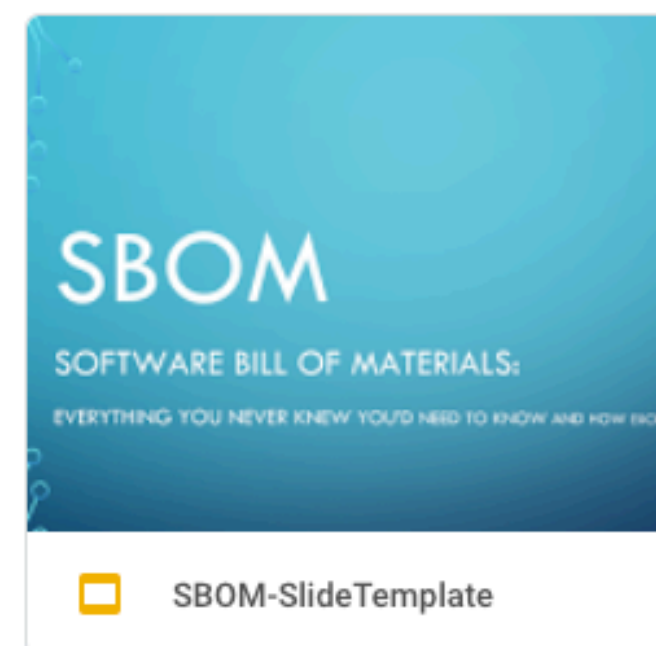
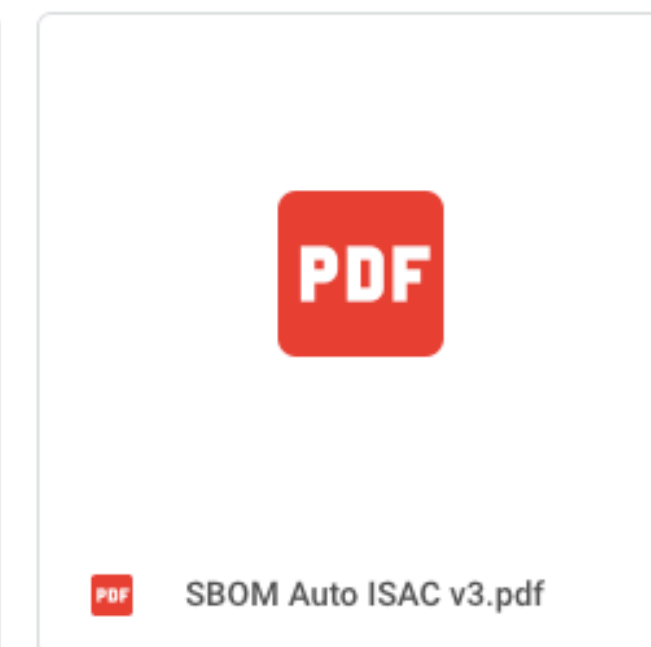
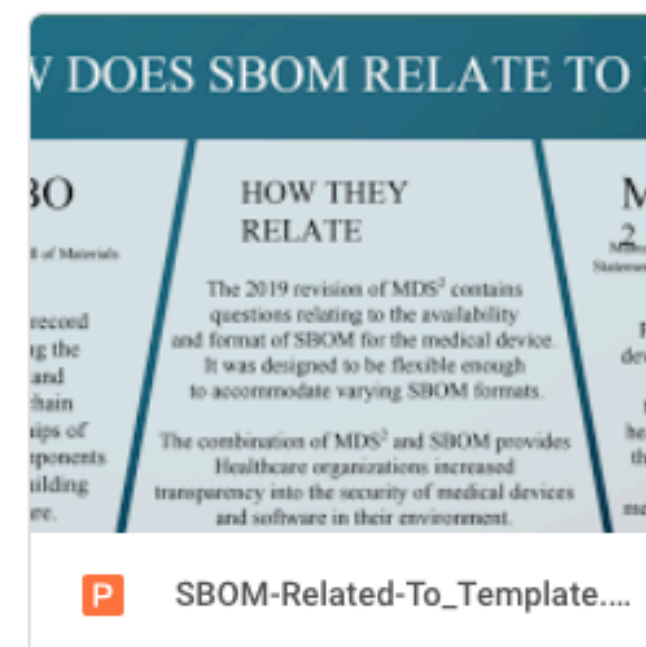
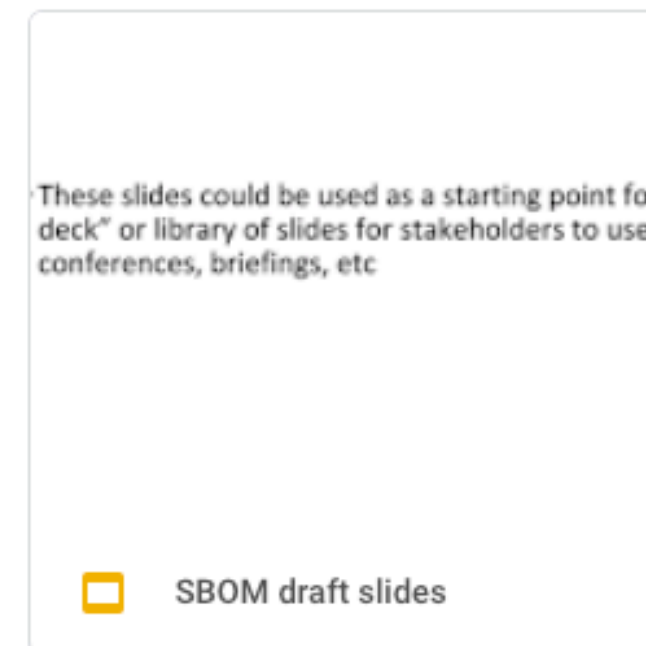
\* Now with memes!

SpongeBob and Dwight memes by @cyber912\_memes  
Flowchart by @CodeCurmudgeon  
SLJ meme via @AlyssaM\_InfoSec



# SBOM SLIDE REPOSITORY

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

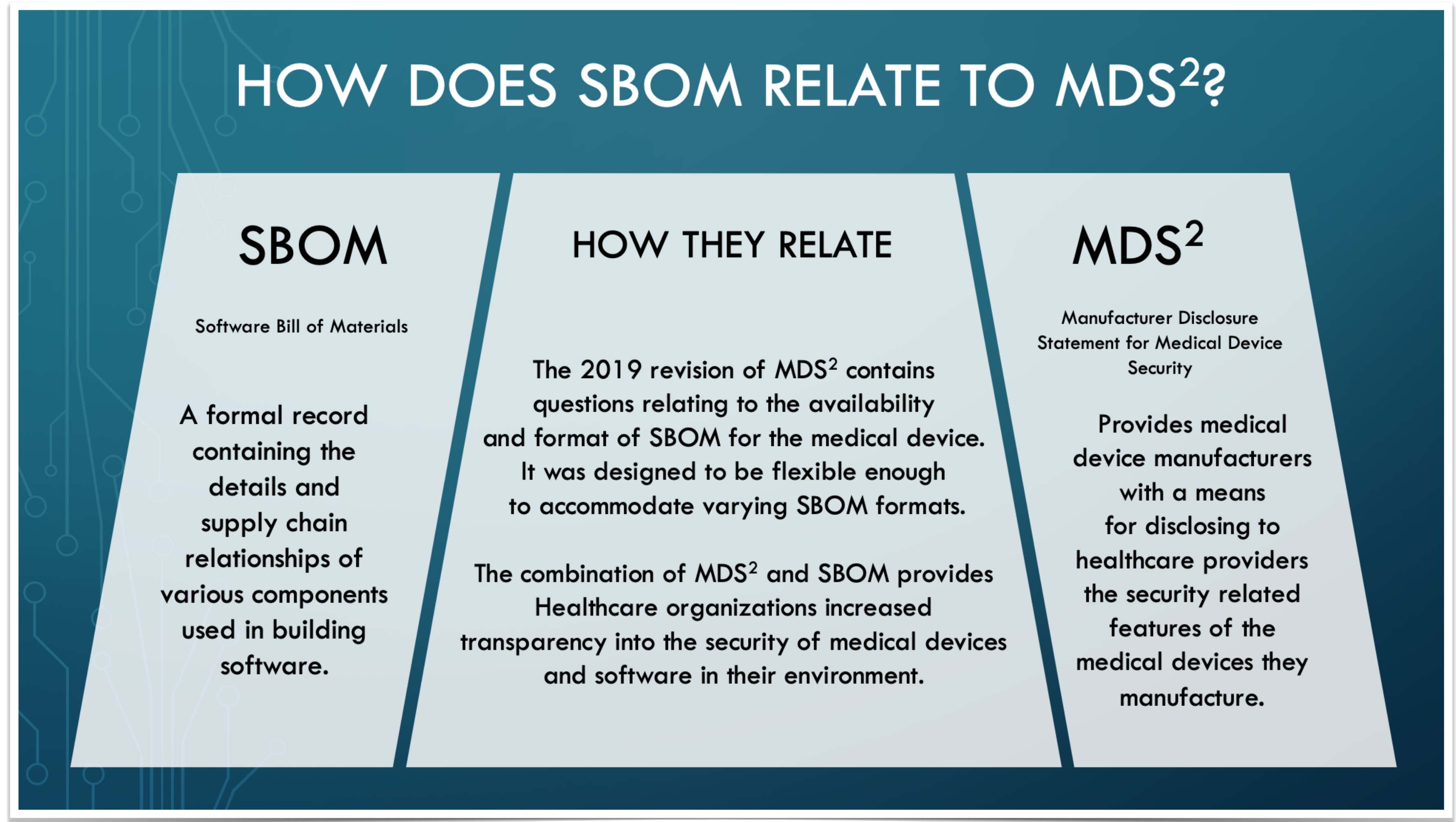




# “HOW DOES SBOM RELATE TO...”

---

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







# ONGOING EFFORTS

---

- FAQ
  - Cost and Investment-related questions
- SBOM Perspectives
  - Asking for SBOMs
  - Supplying SBOMs
- Virtual Engagement Opportunities
  - Webinars, Podcasts, Virtual Conferences, Other
  - RSA Conference 2021: SBOM & Supply Chain Content
- Business Two-Pager being reworked into two documents:
  - Business Customer
  - Producer
- SBOM Related Efforts & SBOM-Adjacent Topics Spreadsheet
- Questions for your Suppliers
- Proof of Concept Conversations & Expansions
- Knowledge Base - Searchable, cross-linked Phase I Documents



# ADDITIONAL SBOM RESOURCES

---

- SBOM News:

- <https://bit.ly/sbom-awareness-news>

- SBOM Recordings, Presentations, and Podcasts:

- <https://bit.ly/sbom-awareness-recordings>

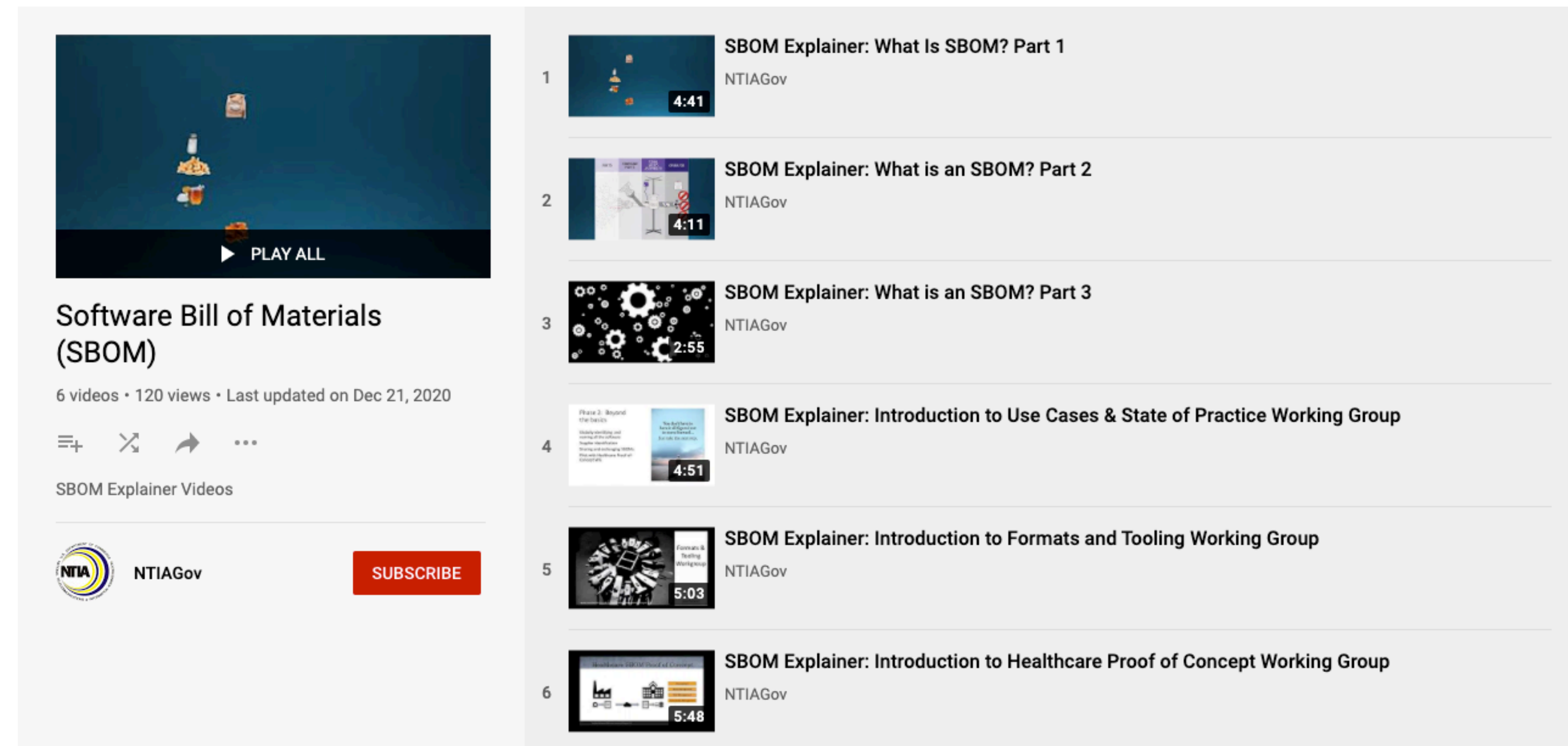
- If you have a news story, recording, presentation, or podcast to add to the lists, please submit a comment in the Google Doc.



# 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](https://ntia.gov/sbom)



# 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



# 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 details and/or forward an existing calendar invitation to:
  - [sbom.calendar@gmail.com](mailto:sbom.calendar@gmail.com)
  - Include:
    - Event Title, Time, & Time Zone
    - Location & Cost, if applicable
    - Description
    - Link to registration or more information



# 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

---

- Use Case Repository
- 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

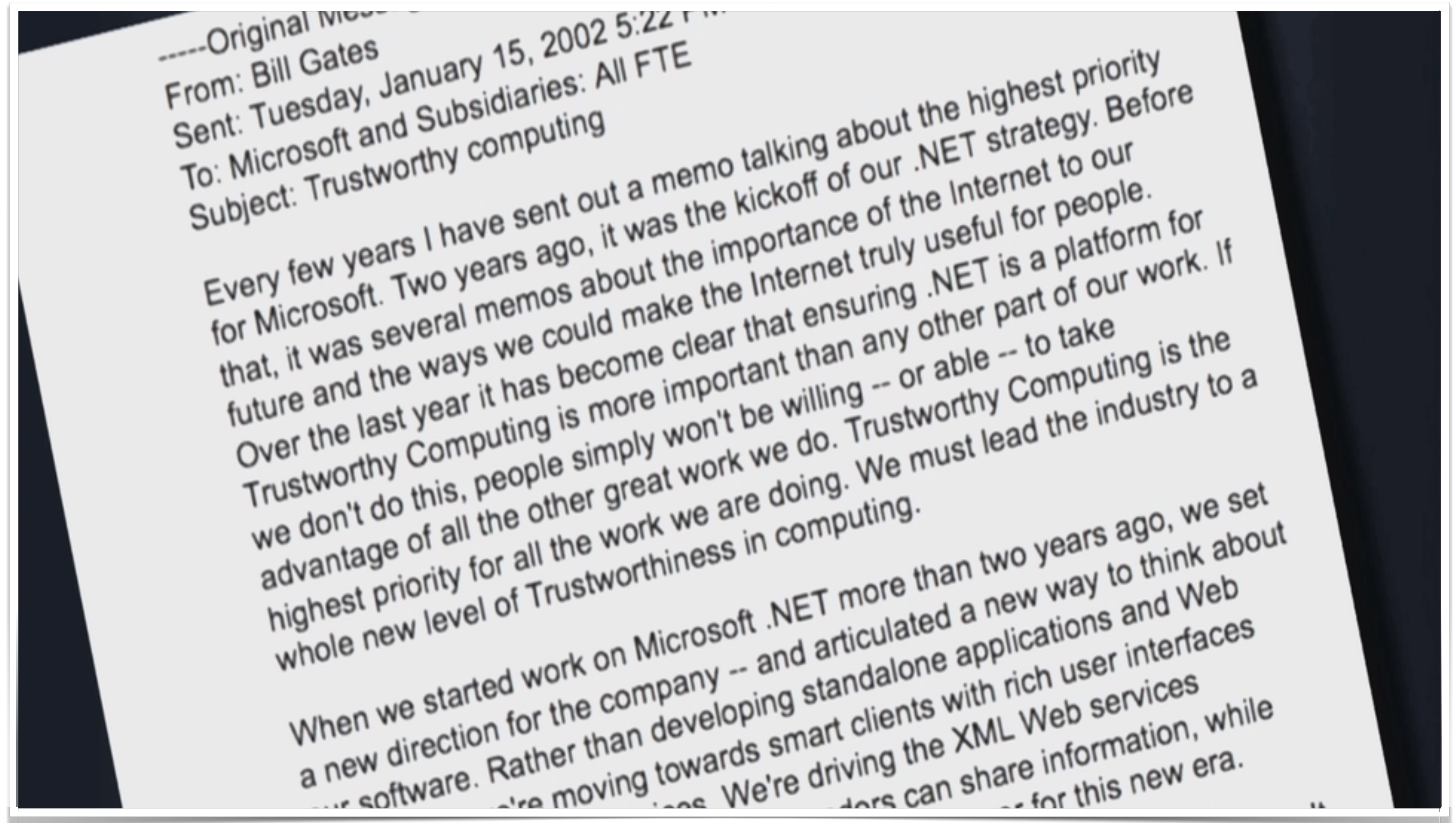
---

- Use Case Repository
- 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



# TRUST & TRUSTWORTHINESS

---





TRANSPARENCY IS COMING

Generated by Font-Generator.com

[iamthecavalry.org](http://iamthecavalry.org)

I AM THE  
Cavalry





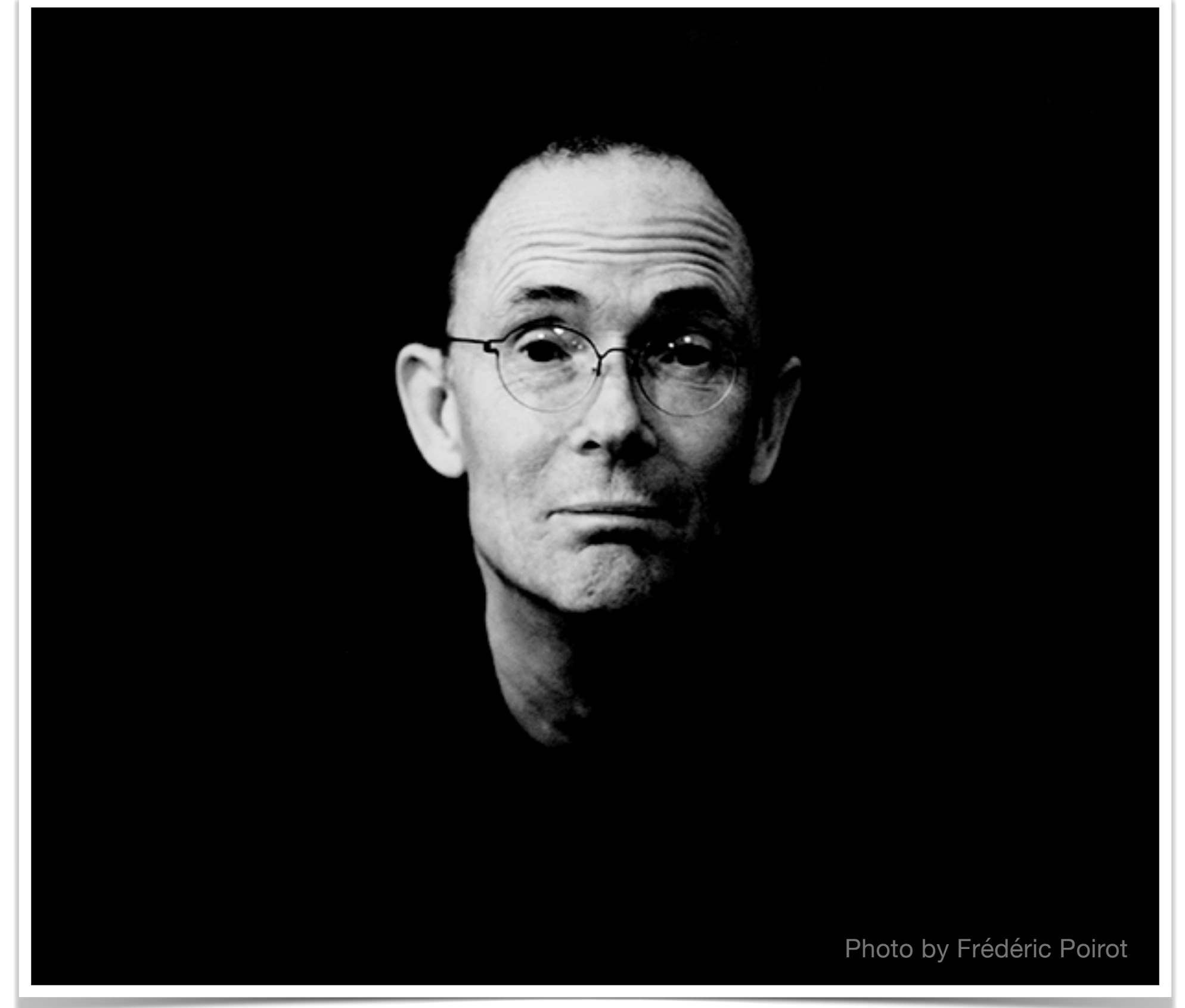


# SBOM IS HERE

---

*“The future is already here —  
it’s just not very evenly  
distributed.”*

*— William Gibson*





# CRITICAL MASS

MARKETPLACE  
TECH

FEB 23,  
2021

SUPPORT MARKETPLACE  
TECH

You need to have secure ingredients to have a secure product

Cyberattacks like the SolarWinds hack are increasingly common because it's hard for companies and governments to verify the security of every company they work with.

▶ LISTEN NOW

<

</>

↓

TAG Cyber

Security Annual

2ND QUARTER 2021

MARKET OUTLOOK & INDUSTRY INSIGHTS

OP-ED

THE TIME HAS ARRIVED FOR SOFTWARE BILL OF MATERIALS

EDWARD AMOROSO

The benefits of Software Bill of Materials (SBOM) are outlined in the context of standards such as SWID and SPDX from NTIA, ISO, CycloneDX, and the Linux Foundation. To address challenges in implementation, a maturity model is proposed here to enable use of SBOM in practical software procurement settings.

INTRODUCTION

Alan Friedman from the US Department of Commerce illustrates a bill of materials this way: "Twinkie buyers often assume the product to be vegan," he says, "but a glance at the list of ingredients reveals use of beef fat." Yeesh. Now - after the inevitable joke that even hungry rats sniff-and-pass at Twinkies, one must admit that if junk food makers can be forced to share their ingredients, then so should software providers.

Stated simply - the time has arrived for a software bill of materials to accompany any code being delivered into a consequential setting, which means pretty much all software. Blessed with a pronounceable acronym - SBOM, the concept seems to polarize observers into two camps: The true believing camp and the no-way-you-can-do-it camp. Below, we examine both arguments - and hopefully convince you that the title of this article is correct.

Specifically, we cover the major arguments for and against SBOM, including a summary of ongoing contributions from several major organizations including NTIA, ISO, CycloneDX, and the Linux Foundation. We also propose here an SBOM maturity scale that allows software providers to provide guidance on the level of assurance that exists in their SBOM. Such claims should assist buyers in their software procurement activity.

CASE FOR SBOM

The conceptual notion of a software bill of materials is simple. Buyers of software would demand a nested inventory of the components used to develop the product or system. The resulting transparency would help buyers establish higher levels of assurance for software

2021 SECURITY ANNUAL - 2ND QUARTER

TAG CYBER

npj | Digital Medicine

www.nature.com/npjdigitalmed

PERSPECTIVE

OPEN

Check for updates

Building resilient medical technology supply chains with a software bill of materials

Seth Carmody<sup>1,2</sup>, Andrea Coravos<sup>3,4,5</sup>, Ginny Fahs<sup>7,8</sup>, Audra Hatch<sup>8,9</sup>, Janine Medina<sup>5,6,8,10</sup>, Beau Woods<sup>5,8,11</sup> and Joshua Corman<sup>6,8,12,13</sup>

PRESS RELEASE

IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain

THE HILL

The US must adopt Software Bill of Materials to thwart cyberattacks

BY CHARLES CLANCY & RICK LEDGETT, OPINION CONTRIBUTORS — 03/15/21 09:00 AM EDT  
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

39



# POST-SBOM ACCELERATION

---

## Ingredients

- Inventory
- Parts
- Lists
- 1..n Suppliers
- BoM (Bill of Materials)

## Known Vulnerabilities

- CVEs ++
- *Potentially* exploitable
- Not “Attack Surface”

## Exploitable Vulnerabilities

- Attack Surface
- Code Flow
- Other mitigations
  
- Direct Exploitation
- Chained attacks
- Deserialization





# COMMUNITY ASK

---

- How you can help Awareness & Adoption:
  - We are seeking **new participants** and **project leads** for ongoing efforts
  - Provide feedback on SBOM Related Efforts document
  - 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](mailto:ntia-sbom-practices@cert.org)






**THANK YOU!**

---





# Q & A

---

