Survey of SBOM Usage in Key Software Projects

Survey Flow

Standard: Consent (2 Questions)
Block: Identification (2 Questions)
Standard: All Shared (5 Questions)

Branch: New Branch
If
If How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... We produce SBOMs for our software Is Selected
Or How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... We use or analyze the SBOMs of other projects (including our dependencies) Is Selected
Or How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... I am familiar with SBOMs, but we do not use them in our project(s) Is Selected

Standard: Familiar Shared (10 Questions)

Branch: New Branch
If
If How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... I am familiar with SBOMs, but we do not use them in our project(s) Is Selected
Or How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... I am unfamiliar with SBOMs Is Selected

Standard: Non-SBOM-User Shared (familiar or unfamiliar) (2 Questions)

Branch: New Branch
If
If How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... We produce SBOMs for our software Is Selected

Standard: SBOM Producers (8 Questions)

Branch: New Branch
If
If Select all statements that apply to your project(s): We produce SBOMs internally to help manage our project Is Selected

Standard: Internal Producer (2 Questions)

Branch: New Branch
If
If Select all statements that apply to your project(s): We produce SBOMs for the purpose of providing them to downstream components (dependents) Is Selected

Standard: External Producer (1 Question)

Branch: New Branch

If

If How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... I am unfamiliar with SBOMs Is Selected

Standard: Unfamiliar (0 Questions)

Branch: New Branch

If

If How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... We use or analyze the SBOMs of other projects (including our dependencies) Is Selected

Standard: SBOM Consumers (7 Questions)

Branch: New Branch

If

If How are SBOMs (Software Bill of Materials) used in your project(s)? Please select all options tha... I am familiar with SBOMs, but we do not use them in our project(s) Is Selected

Standard: Familiar Non-Users (3 Questions)

Standard: OBOMs (4 Questions)
Standard: Demographics (12 Questions)

Page Break

Start of Block: Consent

CF1 Investigating the state of practice in software supply chain management RESEARCH GOAL AND PROCEDURE
The purpose of this study is to investigate issues, needs, and opportunities related to software supply chain management.
The (open source) software supply chain is the set of processes, components, and tools used to develop, build, and publish a software product (a system, library, tool, etc.). Software vendors often create software products by assembling open source software components (aka dependencies) developed by third-party developers or organizations. Common tasks involved in supply chain management include maintaining license compliance among components, managing and screening dependencies, and mitigating security threats introduced in software dependencies.
If you decide to participate, you will take a brief survey/questionnaire. The survey will last about 15-20 minutes during which time you will be asked questions regarding your familiarity and experience with several topics related to the open source supply chain, **including dependency management, Software Bills of Materials (SBOMs), security issues related to the supply chain, and open source licensing.**
We may contact you by email to invite you to participate in a follow-up interview.
RISKS AND BENEFITS There are no foreseeable risks for participating in this research. There are no benefits to you as a participant other than to further research in software engineering and the open source software supply chain. PARTICIPATION You must be at least 18 years old to participate. Your participation is voluntary, and you may withdraw from the study at any time and for any reason. If you decide not to participate or if you withdraw from the study, there is no penalty or loss of benefits to which you are otherwise entitled. There are no costs to you or any other party. Your decision whether or not to participate will not prejudice your future relations with [Organization]. If you decide to participate, you will be entered into a drawing for a $50 USD Amazon gift card upon completion of this survey. We will randomly choose respondents and give out 10 gift cards. CONFIDENTIALITY The data collected by this study will be confidential, including your responses. Any information obtained in connection with this study that can be identified with you will remain confidential and disclosed only with your permission. You will be assigned a code number to protect your identity and all data will be kept secure. If you give us your permission by signing this document, we plan to disclose the results of the questionnaire in any publication resulting from this study. The disclosed results will not be personally identifiable (if needed, they will be anonymized). The de-identified data could be used for future research without additional consent from participants. The Institutional Review Board (IRB) and [committee] that monitor research on human subjects may inspect study records during internal auditing procedures and are required to keep all information confidential. CONTACT This research is being conducted by [Anonymous Author(s)] from [Organization].
Questions regarding the rights of research subjects may be directed to [redacted].
Such committee has reviewed and approved the present research

([protocol]) CONSENT You are welcome to print this page to keep a copy of this form. Do you consent to participate in this survey?

JS

CF2 **YOU ARE MAKING A DECISION WHETHER OR NOT TO PARTICIPATE.**

IF YOU WANT TO PARTICIPATE, PLEASE ENTER YOUR NAME IN THE TEXT FIELD BELOW, AND START THE SURVEY.

Please enter your name.

____

End of Block: Consent

Start of Block: Identification

Q61 The NTIA defines a **Software Bill of Materials (SBOM)** as follows:

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. 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.

*

ID1 How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that pertain to the projects you contribute to:

□ We create SBOMs for the software that we produce (1)

□ We use or analyze the SBOMs of other projects (including our dependencies) (2)

□ I am familiar with SBOMs, but we do not use them in our projects (3)

□ [✓ I am unfamiliar with SBOMs (4)]

□ Other (please specify) (5) ____

End of Block: Identification

Start of Block: All Shared

Display This Question:

If How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that... != I am unfamiliar with SBOMs

Q24 Indicate your agreement with the following statement: “Other well known / well established open source projects are producing SBOMs"

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Display This Question:

If How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that... != I am unfamiliar with SBOMs

Q54 Indicate your agreement with the following statement: “Other well known / well established open source projects are consuming SBOMs"

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Q55 As an open source project, do you publish a list of your project's dependencies?

○ Yes, my projects are required to publish their dependencies (5)

○ Yes, my projects voluntarily publish their dependencies (6)

○ No, my projects do not publish their dependencies (7)

○ I don't know (8)

Display This Question:

If As an open source project, do you publish a list of your project's dependencies? = Yes, my projects are required to publish their dependencies

Or As an open source project, do you publish a list of your project's dependencies? = Yes, my projects voluntarily publish their dependencies

Q25 How do your projects obtain the list of dependencies? Are there any specific tools or techniques used to that end?

____

____

____

____

____

Display This Question:

If As an open source project, do you publish a list of your project's dependencies? = No, my projects do not publish their dependencies

Q81 Why do your projects not publish their dependencies?

____

____

____

____

____

End of Block: All Shared

Start of Block: Familiar Shared

Display This Question:

If How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that... = We create SBOMs for the software that we produce

Or How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that... = We use or analyze the SBOMs of other projects (including our dependencies)

*

P2 Which SBOM formats/standards do your projects use? Select all that apply.

□ SPDX (1)

□ CycloneDX (2)

□ SWID (3)

□ Other (Please Specify) (4) ____

Q10 Indicate your agreement with the following statement: “The use of SBOMs is critical in software development"

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Q13 Indicate your agreement with the following statement: “Current SBOM standards / specifications meet the needs of users and industry”

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Q11 Which of the following deficiencies have you or your projects encountered in current SBOM standards / specifications? Select all that apply.

□ Lack of support for AI/ML-based software (1)

□ Lack of support for some programming languages and/or ecosystems (2)

□ Lack of formal distribution and sharing recommendations (3)

□ Missing data fields (4)

□ Too many competing standards (5)

□ Incompatibilities between standards / specifications (6)

□ Difficulty in understanding standards / specifications (7)

□ Difficulty in reading or understanding created SBOMs (8)

□ Difficulty to verify that information in SBOMs is accurate (9)

□ Over-specification of standards (10)

□ Under-specification of standards (11)

□ Ambiguous or contradictory guidance (12)

□ Others (please specify) (13) ____

Q12 How can we address (some of) the selected deficiencies in SBOM standards / specifications?

____

____

____

Q14 Indicate your agreement with the following statement: “Current SBOM tool support meets the needs of users.”

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Q64 What are some issues that you or your projects have encountered in SBOM tooling (tools that generate/process SBOMs)?

Q15 How can we address current deficiencies in SBOM tooling? Select all that apply.

□ Create SBOM tools for different programming languages and/or ecosystems (1)

□ Create SBOM tools that are language/ecosystem agnostic (2)

□ Ensure that SBOM generators create higher-quality SBOMs (3)

□ Make SBOM tools simpler to use (4)

□ Create and adopt high-quality SBOM libraries (5)

□ Improve the SBOM standards / specifications (6)

□ Support organizations that support SBOMs (7)

□ Others (please specify) (8) ____

Display This Question:

If How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that... = We create SBOMs for the software that we produce

Or How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that... = We use or analyze the SBOMs of other projects (including our dependencies)

Q31 Do your projects have a process/method to verify whether SBOMs completely and correctly report all dependencies and their metadata?

○ Yes (1)

○ No (2)

Display This Question:

If Do your projects have a process/method to verify whether SBOMs completely and correctly report al... = Yes

Q34 What process/method do your projects have to verify whether SBOMs completely and correctly report all dependencies and their metadata?

____

____

____

____

____

End of Block: Familiar Shared

Start of Block: Non-SBOM-User Shared (familiar or unfamiliar)

Q17 What tools and/or techniques do you use for dependency management in your software projects?

____

____

____

____

____

Display This Question:

If How are SBOMs (Software Bill of Materials) used in your projects? Please select all options that... != I am unfamiliar with SBOMs

Q18 Why do you prefer these tools and/or techniques over other methods?

____

____

____

____

____

End of Block: Non-SBOM-User Shared (familiar or unfamiliar)

Start of Block: SBOM Producers

P1 Select all statements that apply to your projects:

□ We produce SBOMs internally to help manage our software projects (1)

□ We produce SBOMs for the purpose of providing them to projects that depend on my software (2)

Q2 At what point(s) in the software development process should SBOMs be generated? Select all that apply.

□ During project planning (1)

□ At the developer's discretion, from source code (2)

□ During each software build (3)

□ During each software deployment (4)

□ When publishing a major software release (5)

□ Others (please specify) (6) ____

□ ⊗I don't know (7)

✱

Q3 Why do your projects create SBOMs? Select all that apply.

□ To meet regulatory requirements (1)

□ To meet software licensing requirements (2)

□ To provide others with information about my project (3)

□ To monitor project dependencies (4)

□ To keep track of dependency vulnerabilities (5)

□ Because my project organization asks me to (6)

□ To make it easier to understand dependencies in complex projects (7)

□ To proactively identify replacements for components that reach end-of-life (8)

□ Others (please specify) (9)

____

□ ⊗I don't know (10)

Q19 What benefits have your projects observed from producing SBOMs? Select all that apply.

□ Increased workflow efficiency (1)

□ Better dependency management (2)

□ Increased understanding of how the systems in my organization work (3)

□ Satisfied client / consumer requirements (4)

□ Increased adoption of your software product(s) (5)

□ Maintaining license compliance (6)

□ Increased ability to locate and resolve security issues (7)

□ Better code reviews (8)

□ Others (please specify) (9) ____

Q5 What tools do your projects use to assist in the creation of SBOMs, if any?

____

____

____

____

____

Q6 Do your projects have any strategies for managing SBOM versions?

○ Yes (1)

○ No (2)

○ I don't know (3)

Display This Question:

If Do your projects have any strategies for managing SBOM versions? = Yes

Q7 What strategies do your projects have for managing SBOM versions? Are there any specific tools involved?

____

____

____

____

____

Q21 What issues have your projects encountered when producing SBOMs? Select all that apply.

□ Difficulties in keeping up with rapidly changing code bases (1)

□ Difficulties in understanding format specifications (2)

□ Lack of adequate tool support (3)

□ Interoperability issues between formats (4)

□ Produced SBOMs are of low quality (5)

□ Lack of support for different environments and languages (6)

□ Required information is unavailable (7)

□ Security risks introduced and/or propagated by incorrect SBOMs (8)

□ Conflicting legal requirements (9)

□ Difficulty in following standards to create SBOMs (10)

□ Underspecification of SBOM standards (11)

□ Slow or cumbersome SBOM generation process (12)

□ SBOM standards are not backwards compatible (13)

□ Generated SBOMs are too large (14)

□ Others (please specify) (15) ____

End of Block: SBOM Producers

Start of Block: Internal Producer

Display This Question:

If Select all statements that apply to your projects: = We produce SBOMs internally to help manage our software projects

And Select all statements that apply to your projects: = We produce SBOMs for the purpose of providing them to projects that depend on my software

Q82 Do your projects share their SBOMs externally?

○ Yes (1)

○ No (2)

Display This Question:

If Do your projects share their SBOMs externally? = No

Q83 Why are your projects' SBOMs not shared externally?

____

____

____

____

____

End of Block: Internal Producer

Start of Block: External Producer

Q5 How do your projects publish / distribute your created SBOMs? Select all that apply.

□ Located in repositories along with source code (1)

□ Downloadable from project website (2)

□ Stored with a trusted third party (3)

□ Available from the project developers upon request (4)

□ Attached to software binaries (5)

□ Others (please specify) (6) ____

End of Block: External Producer

Start of Block: Unfamiliar

Start of Block: SBOM Consumers

*

Q2 What do your projects use SBOMs for? Select all that apply.

□ To meet regulatory requirements (1)

□ To meet software licensing requirements (2)

□ To learn more about other projects (3)

□ To monitor my project's dependencies (4)

□ To keep track of dependency vulnerabilities (5)

□ Because my organization asks me to (6)

□ To make it easier to understand dependencies in complex projects (7)

□ To proactively identify replacements for components that reach end-of-life (8)

□ Others (please specify) (9) ____

□ ⊗I don't know (10)

Q20 Which of the following benefits have your projects observed from using SBOMs? Select all that apply.

□ Improved Vulnerability Detection (1)

□ Improved Dependency Tracking (2)

□ Improved License Compliance (3)

□ Others (please specify) (4) ____

Q4 How often do your projects use SBOMs during software development?

○ Very rarely (1)

○ Once per month (2)

○ Once per week (3)

○ Every day (4)

○ Never (5)

○ Other (please specify) (6) ____

Q5 Do your projects process or analyze the SBOMs of their software dependencies (if available)?

○ Yes (1)

○ No (2)

○ I don’t know (3)

Display This Question:

If Do your projects process or analyze the SBOMs of their software dependencies (if available)? = Yes

Q6 How do your projects process or analyze the SBOMs of their dependencies? What tools, if any, are involved in the process?

____

____

____

____

____

Q22 Which of the following issues have your projects encountered in using SBOMs? Select all that apply.

- □ Defects in SBOM tools (1)
- □ Issues arising from different SBOM standards / specifications (2)
- □ Problems with obtaining and handling up-to-date vulnerability data (3)
- □ Low-Quality SBOMs (4)
- □ Difficulty in comprehending SBOMs or SBOM standards / specifications (5)
- □ Difficulty in verifying the accuracy of generated SBOMs (6)
- □ Missing features in SBOM tools (7)
- □ Lack of SBOM tool support (8)
- □ Inconsistency across SBOM tools and standards / specifications (9)
- □ Difficulties keeping SBOMs and software up to date (10)
- □ Others (please specify) (11) ____

Q16 How do you prefer the SBOMs of other projects to be shared with you? Rank by preference (by dragging the options).

_______ Stored with a trusted third party (1)
_______ Located in repositories along with the source code (2)
_______ Downloadable from project website (3)
_______ Available from the project developers upon request (4)
_______ Attached to software binaries (5)
_______ Other(s) (6)

End of Block: SBOM Consumers

Start of Block: Familiar Non-Users

Q9 Which of the following SBOM formats have you heard of?

□ SPDX (1)

□ CycloneDX (2)

□ SWID (3)

□ Others (Please Specify) (4) ____

Q56 Have you used SBOMs in the past?

○ Yes (1)

○ No (2)

Q23 Why do you not currently use SBOMs?

____

____

____

____

____

End of Block: Familiar Non-Users

Start of Block: OBOMs

Q37 Are you familiar with Operations Bills of Materials (OBOMs)?

○ No (1)

○ Somewhat (2)

○ Yes (3)

Skip To: End of Block If Are you familiar with Operations Bills of Materials (OBOMs)? = No

Q38 How would you describe OBOMs? What are their key features?

____

____

____

____

____

Q40 Do you use OBOMs in your projects?

○ Yes (1)

○ No (2)

○ I Don't Know (3)

Q39 What should OBOMs be used for?

____

____

____

____

____

End of Block: OBOMs

Start of Block: Demographics

*

Q1 How many years of experience in software development do you have?

____

Q2 How would you describe your primary role?

○ Programmer (1)

○ Tester (2)

○ Project Lead (3)

○ Project Manager (4)

○ IT Manager (5)

○ DevOps Engineer (6)

○ Consultant (7)

○ Educator (8)

○ Other (please specify): (9) ____

Q3 What is your highest level of education?

○ Did not graduate from high school (1)

○ High School (2)

○ Some college (3)

○ Bachelor's Degree (4)

○ Master's Degree (5)

○ Doctoral Degree (6)

○ Other (please specify) (7) ____

*

Q4 Which programming languages have you most used in past projects? Select all that apply.

□ Python (1)

□ Java (2)

□ C / C++ (3)

□ Javascript (4)

□ C# (5)

□ Others (please specify): (6) ____

*

Q5 What types of systems have you developed?

□ Operating systems (1)

□ Web applications (2)

□ Mobile applications (3)

□ Desktop applications (4)

□ Middleware (5)

□ Databases (6)

□ Development tools (compilers, prog. languages, etc.) (7)

□ Others (please specify) (8) ____

Q7 For which domains (e.g., banking or healthcare) have you developed applications / systems?

____

Q6 Do you primarily work on open source or closed source projects?

○ Open source only (1)

○ Closed source only (2)

○ Both open source and closed source (3)

Q8 Do you have a background in computer security? Formal (college classes, degree, certification) or informal (self-learning or other training)?

○ Yes, formal (1)

○ Yes, informal (2)

○ No (3)

Q9 Do you have a background in software licensing? Formal (college classes, degree, certification) or informal (self-learning or other training)?

○ Yes, formal (1)

○ Yes, informal (2)

○ No (3)

Q10 How often did you release or help release a new major version of an application / software over the past two years?

Please give your best estimate; if you develop more than one software / application, please answer based on the most frequently updated software / application.

○ Never (1)

○ Annually (2)

○ Quarterly (3)

○ Monthly (4)

○ More frequently (5)

Q11 Which country / countries are you and / or your organization based in?

____

*

Q12 Please enter your email address. This will be used to contact you for compensation. If we are interested in your responses, we may contact you for a follow-up interview, if you are willing.

____

End of Block: Demographics