CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENGY, DHS

PUBLIC LISTENING SESSION ON ADVANCING SBOM TECHNOLOGY, PROCESSES, AND PRACTICES

TOOLING AND IMPLEMENTATION SESSIONS SUMMARY

Software Bill of Materials (SBOM) implementation will be driven by a range of accessible and constructive tools and enabling applications, both open source and commercial in nature. While there has been tremendous progress on the SBOM generation side of tooling, SBOM consumption is still needed. It is important to encourage interoperability among SBOM generation and consumption tools, allowing for healthy competition regarding quality while making sure tools can work together. Over the course of two weeks, CISA met with participants and facilitated SBOM discussions so that participants driving the outcomes, including specific issues of focus and next steps. CISA prepared these summary points from the participants' individual input.

Possible sub-topics

The following sub-topics for SBOM tooling and implementation were identified by participants:

- measuring trust in SBOM tooling
- interoperability
- tooling and data management strategies
- SBOM validation
- tool discovery
- differing hash values at different stages of SBOM creation
- SBOM consumption tools
- implementation details that may need to be added to current SBOM definition
- “over-confidence” in SBOM generation tools
- transitioning from manual to automatic SBOM creation
- data quality measurement
- tool categorization by purpose
- attestations and other data (e.g., signing, error/omissions, accuracy verification)
- SBOM composability (linking SBOMs together, linking to other data like VEX)
- code deployment (if installation changes dependencies, SBOM should reflect what is installed)
- runtime system SBOMs, and
- hash value generation.

Tool ecosystem coordination/collection

The following topics related to tooling ecosystem coordination/collection were noted by participants:

- neutral repository to house various tools
- common taxonomy growth (build off NTIA work)
- feedback from SBOM community on tooling effectiveness
- Plugfests (demonstrate how tools are used, focus on interoperability, generation, consumption)
- fostering SBOM consumption of SBOMs
- creation of tool categorization methodology.

Use Cases

Participants found it valuable to consider some centralized cross-stream use cases. Popular suggestions for use cases in this work stream include:

- automation
- procurement
- consumption
- detection of stale data (e.g., updated SBOM, versioning)
- detecting/defining transitive dependencies
- pre-install/deploy analysis
- third-party analysis distinction (OSS vs. licensed 3rd party components)
- SBOM integration with other security tools (e.g., asset management/vulnerability management)
- embedded providers
- merging multiple SBOMs, and
- successful interoperability between tools.

Interoperability

The following interoperability-based feedback was collected from participants:

- interoperability between vendors is a challenge
- value of Plugfests
- interoperability testing is important
- hash value generation
- guidance for validation downstream.

Other relevant issues

Other relevant issues to SBOM tooling and implementation identified include:

- SBOM sharing/exchanging

- SBOM lifecycle management
- SBOM posting/hosting
- depth of SBOMs, and
- software identity related complications.

Potential outcomes

The most popular participant feedback for potential outcomes of future work related to tooling and implementation include:

- a living catalog of SBOM tools
- tool clearinghouse
- fostering of open-source products (e.g., consumption)
- creation of an SBOM public data set, and
- creating a tool for automated SBOM generation for OSS projects.