CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENGY, DHS

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

SHARING AND EXCHANGING SESSIONS SUMMARY

Moving Software Bill of Materials (SBOMs) and related metadata across the software supply chain will require understanding of how to enable discovery and access, and ensuring solutions are interoperable. Over the course of two weeks, CISA met with participants and facilitated SBOM discussions with the intent of 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 topics for sharing and exchanging SBOMs identified include:

- sharing multiple SBOMs together
- sharing concerns with multiple technology domains
- diverse supply chain considerations
- identification for tracking purposes
- SBOM trust (e.g., signing, validation, verification)
- issues with software/SBOM decoupling
- SBOM visibility and access control policy considerations
- sharing portal scalability
- open interfaces/APIs
- secure sharing
- pain point tracking for current sharing methods
- contract considerations (e.g., limited release)
- software differences may necessitate multiple retrieval methods
- mapping different delivery mechanisms, and
- tool sharing transparency.

Existing solutions & related efforts

Participants identified the following existing solutions and related efforts:

- Digital Bill of Materials (DBOM)
- STIX/TAXII
- persistent uniform resource locators (PURLs)
- OASIS Posture Attribute Collection and Evaluation (PACE)
- Internet Engineering Task Force (IETF) Supply Chain Integrity , Transparency and Trust (SCITT), and
- Open Worldwide Application Security Project (OWASP).

Desirable features

Participants in the listening sessions identified the following desirable features:

- third-party SBOM generation
- discoverability
- access control (building on DRM)
- integrity and validation features (e.g., signatures and assurances)
- legacy software accommodations
- SBOM revocation/deprecation
- mapping to other software delivery mechanisms
- connection to coordinated vulnerability disclosure
- packaging SBOMs alongside containers or blob
- compatibility with other trust-related data, and
- methods to simultaneously update software and associated SBOMs.

Use Cases

Popular responses by participants in the listening sessions for potential use cases are:

- automation
- leveraging existing tools
- software distribution mechanisms (e.g., app store)
- vulnerability management/incident response, and
- considering SBOM revocation through versioning and/or deprecation.

Scoping

The listening sessions identified the following scoping considerations:

- building sharing solutions on other network engineering approaches
- SBOM location (i.e., ship SBOM versus keeping it online), and
- understanding the unique features of OT and other embedded systems.

Other relevant issues

Additional relevant issues to sharing and exchanging SBOMs identified by the listening session participants include:

- SBOM software identity
- SBOM signing
- SBOM completeness
- backporting and rebasing, and
- SBOM process and lifecycle maturity.

Potential outcomes

Participants in the listening sessions identified the following potential outcomes for future work on sharing and exchanging SBOMs:

- a sharing and exchanging pilot program
- an SBOM sharing and exchanging playbook, and
- the creation of an SBOM OSS public repository.