CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENGY, DHS

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

ON-RAMPS AND ADOPTION SESSIONS SUMMARY

Broader Software Bill of Materials (SBOM) adoption may require enabling resources to promote awareness and lower the costs and complexities of adoption to allow newer or less mature organizations provide, request, and use SBOMs to secure and understand their organization's risk. 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

Education and marketing were identified as categories for SBOM on-ramps and adoption sub-topics.

Within the education category, listening session participants suggested:

- discussing the making of SBOM educational materials (e.g., SBOM guide on how to get started)
- the internationalization of SBOM, and
- the creation of methods to measure SBOM adoption, especially among open-source software products.

For marketing sub-topics:

- tracking other SBOM-related efforts to promote collaboration
- SBOM audience identification
- building trust in SBOMs, and
- an ongoing enumeration of SBOM benefits.

The participants also pointed out the value of gathering data on upstream components that do not have SBOMs. Additionally, interoperability and adoption incentives creation were identified as popular challenges to consider as sub-topics.

Target audiences and applications

Both listening sessions provided input on the audience(s) the on-ramps and adoption group should target. The most popular responses were:

- developers (open and closed source)
- executives (e.g., CIO)
- people with entry-level understanding

- upstream third-party vendors, and
- international audiences.

The participants took into consideration those individuals who would have a great impact on industry adoption, expanding knowledge of the general public, and interfacing with those around the globe who may have similar or parallel initiatives.

Use Cases

Participants in the listening sessions suggested that this working group should coordinate all SBOM use cases that are created by different working groups to assist with marketing as well as avoiding substantive overlap. Popular suggestions for use cases in this work stream centered around

- how to drive SBOM educational efforts and
- how to increase SBOM generation among users.

Potential outcomes

Both sessions provided suggestions on what future group engagement might most effectively look like for SBOM on-ramps and adoption. These working group outcome suggestions generally fit within the following categories: best practices, community SBOM space creation, and education.

Popular suggestions for increasing SBOM best practices included:

- the creation of documents discussing sample SBOM contract language
- common SBOM blocker workarounds
- SBOMs creation and maintenance, and
- strategies and best practices concerning legacy devices.

Popular suggestions for creating an SBOM space included:

- the creation an SBOM informational website
- an SBOM news feed, an online SBOM encyclopedia
- a centralized place for SBOM tool review and sales pitches
- an organized way to reach out to international users for SBOM global perspectives, and
- the formation of an SBOM community location where users can ask questions and consult for implementation guidance.

Popular suggestions for increasing SBOM visibility through education included:

- the creation of a video describing SBOM and its benefits

- focusing on educating upstream software providers
- the making of an SBOM-related regulatory summary, and
- having discussions on the marketing and communications surrounding SBOMs.

Properly educating the public and SBOM community may entail reaching out to SBOM stakeholders to solicit feedback on how the adoption process is faring.