This document is scheduled to be published in the Federal Register on 06/01/2022 and available online at **federalregister.gov/d/2022-11733**, and on **govinfo.gov**

9110-9P-P

DEPARTMENT OF HOMELAND SECURITY

Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices

AGENCY: Cybersecurity and Infrastructure Security Agency, DHS.

ACTION: Announcement of public listening sessions.

SUMMARY: The Cybersecurity and Infrastructure Security Agency will facilitate a series of public listening sessions to build on existing community-led work around Software Bill of Materials ("SBOM") on specific SBOM topics.

DATES: Two listening sessions will be held for each open topic specified in Section II of the SUPPLEMENTARY INFORMATION caption as follows:

1. **Topic 1, Session 1**: July 12, 2022 from 9:30 a.m. to 11 a.m., Eastern Daylight Time.
2. **Topic 1**, **Session 2**: July 20, 2022 from 3:00 p.m. to 4:30 p.m., Eastern Daylight Time.
3. **Topic 2, Session 1:** July 12, 2022 from 3:00 p.m. to 4:30 p.m., Eastern Daylight Time.
4. **Topic 2 Session 2:** July 14, 2022 from 9:30 a.m. to 11 a.m., Eastern Daylight Time.
5. **Topic 3, Session 1:** July 13, 2022 from 3:00 p.m. to 4:30 p.m., Eastern Daylight Time.
6. **Topic 3, Session 2:** July 21, 2022 from 9:30 a.m. to 11 a.m., Eastern Daylight Time.
7. **Topic 4, Session 1:** July 13, 2022 from 9:30 a.m. to 11 a.m., Eastern Daylight Time.

8. **Topic 4, Session 2:** July 14, 2022 from 3:00 p.m. to 4:30 p.m., Eastern Daylight Time.

ADDRESSES: The listening sessions will be held virtually, with connection information and dial-in information available at https://www.cisa.gov/SBOM.

FOR FURTHER INFORMATION CONTACT: Justin Murphy, Phone: (202) 961-4350, Email: justin.murphy@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: A Software Bill of Materials ("SBOM") has been identified by the cybersecurity community as a key aspect of modern cybersecurity, including software security and supply chain security. E.O. 14028 declares that "the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."[1] SBOMs play a key role in providing this transparency.

E.O. 14028 defines SBOM as "a formal record containing the details and supply chain relationships of various components used in building software."[2] The E.O. further notes that "[s]oftware developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product."[3] Transparency from SBOMs aids multiple parties across the software lifecycle, including software developers, purchasers, and operators.[4] Recognizing the importance of SBOMs in transparency and security, and that SBOM evolution and refinement should come from the community to maximize efficacy, the Cybersecurity and Infrastructure Security Agency (CISA) is facilitating listening sessions around SBOM, which are intended to advance the software and security communities'

---

[1] E.O. 14028, Improving the Nation's Cybersecurity, 1, 86 FR 26633 (May 17, 2021).
[2] *Id.* at 10(j), 86 FR 26633 at 26646 (May 17, 2021).
[3] Ibid
[4] Ibid

understanding of SBOM creation, use, and implementation across the broader technology ecosystem.

I. SBOM Background

The idea of a software bill of materials is not novel.[5] It has been discussed and explored in the software industry for many years, building on innovation from industrial and supply chain work.[6] Academics identified the potential value of a "software bill of materials" as far back as 1995,[7] and tracking use of third-party code has been identified as a longstanding software best practice.[8]

Still, SBOM generation and sharing across the software supply chain was not seen as a commonly accepted practice in modern software. In 2018, the National Telecommunication and Information Administration (NTIA) convened the first "multistakeholder process" to "promot[e] software component transparency."[9] Over the subsequent three years, this stakeholder community developed guidance to help foster the idea of SBOM, including high level overviews, initial advice on implementation, and technical resources.[10] When the NTIA-initiated multistakeholder process concluded,

---

[5] A brief summary of the history of a software bill of materials can be found in Carmody, S., Coravos, A., Fahs, G. et al. Building resilient medical technology supply chains with a software bill of materials. npj Digit. Med. 4, 34 (2021). https://doi.org/10.1038/s41746-021-00403-w

[6] See "Toyota Supply Chain Management: A Strategic Approach to Toyota's Renowned System" by Ananth V. Iyer, Sridhar Seshadri, and Roy Vasher – a work about Edwards Deming's Supply Chain Management https://books.google.com/books/about/Toyota_Supply_Chain_Management_A_Strateg.html?id=JY5wqdelrg8C

[7] Leblang D.B., Levine P.H., Software configuration management: Why is it needed and what should it do? In: Estublier J. (eds) Software Configuration Management Lecture Notes in Computer Science, vol. 1005, Springer, Berlin, Heidelberg (1995).

[8] The Software Assurance Forum for Excellence in Code (SAFECode), an industry consortium, has released a report on third party components that cites a range of standards. *Managing Security Risks Inherent in the Use of Third-party Components,* SAFECode (May 2017), *available at https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf.*

[9] National Telecommunications and Information Administration (NTIA), Notice of Open Meeting, 83 FR. 26434 (June 7, 2018).

[10] Ntia.gov/SBOM.

NTIA noted that "what was an obscure idea became a key part of the global agenda around securing software supply chains."[11]

However, CISA believes that the concept of SBOM and its implementation need further refinement. Work to help scale and operationalize SBOM implementation should continue to come from a broad-based community effort, rather than be dictated by any specific entity. To support such a community effort to advance SBOM technologies, processes, and practices, CISA will facilitate a series of listening sessions.

II. Topics for CISA Listening Sessions

The list below represents open topics in the field of SBOM and related cybersecurity topics on which CISA intends to facilitate a series of listening sessions. This is not an exhaustive set of open topics identified by the community at large, but represents a set of open topics identified as being priorities by the community. Solutions related to these topics that reflect the diverse needs of the software community will help advance forward progress towards greater software transparency and a more secure ecosystem.

Topic 1: Cloud and online applications – Much existing discussion around SBOM, particularly around SBOM use cases, has focused on on-premise software. Cloud and Software-as-a-Service (SaaS)-based software comprises a large and growing segment of the software ecosystem. Potential sub-topics may include: How should the community think about SBOM in the context of online applications and modern infrastructure? How can the community integrate SBOM work into emerging cloud-native opportunities?

Topic 2: Sharing and Exchanging SBOMs – Moving SBOMs and related metadata across the software supply chain will require understanding how to enable discovery and access. Potential sub-topics may include: How can suppliers and

[11] NTIA, *Marking the Conclusion of NTIA's SBOM Process* (Feb. 9, 2022), https://www.ntia.doc.gov/blog/2022/marking-conclusion-ntia-s-sbom-process.

consumers of SBOMs share this data at scale? What can the community do to promote interoperability of potential solutions?

Topic 3: Tools and Implementation – SBOM implementation will be driven by a range of accessible and constructive tools and enabling applications, both open source and commercial in nature. Potential sub-topics may include: How can the community promote the SBOM tooling ecosystem? What is needed to drive and test interoperability and harmonization?

Topic 4: On-ramps and Adoption – Broader SBOM adoption may require enabling resources to promote awareness and lower the costs and complexities of adoption. Potential sub-topics may include: What can the community do to make it easier and cheaper to generate and use SBOM data? How can the community promote this concept?

III. Process for CISA-Facilitated SBOM Community Collaboration

For each topic, CISA will facilitate interested community members in two open and transparent listening sessions. CISA will act as a facilitator and participants will drive the outcomes, including any specific issues of focus or next steps. CISA will not be seeking any group consensus advice and/or input from the listening sessions. If participants wish to schedule regular meetings or build communication channels, CISA will assist, to the extent possible, in facilitating effective and constructive collaboration. CISA will not request specific outputs from meeting participants, nor is it currently CISA's intent to use information shared during listening sessions to directly address or inform any Federal policy decision. The participants may identify any further resources the global software and security community could use for each identified topic.

Information shared during listening sessions may be made publicly available. For this reason, please do not include non-public or confidential information in your

responses to listening session topics, such as sensitive personal information or proprietary information.

Additional information regarding the listening sessions will be posted at https://cisa.gov/SBOM.

This notice is issued under the authority of 6 U.S.C. 652(c)(10)-(11), 659(c)(4), (9), (12).

Eric Goldstein,
Executive Assistant Director for Cybersecurity,
Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security.

[FR Doc. 2022-11733 Filed: 5/31/2022 8:45 am; Publication Date: 6/1/2022]