9110-9P-P

DEPARTMENT OF HOMELAND SECURITY

2023 CISA SBOM-a-Rama

AGENCY: Cybersecurity and Infrastructure Security Agency, DHS.

ACTION: Announcement of public event.

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

DATES: Wednesday June 14, 2023, from 12:00 p.m. to 6:00 p.m., Eastern Standard Time, or 9:00 a.m. to 3:00 p.m., Pacific Standard Time.

ADDRESSES: The event will be a hybrid event held at the USC Hotel, 3540 S Figueroa St, Los Angeles, CA 90007, as well as virtually, with connection information and dial-in information available at https://www.cisa.gov/SBOM. A form to allow individuals to register their interest in either in-person or virtual participation will be available at https://cisa.gov/SBOM. See the "Participation in the SBOM-a-Rama" section in the **SUPPLEMENTARY INFORMATION** caption for more information on how to participate.

FOR FURTHER INFORMATION CONTACT: Justin Murphy, (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. Executive Order 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.

[1] E.O. 14028, Improving the Nation's Cybersecurity, 1, 86 FR 26633 (May 17, 2021).

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 would be most effective coming from the community, the Cybersecurity and Infrastructure Security Agency (CISA) is facilitating a public event around SBOM, which is intended to advance the software and security communities' 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 industrial and supply chain innovations.[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 is a longstanding software best practice.[8]

---

[2] *Id.* at 10(j), 86 FR 26633 at 26646 (May 17, 2021).
[3] *Ibid.*
[4] *Ibid.*
[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*

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 Telecommunications 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, NTIA noted that "what was an obscure idea became a key part of the global agenda around securing software supply chains."[11] In July 2022, CISA facilitated eight public listening sessions[12] around four open topics (two for each topic): Cloud & Online Applications, Sharing & Exchanging SBOMs, Tooling & Implementation, and On-ramps & Adoption. These public listening sessions resulted in the formation of four public, community-led workstreams around each of the four topics. The groups have been convening on a weekly basis since August 2022. More information can be found at https://cisa.gov/SBOM.

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 the 2023 CISA SBOM-a-Rama.

II. Topics for CISA SBOM-a-Rama

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.
[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.
[12] Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices, https://www.federalregister.gov/documents/2022/06/01/2022-11733/public-listening-sessions-on-advancing-sbom-technology-processes-and-practices.

The goal of this meeting is to help the broader software and security community understand the current state of SBOM and what efforts have been made by different parts of the SBOM community, including CISA-facilitated community-led work and other activity from sectors and governments. Attendees are invited to ask questions, share comments, and raise further issues that need attention. Specific presentations will be made on the community-led efforts around sharing SBOMs, cloud and online applications, tools and implementation, the Vulnerability Exploitability eXchange (VEX) model, and SBOM on-ramps and adoption. The event will also feature presentations and discussion on sectors' and governments' efforts around the world.

A full agenda will be posted in advance of the meeting at https://cisa.gov/SBOM.

III. Participation in the SBOM-a-Rama

This event is open to anyone. CISA welcomes participation from anyone interested in learning about the current state of SBOM practice and implementation, including private sector practitioners, policy experts, academics, and representatives from non-U.S. organizations. A form to allow individuals to register their interest in either in-person or virtual participation will be available at https://cisa.gov/SBOM.

Additional information regarding the 2023 CISA SBOM-a-Rama 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. 2023-10825 Filed: 5/19/2023 8:45 am; Publication Date: 5/22/2023]